Official Cert Guide

Practice tests

Flash Cards

Review Exercises

Study Planner

CCNP and CCIE Collaboration Core

CLCOR 350-801

2nd Edition

ciscopress.com

Jason Ball, CCSI® No. 33717

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, a Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to **www.ciscopress.com/register.**
2. Enter the **print book ISBN:** 9780138200947.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated in your account under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com.** Simply choose Pearson IT Certification as your product group and log in to the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org.**

This page intentionally left blank

CCNP and CCIE Collaboration Core

CLCOR 350-801

Official Cert Guide
2nd Edition

JASON BALL
CCSI No. 33717

Cisco Press
Hoboken, New Jersey

CCNP and CCIE Collaboration Core CLCOR 350-801 Official Cert Guide 2nd Edition

Jason Ball

Published by:
Cisco Press

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

$PrintCode

Library of Congress Control Number: 2023913509

ISBN-13: 978-0-13-820094-7

ISBN-10: 0-13-820094-7

Warning and Disclaimer

This book is designed to provide information about the CCNP and CCIE Collaboration Core 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.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screenshots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

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 intlcs@pearson.com.

Feedback Information

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

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

We greatly appreciate your assistance.

Vice President, IT Professional: Mark Taub

Alliances Manager, Cisco Press: Jaci Featherly
James Risler

Director, ITP Product Management: Brett Bartow

Executive Editor: Nancy Davis

Managing Editor: Sandra Schroeder

Development Editor: Christopher A. Cleveland

Senior Project Editor: Mandie Frank

Copy Editor: Bart Reed

Technical Editor: Daniel Ball

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Ken Johnson

Proofreader: Barbara Mack

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.**

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where:

- Everyone has an equitable and lifelong opportunity to succeed through learning.
- Our educational products and services are inclusive and represent the rich diversity of learners.
- Our educational content accurately reflects the histories and experiences of the learners we serve.
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview).

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

About the Author

Anyone who has worked with **Jason Ball** or has sat in one of his classes knows that his enthusiasm for collaboration is matched only by his engaging zeal for teaching. Jason currently works for Cisco on the Learning & Certifications team, helping manage all the collaboration certification learning content. He has been operating as a collaboration engineer since 2009 and holds 19 different certifications, including a CCNP Collaboration certification and a Cisco Certified Systems Instructor (CCSI) certification. He has been teaching Cisco Voice, Video, and Collaboration certification courses for as many years as he has been involved with Cisco.

Some of his accomplishments include serving as a subject matter expert (SME), developing certification content, performing installations of many Cisco UCS servers with collaboration VMs, and performing as a consultant and technical instructor for many years as well. He also co-wrote the *CCNA Collaboration CIVND 210-065 Official Cert Guide* and the *CCNP Collaboration Cloud and Edge Solutions CLCEI 300-820 Official Cert Guide* for Cisco Press, and he wrote the original *CCNP and CCIE Collaboration Core CLCOR 350-801 Official Cert Guide* for Cisco Press, along with this revision. Jason has two adult children, and he currently resides in Raleigh, North Carolina, with his wife.

About the Technical Reviewer

Daniel Ball is a Solutions Readiness Engineer with a strong background in training and education. Daniel received a Bachelor of Arts degree from the University of Texas at Austin and a Master of Science degree in Education from Shenandoah University. He has been working in the collaboration space for more than 13 years and holds 9 certifications, including a CCNA and a CCNP in Collaboration. Daniel also maintains a growing YouTube channel called *Collab Crush*, which is dedicated to promoting quality training for the Cisco Collaboration solution. Currently, Daniel lives in Kobe, Japan, with his wife, Miki, and two daughters, Midori and Hana.

Dedications

I would like to dedicate this book to my wife, whom I married in May, 1997. The love, encouragement, and support she has offered have been the strength that has sustained me throughout this endeavor. Every accomplishment I have achieved has been encouraged by her cheering for me from the sidelines. She is the best partner and friend anyone could ask for.

Acknowledgments

Special thanks must be awarded to my technical editor. I asked my brother, Daniel Ball, to do this for me because he has all the right expertise to keep me on my toes. He was an English major but worked in a technical position while he was going to school. Back then he was more of a programmer, but later he got into the Cisco Collaboration Solution when Cisco Spark (now Webex) was taking off. Since most of the changes to this edition of the book are related to Webex, it made perfect sense to have him come behind me and check my work. Plus, since he's my brother, he doesn't mind telling me when I'm wrong. So, thank you, Daniel, for having my back and doing such a great job with the technical editing.

I would also like to express my gratitude to Chris Cleveland, development editor of this book. I was so incredibly lucky to work with him again on this project. He is another truly exceptional example of excellence in the workplace. He is the top 1 percent. I'd like to thank Nancy Davis, Mandie Frank, and Brett Bartow. They each have worked patiently alongside me to help make this book a reality.

I dedicated the first edition of this book to the memory of a friend, colleague, and mentor of mine who passed away in March of 2020, so I would like to keep this dedication in this edition as well. When I first started with Tandberg, many years ago, James Lehto was one of the first mentors I had. He was always tough. He had a great depth of knowledge, and he expected others he worked with to have the same depth of knowledge. James also exhibited fairness. If you lacked knowledge, he would help guide you to understanding. This quality made him a great instructor. After Tandberg was acquired by Cisco, James continued to work for Cisco, and as opportunity presented itself, he would use me to develop content or act as a subject matter expert. Through this peer work relationship, we also developed a friendship that I valued to the day he was laid to rest. James was the one who suggested I write a book for Cisco Press and recommended me for the CIVND book years ago. If it wasn't for James, I wouldn't have written this book either. A professor I had in college once said, "What good is knowledge if you never share it?" James lived by that motto, and I live by that motto as well. So, as you read this book, remember James Lehto. For the knowledge shared in this book is not just from me, but from him and others who have shared their knowledge with me over the years.

Contents at a Glance

Contents

Online Elements

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.

Other Features

In addition to the features in each of the core chapters, this book has supplementary study resources on the companion website, including the following:

- **Practice exams:** The companion website contains an exam engine that enables you to review practice exam questions. Use these to prepare with a sample exam and to pinpoint topics where you need more study.

To access this additional content, simply register your product. To start the registration process, go to www.ciscopress.com/register and log in or create an account.* Enter the product ISBN 9780138200947 and click **Submit**. After the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

The Implementing Cisco Collaboration Core Technologies (CLCOR 350-801) exam is the required "core" exam for the CCNP Collaboration and CCIE Collaboration certifications. If you pass the CLCOR 350-801 exam, you also obtain the Cisco Certified Specialist–Collaboration Core certification. This exam covers core Collaboration technologies, including infrastructure and design; protocols, codecs, and endpoints; Cisco IOS XE gateways and media resources; call control; QoS; and Collaboration applications.

TIP You can review the exam blueprint from the Cisco website at https://learningnetwork.cisco.com/s/clcor-exam-topics.

This book gives you the foundation and covers the topics necessary to start your CCNP Collaboration or CCIE Collaboration journey.

The CCNP Collaboration Certification

The CCNP Collaboration certification is one of the industry's most-respected certifications. To earn the CCNP Collaboration certification, you must pass two exams: the CLCOR exam covered in this book (which covers core Collaboration technologies) and one Collaboration concentration exam of your choice, so you can customize your certification to your technical area of focus.

TIP The CLCOR core exam is also the qualifying exam for the CCIE Collaboration certification. Passing this exam is the first step toward earning both of these certifications.

The following are the CCNP Collaboration concentration exams:

- Implementing Cisco Collaboration Applications (CLICA 300-810)
- Implementing Cisco Advanced Call Control and Mobility Services (CLACCM 300-815)
- Implementing Cisco Collaboration Cloud and Edge Solutions (CLCEI 300-820)
- Automating and Programming Cisco Collaboration Solutions (CLAUTO 300-835)

TIP CCNP Collaboration now includes automation and programmability to help you scale and customize your Collaboration infrastructure. If you pass the Automating and Programming Cisco Collaboration Solutions (CLAUTO 300-835) exam, the CLCOR 350-801 exam, and the Developing Applications Using Cisco Core Platforms and APIs (DEVCOR 350-901) exam, you will achieve the CCNP Collaboration and DevNet Professional certifications with only three exams. Every exam earns an individual Specialist certification, allowing you to get recognized for each of your accomplishments, instead of waiting until you pass all the exams.

There are no formal prerequisites for CCNP Collaboration. In other words, you do not have to pass the CCNA Collaboration or any other certifications in order to take CCNP-level exams. The same goes for the CCIE exams. On the other hand, CCNP candidates often have 3 to 5 years of experience in IT and Collaboration.

Cisco considers ideal candidates to be those who possess the following:

- Working knowledge of fundamental terms of computer networking, including LANs, WANs, switching, and routing
- Basic knowledge of digital interfaces, public switched telephone networks (PSTNs), and Voice over IP (VoIP)
- Fundamental knowledge of converged voice and data networks and Cisco Unified Communications Manager deployment

The CCIE Collaboration Certification

The CCIE Collaboration certification is one of the most admired and elite certifications in the industry. The CCIE Collaboration program prepares you to be a recognized technical leader. To earn the CCIE Collaboration certification, you must pass the CLCOR 350-801 exam and an 8-hour, hands-on lab exam. The lab exam covers very complex Collaboration network scenarios. These scenarios range from designing through deploying, operating, and optimizing Collaboration solutions.

Cisco considers ideal candidates to be those who have 5 to 7 years of experience with designing, deploying, operating, and optimizing Collaboration technologies and solutions prior to taking the exam. Additionally, candidates will need to do the following:

- Understand capabilities of different technologies, solutions, and services
- Translate customer requirements into solutions
- Assess readiness to support proposed solutions
- Deploy a Cisco Collaboration solution
- Operate and optimize a Cisco Collaboration solution

The Exam Objectives (Domains)

The Implementing Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam is broken down into six major domains. The contents of this book cover each of the domains and the subtopics included in them, as described next.

The following table breaks down each of the domains represented in the exam:

Domain	Percentage of Representation in Exam
1: Infrastructure and Design	20%
2: Protocols, Codecs, and Endpoints	20%
3: Cisco IOS XE Gateway and Media Resources	15%

Domain	Percentage of Representation in Exam
4: Call Control	25%
5: QoS	10%
6: Collaboration Applications	10%

The following topics are general guidelines for the content likely to be included on the exam; however, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the following guidelines might change at any time without notice. Here are the details of each domain and where the exam objectives are covered in the book:

Domain 1: Infrastructure and Design	Chapter(s) Where This Is Covered
1.1 Describe the Cisco on-premises, hybrid, and cloud collaboration solution design elements described in the SRND/PA	Chapters 6, 9, 13
1.1.a Licensing (Smart, Flex)	Chapter 6
1.1.b Sizing	Chapter 6
1.1.c Bandwidth	Chapter 6
1.1.d High availability	Chapter 6
1.1.e Disaster recovery	Chapter 6
1.1.f Dial plan	Chapter 6
1.1.g Security (certificates, SRTP, TLS)	Chapters 6, 9
1.1.h QoS	Chapters 6, 13
1.2 Describe the purpose of Edge devices in the Cisco Collaboration architecture such as Expressway and Cisco Unified Border Element	Chapters 20, 21
1.3 Configure these network components to support Cisco Collaboration solutions	Chapters 12, 13, 14
1.3.a DHCP	Chapters 5, 6
1.3.b NTP	Chapters 6, 14
1.3.c CDP	Chapters 5, 6
1.3.d LLDP	Chapters 5, 6
1.3.e LDAP	Chapters 5, 6
1.3.f TFTP	Chapters 5, 6
1.3.g Certificates	Chapters 6, 9
1.4 Troubleshoot these network components in a Cisco Collaboration solution	Chapters 30–34
1.4.a DNS (A/AAA, SRV, Reverse Pointer Record (PTR))	Chapter 30
1.4.b NTP	Chapter 30

Domain 1: Infrastructure and Design	Chapter(s) Where This Is Covered
1.4.c LDAP integration on Cisco UCM	Chapters 16, 31, 32
1.5 Explain these components to support Cisco Collaboration solutions	Chapter 14
1.5.a SNMP	Chapter 14
1.5.b DNS	Chapter 14
1.5.c Directory Connector	Chapter 22, 23
1.6 Describe Webex Control Hub features	Chapter 6, 23
Domain 2: Protocols, Codecs, and Endpoints	**Chapter(s) Where This Is Covered**
2.1 Troubleshoot these elements of a SIP conversation	Chapters 15, 30
2.1.a Call set up and tear down	Chapter 30
2.1.b SDP	Chapter 30
2.1.c DTMF	Chapter 15
2.2 Identify the collaboration codecs for a given scenario	Chapters 2, 3, 15
2.3 Deploy SIP endpoints	Chapters 5, 9, 17
2.3.a Manual	Chapter 17
2.3.b Self provisioning	Chapter 17
2.3.c Bulk Administration Tool (BAT)	Chapter 17
2.3.d Onboarding cloud devices	Chapter 22, 23
2.3.e Device onboarding via activation codes (MRA/on-premises)	Chapter 17, 21
2.4 Troubleshoot SIP endpoints	Chapter 30
2.5 Describe SIP OAuth on Cisco UCM	Chapter 6
Domain 3: Cisco IOS XE Gateway and Media Resources	**Chapter(s) Where This Is Covered**
3.1 Configure voice gateway elements	Chapters 15
3.1.a DTMF	Chapters 15
3.1.b Voice translation rules and profiles	
3.1.c Codec preference list	
3.1.d Dial peers	
3.2 Troubleshoot ISDN PRI/BRI	
3.3 Identify the appropriate IOS XE media resources	Chapter 15
3.4 Describe cloud calling hybrid local gateway	Chapter 22, 24
Domain 4: Call Control	**Chapter(s) Where This Is Covered**
4.1 Describe the Cisco UCM digit analysis process	Chapter 18
4.2 Implement toll fraud prevention on Cisco UCM	Chapter 18
4.3 Configure globalized call routing in Cisco UCM	Chapter 18

Domain 1: Infrastructure and Design	**Chapter(s) Where This Is Covered**
4.3.a Route patterns (traditional and +E.164)	Chapters 18, 19
4.3.b Translation patterns	Chapter 19
4.3.c Standard local route group	Chapter 19
4.3.d Transforms	Chapter 19
4.3.e SIP route patterns	Chapters 18, 19
4.4 Describe Mobile and Remote Access (MRA)	Chapters 20, 21
4.5 Describe Webex Calling dial plan features	Chapter 22, 25, 26
4.5.a Locations and numbers	Chapter 22, 26
4.5.b Outgoing and incoming permissions	Chapter 22, 26
4.5.c Transfer and forwarding restrictions	Chapter 22
Domain 5: QoS	**Chapter(s) Where This Is Covered**
5.1 Describe problems that can lead to poor voice and video quality	Chapter 13
5.1.a Latency	Chapter 13
5.1.b Jitter	Chapter 13
5.1.c Packet loss	Chapter 13
5.1.d Bandwidth	Chapter 13
5.2 Describe the QoS requirements for voice and video	Chapter 13
5.3 Describe the class models for providing QoS on a network	Chapter 13
5.3.a 4/5 Class model	Chapter 13
5.3.b 8 Class model	Chapter 13
5.3.c QoS Baseline model (11 Class)	Chapter 13
5.4 Describe the purpose and function of these DiffServ values as it pertains to collaboration	Chapter 13
5.4.a EF	Chapter 13
5.4.b AF41	Chapter 13
5.4.c AF42	Chapter 13
5.4.d CS3	Chapter 13
5.4.e CS4	Chapter 13
5.5 Describe QoS trust boundaries and their significance in LAN-based classification and marking	Chapter 13
5.6 Describe and determine location-based CAC bandwidth requirements	Chapter 13
5.7 Configure LLQ (class map, policy map, service policy)	Chapter 13

Domain 1: Infrastructure and Design	Chapter(s) Where This Is Covered
Domain 6: Collaboration Applications	**Chapter(s) Where This Is Covered**
6.1 Configure Cisco Unity Connection mailbox and MWI	Chapters 27, 28
6.2 Configure Cisco Unity Connection SIP integration options to call control	Chapters 27, 28
6.3 Describe Cisco Unity Connection call handlers	Chapters 27, 28
6.4 Deploy Webex App	Chapter 29

Steps to Becoming a CCNP Collaboration Certified Engineer

To become a CCNP Collaboration Certified Engineer, you must first take and pass the CLCOR 350-801 exam. Passing this exam alone will automatically earn the Cisco Certified Specialist–Collaboration Core certification. All Cisco certification exams are managed by the Pearson Vue testing organization. Use the following steps to sign up for your Cisco exam.

Signing Up for the Exam

The steps required to sign up for the CCNP and CCIE Collaboration Core (CLCOR) 350-801 exam are as follows:

1. Navigate to **https://home.pearsonvue.com/**, select the **For Test Takers** drop-down list, and then select **Schedule an Exam.**
2. In the Start Here: Select Your Program box, enter **Cisco** and then select the **Cisco Systems** option that appears.
3. To schedule a Cisco exam, you must first have a CCO ID you created on the Cisco website. Then you must create a Pearson Vue login and link it to the CCO ID. After all this is created, you must sign in to the Pearson Vue site to schedule the exam. Click **Sign in** from the column on the right side of the screen and enter your login credentials.
4. Two types of exams are available: proctored exams and unproctored online exams. All Cisco certifications use only proctored exams. After logging in, click the **Proctored Exams** button.
5. In the Find an Exam box, enter **350-801** and then click the **350-801: Implementing Cisco Collaboration Core Technologies** name when it appears. Click **Go** to proceed to the next screen.
6. Continue to follow the steps on the screen. You will need to select a testing center, date, and time to take the exam. A schedule of available times for the testing center you select is visible from this site. You will also need to provide payment for the exam you're scheduling. The CLCOR 350-801 exam costs US $400.

Facts About the Exam

The exam is a computer-based test. It consists of multiple-choice questions only. To take the test, you must bring two forms of ID: one must be a government-issued identification card with a photo, and the second can be any official ID with your name on it, such as a Social Security card, employee ID card, or credit card, as long as it has your signature on it.

About the CCNP CLCOR 350-801 Cert Guide

Although this book does not map sequentially to the topic areas of the exam, all topic areas on the exam are covered in this book. This book cannot contain the personal experience and hands-on exposure to the equipment needed to answer some of the questions that may be asked in the exam. However, it was my intent to write this book in a manner that provides a slow buildup to the technologies that are being tested so that you will not only be better prepared to pass the test but also develop a solid understanding of the underlying technologies examined in this book. This book also uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, help you fully understand and remember those details, and help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass the exam only by memorization; instead, it seeks to help you to truly learn and understand the topics. This book is designed to help you pass the CCNP CLCOR 350-801 exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises 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 companion website

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that you should do at the end of the chapter:

- **Review All Key Topics:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The Review All Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these areas.
    - **Define Key Terms:** Although the CLCOR exam may be unlikely to ask a question that asks you to define a term, the exam does require that you learn and know a lot of terminology. This section lists 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.
    - **Complete Memory Tables:** Open Appendix C, "Memory Tables Answer Key," from the book's website and print the entire thing or print the tables by major part. Then complete the tables.
    - **Review Command References:** For some of the chapters that are a little more CLI-intensive, it's useful to have a working familiarity with some of the related command functions and generated output so that you don't have to hesitate too much during the exam when encountering a question related to commands.
    - **Review Questions:** Confirm that you understand the content you just covered by answering these questions and reading the answer explanations.
- **Web-Based Practice Exam:** The companion website includes the Pearson Test Prep practice test engine that enables you to take practice exams. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains 34 core chapters. Chapter 35, "Final Preparation," includes preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CCNP CLCOR 350-801 exam. The core chapters map to the CCNP CLCOR 350-801 exam topic areas and cover the concepts and technologies you will encounter on the exam. Refer back to the exam objective/chapter mapping table as a reference to see which objectives are covered in which chapters.

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book's companion website.

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at www.ciscopress.com and register your book.

To do so, simply go to www.ciscopress.com/register and enter the ISBN of the print book: **9780138200947**. After you have registered your book, go to your account page and click the **Registered Products** tab. From there, click the **Access Bonus Content** link to get access to the book's companion website.

Note that if you buy the Premium Edition eBook and Practice Test version of this book from Cisco Press, your book will automatically be registered on your account page. Simply go to your account page, click the **Registered Products** tab, and select **Access Bonus Content** to access the book's companion website.

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 preceding steps, please visit www.pearsonITcertification.com/contact and select the **Site Problems/Comments** option. Our customer service representatives will assist you.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- You can get your access code by registering the print ISBN (9780138200947) on ciscopress.com/register. Make sure to use the print book ISBN, regardless of whether you purchased an eBook or the print book. After you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.

- Premium Edition: If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at ciscopress.com, click Account to see details of your account, and click the digital purchases tab.

NOTE After you register your book, your code can always be found in your account under the Registered Products tab.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

Step 1. Open this book's companion website as shown earlier in this Introduction under the heading, "The Companion Website for Online Content Review"

Step 2. Click the **Practice Exams** button.

Step 3. Follow the instructions listed there for both installing the desktop app and using the web app.

Note that if you want to use the web app only at this point, just navigate to pearsontest-prep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all test banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep practice test software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks whether there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is an issue only with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

Credits

Figure 3.3a: Anoneditor

Figure 3.3b: Cburnett

Figures 4.5a, 4.12b-4.12g: Evan-Amos

Figures 4.5b, 4.5d: Shaddack

Figure 4.5c: Michael Piotrowski

Figure 4.12a: Meggar

Figures 6.5, 26.1a: Google LLC

Figure 11.5: PuTTY

Figures 14.1-14.3: Microsoft Corporation

This page intentionally left blank

This part covers the following topics:

- **Chapter 1, Introduction to Collaboration:** This chapter will provide a history of voice and video communication, and illustrate the evolutionary path communication has followed leading to the collaboration architecture that exists today.
- **Chapter 2, Audio Basics:** This chapter will provide a broad introduction to audio behavior, discuss the differences between analog and digital audio communication, and explain how the audio codecs we use today came into existence.
- **Chapter 3, Video Basics:** This chapter will provide a broad introduction to light behavior, discuss how light can be used to capture video, and explain how the video codecs we use today came into existence.
- **Chapter 4, Collaboration Endpoint Components and Environment:** This chapter will first examine how audio acoustics behave in an environment where audio communication is set up, and take a close look at the audio components needed for communication. Then this chapter will examine light conditions within an environment where video communication is set up, and take a close look at the video components needed for communication.
- **Chapter 5, Communications Protocols:** This chapter will examine two forms of communication, circuit-switched and packet switched. Circuit-switched communication uses various forms of ISDN, all of which are controlled by the ITU-T standard H.320. Packet-switched communication uses packets over the Internet instead of circuits over a telephony network. Two packet-switching protocols will be discussed in this chapter.
- **Chapter 6, Cisco Solution for Converged Collaboration:** This chapter will introduce the Cisco Collaboration product line, including endpoints, call control infrastructure and applications, all of which will be discussed throughout this book in more detail. This chapter will also discuss the designing aspects that must be considered before deploying a Cisco Collaboration solution.

Part I

AV Fundamentals

Chapter 1: Introduction to Collaboration

Chapter 2: Audio Basics

Chapter 3: Video Basics

Chapter 4: Collaboration Endpoint Components and Environment

Chapter 5: Communication Protocols

Chapter 6: Cisco Solution for Converged Collaboration

CHAPTER 1

Introduction to Collaboration

This chapter covers the following topics:

Audio Communication: This topic will illustrate a brief history of audio communication as it has evolved and provide a high-level overview of audio communication that exists today.

Video Communication: This topic will illustrate a brief history of video communication as it has evolved and provide a high-level overview of video communication that exists today.

Unified Communication: This topic will identify different forms of communication and illustrate how these means of interaction can be leveraged in today's business enterprise.

Driving Change in the Industry: This topic will illustrate how the industry has transformed over the last 20 years and speculate where the industry is heading in the future.

What comes to mind when you hear, or in this case read, the word *collaboration*? To collaborate means to work together with someone else, usually to achieve an end goal or produce a product. Communication today requires so much more than just having a voice conversation with someone else. Cisco has taken on the vision to provide the best products that will help employees within businesses truly collaborate. This is why Cisco, and many other vendors, have embraced the term *collaboration* to replace *communication*. This chapter will provide a history of voice and video communication and illustrate the evolutionary path communication has followed leading to the collaboration architecture that exists today. Topics discussed throughout this chapter include the following:

- Audio Communication
- Video Communication
- Unified Communication
- Driving Change in the Industry

"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
Audio Communication	1–2
Video Communication	3–4
Unified Communication	5
Driving Change in the Industry	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 solution allows businesses to place and receive analog voice calls over a circuit-switched network?
   - **a.** PBX
   - **b.** ISDN
   - **c.** POTS
   - **d.** VoIP
2. What solution allows businesses to place and receive digital voice calls over a packet-switched network?
   - **a.** PBX
   - **b.** ISDN
   - **c.** POTS
   - **d.** VoIP
3. What ISDN standard did the first video endpoints use to communicate?
   - **a.** POTS
   - **b.** H.320
   - **c.** H.323
   - **d.** SIP
4. Which of the following are considered a Telepresence endpoint?
   - **a.** Immersive video system
   - **b.** Conference room video system
   - **c.** Personal desktop video system
   - **d.** All of these answers are correct

5. Which of the following modes of communication allows real-time text messages to be sent and received?

- **a.** Email
- **b.** IM
- **c.** Presence
- **d.** Fax

6. Which of the following protocols allows RTP and RTCP streams to be multiplexed together?

- **a.** TIP
- **b.** SIP
- **c.** H.323
- **d.** H.320

7. Which of the following Cisco products uses cognitive collaboration to enhance the user experience?

- **a.** CUCM
- **b.** CMS
- **c.** CTS3000
- **d.** Webex

Foundation Topics

Audio Communication

What is audio communication? Audio communication is simply information being transmitted in a form that can be heard. Two people talking together over a cup of coffee is audio communication. It can be any form of sound from speech to music. Rhythm alone can be communication. Ancient tribes would use bird calls and animal sounds to communicate without giving away their position. Morse code is even a form of audio communication. Of course, audible sound for the purpose of communication isn't restricted to just humans; it's all over the natural world. For the purpose of this definition, it is important to differentiate audio communication from other audible sounds based on intent. Be it animal or human, when an audible sound is intended to be recognized and understood, audio communication is occurring.

Fast forward from the bird calls of ancient times, humankind has sought to achieve communication over vast distances for many years. Pigeons and other animals have even been used to send messages. Then the discovery of how to use electricity propelled us into a new age of invention and revolution. In the 1830s a man named Samuel Morse created the telegraph system. This system worked by sending electrical pulses over a wire between stations. When those electrical pulses were received, they would transmit a tone, which was sent in a pattern. The code that was created to map those tones to written language is known as Morse code, and it is still used today.

The telegraph incited creative thinkers to imagine ways actual audio voice could be sent over that same electrical wire. This vision was made a reality in 1849 when a man named Antonio Meucci invented the first basic telephone. From that time there were others who invented different versions of the telephone, but it was Alexander Graham Bell who won the first U.S. patent for the telephone in 1876. The telephone system continued to evolve from there. The first manual telephone exchange opened in 1878.

Operators would take incoming calls and manually connect them through to the intended destination. This system worked for a short while, but there was an unexpected interruption to this system known as the common cold. These operators had to be trained to perform their jobs, so when they got sick and couldn't come into work, finding a replacement was no simple task. In 1889, the first automatic telephone exchange was invented, and over the next few years this system would replace the manual telephone exchanges.

This phone system continued to operate for nearly 100 years before the next big revolution would occur with the telephony system. In 1986, a new set of protocols was introduced that allowed the traditional analog phone system to be replaced with a digital phone system known as the Integrated Services Digital Network (ISDN). A more detailed explanation of analog and digital signaling will be provided in Chapter 2, "Audio Basics," and a detailed explanation of ISDN will be provided in Chapter 5, "Communication Protocols"; however, a brief explanation of these different types of communication should be understood at this time. A plain old telephone service (POTS) is the means of audible communication using analog signals transmitted over wire. ISDN is similar to POTS, but the original analog signal is converted to digital format before it is sent across a wire. That digital signal must be converted back to analog at the receiving phone.

Technically, cellular communication preceded ISDN. The first cellular call was placed in 1973; however, cell phones were very inefficient, heavy, and very expensive. It was ten years from that first cellular call before cell phones went on sale in the United States. In 1983, you could buy a cell phone for $4000 USD, the cellular network was limited, and the phones were still too big and heavy to fit in your pocket, or even wear on a sexy clip attached to your belt. The cellular industry didn't start taking off until the mid- to late-1990s. Today cellular technology is very common. It allows audio communication to be transmitted wirelessly across a given area, or cell. These cell towers are very prominent across the globe, enabling people to place and receive calls from virtually any location on the planet, with some obvious limitations. Most modern cell phones also support data connections, opening up many other channels of communication through social media applications and other communication tools, but more on that later.

Before I go into the next advancement in audio communication, an explanation is warranted for another device introduced to business communication systems. This device is known as the private branch exchange (PBX). A PBX operates in a similar fashion to the automatic telephone exchange, except that the purpose of a PBX is to route calls within a business exclusively. PBXs can also connect to the outside world over the public telephone network, but it operates on the same circuit-switched network using POTS or ISDN. In 1997, a company called Selsius Systems released one of the first IP PBXs that supported voice over Internet Protocol (VoIP). Recognizing what that company had created, Cisco quickly swooped it up, and by November 1998, Cisco had acquired Selsius. The original IP PBX was named Call Manager, and this is the same product, though a few upgrades later, that we know as the Cisco Unified Communications Manager (CUCM).

VoIP is an audio technology that allows voice communication to be translated into a binary format and encapsulated into packets and sent across an IP network. This type of communication is known as *packet switched*. Engineers began experimenting with VoIP technologies as early as the 1980s; however, limitations in network bandwidth and audio compression algorithms were too restrictive to develop a product to go to market. By the mid 1990s, the introduction of broadband and high-speed Internet made VoIP a reality beyond what any could have imagined before.

Video Communication

Now that audio communication has been defined, and the history of how audio communication evolved has been scrutinized, the next form of communication to examine is video communication. So, what is visual communication? Visual communication is a method of communicating through sight. Different types of visual communication could include theater, dance, mime, flag signal waving, sign language, hand signals from a bike or car such as flipping someone the bird, and so on. One of the most common forms of visual communication that people use every day is body language. Proper etiquette teaches how to use body language to better communicate with other people, such as maintaining eye contact, nodding to communicate that the spoken message has been heard, or raising a hand to identify to the speaker that you have a question. Visual communication could also be a shrug of the shoulders or a facial expression. Crossing of the arms suggests the listener is closed off to the message being communicated, but don’t mention that to your spouse.

I have taught many Cisco classes, both on-site and remote over a medium such as Cisco Webex. Most students have identified a preference to on-site classes because the environment is more conducive to learning. Even from an instructor perspective, an on-site class is preferred over a Webex class. The reason has everything to do with body language. While teaching, the instructor can watch the students for visual clues as to whether a concept is being understood. If students have confused looks on their faces, then the instructor can rephrase the explanation or ask probing questions to identify where the point of confusion occurred. I have been known to stop teaching and break for lunch because it was visibly obvious that the students needed sustenance before they were going to absorb any more information. The same has been true at the end of a long day, that the students’ minds were suffering from information overload. So, class ended to allow the mind to rest and the information to soak in and resonate before starting again the next day. Remote classes have their advantages too, but the point here is centered around the importance of visual communication. Have you ever listened to a sporting event over the radio? Although the sports announcers do a pretty good job of providing a play-by-play account of what is actually going on during the event, an audible interpretation is not the same as seeing the event for yourself. There is so much more information that can be gathered through seeing than by simply hearing. So, as the adage goes, “a picture is worth a thousand words.”

Technologically speaking, a lot of different video communication devices are available on the market today. A walk through Times Square in New York City is a perfect example. This part of the city is literally lit up with the lights from digital signs that encompass the whole of Times Square. Information is communicated through advertisements, stock information, and live TV. Some of the signs are even interactive with the crowds of people meandering through the streets. Other common forms of communicating through video today include television, YouTube video clips, and other social media applications. Recent years have given rise to a new way of communicating over video, which involves calling over a video phone. This form of video communication has become known as video telepresence.

Video telepresence allows participants at different locations to see visual cues while audio communication accompanies the communication. Video telecommunications is a relatively young industry. It was first conceived as early as 1870, but the technology to support the idea would not develop for another 50 years. With the invention of the television, the idea of video communication began to develop. The earliest video telephony systems were simply an analog TV and camera set up at two locations. A lot of other special equipment accompanied this setup, making it very expensive to deploy and use. Although many companies contributed to the development of this industry, two companies stand out above the rest.

The first worth mentioning was a Norwegian company known as Tandberg. Based in Oslo, Norway, Tandberg first incorporated in 1933. The company's main products were radios, televisions, and reel-to-reel tape recorders. After filing for bankruptcy in 1978, the company split off into two distinct organizations. Tandberg Data continued to market and sell the same products to consumers. The original Tandberg company changed its focus to telepresence communications. Tandberg launched its first telepresence endpoint in 1989, which used the ISDN standard H.320 as the medium to communicate. By 1995, Tandberg opened its first office in the United States. After making a key acquisition in 1999, Internet Technology AS, by 2000 Tandberg had launched its first video telepresence endpoint that could support video calling over ISDN or IP. The protocol used for IP communication at this time was the ITU-T standard H.323. The year 2004 was big for Tandberg, which acquired a company called Ridgeway Systems, providing the company with firewall traversal capabilities not yet seen in the industry. Tandberg also released a new endpoint product line that year called the MXP series. By 2005, Tandberg incorporated a new IP protocol into its endpoints for IP communication known as Session Initiation Protocol (SIP). As history will tell you, SIP has become the preferred protocol for use in today's networked environments. Between key acquisitions and superb product development, Tandberg forged a path to become the industry leader in video telepresence until 2010, when Cisco acquired Tandberg. Building on the foundation laid by Tandberg, Cisco has held the reigning title as the industry leader in voice and video communication across the world to date.

Another company that is worth mentioning was called PictureTel Corporation. Founded in the United States in 1984, PictureTel quickly grew to become the telepresence industry leader in the early days of video communication. The company's first ISDN-based video endpoint was released in 1986. By 1990, two of PictureTel's lead engineers broke off to form a new company called Polycom. PictureTel was later acquired by Polycom in 2001. The reason PictureTel is worth mentioning has to do with the contributions the company made to jump-start this new industry. The company got its start based on a 1981 MIT research paper combining block-based motion compensation and transform coding. This idea of block-based motion compensation and transform coding is what most of the video compression codecs used today are based on. Without that contribution, who knows where the world of video telepresence would be.

Key Topic

In today's market, many different types of video systems allow a variety of means to communicate. Software clients can be downloaded to computers, tablets, and smartphones, so video communication can be used while on the go. Immersive Telepresence systems can be used to enhance the virtual session for a face-to-face in-person experience. Personal video systems, meeting room video systems, and varying vertical solutions are used by businesses worldwide. Video telepresence allows for business-to-business (B2B) and business-to-consumer (B2C) communication. Not only does visual communication in technology allow participants to see one another, but content also can be shared between devices so that participants at separate locations can see the same documents, drawings, presentation slides, or any other content being shared.

Unified Communication

Key Topic

As was mentioned before, there are more ways to communicate in today's world than just audio and video. *Instant messaging (IM)* is a term that became relevant in 1990. IM is a text-based communications tool that allows real-time text messages to be sent over the Internet. IM was made popular by industry giants such as Microsoft Messenger, Yahoo!, AOL AIM, and others like them. A communications tool that often accompanies IM is known as presence. Presence is an indicator light that identifies if a user is online, offline, away, or busy.

Non-real-time communication services are also used today, such as email. Although email was technically first used in the mid-1970s, it wasn't commonly used until the late 1980s and early 1990s when the Internet was more widely accessible. Fax machines are not commonly used anymore, but on occasion you will still find some businesses that use them to share documents. Government offices tend to be slower to adapt new technologies, so fax machines are still often used in these types of establishments. Some banking institutions and credit unions will use fax machines to share signed legal documents. Voicemail is another common non-real-time communication service. Voicemail refers to a computer-based system that allows a user to record a personal greeting, which will be played when audio calls are not answered within a predefined amount of time. After the greeting plays, the caller has the option to leave a voice message, which can be played back at the main user's discretion.

Couple audio and video with presence, instant messaging, and persistent chat, and there are a lot of ways people can communicate with one another. Plus, there are other forms of communication not mentioned here, such as social media applications. Compound all of this with vendor autonomy and proprietary protocols, and the world of communication becomes quite complex. The answer to that complexity is Unified Communications (UC).

Key Topic

UC is not necessarily a single product, nor a single manufacturer, but more like a set of products that provides a consistent unified user interface and experience across multiple devices and media types. Ideally, it would be better to use a single vendor's products for an enterprise UC solution, but realistically that is not always possible. In its broadest sense, UC can encompass all forms of communications that are exchanged via the medium of the TCP/IP network. UC allows an individual to send a message on one medium and receive the same communication on another medium. A good example of this is when someone receives a voicemail message; the person receiving the message can choose to access it through email or hear an audio playback through a phone. For those of you who are fans of the TV sitcom *The Office*, there is a good example of a UC product on that show called WUPHF. The character Ryan Howard created a software application called WUPHF that would take incoming communication over any media and would resend it out to the intended target as a Facebook message, Tweet, IM chat, SMS text message, fax, and phone call. As humorous as the concept was in the show, the idea behind it is great. UC is the ability to unify multiple modes of communication under a single platform. This is what Cisco has strived for over many years and what the company has brought to fruition in multiple product platforms available today.

Driving Change in the Industry

Telepresence is the way of the future. As a technology, video communication has been around for approximately 40 to 50 years; however, the growth of video conferencing has depended heavily on the availability to run on a reliable digital communication network. In the 1980s, when ISDN standards were first introduced, the race began to build and deliver the first video telecommunications device. PictureTel was the clear front-runner in this market, but over a short period that title would change hands several times. Polycom began to pick up steam by creating several proprietary audio compression codecs that would later be adopted as standards. Wielding this superior grasp on the technology, and by acquiring some key companies, Polycom quickly propelled itself to become an industry leader in the video communications market.

There was a big drawback to video communications devices at this time. The technology was new and still being developed. Most system components had to be invented so that the systems would perform in a functional manner. Plus the demand for a video phone was very low. These factors made purchasing these video phones very expensive. Then factor in the fact that ISDN was still relatively new itself, so placing a video call over ISDN was quite expensive as well. All of this changed in the late 1990s and early 2000s with the introduction of broadband and high-speed Internet. Now the race was not to simply come out with a video endpoint, but to come out with an endpoint that was capable of calling over IP, a much less expensive medium for communication. Tandberg was quick to respond with an endpoint that used the H.323 standard for IP communication. Other companies came into the market as well, such as Sony, HP, Radvision, VTEL, and Aethra. Other companies were in the VoIP game, such as Cisco, Siemens, Vonage, and Avaya. As the race for delivering video communications over IP continued, Tandberg made a strategic addition to its systems, allowing IP communications over the IETF SIP protocol. After this newish protocol introduction to the system, the company developed a superior line of endpoints and began to give Polycom a run for its money as the video communications front runner.

Toward the end of the 2000s and early 2010s, the video communications race changed once again. This time the race was focused on who could provide the best video communication experience. The idea was to use the best audio and video products on the market to create an environment that was indistinguishable from sitting in the same room with the people on the other end of the call. In late 2006, Cisco launched the CTS3000 Telepresence room system. *Telepresence* was the term first used here to describe the superior quality of the video call. This system supported three screens, three cameras, and three endpoints that all worked together to provide a life-sized video presence that almost gave the sensation of being in the same room as the participants connected in the call. Unfortunately, the CTS3000 system had one major drawback. For it to work the way Cisco intended, the company created a proprietary multiplexing protocol that compressed the RTP and RTCP streams. This meant that the only systems the CTS3000 could call were other CTS3000s. In 2008, Tandberg launched a telepresence room system called the T3, which stood for Tandberg 3-screen. This room system looked like something out of a science fiction movie. In fact, many people referred to it as the bridge on the Starship Enterprise from *Star Trek*. The T3 was far more advanced than the Cisco CTS3000 system, and it had the capability to call any other video communication device, including Cisco's flagship product, the CTS3000. Less than six months later, Tandberg launched another product called the Telepresence Server. This server could host multipoint calls for telepresence endpoints, and it could act as a gateway between the Cisco

CTS3000 and other video communications devices. It was obvious to Cisco that the company was outmatched, so by October 2009 Cisco made an offer to acquire Tandberg. The vote was approved by Tandberg shareholders in December 2009 to sell to Cisco for $3.4 billion.

Key Topic

Things got really interesting after that. Several other video communication companies protested the sale of Tandberg to Cisco. So, the first ever video telecommunications summit was held. Several changes were decided upon during that meeting. First, some terminology was officially canonized. Devices capable of high-quality video communication would now be referred to as *telepresence endpoints*. The enhanced room systems, such as the T3 and CTS3000, would be referred to as *immersive telepresence endpoints*. The most significant change, however, was that the proprietary multiplexing protocol that Cisco created was offered as an open-source protocol that any vendor could use, and it was named the Telepresence Interoperability Protocol (TIP). By May 2010, Cisco closed on the acquisition of Tandberg and got busy to make use of the solutions the company now had at its disposal. In the years that followed, Cisco has provided telepresence innovations that have driven the growth of the industry. Some of the innovations include One Button to Push (OBTP), which makes connecting to a meeting as simple as pressing one button; Smart Scheduling; rendezvous conferencing; and now the next big change in the video telepresence race, cloud and hybrid collaboration.

Many companies began transitioning to the cloud several years ago. Microsoft announced the Office 365 platform, which is cloud-based. Life-Size, another video telepresence company that historically focused on endpoints exclusively, began offering infrastructure services in the cloud to which its endpoint product line could register. Newer companies were established that were centered around a cloud-based telepresence. Even data centers are now reaching out to the cloud, such as Amazon's AWS, Microsoft's Azure, and Google Cloud. It was not hard for Cisco to see the writing on the wall as to where the industry was heading. Cisco already had the Webex conferencing solutions, which are cloud-based. In an attempt to go beyond what Webex could offer, in 2013 Cisco came out with a product called Cisco Project Squared. After about a year of development, Cisco introduced some changes to this new cloud offering and changed the name to Cisco Spark. This platform ran for four years and continuously evolved into a very powerful cloud-based tool that companies could use for VoIP phone and telepresence endpoint registration and calling, instant messaging, document sharing, and multipoint conference meetings. Then in May 2018, Cisco changed the name once again to unify Spark with the Webex platform and called the new application Webex Teams. In 2019, Cisco combined a cloud calling platform it had acquired called BroadSoft to the Webex platform, creating the new Webex Calling solution. This new calling solution was much more robust, offered many more features, and could scale to any size company.

This actually created a problem. There were now three services called Webex that each performed a different function. There was the original *Webex Meetings*, which had its own app and web interface. There was *Webex Teams*, formerly Cisco Spark, which had its own app for messaging and used the Webex Control Hub as the web-based interface. Then there was *Webex Calling*, formerly BroadSoft, which used its own calling app and web interface. Cisco engineers worked tirelessly to unify these three services under a single pane of glass, as they call it. In 2021, the answer came in the release of a new application simply called the Webex app, which can be used for calling, meetings, and messaging. The term *Webex Teams* was retired, and all administration of these three services can be leveraged through the Webex Control Hub web interface.

Key Topic

At the same time that Webex Calling was being introduced to the Webex solution, Cisco was also developing a new concept that has once again changed the face of telepresence. Cognitive collaboration incorporates artificial intelligence (AI) into the collaboration products to help users in various aspects of their job. Webex is now interactive, much like Amazon Alexa, where you can talk to your telepresence endpoint registered to Webex in the cloud, and it will provide information in response or call a participant at your vocal command. If employees of a company use Webex Meetings to communicate with people outside their organization, a new tool called People Insight will provide background information on the other participants connected so that employees can know more about the people they're connecting with. Cisco is continually researching other cognitive tools to incorporate into the user experience. Webex was the communications solution on board the Artemis space shuttle launched by NASA in 2022 to return to the moon. Cisco is also working with some automobile companies to utilize Webex with the cars' internal systems. Clearly, communication has gone beyond simple voice and video. There are so many ways to communicate and share information. Collaboration involves using all the tools at your disposal to work together with other people. This is why Cisco calls its products *collaboration*.

What new innovations will the future hold? Will 3D projection become a reality, such as with Princes Leia in the Star Wars movie, *Episode IV—A New Hope*? Perhaps 3D printing will be incorporated into these solutions in some capacity. Interactive automobiles and video walls in homes could become commonplace in the future. Android assistants could be used in corporations for various tasks. If history has proven anything, it is that people are limited only by imagination. If you can dream it, it can become reality.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 1-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 1-2 Key Topics for Chapter 1

Key Topic Element	Description	Page Number
Paragraph	ISDN and POTS Explained	7
Paragraph	VoIP Explained	7
Paragraph	Video Telepresence Applications	9
Paragraph	IM and Presence Explained	10
Paragraph	UC Explained	10
Paragraph	Telepresence, Immersive Telepresence, and TIP Defined	12
Paragraph	Cognitive Collaboration Explained	13

Define Key Terms

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

B2B, B2C, H.320, H.323, IETF, IM, ISDN, ITU, OBTP, PBX, POTS, Presence, SIP, TCP/IP, Telepresence, TIP, UC, VoIP

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What product was invented in the late 1990s that is used to control VoIP phone?
2. What are the three communications protocols used for calls with video endpoints?
3. What were the three non-real-time communication services discussed in this chapter?
4. What are the two cognitive collaboration integrations with Webex discussed in this chapter?

This page intentionally left blank

CHAPTER 2

Audio Basics

This chapter covers the following topics:

Basic Understanding of Sound: This topic will introduce a basic understanding of how sound behaves, including wave propagation, technical properties of sound waves, and noise.

Analog vs. Digital Signals: This topic will compare noise on an analog signal compared to noise on a digital signal, observe the principle of the Nyquist-Shannon theorem, and identify how bandwidth conservation can be achieved through data compression.

ITU Audio Encoding Formats: This topic will identify the most commonly used audio codecs in a Cisco solution and analyze the various aspects of each codec.

The preceding chapter provided a backward look into the evolution of communications and a high-level overview of the technologies that exist today that allow us to collaborate at many levels. This chapter will begin to dive into the intricate details that encompass the vast world of audio communication. As you read through this chapter, you will find that the chasm that embodies audio communication is only a foot wide but a mile deep. Although this chapter will not cover every aspect of audio communication, it will provide a solid foundation to build your knowledge on. Topics discussed in this chapter include the following:

- Basic Understanding of Sound
- Wave Propagation
    - Technical Properties of a Sound Wave
    - Understanding Noise
- Analog vs. Digital Signals
- Nyquist-Shannon Sampling Theorem
    - Data Compression Equals Bandwidth Conservation
- ITU Audio Encoding Formats

This chapter covers the following objective from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

2.2 Identify the collaboration codecs for a given scenario

“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
Basic Understanding of Sound	1–4
Analog vs. Digital	5–8
ITU Audio Encoding Formats	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. Through which of the following mediums will sound travel the fastest?

a. Air

b. Water

c. Concrete

d. Gypsum board

2. The measure of the magnitude of change in each oscillation of a sound wave is a description of which term?

a. Frequency

b. Amplitude

c. Wavelength

d. Pressure

3. Which of the following is used to calculate the average amplitude of a wave over time?

a. Newton’s second law of motion

b. Sine waves

c. Pascals

d. Root mean squared

4. What is the primary issue with using repeaters for analog signals?
   - a. Noise riding on the original audio signal is also amplified by the repeaters.
   - b. Distances may be too great to host enough repeaters.
   - c. Noise from the repeaters can be interjected into the audio signals.
   - d. There are no issues with using a repeater for analog signals.
5. Which of the following is a benefit of digital audio over analog audio?
   - a. Digital signals are more fluid than analog signals.
   - b. Digital signals have a more natural sound than analog signals.
   - c. Digital signals are immune to ambient noise.
   - d. Digital signals are not based on timing like an analog signal is.
6. What is the maximum bit rate the human ear can hear at?
   - a. 24 bit
   - b. 21 bit
   - c. 144 bit
   - d. 124 bit
7. Which of the following supports 24 circuit channels at 64 Kbps each?
   - a. DS0
   - b. DS1
   - c. T3
   - d. E1
8. Which of the following describes lossless compression?
   - a. This algorithm searches content for statistically redundant information that can be represented in a compressed state.
   - b. This algorithm searches for nonessential content that can be deleted to conserve storage space.
   - c. Compression formats suffer from generation loss.
   - d. Repeatedly compressing and decompressing the file will cause it to progressively lose quality.
9. Which of the following codecs supports both compressed and uncompressed data?
   - a. G.711
   - b. G.729
   - c. G.722
   - d. G.723.1
10. Which of the following codecs supports lossless compression?
    - a. G.729
    - b. G.722
    - c. iLBC
    - d. iSAC

Foundation Topics

Basic Understanding of Sound

Sound is the traveling of vibrations through a medium, which in most cases is air, generated by a source as waves of changing pressure. These waves of changing pressure in the air, in turn, vibrate our eardrums, allowing our brains to perceive them as sound. How often these pulses of pressure change in a given time period can be measured. We can also measure how intense each pressure change is and how long the space is between each wave. Two factors that relate to sound must be considered: the source and the medium.

Anything that can create these vibrations can be the source of sound. These sources could include human vocal cords or animal larynx, such as birds chirping, lions roaring, or dogs barking. Sound could also be sourced from stringed instruments, such as a guitar, violin, or cello. Percussions cause sound, such as drum skins or even the diaphragm of a loudspeaker. All these things in some way vibrate particles to make sound. A tree falling in the forest will make sound, whether you hear it or not.

The medium sound travels through can affect how that sound is perceived. Have you ever dipped your head underwater in a swimming pool and tried to talk with someone else? Although you can hear the other person, understanding what that person is saying becomes difficult, even when you are both in close proximity. It's important to understand that the speed of sound is constant within a given medium at a given temperature. Generally, the term *speed of sound* refers to a clear, dry day at about 20° C (68° F), which would have the speed of sound at 343.2 meters per second (1,126 ft/s). This equates to 1,236 kilometers per hour (768 mph)—about 1 kilometer in 3 seconds or approximately 1 mile in 5 seconds. The denser the medium, the faster sound will travel. Because air is thicker at lower elevations, and temperatures are usually higher, sound will travel faster but will degrade faster as well. However, in a vacuum, sound will travel much slower because there are no particles to propagate the sound waves, but sound can be heard much clearer at farther distances because they will degrade much slower. Table 2-2 illustrates the speed of sound through four different mediums.

Key Topic

Table 2-2 Speed of Sound Through Four Common Mediums

Medium	Speed (Meters per Second)	Speed (Feet per Second)	Speed Factor
Air	344	1130	1
Water	1480	4854	4.3
Concrete	3400	11,152	9.8
Gypsum Board	6600	22,305	19.6

Wave Propagation

Stand next to a still body of water, pick up a pebble, and toss it to the middle of the pond. As the pebble breaks the surface, it displaces the water it comes in immediate contact with. Those water particles displace other water particles as they are pushed out, so you get a rippling effect that grows from the point where the pebble originally made contact out to the edges of the pond. Once the ripples meet the outer edges of the pond, the rings will begin to move back in, and the ripples will continue until the energy created by tossing the pebble into the water runs out.

This principle is the same one on which sound propagates. When sound is created at the source, the vibrations radiate out in waves, like the ripples in a pond, except they travel in every direction. These sound waves bounce off particles of different mediums in order to travel outward. As the sound waves bounce off particles, some of the energy is absorbed so the vibration weakens. The density of a medium plays a part in how fast a sound wave can propagate or move through it. The more tightly that particles of matter are packed together, the faster a sound wave will move through it, but the sound wave will degrade faster as well. So sound travels faster through a solid than a liquid and faster through a liquid than a gas, such as air. As the sound expands across a larger area, the power that was present at the source to create the original compression is dissipated. Thus, the sound becomes less intense as it progresses farther from the source. The sound wave will eventually stop when all the energy present in the wave has been used up moving particles along its path.

Observe the analogy of the pebble in the pond. When the ripples first begin, they will be taller and closer together. As the energy dissipates, the ripples will become shorter and farther apart, until eventually they cease to demonstrate any effect on the water's surface. This effect can be observed with sound as well. Stand in a canyon and shout out toward the cliffs. The sound you create will travel out and reverberate off the cliffs and return to you. However, what you hear will sound degraded. You may even hear yourself multiple times in an echo, but each time the sound will be weaker than the time before until you can't hear anything at all. If someone shouted out to you under a body of water, by the time the sound reached your ears, it would have degraded so much from bouncing off all the many particles in the water that you would not be able to articulate what was said.

Technical Properties of Sound

All forms of energy can be measured. Light and sound sources in nature are forms of energy. Acoustical energy consists of fluctuating waves of pressure, generally in the air. One complete cycle of that wave consists of a high- and low-pressure half-cycle. This means that half of a sound wave is made up of the compression of the medium, and the other half is the decompression, or rarefaction, of the medium. Imagine compressing a spring and then letting it go. Now imagine that the spring represents air molecules and your hand is the acoustic energy. Figure 2-1 illustrates the technical properties of a sound wave.

To better understand how sound waves are measured, we must define some terms. *Frequency* is the rate of the air pressure fluctuation produced by the acoustic energy wave. To be heard by human ears, wave frequencies must be between 20 and 20,000 cycles per second. Although there is more to it than just frequency, in general, the frequency of a sound wave corresponds with the perceived pitch of the sound. The higher the pitch, the higher the frequency. When we are talking about sounds and music, there is not just one single frequency, but many different frequencies overlapping with each other. This means many different frequencies are being represented within a single signal. The bandwidth of a particular signal is the difference between the highest and the lowest frequencies within the signal.

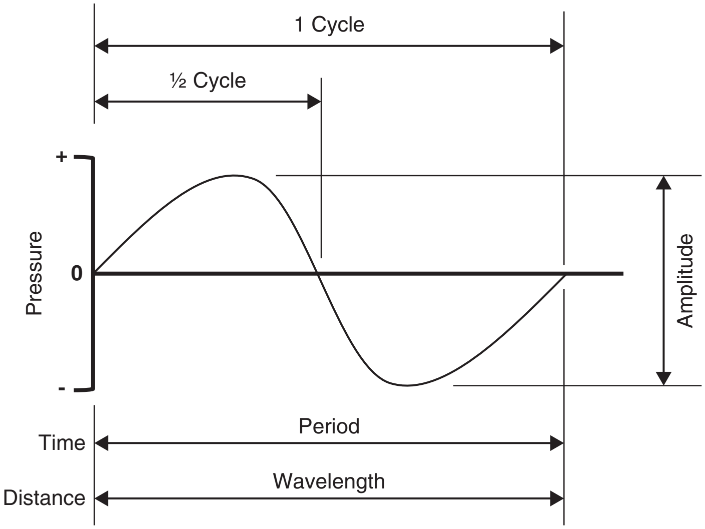


Figure 2-1 *Technical Properties of a Sound Wave*

Amplitude is the measure of the magnitude of change in each oscillation of a sound wave. Most often this measurement is peak-to-peak, such as the change between the highest peak amplitude value and the lowest trough amplitude value, which can be negative. Bear in mind the relationship between amplitude and frequency. Two waveforms can have identical frequency with differing amplitude and identical amplitude with differing frequency. For sound waves, the wave oscillations are representative of air molecules moving due to atmospheric pressure changes, so the amplitude of a sound wave is a measure of sound pressure. Sound pressure is measured in pascals or millibars:

1 pascal = 1 newton per square meter

1 millibar = 100 pascals

A newton is the standard international unit for force. It is equal to the amount of net force required to accelerate a mass of one kilogram at a rate of one meter per second squared. Newton's second law of motion states F = ma, multiplying m (kg) by a (m/s^2); the newton is, therefore, N = kg(m/s^2).

A frequency spectrum is the complete range of frequencies that can be heard, just as the visible spectrum is the range of light frequencies that can be seen. Devices and equipment can also have frequency spectrums, or ranges.

Basic sine waves cannot have an "average" per se. Rather, it would equal zero because the wave peaks and valleys are symmetrical above and below the reference of zero. What is much more helpful when discussing the average amplitude of a wave over time is called root mean squared (RMS). RMS is often used to calculate a comparable measure of power efficiency, such as in audio amplifiers. RMS measures mean output power to mean input power. RMS is just the squaring of every point of a wave and then finding the average. Squaring a negative value always results in a positive value. RMS gives us a useful average value for discussing audio equipment and comparing amplitude measurements. Basically, RMS is much more similar to the way we hear sound, as opposed to measuring just the peaks of a wave, because we don't hear just the peaks.

A sound wave emanating from a source is like an expanding bubble. The power of the sound would be the energy on the surface of the bubble. As the surface of the bubble expands, that energy is used up in order to move, or vibrate, the air ever farther outward. That means eventually the power that the bubble started with at its source would be expended. The power of sound, or sound's acoustical power, is a measure of amplitude over time. The sound had a particular measurement at the moment it was emitted from the source, but as it travels, over time the power decreases as the energy present in the sound wave is expended transmitting itself through the medium. The transmission of acoustical energy through a medium is measured in watts. A watt is just the rate of transfer of energy in one second or one joule per second. A joule is equal to the energy expended in applying a force of one newton through a distance of one meter. The following equation is used to calculate sound's acoustical power:

$$J=kg*m^2/s^2=N*4444m=Pa*m^3=W*s$$

where

- N is the newton.
- m is the meter.
- kg is the kilogram.
- s is the second.
- Pa is the pascal.
- W is the watt.

Understanding Attenuation and Noise

When Alexander Graham Bell placed his first audio call to his assistant, Watson, it was only to the next room. Bell's journal records that the audio was loud but muffled. There are two reasons why the sound was hard to hear: attenuation and noise.

Key Topic

Attenuation, as has previously been discussed, is the degrading of the sound wave as it loses energy over time and space. When the telephone was first made available to the public market, telephone companies had to set up repeaters to account for this loss in signal strength. These repeaters could boost the intensity of the analog wave at different points along the path between two telephones, or nodes. This allowed telephone calls to traverse much longer distances. However, telephone repeaters solved only half the problem.

In audio terms, noise doesn't necessarily refer to something you hear. *Noise* can also refer to inaccuracies or imperfections in a signal transmission that was not intended to be present. Noise comes in different forms, like acoustical, digital, or electrical. Noise can be introduced to a signal in many ways, like faulty connections in wiring or external signal interference. In telephony, as audio signals are transmitted across a wire using electrical signals, those same wires can pick up energy from external sources and transmit them along the same current carrying the audio signal. If you are old enough to remember using analog phones, you might also remember hearing a crackling sound in the background during a phone call. That background noise was caused by interference.

When an analog signal must be transmitted a long distance, the signal level is amplified to strengthen it; however, this process also amplifies any noise present in the signal. This amplification could cause the original analog signal to become too distorted to be heard properly at the destination. Therefore, it is very important with analog transmissions to make sure the original audio signal is much stronger than the noise. Electronic filters can also be introduced, which helps remove unwanted frequency from the analog signal. The frequency response may be tailored to eliminate unwanted frequency components from an input signal or to limit an amplifier to signals within a particular band of frequencies. Figure 2-2 illustrates how noise riding on an analog signal can be amplified at repeaters.

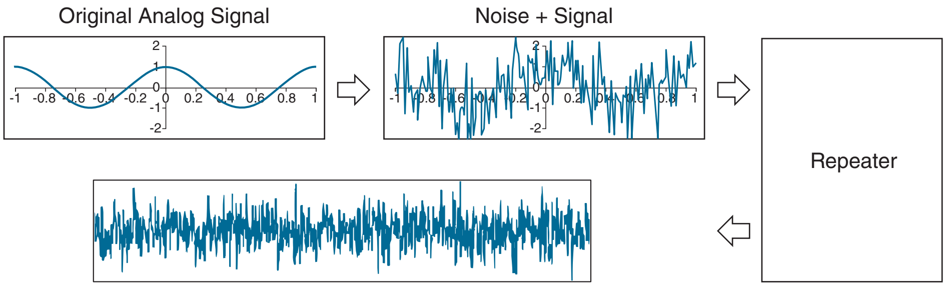


Figure 2-2 *Amplification of Noise on an Analog Signal*

Analog vs. Digital Signals

Key Topic

An analog signal is a continuous signal that contains a time variable representative of some other time-varying quality, such as the voltage of the signal may vary with the pressure of the sound waves. In contrast, a digital signal is a continuous quantity that is a representation of a sequence of discrete values that can take on only one of a finite number of values. There are only two states to a digital bit, zero or one, which can also be perceived as on or off. These are referred to as *binary digits*. Another way to compare analog signals with digital signals could be to think of them as light switches. A digital signal operates like a regular light switch; it is either on or off. An analog signal is more like a dimmer switch that is fluid and allows varying levels of light.

Another good way to mentally picture the difference between analog and digital is to think of two types of clocks. An analog clock has hands that point at numbers, by slowly rotating around in a circle, and digital clocks have decimal number displays. The analog clock has no physical limit to how finely it can display the time, as its hands move in a smooth, pauseless fashion. If you look at the clock at just the right moments, you can see the hand pointing between two minutes or even two seconds, such as it could read 3:05 and a half. The digital clock cannot display anything between 3:05 and 3:06. It is either one or the other; there is no variance between the two times.

When it comes to sound quality, there is much debate as to whether analog or digital sounds better. Vinyl records, or LP (long play) records, are an example of raw analog audio that has been recorded. CDs or MP3s are examples of digital audio that has been recorded. The science behind audio quality definitively determines that analog has a better sound quality than digital because analog is the most natural and raw form of sound waves, and analog is the only form of audio sound waves our ears can articulate. Digital recordings take an analog signal and convert it into a digital format. When that digital recording is played back, it must be converted back to analog before the audio is played over speakers. Because digital conversion cannot make a perfect copy of the original fluid audio sound wave, some of that sound quality is lost when the digital signal is converted back into analog.

This issue of conversion raises a question: if analog audio is better than digital audio, why use digital at all? In conjunction with the preceding examples, digital copies allow a higher quantity of audio to be stored. If you go to a music store or download music from the Internet, you can store more songs in a smaller container, such as an MP3 player or an iPod. Bringing the subject back to communications, an analog signal cannot travel very far without suffering from attenuation. Digital signals can travel much farther than analog signals and don't degrade in the same manner. Digital repeaters will amplify the signal, but they may also retime, resynchronize, and reshape the pulses. Additionally, analog signals are very sensitive to ambient noise, which can quickly degrade the sound quality. Digital signals use binary digits of zero or one, so they are immune to ambient noise.

It is much easier to identify and remove unwanted noise from a digitally sampled signal compared to an analog signal. The intended state of the signal is much easier to recognize. When discussing potential errors in a transmitted signal, error checking and correction are made much easier by the very nature of digital representation. As a digital signal enters a digital repeater, an algorithm will first check to see if the information that is supposed to be there still exists or if it's missing. Assuming the correct information is there, next it will check the state of each digital bit in question: on or off (a one or zero). Finally, it will check that the position of each bit is correct: is the bit on when it's supposed to be off or vice versa?

When an analog signal must be transmitted a long distance, the signal level is amplified to strengthen it; however, this also amplifies any noise present in the signal. Digital signals are not amplified. Instead, for long-distance transmission, the signal is regenerated at specific intervals. In this manner, noise is not passed along the transmission chain.

Nyquist-Shannon Sampling Theorem

Key Topic

Always keep in mind that digital signals are just long strings of binary numbers. Analog signals must be somehow converted into strings of numbers to be transmitted in the digital realm. When a continuous analog signal is converted to a digital signal, measurements of the analog signal must be taken at precise points. These measurements are referred to as *samples*. The more frequent the sample intervals, the more accurate the digital representation of the original analog signal. The act of sampling an analog signal for the purpose of reducing it to a smaller set of manageable digital values is referred to as *quantizing* or *quantization*. The difference between the resulting digital representation of the original analog signal and the actual value of the original analog signal is referred to as *quantization error*. Figure 2-3 illustrates how quantizing an analog signal would appear.

In Figure 2-3, each movement upward on the Y-axis is signified by a one-binary digit. Each movement horizontally on the X-axis is signified by a zero-binary digit. Each movement downward on the Y-axis is signified by a negative one-binary digit. In this manner an analog signal can be quantized into a digital signal. However, notice that the binary signal is not exactly the same as the original analog signal. Therefore, when the digital signal is converted back to analog, the sound quality will not be the same. A closer match can be obtained with more samples. The size of each sample is measured in bits per sample and is generally referred to as *bit depth*. However, it will never be exact because a digital signal cannot ever match the fluid flow of an analog signal. The question becomes, can a digital signal come close enough to an analog signal that it is indistinguishable to the human ear?

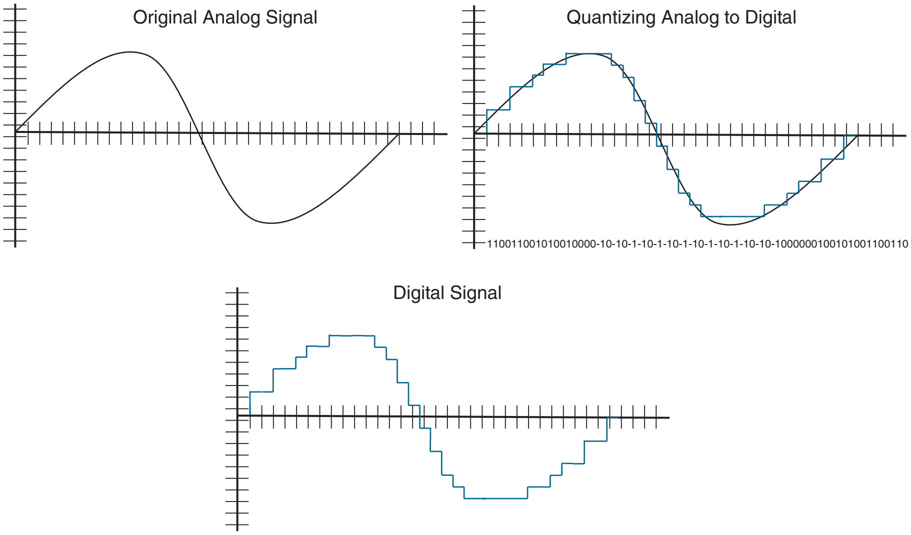


Figure 2-3 *Quantizing an Analog Signal*

When an audio signal has two channels, one for left speakers and one for right speakers, this is referred to as *stereo*. When an audio signal has only one channel used for both left and right speakers, this is referred to as *mono*. Using the preceding quantizing information, along with whether an audio signal is stereo or mono, it is relatively simple to calculate the bit rate of any audio source. The bit rate describes the amount of data, or bits, transmitted per second. A standard audio CD is said to have a data rate of 44.1 kHz/16, meaning that the audio data was sampled 44,100 times per second, with a bit depth of 16. CD tracks are usually stereo, using a left and right track, so the amount of audio data per second is double that of mono, where only a single track is used. The bit rate is then 44,100 samples/second × 16 bits/sample × 2 tracks = 1,411,200 bps or 1.4 Mbps.

When the sampling bit depth is increased, quantization noise is reduced so that the signal-to-noise ratio, or SNR, is improved. The relationship between bit depth and SNR is for each 1-bit increase in bit depth, the SNR will increase by 6 dB. Thus, 24-bit digital audio has a theoretical maximum SNR of 144 dB, compared to 96 dB for 16-bit; however, as of 2007 digital audio converter technology is limited to an SNR of about 126 dB (21-bit) because of real-world limitations in integrated circuit design. Still, this approximately matches the performance of the human ear. After about 132 dB (22-bit), you would have exceeded the capabilities of human hearing.

Key Topic

To determine the proper sampling rate that must occur for analog-to-digital conversion to match the audio patterns closely, Harry Nyquist and Claude Shannon came up with a theorem that would accurately calculate what the sampling rate should be. Many audio codecs used today follow the Nyquist-Shannon theorem. Any analog signal consists of components at various frequencies. The simplest case is the sine wave, in which all the signal energy is concentrated at one frequency. In practice, analog signals usually have complex waveforms, with components at many frequencies. The highest frequency component in an analog signal determines the bandwidth of that signal. The higher the frequency, the greater the bandwidth, if all other factors are held constant. The Nyquist-Shannon theorem states that to allow an analog signal to be completely represented in digital form, the sampling rate must be at least twice the maximum cycles per second, based on frequency or bandwidth, of the original signal. This maximum bandwidth is called the *Nyquist frequency*. If the sampling rate is not at least twice the maximum cycles per second, then when such a digital signal is converted back to analog form by a digital-to-analog converter, false frequency components appear that were not in the original analog signal. This undesirable condition is a form of distortion called *aliasing*. Sampling an analog input signal at a rate much higher than the minimum frequency required by the Nyquist-Shannon theorem is called *over-sampling*. Over-sampling improves the quality or the digital representation of the original analog input signal. Under-sampling occurs when the sampling rate is lower than the analog input frequency.

The Nyquist-Shannon theorem led to the Digital Signal 0 (DS0) rate. DS0 was introduced to carry a single digitized voice call. For a typical phone call, the audio sound is digitized at an 8 kHz sample rate using 8-bit pulse-code modulation for each of the 8000 samples per second. This resulted in a data rate of 64 kbps.

Because of its fundamental role in carrying a single phone call, the DS0 rate forms the basis for the digital multiplex transmission hierarchy in telecommunications systems used in North America. To limit the number of wires required between two destinations that need to host multiple calls simultaneously, a system was built in which multiple DS0s are multiplexed together on higher-capacity circuits. In this system, 24 DS0s are multiplexed into a DS1 signal. Twenty-eight DS1s are multiplexed into a DS3. When carried over copper wire, this is the well-known T-carrier system, with T1 and T3 corresponding to DS1 and DS3, respectively.

Outside of North America, other ISDN carriers use a similar Primary Rate Interface (PRI). Japan uses a J1, which essentially uses the same 24 channels as a T1. Most of the world uses an E1, which uses 32 channels at 64 kbps each. ISDN will be covered in more depth in Chapter 5, “Communication Protocols.” However, it is important to note that the same sampling rate used with DS0 is also used in VoIP communications across the Internet. This led to a new issue that in turn opened up a new wave of advancement in the audio communication industry: How could digital audio signals be sent over low-bandwidth networks?

Data Compression Equals Bandwidth Conversion

The answer to the question regarding digital audio signals being sent over low-bandwidth networks came with the development of data compression. Bandwidth is the rate that data bits can successfully travel across a communication path. Transmitting audio can consume a high amount of bandwidth from a finite total available. The higher the sampled frequency of a signal, the larger the amount of data to transmit, resulting in more bandwidth being required to transmit that signal. Data compression can reduce the amount of bandwidth consumed from the total transmission capacity. Compression involves utilizing encoding algorithms to reduce the size of digital data. Compressed data must be decompressed to be used. This extra processing imposes computational or other costs into the transmission hardware.

Key Topic

Lossless and *lossy* are descriptive terms used to describe whether or not the data in question can be recovered exactly bit-for-bit when the file is uncompressed or whether the data will be reduced by permanently altering or eliminating certain bits, especially redundant bits. Lossless compression searches content for statistically redundant information that can be represented in a compressed state without losing any original information. By contrast, lossy compression searches for nonessential content that can be deleted to conserve storage space. A good example of lossy would be a scenic photo of a house with a blue sky overhead. The actual color of the sky isn't just one color of blue; there are variances throughout. Lossy compression could replace all the blue variances of the sky with one color of blue, thus reducing the amount of color information needed to replicate the blue sky after decompression. This is, of course, an unsubtle oversimplification of the process, but the concept is the same.

It is worth noting that lossy compression formats suffer from generation loss; repeatedly compressing and decompressing the file will cause it to progressively lose quality. This is in contrast with lossless data compression, where data will not be lost even if compression is repeated numerous times. Lossless compression therefore has a lower limit. A certain amount of data must be maintained for proper replication after decompression. Lossy compression assumes that there is a trade-off between quality and the size of the data after compression. The amount of compression is limited only by the perceptible loss of quality that is deemed acceptable.

ITU Audio Encoding Formats

Codec stands for coding and decoding. A codec is a device or software program that is designed to code and decode digital data, as well as compress and decompress that data. Therefore, an audio codec is a device or software that is designed to process incoming analog audio, convert it to digital, and compress the data, if necessary, before sending that data to a specific destination. The codec can also process incoming data, decompress that data if necessary, and convert the digital data back to analog audio. Many proprietary codecs have been created over the years. However, in an effort to unify communications, the International Telecommunications Union (ITU) created a standardized set of audio codecs. The ITU is a specific agency of the United Nations whose chief responsibilities include the coordination of the shared global use of the usable RF spectrum, and the establishment of standards to which manufacturers and software designers comply in order to ensure compatibility. Table 2-3 outlines some of the more common audio codecs used in a Cisco collaboration solution. Each codec that starts with a "G" is an ITU codec.

Key Topic

Table 2-3 Audio Codecs Commonly Used by Cisco

Codec and Bit Rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Bandwidth MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G.711 (64 Kbps)	80	10	4.1	160	82.8	87.2
G.729 (8 Kbps)	10	10	3.92	20	26.8	31.2
G.723.1 (6.3 Kbps)	24	30	3.9	24	18.9	21.9
G.723.1 (5.3 Kbps)	20	30	3.8	20	17.9	20.8

Codec and Bit Rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Bandwidth MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G.726 (32 Kbps)	20	5	3.85	80	50.8	55.2
G.726 (24 Kbps)	15	5	3.61	60	42.8	47.2
G.728 (16 Kbps)	10	5		60	28.5	31.5
G.722_64k (64 Kbps)	80	10	4.13	160	82.8	87.2
iLBC_Mode_20 (15.2 Kbps)	38	20	4.14	38	34.0	38.4
iLBC_Mode_30 (13.33 Kbps)	50	30	4.14	50	25.867	28.8

Table 2-3 is not an exhaustive list of codecs available today, and it is important to note that ITU codecs are used with SIP communication as well. Table 2-3 is divided into seven columns. The first column identifies the codec and the number of bits per second needed to transmit the payload in each packet for a voice call. The codec bit rate = codec sample size / codec sample interval. The next column is the codec sampling size based on bytes. This is the number of bytes captured by the codec at each codec sample interval. Column three is the codec sampling interval. This is the sample interval at which the codec operates. For example, the G.729 codec operates on sample intervals of 10 ms, corresponding to 10 bytes (80 bits) per sample at a bit rate of 8 kbps. The next column is the Mean Opinion Score (MOS), which is a system of grading the voice quality of telephone connections. With MOS, a wide range of listeners judge the quality of a voice sample on a scale of one (bad) to five (excellent). The scores are averaged to provide the MOS for the codec. The last two columns show the bandwidth needed to transmit the audio with overhead added in. The bandwidth MP or FRF.12 shows the Layer 2 header values added to the original payload, and the bandwidth ethernet shows the Layer 3 header values added on top of the Layer 2 headers.

Key Topic

Based on the Nyquist-Shannon theorem, the first audio codec created by the ITU is G.711. Originally released in 1972, G.711 is also referred to as pulse-code modulation (PCM) and was introduced for use in telephony. It is the required minimum standard in both H.320 for circuit-switched telephony and H.323 for packet-switched telephony. It is considered a *narrow-band* codec since it processes only frequencies between 300 and 3400 Hz, although an annex has been added to extend the frequency range. It uses a sampling frequency of 8 kHz and has a bit rate of 64 kbps. Two algorithm types are associated with G.711: G.711 mu-law and G.711 a-law. G.711 mu-law is a *companding algorithm*, which reduces the dynamic range of an audio signal. G.711 mu-law is used throughout North America and Japan. The algorithm used with G.711 a-law is common throughout the rest of the world where E1 circuits are used, and it is the inverse of the mu-law algorithm. All G.711 codecs are uncompressed.

G.729 is a lossy compressed audio codec and is the most common compression algorithm used in low-bandwidth environments. It has been used in videoconferencing applications for some time and attained its ITU recommendation in 1996. It can operate at a low rate of 4000 Hz. There are several annexes to the G.729 codec, the ones most commonly used with Cisco being G.729r8 and G.729br8. Both codecs operate at 8 Kbps, but G.729br8 contains built-in VAD that cannot be disabled.

Now compare the two previously mentioned codecs with G.722. Released in 1988, this codec can operate as a lossy compressed codec or an uncompressed codec, depending on the annex being run. G.722 addressed some of the speech quality issues presented by the limited bandwidth of the G.711 codec. In contrast to G.711, G.722 is considered a *wideband* codec and processes frequencies between 50 and 7000 Hz. It also samples audio at 16 kHz and operates at 48, 56, or 64 kbps. When G.722 audio is used over an H.323 call, the packets are framed using the 802.3 standard and are sent at 60-millisecond intervals.

Two other commonly used codecs with Cisco collaboration solutions are iLBC and iSAC. These are not ITU codecs, but they are open standards that can be used by any organization. Internet Low Bitrate Codec (iLBC) was originally drafted for the WebRTC project. It was adopted by the IETF in 2002 and ratified into SIP communications in 2003. Internet Speech Audio Codec (iSAC) was originally created by Global IP Solutions. iSAC was acquired by Google in 2011, incorporated into the open-source WebRTC project, and later ratified into the SIP protocol by the IETF. The iSAC codec is an adaptive wideband speech and audio codec that operates with short delay, making it suitable for high-quality real-time communication. It is specially designed to deliver wideband speech quality in both low and medium bit-rate applications. The iSAC codec compresses speech frames of 16 kHz, 16-bit sampled input speech, each frame containing 30 or 60 ms of speech. The codec runs in one of two different modes called channel-adaptive mode and channel-independent mode. In both modes iSAC is aiming at a target bit rate, which is neither the average nor the maximum bit rate that will be reached by iSAC, but it corresponds to the average bit rate during peaks in speech activity.

In channel-adaptive mode, the target bit rate is adapted to give a bit rate corresponding to the available bandwidth on the channel. The available bandwidth is constantly estimated at the receiving iSAC and signaled in-band in the iSAC bit stream. Even at dial-up modem data rates, iSAC delivers high quality by automatically adjusting transmission rates to give the best possible listening experience over the available bandwidth. The default initial target bit rate is 20,000 bits per second in channel-adaptive mode.

In channel-independent mode, a target bit rate has to be provided to iSAC prior to encoding. After encoding the speech signal, the iSAC codec uses lossless coding to further reduce the size of each packet and hence the total bit rate used. The adaptation and the lossless coding described here both result in a variation of packet size, depending both on the nature of speech and the available bandwidth. Therefore, the iSAC codec operates at transmission rates from about 10 kbps to about 32 kbps.

The best quality audio codec available to date is Advanced Audio Codec-Low Delay (AAC-LD). It is also referred to as Low-overhead MPEG-4 Audio Transport Multiplex (LATM), and this codec is most commonly used with SIP communication. Since 1997 this codec has been used to offer premium stereo audio by over-sampling analog audio signaling. Sampling rates range between 48 Kbps and 128 Kbps, with a frequency range of 20 kHz. Although this codec does offer excellent audio quality during calls, the trade-off is the high cost in bandwidth when this codec is used.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

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

Key Topic

Table 2-4 Key Topics for Chapter 2

Key Topic Element	Description	Page Number
Table 2-2	Speed of Sound Through Four Common Mediums	19
Paragraph	Behavior of Sound Waves as They Propagate	20
Section	Technical Properties of Sound	20
Paragraph	Define Attenuation and Noise	22
Paragraph	Define Analog and Digital Audio Signals	23
Paragraph	Samples and Quantization Explained	24
Paragraph	Nyquist-Shannon Theorem Explained	25
Paragraph	Lossless and Lossy Compression Explained	27
Table 2-3	Audio Codecs Commonly Used by Cisco	27
Paragraph	G.711, G.729, and G.722 Explained	28

Define Key Terms

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

> Acoustical Power, Aliasing, Amplitude, Analog Signal, Bandwidth, Bit Depth, Data Compression, Digital Signal, DS0, DS1, DS3, Electronic Filters, Frequency, Frequency Spectrum, Lossless, Lossy, Millibar, Mono, Newton, Over-sampling, Pascal, PCM, Quantization, Quantization Error, RMS, Samples, Sine Wave, Sound Pressure, Stereo, Undersampling, Watt, Wavelength

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Name the technical properties of a sound wave.
2. What are the three digital signal rate forms, and how do they translate into T-carrier rate forms?
3. List the top three ITU codecs used for audio and the three SIP audio codecs mentioned in this book.

This page intentionally left blank

CHAPTER 3

Video Basics

This chapter covers the following topics:

Basic Understanding of Light: This topic will provide a basic understanding of light behavior, break down aspects of light into chrominance and luminance, and discuss light temperature.

Capturing and Cameras: This topic will discuss frame rates, explain what pixels are and how they impact resolution, and overview common encoding techniques for video.

Standard Video Codecs: This topic will examine video compression and discuss varying video quality based on video codecs.

Video Container Formats and Codecs: This topic will compare and contrast the H.264 video codec with the latest H.265 HEVC video codec. This topic will also discuss how content can be shared in a video stream during video communication.

As mentioned in Chapter 1, "Introduction to Collaboration," video communication is a relatively young industry. As such, most of the development within this industry has occurred within the last 30 years. Microsoft released one of the first consumer products that allowed video communication from a desktop application with the release of Windows 95, but it didn't resonate with people for several reasons. Networks couldn't support the bandwidth required, so quality was an issue, and consumers couldn't envision the need for video communication. Most of the early use cases for video communication occurred within the business sector, which in turn influenced the standards that soon followed. In today's market several consumer video communication products are available, such as Skype and Apple's FaceTime. However, it is still the private and public sectors that continue to drive the industry forward. To fully understand how video communication works, we need a more in-depth examination of light behavior. Topics discussed in this chapter include the following:

- Basic Understanding of Light
- Chrominance and Luminance
  - Color Temperature
- Capturing and Cameras
- Frame Rates
  - Understanding Pixels and Resolution
  - Common Encoding Techniques

- Standard Video Codecs
- Video Compression
  - Video Quality
- Video Container Formats and Codecs
- H.264 Compared to H.265 HEVC
  - Content Channels

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

2.2 Identify the collaboration codecs for a given scenario

"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
Basic Understanding of Light	1–4
Capturing and Cameras	5–9
Standard Video Codecs	10–11
Video Container Formats and Codecs	12

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 are the three primary colors?
   a. Red, white, blue
   b. White, black, red
   c. Red, green, blue
   d. Red, yellow, blue

2. Which of the following terms is used to identify colors in light?
   a. Chrominance
   b. Luminance
   c. Composite
   d. Component
3. In the formula G = (Y – 0.299R – 0.114B) / 0.587, what does Y stand for?
   a. Luminance
   b. Chrominance
   c. Composite
   d. Component
4. Which of the following colors has the warmest temperature?
   a. Blue
   b. Red
   c. Green
   d. Yellow
5. Which of the following light filtration techniques lets about one-third of each color in and maps the saturation levels of each color per pixel in a mosaic effect?
   a. Foveon X3
   b. 3CCD
   c. Bayer
   d. 3 Chip
6. What is the lowest frame rate that still allows the human brain to perceive motion?
   a. 15 fps
   b. 24 fps
   c. 25 fps
   d. 30 fps
7. For what reason do NTSC and PAL use different frame rates?
   a. Different standards warrant different frame rates.
   b. Different resolutions warrant different frame rates.
   c. NTSC uses radio waves for broadcasting and PAL uses microwaves.
   d. The hertz rate on different power grids warrants different frame rates.
8. When given the resolution 1280 × 720p30, what does the 1280 represent?
   a. Pixels
   b. Lines
   c. Frame rate
   d. Scanning
9. When given the resolution 1280 × 720p30, what does the **p** represent?
   a. Pixels
   b. Progressive

- **c.** Picture
- **d.** Photons

10. What is the standard segmentation for macroblocks?

- **a.** 2 × 2
- **b.** 4 × 4
- **c.** 8 × 8
- **d.** 16 × 16

11. Which of the following video codecs was based off the MPEG-4 codec?

- **a.** H.261
- **b.** H.263
- **c.** H.264
- **d.** H.265

12. What is the maximum bit rate reduction that can be expected using the H.265 HEVC codec over H.264?

- **a.** 25%
- **b.** 50%
- **c.** 68%
- **d.** 75%

Foundation Topics

Basic Understanding of Light

There has been much debate among physicists over the last 400 years as to whether light is a particle or a wave, and there are conclusive studies that definitively prove both theories. Light was originally believed to be a particle based on a study by Sir Isaac Newton; however, several contemporary physicists concluded that light is a wave, and so the debate began. In the mid-1800s, a Scottish physicist named James Clerk Maxwell, who was studying electromagnetic waves, proved beyond anyone's doubts that light is not just a wave, but an electromagnetic wave. Much went into the explanation of Maxwell's theory, but in the end, Maxwell showed that the speed of an electromagnetic wave is the same as the speed of light. Maxwell ended the debate, proving light is a wave until it was examined by the famous physicist Albert Einstein as he studied quantum mechanics. Einstein's theory is that light is a particle, specifically a photon, and that the flow of a photon is a wave. Based on Einstein's theory, the energy of light is in direct correlation to its oscillation frequency, but the intensity of light correlates with the number of photons. Thanks to Einstein's theory, we now understand that light is both a particle and a wave.

Building on Maxwell's discovery that electromagnetic waves are light waves, you can begin to understand that spectrums of light extend beyond what you see. Just a small portion of the electromagnetic radiation (EMR) spectrum is what we refer to as *visible light*. Some EMR is visible to the human eye and is a form of energy emitted and absorbed by charged particles, called *photons*. EMR has both electric and magnetic field components and exhibits wave-like behavior as it travels through space. Figure 3-1 illustrates where visible light exists compared to other spectrums of light.

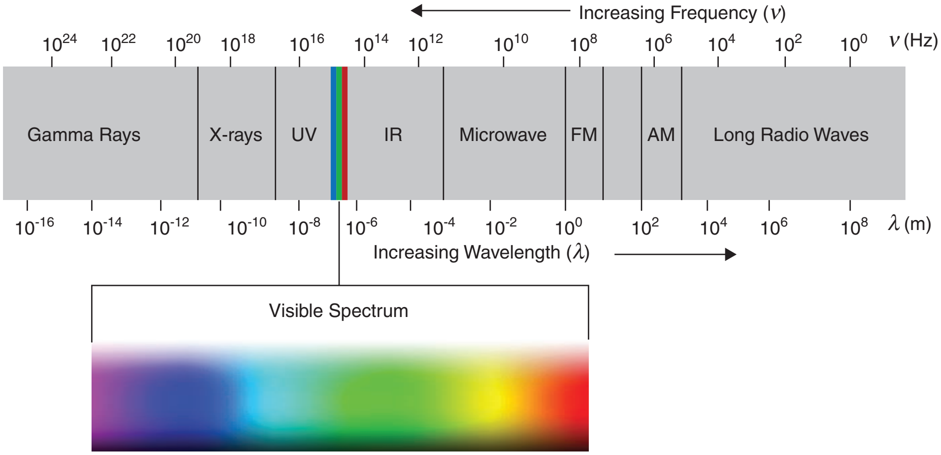


Figure 3-1 *Light Spectrums*

In common with all types of EMR, visible light is emitted and absorbed in tiny packets called photons and exhibits properties of both waves and particles. For example, a lens might refract a single photon or exhibit wave interference with itself but also act as a particle, giving a definite result when its position is measured. In a vacuum, EMR propagates at a characteristic speed, the speed of light. The speed of light is constant in a vacuum at exactly 299,792,458 meters per second. Note that sound waves require a medium and therefore cannot propagate in a vacuum.

Key Topic

The behavior of EMR depends on its wavelength. Higher frequencies have shorter wavelengths, and lower frequencies have longer wavelengths. When EMR interacts with single atoms and molecules, its behavior depends on the amount of energy per photon it carries. Photons are at the lower end of the energies that are capable of causing electronic excitation within molecules. Excitation would lead to changes in the bonding or chemistry of said molecule. At the lower end of the visible light spectrum, such as infrared, EMR becomes invisible to humans because its photons no longer have enough individual energy to cause a lasting molecular change in the molecules within a human retina. It is these photons exciting molecules with the human eye that trigger molecular changes, which cause the sensation of vision. Above the range of visible light, ultraviolet light becomes invisible to humans mostly because it is absorbed by the tissues of the eye—in particular, the lens. EMR is categorized by the frequency of its wave. The electromagnetic spectrum, in order of increasing frequency and decreasing wavelength (refer back to Figure 3-1), consists of radio waves, microwaves, infrared radiation, visible light, ultraviolet radiation, X-rays, and gamma rays.

Chrominance and Luminance

When we see a color in an object, such as a red rose, the rose is not actually red. The surface of those petals absorbs all colors in the light spectrum except red, which are reflected back out. So, when those red light waves enter our eye, we perceive the rose as being red. If an object were to reflect all colors in a light spectrum, then we would perceive that color as white. If an object were to absorb all light in a spectrum, then we would perceive that color as black. The visible color spectrum can be divided into three primary colors—red, blue, and green. Mixing various aspects of these three primary colors is what creates the whole spectrum of color humans can see. Now, this may be confusing to some of you who were taught since grade-school that the three primary colors are red, blue, and yellow. So, let me explain why green is referred to as the third primary color instead of yellow.

Humans see color not just by using the eye, but also through processing the light wavelengths in the brain. The previous section identified differing spectrums of light, which are based on frequency and wavelength. Frequency and wavelength also determine the different colors of light we can see within this visible spectrum. Red light waves have the lowest frequency but the longest wavelength. Blue light waves have the highest frequency but the shortest wavelength. Green light waves, not yellow, are exactly in between the frequency and wavelength of red and blue light waves. As light enters the eye, it is focused through the lens to the back of the eyeball called the retina. The retina is covered in millions of tiny cells called cones and rods, based on their shape. These cells are considered part of the brain because their purpose is to process the light into impulses and pass that information to the cortex of the brain.

Key Topic

Cones are concentrated around the center of the retina near the optic nerve. There are six million cones in each human eye, and they are divided into three types. Each type of cone is sensitive to a different primary color in the visible light spectrum, so as light reflecting off an object enters the eye, the amount and brightness of each light wave provide enough information to the brain to interpret and associate the color being observed. In the video technology world, this is referred to as the *chrominance* of light.

Where cones are concentrated near the center of the retina, rods are concentrated around the edges of the retina. There are over 120 million rods in each human eye, but they mostly process black and white information. This information is used to help our brain interpret depth perception through varying levels of brightness. It is the rods that help your eyes adjust when you turn out the light in a room. In the video technology world, this is referred to as the *luminance* of light. Figure 3-2 illustrates the variances between wavelengths within the visible spectrum of light.

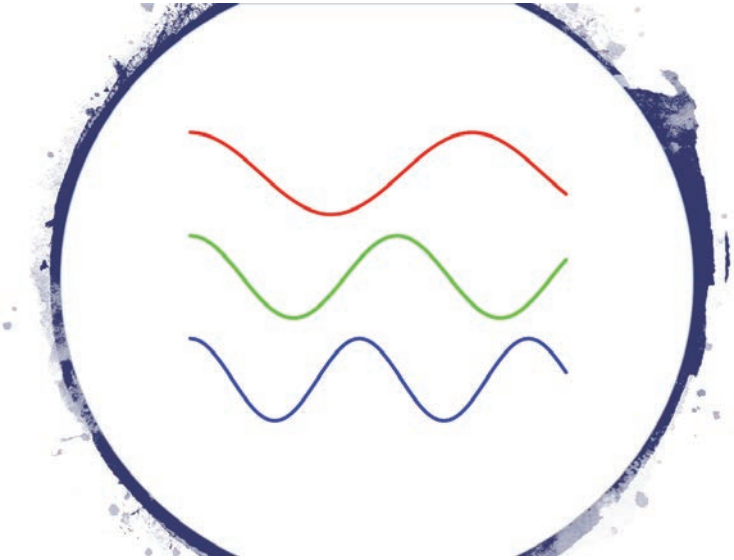


Figure 3-2 *Variances Between Wavelengths Within the Visible Spectrum of Light*

The saying "Not everyone sees things the same way" may not only refer to someone's perspective. All people have varying visual frequency response curves. Changes in how the brain processes light perceived by cones can cause what is known as color blindness. It is very rare for anybody to have total color blindness, where no color can be seen. More commonly, when someone is diagnosed with color blindness, it is usually with one or two colors. Red and green dichromatism is a diagnosis where red and green are indistinguishable from one another. Changes in how the brain processes light perceived by rods can cause issues with depth perception. Since rods deal with light levels, issues with depth perception are more common at night, or in the dark.

Brightness changes can be properly referred to as luminance (luma), and color changes can be properly referred to as chrominance (chroma). As scientists and engineers understand more about the human eye and how people see, technology has evolved to mimic this function through cameras and displays. For many years two organizations shaped how these video technologies were developed. The National Television System Committee (NTSC) was formed in North America and controlled how broadcast television operated in the USA and Canada. Phase Altering Line (PAL) was created in Europe and controlled how broadcast television operated for the UK, Europe, South America, and most of the rest of the world. The NTSC identified that the perceived brightness, or luminance, of an image can be found from the following formula:

$$\mathbf{Y} = 0.299R + 0.587G + 0.114B$$

Y = *luminance (perceived brightness of light)*

R = *strength of red light*

G = *strength of green light*

B = *strength of blue light*

This formula allows only three chrominance signals to be sent without the luminance signal, because the luminance signal can be derived from the chrominance signals at the destination. In YUV signaling, which was developed by PAL, the luminance information is sent as one signal, **Y**, whereas the chrominance information, or color, is sent as two signals: **U=Y – Blue** and **V=Y – Red**. We are still sending three separate signals, which allow us to reproduce any color, but the signals have different individual meanings. Therefore, if we transmit the luminance signal (**Y**) along with a red (**R**) and blue (**B**) signal, we can reproduce the green (**G**) information at the receiving end. G = (Y – 0.299R – 0.114B) / 0.587

Key Topic

Other formulas use differing standards, and each can be grouped into two categories:

- In **composite video**, all the video information is combined into a single line level.
- In **component video**, a video signal is split into two or more component channels.

Historically, the term *YUV* is used for a specific *analog encoding* of color information in television systems. YUV is a component video process, where Y represents the luminance component, and UV represents the chrominance components. The YPbPr color model (used in analog component video) and its digital version YCbCr are more or less derived from YUV. The YUV formula was backward compatible with black-and-white TVs and offered the ability to keep luminance separate from chrominance. The chrominance signals could be compressed more, as that information is less important, and emphasis could be put on the luminance information. Other forms of component video processing could include RBG and HDMI. Examples of composite video could include RCA, VGA, and S-Video. S-Video does break out luminance from chrominance, but because all the chrominance components are sent as one signal, it is still considered composite video.

Color Temperature

All light has a specific temperature and that temperature will affect the lighting arrangement in a video communication environment. If you have a mismatch of light temperatures in the image that you are trying to capture, that mismatch will result in a color variation over the image. Such problems are well known to professional and amateur photographers alike. For example, it is still common today to be able to purchase film designed for either daylight or artificial light. This distinction is particularly important when flash bulbs are required. Often, film sees daylight as having a bluish tinge, whereas artificial light has a yellowish tinge. Film producers refer to light as being either warm (red shift) or cold (blue shift). Theaters and filmmakers place a lot of emphasis on adjusting light toward the lower end of the scale to create a reddish tinge.

Office environments are purposefully designed with a mix of functional lighting that offers a degree of comfort. More importantly, when a room is used for video communication, a range of light known as cool white light should be used. This effect can be achieved by using lighting in the region of 4500 Kelvin. Light temperatures affect room design in more ways than most people generally realize. Every color in a room gives off a temperature. When these temperatures are mixed, some startling effects can occur. This problem is exacerbated by a range of contributors, such as clothing, skin tones, make-up, natural light from windows or skylights, and artificial lighting.

Most light fixtures emit a range of light frequencies, not just a single frequency, so measuring the “color” of a light source is not just measuring the frequency. When objects get very hot, they start to glow and emit light. The hotter the object gets, the higher the frequencies of light it produces. The concept of black-body radiation is used to provide a scale, measured in temperature (Kelvin) by which we can assess the light being emitted by a light fixture.

Capturing and Cameras

Now that the groundwork has been laid explaining how light affects vision, it’s time to turn the conversation toward the components used for video communication. Important aspects to understand include how cameras capture images, how moving pictures operate, and how captured images can be re-created on a display at a remote location. It is also important to understand some common encoding techniques.

Digital cameras work similarly to solar panels in that they use photosensitive panels to change light energy into electrical energy. Two main types of digital cameras are available on the market today:

- Charge-coupled device (CCD) image sensors
- Complementary metal-oxide-semiconductor (CMOS) image sensors

An image sensor detects variable attenuation of light waves and converts them into electrical current. The small cameras in laptop computers, smartphones, and tablets usually use CMOS because they are less expensive and have a lower power consumption. CCD sensors are more commonly used in high-end video cameras.

Cameras detect changes only in light levels, not color, so the light must be split or filtered in some way to get the color values out. Three common techniques are used to separate color in cameras:

Key Topic

- **Foveon X3 sensors** use a method similar to how color film for photography works. An array of layered pixel sensors separates light via the inherent wavelength-dependent absorption property of silicon, such that every location senses all three color channels.
- **3CCD** (also known as three-chip cameras) colors are determined by sending the light through a prism, which separates the light into the RGB spectrum frequencies. Each color is measured on an individual light sensitive chip.
- The most common pattern for the filters is a mosaic called **Bayer**, which lets about one-third of each color in and maps the saturation levels of each color per pixel in a mosaic effect.

Regardless what method is used to filter color from light, the effect is the same. Varying saturations of color are mapped to electrical impulses so that the data can be compressed and sent across a network to a destination. Figure 3-3 illustrates how the Foveon X3 sensor operates compared to the Bayer sensor.

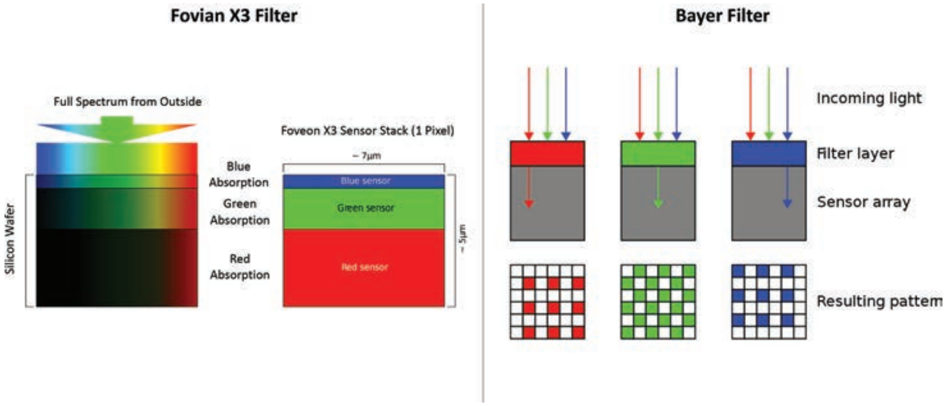


Figure 3-3 *Foveon X3 Sensor vs. Bayer Sensor*

Frame Rates

Now that you understand how cameras capture images, the next topic to understand about video communication is frame rates. Frame rates impact both video capture and video display. When movies first came out, they were referred to as *moving (or motion) pictures*. This is a more accurate description because what we see in video is actually a series of still images, called a reel, that give the illusion of motion. Each still image is called a frame, and the number of frames that are shown per second (frames per second, or fps) is known as frame rate. So how high of a frame rate must be achieved to fool the brain into seeing fluid motion?

Key Topic

The human brain can perceive motion up to about 50 fps. However, even when frames move at slow rates of change, our brains will try to fill in the missing information. Imagine a dog running behind a white picket fence. You know that every few inches a plank of wood obstructs some of your view of the dog, but your brain fills in the missing information unconsciously; there is never any question in your mind that it is anything but a dog running behind a fence. Strobe lights work in a similar fashion. Adjusting the flicker frequency of the light can make images appear as though they are moving in slow motion as our brains stitch the images together. At some point, the frame rate is so slow that our brain will no longer perceive motion. In film circles, the phenomenon of afterimage is referred to as *persistence of vision*. It is generally understood that motion shown at less than 15 fps will be noticeably distracting due to flicker. For images shown above 15 fps, our brains do not realize instantly that a change in an image has occurred. The higher the frame rate, the greater the sense of fluid motion. Film for cinema generally runs at 24 fps, but the projector shutters were designed to flash twice per frame of film, so the screen actually flickers 48 times per second, or 48 Hz, which is less noticeable to the human eye.

Key Topic

In countries where NTSC is used, the frame rate is usually 30 or 60 fps for TV or video communication. In countries where Phase Alternating Line (PAL) is used, the frame rate is usually 25 or 50 fps. The reason for this difference has to do with the power supply to lighting. Did you know that the lights in your home and office flicker? Unless the ballast is broken in fluorescent lights, you probably have not noticed. The reason is that the flicker is so fast that your brain processes it as continuous light, much like with moving pictures. Most power supplied to buildings across the globe uses an alternating current (AC). AC power is supplied in pulses rather than one continuous flow, such as with direct current (DC) power. Low-powered electric fences operate in a similar manner. If you are ever brave enough to touch an electric fence (though, speaking from experience, I do not recommend it), you will feel a shock every second or so. The AC on these types of fences pulse at a much slower rate than the power in a home or office. Throughout North America and in Japan, the AC power operates at 60 Hz, meaning there are 60 pulses per second. Throughout most of the rest of the world, the AC power operates at 50 Hz. This is where it gets interesting. The frame rate must match a multiple of the hertz rate of power; otherwise, the video is affected. Have you ever watched a video or TV show and noticed lines running up the screen? This is one of the effects caused by the frame rate and hertz rate being out of sync. Therefore, in countries that use NTSC standards, the frame rate must be 30 or 60 fps to match the 60 Hz power grid. In countries that use PAL standards, the frame rate must be 25 or 50 fps to match the 50 Hz AC power grid. A few years ago, some televisions that support 120 fps were introduced. In my opinion, purchasing one of these would be a waste of money because the human eye cannot process video beyond about 50 fps. Any frame rates beyond 60 fps have no added benefit to video quality. In contrast, an increase in pixel saturation has much to do with video quality. It is debated heavily that the human eye can detect much faster speeds than what is claimed in this book. However, there is evidence to support both sides of the argument. Therefore, you must decide for yourself if a faster fps display is worth the money. As for me and my house, we will watch TV at 60 fps.

Understanding Pixels and Resolution

All computer monitors, televisions, and displays of any sort that are used in technology today use pixels to create the images people see. *Pixel* is a contraction of the words *picture* and *element*, and this term generally is used to describe the smallest component of a digital image. Pixels are tiny colored dots that, when combined, create a larger image, similar to a mosaic. The image in Figure 3-4 was blown up three times to reveal the pixels that make up the picture.

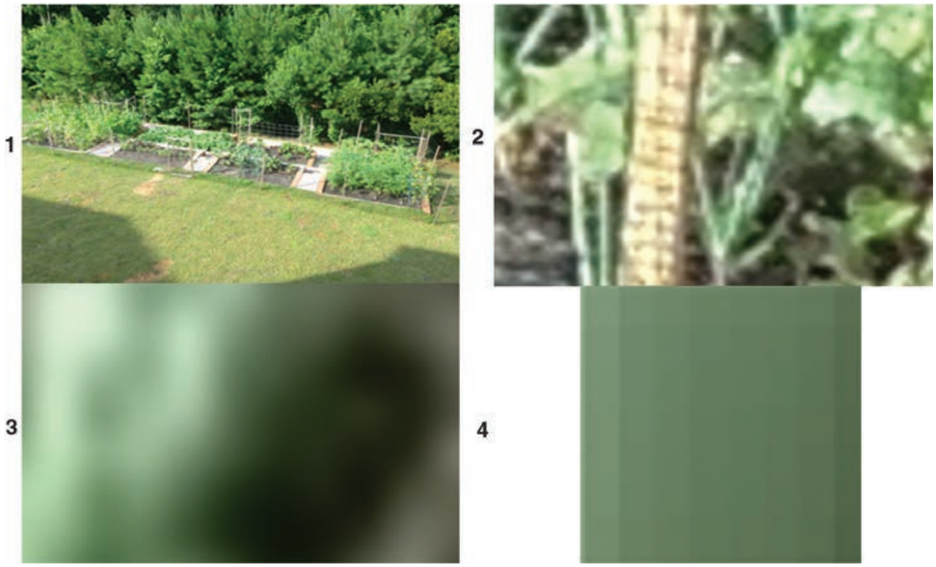


Figure 3-4 *Pixels Within an Image*

In Figure 3-4, image 1 is the original image of a backyard garden taken at some distance away. When this image is zoomed in, as can be seen in image 2, only the pixels within the image are enlarged. The images in this picture still resemble plants in the garden, but the image now appears blurry. The third graphic is zoomed even closer, and now the pixels are so large that the original picture is indistinguishable. This leads to the fourth image, which is a single pixel from within the original picture. When the pixel saturation is increased in the image, closer images can be made clearer.

Key Topic

The number of pixels within a digital frame is called *resolution*. Frames are made up from lines of pixels. When you see a resolution, such as 1280 × 720, the first number identifies how many pixels exist in each line, and the second number identifies how many lines exist per frame. The total pixel saturation is the two numbers multiplied together.

The conversation now comes around to the *aspect ratio* of an image, which describes the proportional relationship between an image's width and its height. An aspect ratio is commonly expressed as two numbers separated by a colon. For an *x*:*y* aspect ratio, the first number, *x*, represents the width, and the second number, *y*, represents the height. No matter how big or small the image is, if the width is divided into *x* units of equal length and the height is measured using this same length unit, the height will be measured to be *y* units. For example, in a group of images that all have an aspect ratio of 16:9, one image might be 16 inches wide and 9 inches high, another 16 centimeters wide and 9 centimeters high, and a third might be 8 yards wide and 4.5 yards high. Thus, aspect ratio concerns the *relationship* of the width to the height, not an image's actual size, but the aspect ratio can influence the pixel saturation.

One missing piece of the resolution puzzle is how these lines of pixels are populated on a display screen. There are two scan types used on all digital displays:

Key Topic

- **Progressive scanning:** This type of scanning begins in the top-left corner of the screen and populates the pixels across line 1, then moves down to line 2, again beginning on the left side of the screen, and so on until all lines within the frame have been populated. Then on the next frame, the scanning begins again, working from line 1 to 2 to 3 and so on. The main aspect of progressive scanning is that each frame is populated with all lines.
- **Interlaced scanning:** In contrast to progressive scanning, interlaced scanning populates only the odd lines on the first frame, then all the even lines on the second frame. The third frame is populated with the odd lines again, and the fourth frame with even lines, and so on.

When you look at the resolution for video, you will see a *p* or an *i*, which indicates whether progressive or interlaced scanning is being used. For example, if you were to see 1280 × 720p30, this can be read as 1280 pixels per line, 720 lines per frame, progressively scanned at 30 frames per second. Figure 3-5 illustrates the scanning process of progressive versus interlaced.

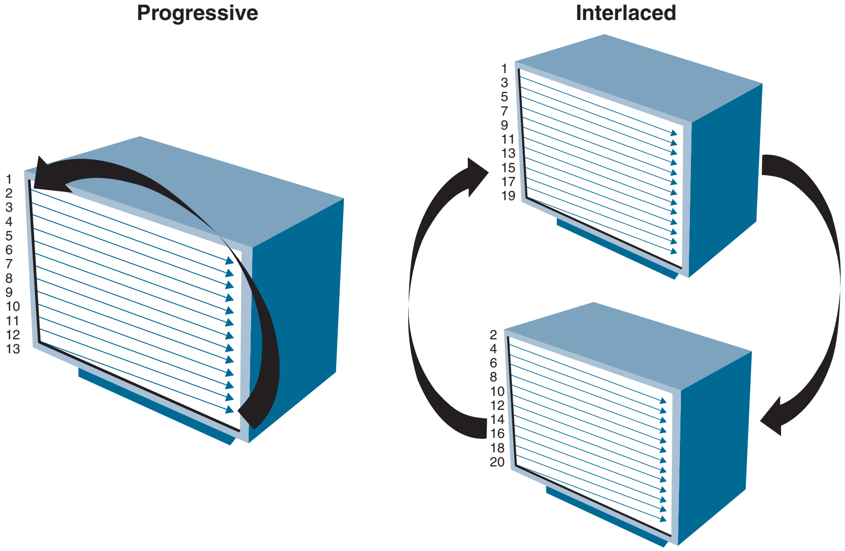


Figure 3-5 *Progressive vs. Interlaced Scanning*

There has been much debate as to which scanning method is better, but there do seem to be unique circumstances when one method is used over the other. Home TVs usually ship with interlaced set as the default scan source. Video endpoints usually ship with progressive set as the default. It seems that playback devices, such as home TVs, tend to gravitate toward interlaced, and live video systems, such as video endpoints, tend to gravitate toward progressive. Both system types provide the capability to change these settings. In my opinion, you can decide for yourself whether one scan source is better than the other. When you have time, go to your television and change between interlaced and progressive to see which you prefer. Be warned; you may not see any difference between them.

Common Video Encoding Techniques

Throughout this chapter, I've referred to NTSC and PAL. Analog TV transmission systems, which dominated the airwaves for most of the 20th century and the first decade of the 21st century, use one of three different types of signal encoding, depending on country or region: NTSC is used throughout North America, PAL is used throughout Europe and Australia, and SECAM is used in France and the former Soviet Union. NTSC and PAL are the most pervasive of the three, and these two standards are defined as follows:

- NTSC
- 525 lines of transmitted signal, of which 480 lines are actual visible picture content
  - 29.97 (or 30) fps
  - 75-ohm termination
- PAL
- 625 lines, of which 576 lines are actual visible picture content
  - 25 fps
  - 75-ohm termination

Just as audio has standard techniques for digitization, such as pulse-code modulation (PCM), so too video has standardized uncompressed video formats. ITU-R BT.601 defines the color space, resolutions, and frame rates for encoding interlaced analog video signals into digital video form. A signal that conforms to the BT.601 standard can be regarded as if it is a digitally encoded analog component video signal, such as including data for the horizontal and vertical sync and blanking intervals. BT.601 has been reused in several other standards, such as MPEG. ITU BT.709 defines the color space, resolutions, and frame rates of widescreen high-definition television using the 16:9 aspect ratio. Common intermediate format (CIF) was designed by the ITU as a compromise between NTSC and PAL resolutions for digital video transmission, particularly regarding video communication. Source input format (SIF) was defined by the ISO as part of MPEG-1. Often referred to as a *constrained parameters bitstream*, SIF defines the minimum specifications any decoder should be able to handle to provide a decent balance between quality and transmission performance. Sometimes SIF is also referred to as standard intermediate format, albeit incorrectly. CIF and SIF exist because of the differences between PAL and NTSC cameras and displays; however, it is quite possible that you will not run into either of these today due to end-to-end all-digital systems that now exist. Table 3-2 identifies some of the common encoding techniques used in digital video communication. Take note of some of the PAL resolution similarities across CIF and SIF. All of the digitization techniques mentioned here use the 4:3 aspect ratio.

Key Topic

Table 3-2 Common Encoding Techniques Used in Digital Video Communication

CIF (Common Intermediate Format)	SIF (Source Input Format)
SQCIF = 128 × 96	N/A
QCIF = 176 × 144	QSIF = 176 × 140
SCIF – 256 × 192	SIF (NTSC/525) = 352 × 240
CIF = 352 × 288	SIF (PAL/625) = 704 × 480

CIF (Common Intermediate Format)	SIF (Source Input Format)
DCIF = 528 × 384	N/A
2CIF = 704 × 288	N/A
N/A	4SIF (NTSC/525) = 704 × 480
4CIF = 704 × 576	4SIF (PAL/625) = 704 × 576
16CIF = 1408 × 1152	16SIF = 1408 × 960

When digital images are transmitted, the color and brightness information is actually coded into numerical values that contain all the information about each individual pixel within the image. Similar to converting analog audio to digital format, the more samples taken of a video image, the more accurate the digital representation will be. When digitizing an image, you are basically just dividing the image into tiny little regions, which are referred to as pixels. The more pixels, the better the resolution.

Several digital television (DTV) formats are in existence around the world, but most standard definition formats are based around NTSC or PAL resolutions so that they can be displayed easily on conventional TV screens. The most common DTV resolutions are NTSCs 480i and PALs 576i. The actual usable resolution of each, respectively, is 704 × 480 and 704 × 576, as only the center 704 horizontal pixels carry actual image. Regarding digital 480i content, where pixels actually determine the entire resolution, 480i resolution would be 640 × 480. In the case of CIF, as you can see from Table 3-2, the resolution is 352 × 288, or 101,376 pixels.

Digital television transmissions can take advantage of recent advancements in data compression and video display technology to deliver higher-quality images than standard analog TV formats. Digital TV provides various alternative options for TV formats, including progressive scanning and 16:9 widescreen aspect ratios. New formats for digital television broadcasts use the MPEG-2 video codec and include the following:

- **ATSC:** USA, Canada, Korea
- **Digital Video Broadcasting (DVB):** Europe
- **ISDB:** Japan
- **ISDB-Tb:** Uses the MPEG-4 video codec. Brazil, Argentina
- **Digital Multimedia Broadcasting (DMB):** Korea

ATSC replaced much of the analog NTSC television system in the United States as of June of 2009. In July 2008, ATSC was updated to support the ITU-T H.264 video codec. The new standard supports 1080p at 50, 59.94, and 60 frames per second; such frame rates require H.264/AVC High Profile Level 4.2, while standard HDTV frame rates require only Levels 3.2 and 4, and SDTV frame rates require only Levels 3 and 3.1.

Standard Video Codecs

Many video compression standards exist today, and each standard has its purpose because “video” can mean many different things. Much of this chapter has focused on broadcast video because the entertainment industry has driven a lot of the development in video transmission. Since high-speed Internet was introduced, many more applications for video have taken root and grown into their own subset of video. YouTube, Netflix, Amazon Prime, and Hulu have revolutionized streaming video. Major broadcasting networks have even joined the race to stream video over the Internet. Streaming video requires different standards from broadcast video. Many companies offer proprietary protocols for streaming video as well, such as Apple and Microsoft. Video communication requires a whole other set of standards regarding how to compress and send live video streams across the Internet. As cloud services become more prevalent in today's technological world, even newer standards are being developed. Before getting into the main standards that exist today, it is important to understand how video compression works.

Video Compression

In video communication, a frame is broken down into several components for the purpose of video compression and prediction. The first unit in an image division is called a *macroblock*. These units are a collection of pixels generally 16 × 16 in size but can be divided into 8 × 8 and 4 × 4 sizes as well. Each macroblock can be broken down into smaller units.

One such unit a macroblock can be broken down into is called a *transform block*. These transform blocks serve as input to a linear block transform. In the YCbCr color space, each single 16 × 16 macroblock consists of 16 × 16 luma (Y) samples and 8 ×8 chroma (Cb and Cr) samples. These samples are split into four Y blocks, one Cb block, and one Cr block. Figure 3-6 illustrates how frames can be broken down into macroblocks and transform blocks.

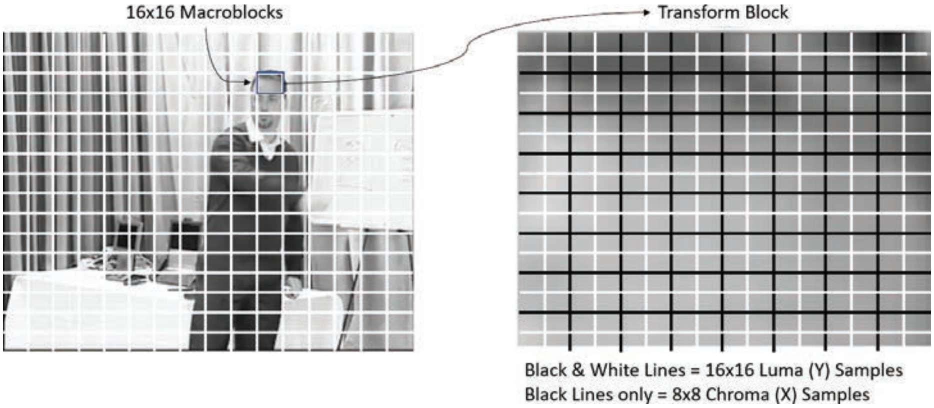

16x16 Macroblocks
Transform Block
Black & White Lines = 16x16 Luma (Y) Samples
Black Lines only = 8x8 Chroma (X) Samples

Figure 3-6 *Macroblocks and Transform Blocks*

Distinct from transform blocks, a macroblock can be split into prediction blocks. In early standards, motion compensation was performed with one motion vector per macroblock. In more modern standards, a macroblock can be split into multiple variable-sized prediction blocks, called *partitions*. In an interpredicted macroblock, a separate motion vector is specified for each partition. Correspondingly, in an intrapredicted macroblock, where samples are predicted by extrapolating from the edges of neighboring blocks, the prediction direction is specified on a per-partition basis. These prediction partition sizes range from 4 × 4 to 16 × 16 samples for both interprediction (motion compensation) and intraprediction.

Key Topic

Sending uncompressed video requires a lot of bandwidth, which is why video compression is essential, especially for live video communication. Once the macroblocks of a frame have been mapped out, video codecs search for changes in the pixels of each macroblock both before and after each frame. These techniques are known as *spatial and temporal redundancy*. Video compression involves sending only the macroblocks where change has been detected; therefore, less bandwidth is required to maintain the video connection. As motion increases and more of each frame needs to be refreshed, more bandwidth is required to compensate for the increased amount of data that needs to be sent. You can test this if you have access to a video endpoint. Place a video call and sit really still for the first minute or so. The video should come in very clear. Then start waving your hand in front of the camera, and you should see the video degrade as the codec tries to keep up with the amount of data that needs to be sent. You can also try this using different connection rates. Try it with a 768 kbps call, 512 kbps call, 384 kbps call, and a 256 kbps call. You should notice that the higher bandwidth rates can keep up with the increase in motion longer than the lower bandwidth rates. But all bandwidth rates will degrade, which is why video compression is so essential.

Video Quality

Three primary video codecs are used across different mediums. They are H.261, H.263, and H.264. Some of the mediums they are used with include ITU H.320, ITU H.323, and IETF SIP. Some streaming applications leverage H.264 as well, such as Netflix, YouTube, and other similar websites.

- **H.261** is the lowest video standard and was the first of the ITU video codecs. This codec will support QCIF and CIF formats, and uses 64 kbps to 2 mbps of bandwidth to transmit and receive video. Today, this standard is typically only used by legacy devices.

- **H.263** came out after H.261 and offers superior advantages. H.263 has better compression, especially in lower bit rate range, and uses basically the same bandwidth. H.263 also offers support for SQCIF 4CIF and 16CIF at a little less than 30 fps, hence a crisper image.

- **H.264**, sometimes called MPEG-4, was introduced at a time when HD communication was being more readily used. This standard was created by the ITU in cooperation with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It currently is the most often used for high-definition video. It is based off MPEG-4 and delivers video that is at the same quality as H.263. The reason it is so favored currently is its capability to deliver video at half the bandwidth usage as H.263.

Video Container Formats and Codecs

Video codecs can refer to either a physical device or coded software that enables video compression and decompression of digital video. An endpoint is a video codec because it does all the coding and decoding of the data. The previous codecs mentioned, such as H.264, are also video codecs because they define how data should be coded and decoded. Like audio, video was historically stored as analog signals on magnetic tape, but the digital revolution made it feasible to begin storing and using video in digital form.

There is always a complex balancing act happening between several factors regarding the quality of encoded video, such as the data bit rate, the complexity of the compression algorithms, robustness to data error correction, how easy it is to edit the compressed version, the capability of random access, transmission delay, and so on. A variety of video compression formats can be implemented on PCs and in consumer electronics equipment, and it is likely that multiple codecs are available within the same product, thus avoiding the need to choose any one specific format. Compatibility is key for ubiquity.

Most common video codecs use standard video compression formats, which make them compatible with each other. For example, video created with a standard MPEG-4 Part 2 codec such as Xvid can be played back using any other standard MPEG-4 Part 2 codec, such as Ffmpeg MPEG-4 or DivX Pro. As with audio, there are also container formats, some of which can be linked to the formats they support. The .MPEG/.MPG file container only supports MPEG-1 and MPEG-2 format standards. Others are not so clear, like .FLV file containers.

H.264 Compared to H.265 HEVC

H.264 Advanced Video Coding (AVC) is a block-oriented motion-compensation-based video compression standard that also goes by the name MPEG-4 Part 10, Advanced Video Coding (MPEG-4 AVC). At the time this book was written, it is one of the most commonly used formats for the recording, compression, and distribution of video content. The purpose of developing H.264 AVC was to create a standard capable of providing great video quality at substantially lower bit rates than previous standards without increasing the complexity of design so much that it would be impractical or expensive to implement. An additional goal was to provide enough flexibility to allow the standard to be applied to a wide variety of applications on a wide variety of networks and systems. Some of the more prevalent applications that use H.264 AVC include broadcast video, DVD storage, RTP/IP packet networks, and multimedia telephony systems. H.264 AVC supports low and high bit rates, as well as low- and high-resolution video. H.264 is typically used for lossy compression, although it is also possible to create truly lossless-coded regions within lossy-coded pictures or to support rare use cases for which the entire encoding is lossless.

The H.265 High Efficiency Video Codec (HEVC) is the newest draft compression standard ratified in 2013. It’s a logical successor to H.264 AVC, which is aimed at reducing the bit rate significantly, and it leverages new compression and prediction techniques. In many ways, HEVC is an extension of the concepts in H.264 AVC. Both work by comparing different parts of a frame of video to find areas that are redundant, both within a single frame and between consecutive frames. These redundant areas are then replaced with a short description instead of the original pixels. The primary changes for HEVC include the expansion of the pattern comparison and difference-coding areas from 16 × 16 pixel to sizes up to 64 × 64, improved variable-block-size segmentation, improved intraprediction within the same picture, improved motion vector prediction and motion region merging, improved motion compensation filtering, and an additional filtering step called sample-adaptive offset filtering. Now comes the bad news. To process all this data, a higher dependency on the hardware is required. As previous versions of video codecs were introduced, a mere software upgrade was all that was needed for those endpoints to support the newer codec. With H.265 HEVC, more signal processing capability for compressing the video is needed, so a simple upgrade patch will not render an older endpoint capable of supporting this newer codec. For this reason, the H.264 AVC codec is still the prominent codec used today, but the market is releasing a whole new line of products with a superior experience for users. Table 3-3 compares the H.264 AVC codec to the H.265 HEVC codec.

Key Topic

Table 3-3 H.264 AVC Compared to H.265 HEVC

	H.264 AVC	H.265 HEVC
Name	MPEG 4 Part 10, AVC	MPEG-H Part 2 HEVC
Approved date	2003	2013
Progression	Successor to MPEG-2 Part	Successor to H.264/AVC
Key improvement	■ 40%–50% bit rate reduction compared with MPEG-2 Part ■ Available to deliver HD sources for Broadcast and Online	■ 25%–50% bit rate reduction compared with H.264 at the same visual quality ■ It is likely to implement Ultra HD, 2K, 4K for Broadcast and Online (OTT)
Highest Resolution Supported	Supports up to 4K	Supports up to 8K
Highest Frame Rate Supported	Supports up to 59.94 fps only	Supports up to 300 fps

Cisco was the first company to introduce video communication endpoints that support H.265 HEVC. The first endpoint Cisco released is called the Cisco SX80 Integrator Video Telepresence Endpoint. Based on the technology in the SX80, Cisco later came out with the MX700 and MX800 endpoints, which are run using an SX80 built into them. Cisco also released a new immersive telepresence endpoint called the IX5000 series, which also supports H.265 HEVC. Since then, Cisco has made some changes to its endpoint portfolio. These changes will be explained in more detail in Part II of this book, but essentially, all Cisco Webex endpoints now support H.265 HEVC.

Content Channels

One last aspect of video communication must be explained. One of the great advantages of communicating over video is the ability to share content though the video systems. For content from an external device, other than a camera, to be shared to the far end of the conference, one of two things must happen. Either the video stream from the camera must be replaced with the media device from which content will be shared, or an additional media stream must be added to the overall package to allow for the far end to see both the presenter and the image being shared. The latter option requires yet another protocol to be employed. In SIP communications, the protocol to be employed is called Binary Floor Control Protocol (BFCP). In H.320 and H.323 communications, the additional protocol to be employed is called H.239.

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 35, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 3-4 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 3-4 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
Paragraph	Visible Spectrum of Light Explained	36
Paragraph	Chrominance and Luminance Explained	37
List	Component Video vs. Composite Video	38
List	Light Filters in Cameras	40
Paragraph	Perceived Motion at Certain Frame Rates	41
Paragraph	NTSC and PAL Frame Rates	41
Paragraph	Resolution	42
List	Progressive vs. Interlaced Scanning	43
Table 3-2	Common Encoding Techniques Used in Digital Video Communications	44
Paragraph	How Video Compression Works	46
Section	Video Quality	47
Table 3-3	H.264 AVC Compared to H.265 HEVC	49

Define Key Terms

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

3CCD, Bayer, BFCP, CCD, Chrominance, CIF, Component Video, Composite Video, CMOS, EMR, Foveon X3 Sensors, Frame, Frame Rate, H.239, H.261, H.263, H.264, H.265 HEVC, HDMI, Interlaced Scanning, ITU BT.709, ITU-R BT.601, Luminance, Macroblock, Pixel, Pixel Saturation, Prediction Blocks, Progressive Scanning, RBG, RCA, Resolution, SIF, S-Video, Transform Blocks, VGA, Visible Spectrum, YCbCr, YPrPb, YUV

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Explain the difference between *composite* and *component*.
2. Identify the two main digital cameras available today and the three main light-filtering techniques.
3. Transform blocks are broken down into what two main components?
4. What are the two main content sharing protocols that are used in video communications?

This page intentionally left blank

CHAPTER 4

Collaboration Endpoint Components and Environment

This chapter covers the following topics:

Physical Components: This topic will examine the physical components that make up an endpoint.

Sound Behavior: This topic will discuss the behavior of sound in a room and the tools available to adjust how audio is perceived. The topic will then examine audio input and output devices, speaker and microphone placement, and issues to watch out for when designing a room for audio communication.

Light Behavior: This topic will examine video input and output devices, along with lighting conditions. Focus also will be placed on factors such as camera angle, video etiquette, and special conditions surrounding immersive telepresence.

Now that we've established a fundamental understanding of sound and light, the focus will turn toward the environmental conditions and equipment that affect audio and video quality. The standards and codecs can go only so far in providing good conditions for communications. Many factors within an environment itself can also negatively or positively impact the user experience. Topics discussed in this chapter include the following:

- Physical Components
- Sound Behavior
    - Microphone Types and Transducers
    - Pickup Patterns and Positioning
    - MIC Level and Line Level
    - Speakers: Active versus Passive
    - Audio Cables and Connectors
    - AEC (Acoustic Echo Canceller)
    - Microphone and Speaker Placement
    - Room Design for Noise Reduction
- Light Behavior
    - Camera Field of View, Depth of Field, and Zoom
    - White Balance
    - Lighting Conditions

- Room and Environment Considerations
- Displays: Monitors and Projectors
- Video Cables and Connectors
- Immersive Telepresence
- Video Etiquette

"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
Physical Components	1
Sound Behavior	2–7
Light Behavior	8–12

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 is referred to as a codec?
   - **a.** Microphones and speakers
   - **b.** Cameras and displays
   - **c.** Endpoint
   - **d.** Network
2. Which of the following conditions is most likely to absorb the energy of a sound wave?
   - **a.** Lower frequencies
   - **b.** Higher frequencies
   - **c.** Concrete walls
   - **d.** Gypsum board walls

3. Sound waves reflecting off many complex surfaces and dispersing radiated energy so that it is less direct or coherent is referred to as what?
   a. Reflection
   b. Diffusion
   c. Absorption
   d. Echo
4. What is the difference between a condenser mic and a dynamic mic?
   a. Dynamic mics do not require an external power source
   b. Condenser mics do not require an external power source
   c. Dynamic mics have a tighter pickup area
   d. Condenser mics have a tighter pickup area
5. Which of the following mics has a 360-degree polar pickup pattern?
   a. Cardioid
   b. Supercardioid
   c. Unidirectional
   d. Omnidirectional
6. Professional-grade products use a measurement scale called decibel-unloaded, or dBu. What is the dBu range for line-level inputs?
   a. −10 dBu
   b. −4 dBu
   c. +4 dBu
   d. +10 dBu
7. Which of the following is an unbalanced audio connector?
   a. TS
   b. TRS
   c. XLR
   d. HDMI
8. The distance from the back of the lens to the frame sensor in a camera is referred to as what?
   a. Aperture
   b. Zoom
   c. Focal length
   d. Magnification
9. What tint will an image take on when the color temperature is cooler?
   a. Red
   b. Blue
   c. White
   d. Green

10. What is the maximum color temperature in kelvins recommended for video communication rooms?

- **a.** 3200 k
- **b.** 3900 k
- **c.** 4100 k
- **d.** 5000 k

11. Which of the following is the ideal location of a camera in a video communication room?

- **a.** Centered just above the display
- **b.** Centered just under the display
- **c.** Centered high on a wall above the display
- **d.** Multiple cameras placed around the room for different perspectives

12. Which of the following is an example of a composite video connector?

- **a.** HDMI
- **b.** DVI-D Dual Link
- **c.** DVI-D Single Link
- **d.** Y/C

Foundation Topics

Physical Components

Key Topic

Endpoints encompass many different form factors and span from software-based applications used on a laptop to personal deskphones, meeting room systems, and immersive Telepresence rooms (which are entire rooms equipped for and used solely for video communication). Whereas the term *endpoint* can refer to an audio-only phone or a video communication system, the term *video endpoint* refers specifically to any system that is used to make a video call. Regardless of the size, type, or purpose of an endpoint, all video endpoints share certain basic components, including a monitor, camera, microphone, speakers, codec, power, and some sort of network connection. Each video endpoint can differ in complexity, but all these components must exist for an endpoint to be fully functional. Each of these components can be divided into one of five categories: audio input, audio output, video input, video output, and cables and linkage. Figure 4-1 illustrates the physical components and form factors of endpoints.

The monitor is the video output device used to display video data received during a video call. It can also display data, such as a presentation received during a meeting. In addition, it displays the menus for the endpoint itself. The endpoint menu can be used to place or answer a call; change administrator settings; pan, tilt, or zoom the camera; and share content during a call. Some video endpoints have a monitor built in, but for integrator-type systems that do not come with a monitor, careful consideration should be taken to select an appropriate display.

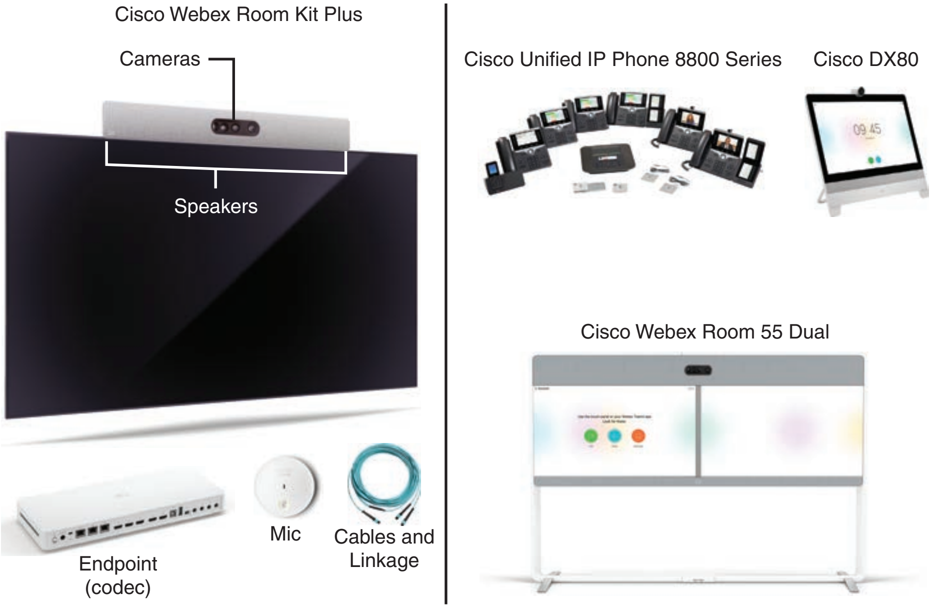


Figure 4-1 *Physical Components of Endpoints in Various Form Factors*

Cameras are video input devices used to capture the video data that the endpoint will be transmitting. The quality of the image sent is limited, in part, to the camera's capability to capture an image. A built-in laptop camera might not produce the same quality image that a 1080p camera is capable of producing. The camera position is also an important consideration. Often the camera can be panned, tilted, or zoomed in or out depending on the preference of the user. Typically for video communication purposes, these will be Pan, Tilt, Zoom (PTZ) cameras or might even incorporate voice tracking and other automated features.

Microphones are audio input devices that capture the audio for the data. A software endpoint running on a computer, smartphone, or tablet will typically utilize the microphone built into the system. This is also true for endpoints that have a microphone built into them, but an integrator system will use external microphones that can be placed strategically around a room. The type and placement of the microphones play important roles in the quality of the sound that is heard by the far-end participants in the call.

Speakers are audio output devices used to broadcast the audio at the far end of the call. Just as with some of the other components mentioned, speakers are included in some endpoints, whereas they may be external to the endpoint system on others, such as with integrator systems. Much to the same effect as microphones, speakers should be strategically placed within a room to enhance the quality of audio heard.

Cables are used to connect the different systems together, supply power to the system, and link the network connections so that transmissions can be sent to a remote destination. All-in-one endpoints have only one or two cables that need to be connected. Some endpoints, such as the Cisco DX80, require a power cable and an Ethernet cable. Other endpoints, such as the Cisco SX10 or Cisco 8865 video phone, require only the Ethernet cable because it can supply both Power over Ethernet (PoE) and the data connection over the same cable. Integrator endpoints will require more cable connections to support all the peripheral devices, such as the microphones, speakers, cameras, and monitors along with power and Ethernet. Older legacy endpoints may even support BRI or PRI ISDN connections natively on the endpoint.

The term *codec* refers to the device used in the encoding and decoding of the audio, video, data, and control streams sent and received during a call. The codec is software within the endpoint that receives incoming audio and video from the microphones and cameras, encodes it, and sends it out across the data network. When already-encoded data comes into an endpoint from a far-end destination, the codec will decode this information before sending it out the speakers and monitor. As mentioned in the preceding chapter, the term *codec* is also used to describe the coding standard used for a signal, such as H.264. An endpoint uses codecs like H.264, so it too is referred to as a codec because it is doing the actual coding and decoding.

Sound Behavior

As discussed at some length in Chapter 1, "Introduction to Collaboration," sound waves will continue to move radially outward from the original source unless obstructed by an obstacle or until the energy runs out. In general, when a sound wave hits an obstacle, part of the wave will be reflected away and part will be absorbed, or transmitted, through the obstacle. To what degree sound waves are reflected or absorbed depends on physics, but basically, it's determined by the density and texture of the obstacle. The proportion in which a sound is reflected, absorbed, or transmitted depends on the shape and density of the material and the frequency of the sound.

When a boundary or obstacle, such as a wall, ceiling, or column, is encountered by a sound wave, some of the sound energy will be absorbed within the material. Absorption is similar to transmitting through an object, except that with absorption, the sound waves will completely dissipate within the object of obstruction. Different materials reflect some frequencies more efficiently than others, due to their roughness or absorbency characteristics. Also, lower frequency waves have an easier time being absorbed into solid surfaces than high frequencies. This is why your neighbors always complain about your bass rather than your treble.

Reflection is caused when an object of obstruction causes sound waves to bounce, or reflect, into another direction. Most hard surfaces will reflect sound waves. The path taken by reflected waves works much like you would expect a billiard ball that has banked off the bumpers of a pool table. The law of reflection is "the angle of incidence equals the angle of reflection." In other words, the angle after the impact will be equal to the angle before the impact. Think of how the balls on a pool table behave as they bounce, or reflect, off the walls of the table. Those bank shots are difficult for an inexperienced player to achieve due to the need to match the angle the ball must travel to the wall with the angle it will reflect, but the principle is the same as with sound waves.

As sound waves are reflected, diffusion occurs too. Diffusion is caused by sound waves reflecting off many complex surfaces and is the process of dispersing radiated energy so that it is less direct or coherent. Coherent reflections, or reflections you can distinguish, are what tend to cause problems in a listening environment. The plastic cover over a fluorescent light acts as a diffuser, making the light spread out in a more randomized way so it is less harsh. A textured wall, such as brick, would be better at diffusing sound than a completely flat surface, such as a concrete wall.

Reflections will happen all over an average room. So why don't all those reflections make it difficult to hear the original source? In some cases, that is exactly what happens. However, sound reflections actually help humans to aurally perceive the size of spaces we are in and are important to our hearing in general. Experiments have been conducted in anechoic chambers to understand human reactions to environments containing no ambient sounds. An anechoic chamber is a room massively insulated with layers of concrete and steel to block out exterior sources of noise. It's also internally lined with crosshatched buffers that absorb all sound; even the floors are typically suspended mesh to stop any sound of footfalls. These chambers are like black holes for sound. Staying inside one longer than 15 minutes has been known to cause extreme symptoms in some people, from claustrophobia and nausea to fear, panic attacks, and aural hallucinations. There is a reason that sensory deprivation is considered an act of torture. The presence of ambient sounds and reflections communicates to the brain the normalcy of an environment. When ambient sound is absent, that signals the brain there is some kind of problem. Therefore, too much reflection can be bad, and not enough reflection can also be bad. The key is finding the right balance of reflection, which is referred to as *sound balancing* a room.

Key Topic

The reception of multiple reflections off walls and ceilings within a few milliseconds of each other causes reverberations, which is the prolonging of a sound. Reflections can actually be categorized into four main groups:

- Direct sound
- Early reflections
- Coherent late reflections, also known as echoes
- Incoherent late reflections, also known as reverberation

Direct sound is pretty obvious; it's the first and primary sound waves that hit your ears. In audio production environments, a direct sound can be referred to as being "dry," and all other sound is referred to as being "wet."

Early reflections are sound waves that bounce off obstructions but arrive at your ears at almost precisely the same time as the direct sound coming from the sound source. These reflections are measured in milliseconds, and human brains do not distinguish these early reflections as "new" or separate sounds. People hear the reflections instantly as part of the richness of the original sound wave. Early reflections must usually arrive at your ear in less than 30–40 milliseconds for your brain to consider them to be indistinguishable from the original sound.

Late reflections fall into two types: the diffuse and incoherent type we think of as reverb, or reverberation, and the more coherent type we generally call echoes. Reflections from surfaces that stand out from normal reverberation levels are the ones we typically identify as echoes. In this case, the arrival of the late reflection sound waves has passed a certain millisecond tolerance, so those waves will be perceived as a second sound rather than the prolonging of the first sound. Reverb is essentially a bunch of echoes, where the reflections are so close and mixed together that the results are perceived as a single prolonged sound. Reverb generally reduces articulation of sounds such as speech, but is desirable when listening to music, as it is perceived to add a warmth or richness.

Reverberated sounds will eventually lose energy and drop below the level of perception. The amount of time a sound takes to die away is called the *reverb time*. A standard measurement of an environment's reverb time is the amount of time required for a sound to fade to 60 dB. A sound that remains audible for a long time before the room absorbs it has a long reverberation time. Reverberation time is controlled by the size and shape of a room; however, the objects in the room also have an influence. Reflective objects such as hardwood floors increase reverberation time because the sound waves have more opportunity to reflect. By contrast, materials such as carpet and drapery are absorbent and decrease reverberation time because they absorb the sound waves and do not give them a good opportunity to bounce. Even air qualities such as humidity can affect reverb time. Most building materials are given a noise reduction coefficient (NRC) rating that informs the degree that a substance absorbs sound energy. Should the need arise in a room where reverberations are noticeable, acoustic paneling can be used to remediate the issue. Cisco recommends NRC ratings greater than 0.75 for acoustic paneling.

Another issue to keep in mind when designing a room is background ambient noise. This could include air flow through the HVAC system, the buzz of lights, noise coming through the walls from a neighboring room, or hallway traffic outside the room. Sounds coming from outside could also cause ambient noise issues, such as street traffic, planes, or subways and trains. Best practice is to control the environment such that any ambient noise is less than 45 dB.

The sound behavior described up to this point could occur whether technology is being used or not. An engineer designing a room for technological applications, such as a conference room, should be even more mindful of sound behavior because microphones can be more sensitive to sound in a room than the human ear. A person sitting in a room may not notice the air blowing out a vent, but if ceiling-mounted microphones were used in that room, the microphones could pick up that noise and magnify it before sending it to the destination. This could cause a real distraction to the participants at the other end of the call. There is only so much that can be altered within a room to balance the sound. Therefore, some technology applications assist in controlling sound picked up by a microphone.

Gain refers to the capability of a system to increase the power or amplitude of a signal between the input and the output of a given circuit. Gain can come in the form of amplification or attenuation for either a digital or analog process. No change in the signal as it passes through the microphone is called *unity gain*, or just unity. Headroom can be thought of as a safety zone for unintended peaks of a signal. It becomes particularly important when a signal may go through several opportunities for gain adjustment within a given system. Microphones, mixers, and amplifiers should be adjusted to always allow adequate headroom to avoid clipping.

Clipping is a form of distortion that occurs when a signal exceeds the maximum dynamic range of an audio channel. When you view a clipped sound wave, it will look as though someone chopped off all the peaks. In the analog world, musicians sometimes desire clipping because the distortion isn't a clean slice like in the digital realm. Digital clipping sounds very harsh and is usually avoided at all costs. The clipping referred to here is also known as *hard clipping*. Soft clipping is less harsh and is commonly called *overdrive*. You may have seen an overdrive knob on a guitar, for example. Soft clipping is not common in the audio and video communication world. Automatic gain control (AGC) makes dynamic adjustments to gain, typically on a microphone signal, to maintain an optimal level for different speakers.

A great example is conference phones because you can hear the volume level change as each new person begins speaking, especially if the speakers are different distances from the microphone pickup area. The term *good levels* refers to an audio signal that is significantly higher than the noise floor, but not so strong as to cause clipping, and may also indicate leaving appropriate headroom. Figure 4-2 illustrates how clipping can appear and how the gain controls should be set in an ideal environment.

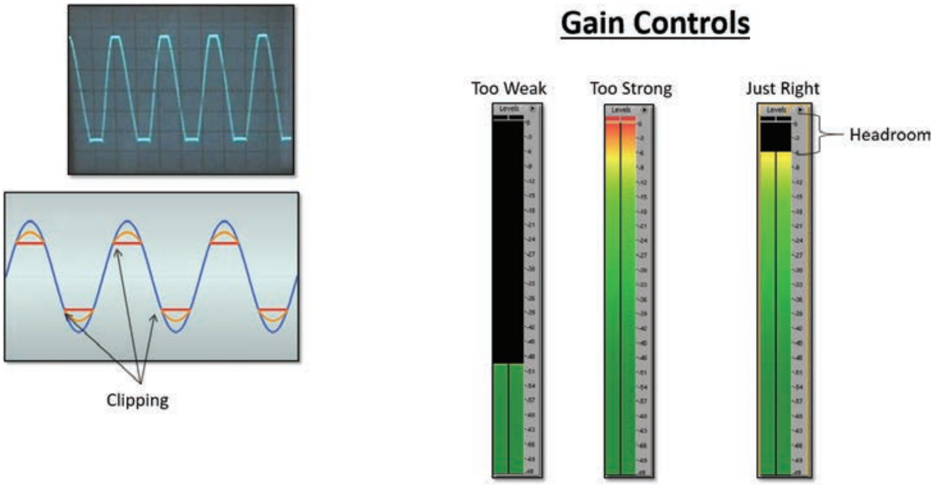


Figure 4-2 *Gain Controls and Clipping*

Microphone Types and Transducers

Because a microphone converts acoustic energy into an electrical signal, it is another form of a transducer. There are many different types of microphones with many different applications, a few of which will be mentioned in the content that follows. Some of the specifications most commonly found with microphones include the following:

- **Dynamic Range:** The range of amplitudes that can be accurately captured by the microphone. This range is usually represented in dB at a certain frequency, typically 1 kHz.
- **Frequency Response:** The range of frequencies accurately captured.
- **Polar Pattern:** The directionality pattern of highest sensitivity for the microphone element.

For best results, microphones should always be used for the applications for which they are designed. Many mics work well only in certain environments and deliver very poor results when used outside these areas. Most mics have transducer elements that fall into one of two categories: dynamic and condenser.

Key Topic

Dynamic microphones are also known as passive microphones because they do not require an external power source to operate. Instead, as sound waves strike the diaphragm, its vibrations move a magnet surrounded by a stationary coil, resulting in an electrical signal being transferred through the cable and ultimately to the pre-amp. Rather than employing a moving coil using an electromagnetic principle, condenser mics operate on electrostatic principles in which two conductive plates in close proximity to each other exchange a charge as the plates vibrate. This operation requires that an external power source be used to supply the charging voltage to the element, usually in the form of phantom power. A variation on the condenser mic is the *electret* mic, which utilizes a small battery to charge the diaphragm. Because condenser mics require a power source, most modern mixers have the option to turn on phantom power, which supplies a voltage, usually +48v, to any mic that requires it. It is called *phantom power* because it doesn't show up on dynamic mics, thereby protecting the element from possibly damaging voltage. It is advisable to check the requirements for your mics of choice to ensure that your mixer or digital signal processor (DSP) can effectively supply the required voltage. If not, external phantom power supplies also are available. Figure 4-3 illustrates the physical differences between condenser microphones and dynamic microphones.

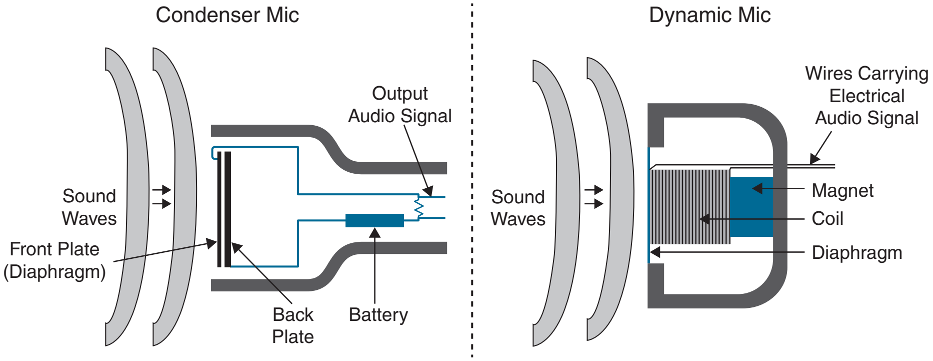


Figure 4-3 *Condenser Mic and Dynamic Mic Physical Differences*

Many different types of microphones are available on the market today. Some of the more common types of microphones are the types you would typically see in a conference room setting:

- **Handheld mics** are the most common style microphones. These are typically dynamic mics and as a result have lower sensitivity. They can be both wireless and wired.
- **Lapel mics**, also known as tie-clip or lavalier mics, are almost always condenser mics and generally are more sensitive and have a tighter polar pattern than handheld mics because they are intended to be used further from the speaker's mouth.
- **Desktop** or **podium mics** are usually condenser style and work well at greater distances from the speaker. They can be considered more forgiving for the inexperienced user, but as a result can require more processing to avoid feedback situations.
- **Ceiling-mounted mics**, also known as choir mics, are best utilized in multiuse rooms with moveable furniture or in cases where tabletop mics interfere with meeting operations. Significant design considerations need to be taken into account with these condenser-style mics due to their extreme sensitivity.
- **Boundary (or PZM) mics** are designed with a low-profile form factor for tabletop use. With these, as with other highly sensitive condenser mics, processing may be required if multiple units are in use.

Pickup Patterns and Positioning

The polar pickup patterns of all microphones can be broken down into two major types:

- **Directional, also called Unidirectional:** Directional mics are intended for pointing at a more selective group of audio sources. They typically have a greater sensitivity, and resistance to feedback is achieved with this class of mics.
- **Omnidirectional:** Omnidirectional mics are intended to be at the center of a group of audio sources, such as in the center of a conference room table, with a 360-degree pickup area. An omnidirectional mic can pick up sound equally in all directions. As a result, these mics tend to have lower sensitivity and are also more prone to feedback due to the nature of sound reverberation and other acoustical factors.

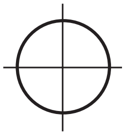
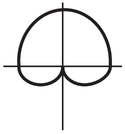
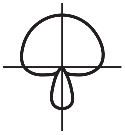
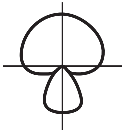
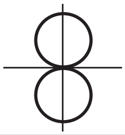
Pickup patterns of directional mics can be broken down further into several categories. The *cardioid* pickup pattern is shaped like a heart. The mic's effective pickup area primarily focuses on the area in front and to the sides of the microphone. Vocal mics are typically one of the cardioid styles. The *supercardioid* polar pickup pattern has a narrower range of focus, but as a result of this narrowing, a small lobe develops behind the mic and may require consideration. *Hypercardioid* has an even narrower focal range, and a larger lobe at the rear of the mic develops.

Bidirectional mics pick up equally in two directions, usually at 180 degrees opposed. Shotgun mics have a very narrow pickup range but can also pick up sound from the greatest distances. The distance factor is the ability of a microphone to pick up sound from a distance as related to an omnidirectional mic. Critical distance is the distance between the person who is speaking and the microphone as it relates to other active mics. A good rule of thumb is a 1:3 ratio. So, if the person speaking is 3 feet from the target mic, the next closest mic should be no closer than 9 feet.

Table 4-2 identifies the pickup patterns of different microphones with other relevant information.

Key Topic

Table 4-2 Microphone Pickup Patterns

Polar Pattern Name	Omnidirectional	Cardioid	Supercardioid	Hypercardioid	Bidirectional
Polar Pattern					
Angle of Coverage	360	130	112	103	90
Null Angle (Angle of Maximum Rejection)	N/A	180	120	108	90
Rear Rejection	0	23 dB	14 dB	7 dB	0

Polar Pattern Name	Omnidirectional	Cardioid	Supercardioid	Hypercardioid	Bidirectional
Ambient Sensitivity	100%	32%	26%	24%	32%
Distance Factor (in Meters)	1	1.8	1.9	2.1	1.6

Mic Level and Line Level

There are some considerations to heed when configuring and setting up systems with a variety of sources. Among the primary concerns during configuration are the various levels of audio signals in play and how those signals need to be handled. Dynamic mics have a lower voltage output that require amplification to boost their signal. This amplification can be performed with a preamp, mixer, or other amplifier device that possesses a gain control. Condenser mics have a higher output and might not need any amplification, or else much less. Most of the time these different mics offer a plug-and-play experience because line-level plugs are different from mic-level plugs. However, in some circumstances an engineer may need to manually configure a solution that requires mic or line levels. Certain Cisco endpoints, for example, allow the mic inputs to be configured as mic or line level. When the microphones plug directly into the endpoint itself, mic level can be used, which is the default setting. When more microphones are being used than the endpoint can support, such as a series of ceiling-mounted microphones in a conference room, an amplifier external to the endpoint may be required. The amplifier can be plugged into the same input on the endpoint where a microphone would have been plugged, but the setting for that input must be changed to line level to support the amplifier being connected.

Line level is usually the output of any device with an internal pre-amplifier, including MP3 players, mixers, TVs, and CD players. Mixer outputs are usually line level by default, but many are configurable to output mic level when needed. Line level can be expressed in a few ways, each with its own context. The decibel-volt, or dBv, is usually used with consumer audio equipment, and line level for that range of products is approximately −10 dBv. Professional-grade products use a different measurement scale called the decibel-unloaded, or dBu. Line levels for these products range around +4 dBu. In absolute terms, the actual peak-to peak voltage of a −10 dBV signal is about .447 volts, whereas a signal at +4 dBu equals a p-p voltage of around 1.7 volts. As you can see, there is quite a range here, depending on the equipment you choose, and allowances are needed to prevent overdriving the amplifier. Speakers also require amplifiers to project sound.

Speakers: Active versus Passive

Just as there are two types of microphones, there are also two types of speakers:

- **Active speakers** have amplifiers built into the speaker body. Active speakers need to have both a power supply and line-level audio wires connected to them. Computers, televisions, and endpoints use active speakers. Advantages of using active speakers include a self-contained form-factor, portability, and the number of speakers supported is not limited by external amplification limits. Field cables are only line level, thereby resolving cable isolation issues caused by unshielded speakers.

- **Passive speakers** do not have built-in amplification. They require an external amplifier to supply the appropriate signal; however, only unshielded audio cables need to be run to the speakers themselves because wall power is run only to the amplifier. Advantages of passive speakers include lighter weight for portability and, typically, better fidelity, which allows the "steering" of the signal with customized crossovers and bi-amplification. Concert halls typically use passive speakers. In video conferencing, ceiling-mounted speakers are usually passive speakers.

Audio Cables and Connectors

An audio system has different signal types depending on both the source and destination of the signal and the way the signal is referenced to ground. For these signals to get from one device to another with minimal noise interference, the industry has created various connectors with which to make solid and trouble-free connections at each end of the cable. These connectors can be broken down into two primary classes: unbalanced and balanced. Figure 4-4 illustrates the differences between unbalanced and balanced audio cables.

Key Topic

Unbalanced cables have two wires: one carries the positive (+) side of the signal, and the other wire shares both the negative () side of the signal and the grounding shield. These cables are more typically found on consumer-level items. Inside the cable itself, the signal wire is typically in the center of the cable with the ground wire surrounding it. The ground wire serves two functions. It carries part of the audio signal and serves to shield the main signal wire to some degree from outside interference from noise. It does help reject some noise, but the wire itself also acts like an antenna and picks up noise. Unbalanced cables work fine in short runs, but they should have a maximum length of 15–20 feet, or 4–6 meters. RCA connectors are always used on unbalanced cables. Tip-sleeve (TS) connectors are unbalanced but resemble tip-ring-sleeve (TRS) connectors, which are balanced. An easy way to tell them apart is to look at how many rings are on the end of the connector. If it has one or two rings, the cable is unbalanced. If it has three rings, the cable is balanced.

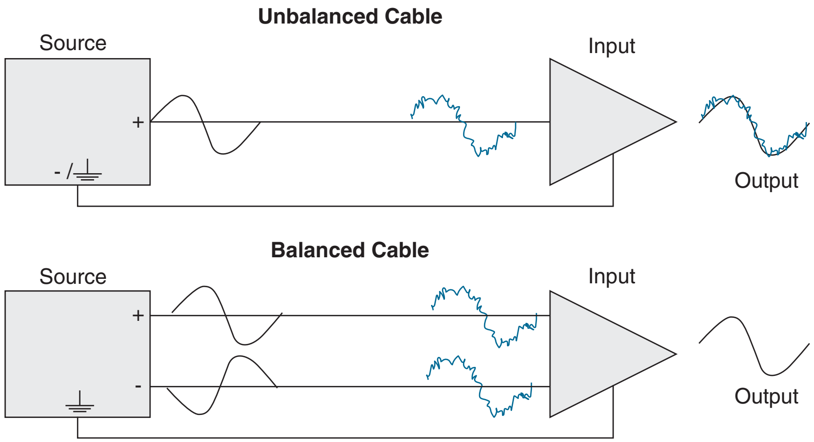


Figure 4-4 *Unbalanced and Balanced Cables*

Balanced cables are characterized by three wires in the cable, two of which carry the identical signal 180 degrees out of phase with each other. The third is the ground that encompasses the other two wires to protect them from outside noise. This allows for better isolation of the signal from EMI noise. The positive conductor carries the original audio signal, and the negative conductor carries the inverse of the original audio signal. If you sum two signals that are identical but are reversed in polarity, the signals cancel out, leaving you with silence. When a positive is added to its negative counterpart, the outcome will always be zero, such as +20 added to –20 equals 0. Normally, you would not want audio gear that flips the polarity of your signal, but in this case you do. Both copies of the signal, positive and negative, pick up the same noise as they travel along the cable, and that noise is identical on the two wires in the cable. The component receiving the audio signal will flip the inverted signal back into its original orientation and invert the noise riding on the negative wire. Flipping the polarity of what arrives at the receiving gear will produce the original signal intact, and the noise, which now has reversed polarity, will be removed. What you end up with is a welcome result: a signal that's preserved and noise that's canceled. Because of this function within balanced cables, they can support much longer cable runs at 50–100 feet, or 15–30 meters. Standard connectors designed for use with balanced signals are XLR and TRS. Figure 4-5 identifies the most common balanced and unbalanced connectors available on the market today.

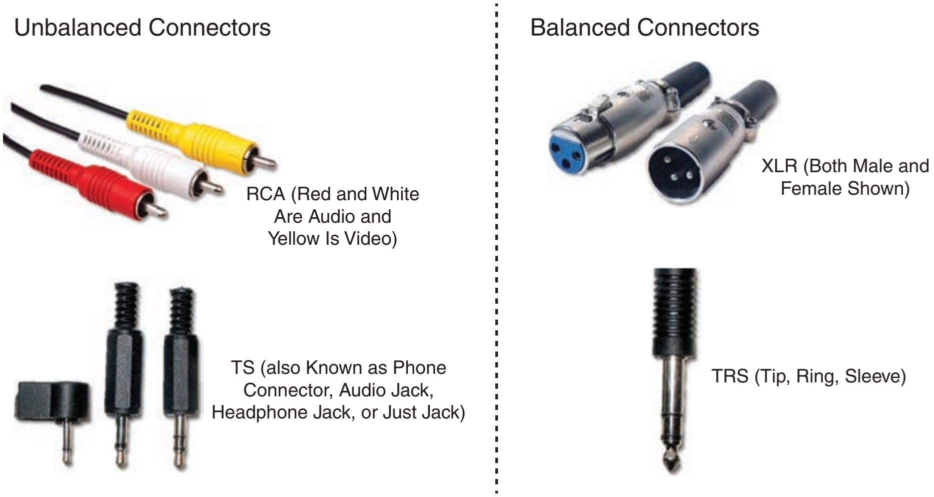

Unbalanced Connectors
Balanced Connectors
RCA (Red and White Are Audio and Yellow Is Video)
XLR (Both Male and Female Shown)
TS (also Known as Phone Connector, Audio Jack, Headphone Jack, or Just Jack)
TRS (Tip, Ring, Sleeve)

Figure 4-5 *Balanced and Unbalanced Connectors*

Acoustic Echo Canceller (AEC)

Imagine two conference rooms, each with ceiling-mounted microphones and ceiling-mounted speakers. As a person in one of those rooms speaks, the microphone picks up the audio. That sound is carried from the mic to the endpoint, across the network, to the endpoint on the far end where the audio is ultimately delivered to the amplifier, which sends it out the speakers. The speed that this audio is able to travel, whatever that distance might be, is almost instantaneous. However, a delay does in fact occur, and that delayed audio is detected by the far-end microphones. The audio picked up from the speakers on the far-end microphone would be sent back to the original location, causing an echo at the near end. You may have experienced something like this before, and it can be very distracting, sometimes to the point that it is intolerable. It doesn't matter whether the microphones and speakers are ceiling mounted or not; this unnatural echo will occur no matter what. All analog mics produce echo because echo is leakage of the analog signal in the RX path to the TX wire. The echo becomes noticeable to the listener as the leakage increases.

Key Topic

This is where Acoustic Echo Canceller (AEC) comes into play. AEC works by comparing the audio input from the near-end mic against the audio input from the far-end mic and subtracting the common delayed audio. This is the significance of that delay. Participants can be speaking at the same time from both locations, and AEC is able to filter out the delayed audio and reduced echo. This process happens on both ends of the audio communication by the endpoint reducing the local loudspeaker contribution to the local microphone. It is important to understand that AEC reduces echo, but it does not completely eliminate the echo. Figure 4-6 illustrates how AEC works to prevent echo from occurring.

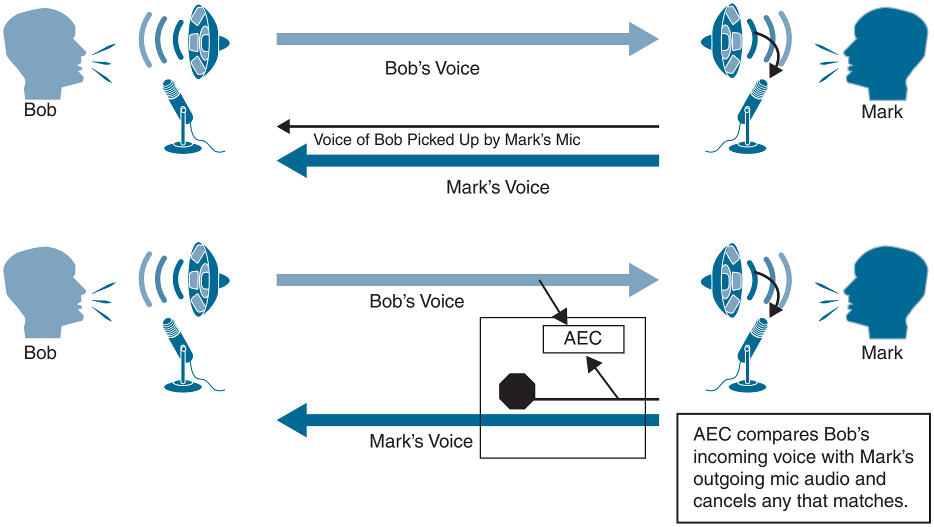

Bob
Bob's Voice
Mark
Voice of Bob Picked Up by Mark's Mic
Mark's Voice
Bob
Bob's Voice
AEC
Mark
Mark's Voice
AEC compares Bob's incoming voice with Mark's outgoing mic audio and cancels any that matches.

Figure 4-6 *Acoustic Echo Cancellation (AEC)*

AEC samples the signal being sent through the loudspeaker and establishes this as the reference signal. From this signal, the AEC compares the signals with the use of a predictive filter and learns to determine the difference between the near-end and far-end signals. This process is referred to as *training* or *convergence*. It usually takes a few sampling cycles for the algorithm to get sufficient sampling for effective filtering, and there are notable limitations that should be accounted for. AEC cannot correct direct acoustical anomalies in the room. It has a limited capability to correct the effect of room acoustics to the far end. Presenters need to be 1–2 feet from the target mic for AEC to operate effectively. Finally, in situations of high network latency, sometimes as low as 200 ms, AEC can become ineffective. Many different devices use AEC, and if two devices in the same room are trying to cancel out echo, they will cancel each other out; thus, echo will be heard. In the first example provided, if ceiling-mounted microphones are being used, an amplifier or mixer external to the endpoint may have AEC enabled. The endpoint also has AEC enabled. Therefore, an engineer must disable AEC on one of the devices for it to work properly.

Microphone and Speaker Placement

The placement of microphones and speakers is critical in determining the quality of an audio call. The location of the microphone should be directly related to the type used and as close to equal distance from all participants as possible. As discussed previously, different microphones pick up audio in different patterns, so special emphasis should be placed on how each microphone should be positioned based on the polar pattern. Equal to the importance of microphone placement, speaker placement is also essential.

A microphone's polar pattern is the pattern in which a microphone picks up sounds. An omnidirectional microphone's polar pattern is nearly spherical. Omnidirectional microphones can be found on desktops or hanging from ceilings. This type of microphone should be placed in the middle, or directly above the middle, of the participants so that no participants are outside the sphere of where the microphone can pick up sound. A directional microphone, of which the cardioid microphone is the most common, is typically used as a desktop microphone. It has a polar pattern that could be described as kidney shaped, with a dead zone behind the microphone. Therefore, a cardioid microphone should be placed at the end of a table, with the dead zone directed away from where participants are positioned. When both directional and omnidirectional microphones are positioned in environments where multiple microphones are being used, the polar patterns should overlap. Figure 4-7 illustrates the positioning of these two types of microphones in meeting rooms.

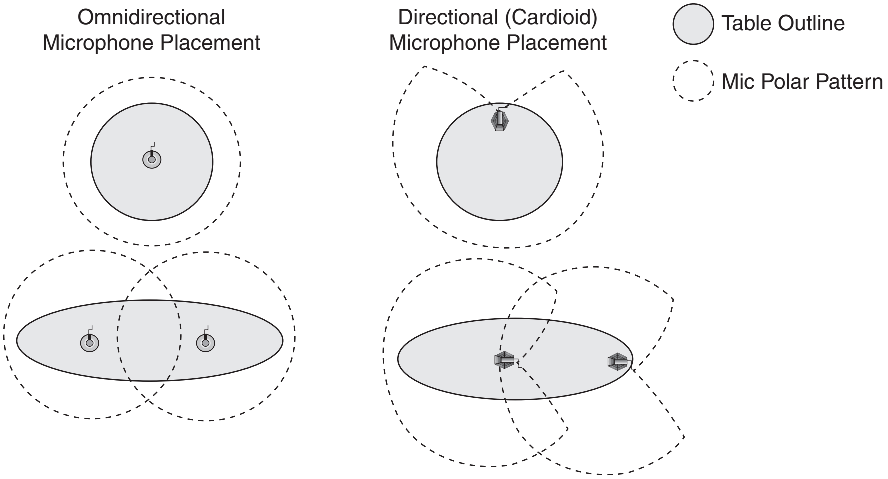


Figure 4-7 *Microphone Placement in Meeting Rooms*

Where speakers are placed within a meeting room could also impact the quality of audio. Many audio-only and video endpoints have the speakers built into the system. Video endpoints may use a third-party display with built-in speakers for the endpoint. In these cases, the placement of the speakers is less of a concern. Audio-only speakerphones are generally placed in the center of a table, and that is ideal. Video endpoints that use speakers built into the endpoint itself or the speakers built into a display should be positioned at the front of a room, which is the superlative location for video calling. The speakers are behind and out of range of the microphones, which will prevent feedback. Also, in a video call, the sound comes from the direction in which the far-end participants are seen. This will provide a more natural flow of sound. If someone were sitting in front of you speaking, you wouldn't expect to hear the person's words coming from behind or above you. If external speakers were set up around the room, the audience would be looking at the person speaking in front of them but hear the speakers from perhaps their right or left side, or behind them. This could be disruptive. Likewise, you would never want to set up surround sound for a meeting room because of the same unnatural result. The one exception to this would be in a large theater-style setting. Due to the room's size, additional speakers should be put on the sides but still face out from the person speaking. This position helps to keep the listeners' orientation facing forward while achieving the volume level needed for the entire group to hear the person speaking clearly. In some custom meeting room integrations, the room will be designed with ceiling-mounted speakers above each participant chair in the room. Although this is not the ideal positioning of speakers within a room, for larger meeting room settings, this setup does distribute the audio more evenly throughout the room.

Cisco has a website at https://projectworkplace.cisco.com that provides many room design ideas. There, you can find pictures to help you visualize what a room will look like, and you can click through various customization options to change the room based on endpoint selection, participant capacity, and general purpose of the room. You can even open a schematic of the room to scale that will illustrate a two-dimensional drawing of the room's layout with measurements and total room layout, and you can then send these plans to an architect for official blueprint design. Figure 4-8 illustrates one of the schematic drawings available on Cisco's project workplace website.

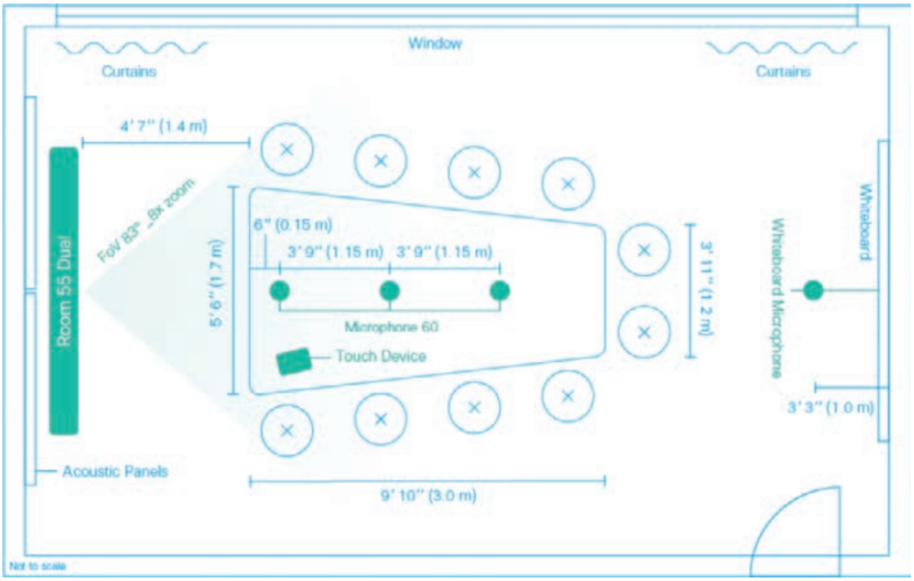


Figure 4-8 *Project Workplace Meeting Room Design*

Room Design for Noise Reduction

You learned about sound behavior at the beginning of the chapter. You should now understand that sound behavior can help identify external noises that can ruin a call, and it can help identify appropriate measures to take so that ideal conditions are met for premium audio quality within a meeting room. I placed a great deal of emphasis on the technical components that help improve sound quality. Such components include using appropriate microphones, speakers, and cables. You also learned about using balanced audio cables instead of unbalanced, and proper placement of microphones and speakers within a room. Beyond these technical measures, you can take many other steps to improve audio quality if you understand the behavior of sound.

It is important to take steps to eliminate as much external noise as possible. First, the location of the meeting room is very important. Location may not always be within your control, but when designing a new room or preparing for a buildout of an office space, you should look for some key aspects in the meeting room location. When you have the option, select a location that is as quiet as possible. Usually, this will be an interior room, with no windows, and away from a main walkway. The less foot traffic that exists outside the room, the less chance of unwanted noise from the office interfering with a call. Locating the room on the interior of the building will keep it away from windows where noise from outside the building can interfere, such as from a siren, car horn, or airplane. Special consideration should be given to the size of the room as well. The larger and more open the room, the more likely that sounds will tend to echo and become distracting. If this room is being custom built, other considerations can be included, such as insulating the walls and providing a solid door without sidelights, which are windows in the sides of the door.

Most often, customizing these aspects of a room is not possible; however, several other modifications can be made to a meeting room to improve the sound quality:

- If there are windows in the room, hanging curtains will help reduce outside noise.
- Replacing ceiling tiles with tiles rated higher for noise reduction will provide a noticeable change, along with acoustical panels that can be hung on the walls.
- Use padded placemats on conference tables to help remove some of the echo in a room.
- The floors should always be carpeted, but if they're not, placing area rugs will also help with echo and reverberation.
- Believe it or not, placing a plant or two in a meeting room not only will liven up the place but also will help with the sound quality. Plus, plants love when you talk to them, so they should be happy in a room built for talking.

Key Topic

Knowledge is power is time is money. Or, if you have watched the TV sitcom *Parks and Recreation*, then "time is money, money is power, power is pizza, and pizza is knowledge." Either way, you cannot dispute the importance of knowledge. When it comes to soundproofing a room, educating the office staff is an essential step. Congregating outside the meeting room should be discouraged. The door should be closed when the room is in use to help quiet external sounds. Notifying others that a meeting is in progress will help keep people mindful of what is happening around them. If the meeting room is in a location where external sounds cannot be eliminated, educating staff to mute the microphone unless speaking will help prevent distractions. Not all calls are from a quiet meeting room with a door. If staff members are using a software endpoint or a phone that supports headphones, the use of headphones and a small microphone can help reduce the external sounds.

Light Behavior

Up to this point, this chapter has covered sound behavior, what audio equipment should be used to improve audio quality, and room remediations that can improve audio quality. In like manner, I will turn the focus of this chapter over to light behavior. The next several sections will examine cameras, display cables, room remediation, and video communication etiquette.

Camera Field of View, Depth of Field, and Zoom

Chapter 3, "Video Basics," delved into the inner workings of how a camera operates. Now we will redirect our attention to the actual image detected and transmitted by the camera, more specifically the lens of the camera. Three primary parameters to be familiar with are field of view, depth of field, and zoom.

The *field of view* is exactly what it sounds like, which is the width and height of the image. Although it can also affect the amount of detail that is visible in the observed image, the field of view is what can be seen through the camera's lens. Some estimates suggest the human eye has a horizontal field of view of about 210 degrees and a vertical field of view of about 150 degrees. Other more conservative estimates put the horizontal and vertical fields of view at 120 degrees. These estimates do not take into account the movement of the eye, which does not change the field of view, but it does quickly change the perspective. The field of view on a camera can be adjusted with zoom or with a different lens if the camera has a fixed focal-length lens. *Focal length* refers to the capability of a lens to magnify the image of a distant subject. The focal length, or size of a camera lens, is the distance from the back of the lens to the frame sensor. Smaller-lens cameras are sometimes referred to as wide-angle because they produce a greater field of view than cameras with a larger lens, despite there being specific lenses for such wide-angle applications. Cameras with larger lenses are conversely referred to as *narrow-angle* as they have a smaller field of view. Calculating field of view is a topic that can go much deeper than is discussed here.

Depth of field refers to the objects, from nearest to farthest, that are in sharp focus. You may have noticed while watching a television show that the camera is focused on someone close up, but a person standing in the background is blurry. This effect is caused by a shallow depth of field. Then the camera will adjust the focus on the person in the background, and everything in the foreground will become blurry. This effect is caused by a deep depth of field. The following three main factors control the depth of field:

- **Aperture:** This factor refers to the amount of light allowed through the lens to the camera sensors. The size of your aperture, which is the diameter of the hole through which light enters the camera, controls the amount of light entering your lens. Using the aperture of your lens is the simplest way to control your depth of field. A larger aperture, or more light, will produce a shallower depth of field. A smaller aperture, or less light, will produce a deeper depth of field.

- **Distance from the object to the camera:** Distance from the object to the camera can also affect the depth of field. The closer an object is to the camera, the shallower the depth of field becomes. Therefore, moving farther away from the object will deepen the depth of field.

- **Focal length of the lens on your camera:** Focal length was discussed previously regarding field of view. This topic can be very complex, but the simple answer is that the longer you set your focal length, the shallower the depth of field.

The third parameter that affects a camera image is *zoom*. The adjustability of a lens that allows the illusion of bringing objects closer or increasing magnification is referred to as zoom. This is very similar to focal-length lenses, except that focal-length lenses are typically fixed, whereas a camera with zoom capability can be adjusted based on the environmental conditions. When you are looking at specifications for a digital camera, both the optical and digital zoom measurements are listed as a number and an *X*, such as 3X or 10X. A larger number signifies a stronger magnification capability. Cameras are also identified by their focal length, which could be a single number, such as 35 mm, or a range, such as 28 mm to 280 mm. In most cases, a 50 mm lens measurement is considered normal with no magnification and no wide-angle capability. Putting these two measurements together, the multiplier is the difference between the smallest and largest focal-length measurements of the lens. For example, if a 10X optical zoom lens on a digital camera has a minimum focal length of 35 mm, the camera would have a 350 mm maximum focal length. However, if the digital camera offers some additional wide-angle capabilities and has a minimum 28 mm equivalency, then the 10X optical zoom would have a maximum focal length of only 280 mm. Obviously, this can impact both the depth of field and the field of view. Figure 4-9 illustrates the differences between a 50 mm zoom lens and a 200 mm zoom lens.

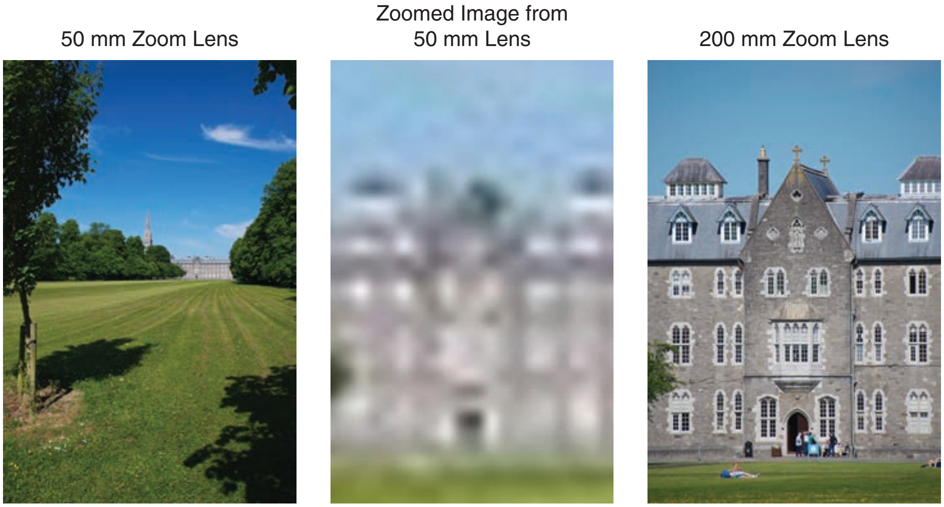


Figure 4-9 *50 mm Zoom Lens versus 200 mm Zoom Lens*

White Balance

Key Topic

Although the mind cannot always perceive it, objects in different kinds of light are affected with regard to the color temperature in which they are seen. If the light source is cooler, the subject being viewed will appear to have a bluish tint. This effect is common with fluorescent lighting. If the light source is warmer, the subject being viewed will appear to have a reddish tint. This effect is more common with natural lighting, such as the sun. Incandescent lighting can give off a yellowish tent. This effect is not often observed by the human eye because the brain corrects this anomaly; however, without some kind of filter, cameras will pick up the aberration and transmit it to the destination.

White balance is a setting used in cameras to set the reference value for white so that color anomalies caused by color temperature can be corrected. These settings can be either manual or automatic, depending on vendor and model. The manual setting is usually more accurate. One way to set white balance manually is to place a totally white card in front of the camera. When the white balance button is pressed, the camera identifies the color observed as white, so when cool fluorescent lights make an image appear blue, the camera can adjust the image accordingly.

Automatic white balance sets the camera to a known reference value, regardless of room lighting. The caveat is that if the room lighting is different from the camera's reference, the color correction could be inaccurate. In some cases, rooms have mixed-lighting environments with both daylight sources and fluorescent sources in different parts of the room. If a camera pans to different parts of the room, the color values can change dramatically. This is why, in part, it is recommended to locate meeting rooms that use video communication systems in the interior of a building so that there are no windows. If you cannot avoid windows in the meeting room, you can use shades or curtains to block out the natural light from coming into the room during the meeting. Another point of consideration is to use fluorescent lighting with bulbs that produce a temperature of 4000–4100 K.

Lighting Conditions

Lighting enhances the perception of the environment around you, and it can be used to set a mood to an environment. A soft candlelit room is soothing and relaxing as light dances on the walls from the flicker of the candle's flame. Warm reddish lights used in theater environments give audiences the sensation of being at home. Office environments use brighter but cooler lights to accentuate an atmosphere of business. Equal consideration should be pondered when designing a meeting room for video communication. Lighting in meeting room settings is rarely ideal, but the same three-point lighting technique still applies. Three-point lighting consists of key light, fill light, and back light.

Key Topic

Key light in a conference room can be the overhead fluorescent lights, but some track lighting systems allow positioning the lights to better suit the needs of the room. For most office environments, the ideal lighting should be indirect fluorescent lighting. Some vendors recommend a range of 3200 K to 4100 K for the color temperature of the light. Direct light can be harsh, especially while in a video call. On a sunny day, people wear sunglasses to diffuse the light before it enters their eyes. When fluorescent overhead lighting is used for key lighting, you can use diffused lighting systems in meeting rooms where video communication will occur. Some lighting systems already use reflection as a method of making light less direct. The ability to dim the lights with a dimmer switch is another great way to diffuse the light in a meeting room. Also, you should avoid direct down lights when possible. If track lighting is being used, angle the lights away toward the floor or a wall behind the participants.

Fill light, also referred to as soft light, is a very cool light that is directed toward the participants in the meeting. Some video communication systems come equipped with soft facial lighting. The light from the monitor can act as a fill light, as well as reflected light from the meeting room table. For this reason, it is recommended that the wood or surface of the table be a brighter color to allow the light in the room to be reflected back up toward the participants. Darker colors will absorb the light and not provide the fill lighting needed for video calls. However, you should be mindful of surface reflections. Remember that just like sound waves, light waves will be reflective off a hard surface at an angle equal to the incoming angle. Knowing this should make it relatively simple to predict where reflections could be an issue.

Although *back light* is not the most essential lighting needed, it is ideal in rooms that use video endpoints for live video calls. Back light is used to give the participants soft highlights and definition from behind where they're positioned. In this way, the participants are separated from the background, and the lighting gives them a more natural 3D presence during the call. The ultimate goal is to allow the technology surrounding participants to melt away so that they feel as if they are in the same room as the people on the other end of the call. Back lighting takes the experience of a video call one step closer to this goal.

The optimal lighting is a combination of key, soft, and back lighting. Any one type of light on its own is problematic, but when they're combined, the end result is excellent. Key lighting helps illuminate the face, while a soft light helps cut down the contrast, and back lighting can help make the person in the video feel more real and less two-dimensional. Shoulder lighting should not exceed two times the facial lighting, and the lighting should not fluctuate more than 100 lux within the camera's field of view. Figure 4-10 illustrates each of these lighting techniques working independently and together.

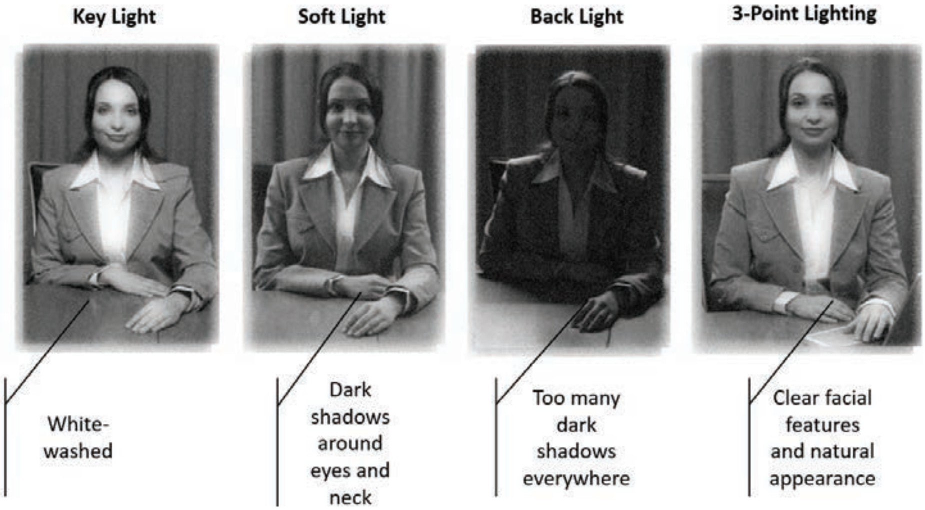

Key Light
Soft Light
Back Light
3-Point Lighting
White-washed
Dark shadows around eyes and neck
Too many dark shadows everywhere
Clear facial features and natural appearance

Figure 4-10 *Three-Point Lighting Technique*

Control of light in general is important. Be careful not to oversaturate the subjects you are lighting. Too much light can wash out your subjects on camera, as shown in Figure 4-10 with key light only. Natural light coming through a window is bad for video communication. Rooms with lots of windows are often equipped with shades or blackout curtains to control the amount of exterior light penetrating the room. You also should avoid pointing the camera toward windows with blinds or other hanging treatments that may allow light seepage. Ensure that participants do not sit with their backs toward an uncovered window. The brightness of the background will make the participants seem darkened, and facial features will be harder to make out. The same effect as the back-light-only view in Figure 4-10 will occur.

Blinds are not ever recommended in rooms where video communication will take place. Shadows cast by the window frame or blinds can cause a problem as well, throwing off the white balance of the video. Over a video call, those shadows are enhanced, and you could appear to have stripes caused by the shadows. If the meeting room has windows, it is a best practice to cover them with a heavy drape that blocks out the light completely.

Room and Environment Considerations

Beyond lighting, several other considerations should be taken into account when designing a room for video communication. Careful reflection should center around tables and other furniture, as well as camera positioning, such as keeping access points out of the camera's field of view, and properly positioning the camera angle to the participants within the room. Other aspects include backgrounds, wall color, and even carpeting.

Table surfaces should be considered carefully. Light-colored tops are favorable, such as natural maple or walnut wood tops, without stain, and varnished to a nice sheen. You should avoid choosing bold colors and wood grains that present bold patterns. These patterns could have a negative effect with the cameras and cost a lot in bandwidth. An oval-shaped, or racetrack-style, table is usually suggested for rooms with up to six people. Larger rooms can benefit from trapezoidal tables. These table styles reduce the effect of forced perspective and allow everybody in the room to be visible from the camera. Chairs should be low backed to avoid blocking the view of people in the back when the room layout is designed with rows of participants. Other furniture located in the meeting room designed to hold audiovisual equipment should have adequate ventilation. Most electronic equipment produces a lot of heat. Routing cables for table power access, microphones, control pads, and display connectors should be carefully routed to avoid tripping hazards when possible.

There are many aspects to consider when setting up cameras in a meeting room. Cameras can be wall mounted or set on a credenza. There are also mounting brackets designed to hold cameras on top of the display. The following conditions will help determine where to best position cameras in the meeting room. Cameras should be positioned so that they are opposite the entrance doorways, but these entryways should be just outside the cameras' field of view. As mentioned previously, motion should be limited when possible, because excess motion will cost more bandwidth as the video system is forced to refresh more data within each frame. Doors opening or people moving behind a sidelight may cause these unwanted distractions, not to mention the fact that passersby poking their heads in a room while a meeting is in progress can be distracting to participants on both ends of the call. How participants are positioned around a table is important as well. You should avoid room layouts that would place anyone with their backs to the camera. If this position cannot be avoided, consider using dual cameras in a room, with one positioned at each end of the room.

Key Topic

During an endpoint installation, the position of the camera is a critical component. This is especially true on custom installation jobs that use integrator video endpoint kits. The idea is to position the camera and display in association with one another so that participants in the room can maintain eye contact with the participants at the far end of the call. The "eyes" of the participants on the far end of the call will always be the camera, not the display. However, it is very unnatural and uncomfortable to stare into a camera when a video of the person talking is shown on the display. Assuming that the participants in a room are looking at the camera, if the camera is set too high, the participants sitting in front of the camera will have to crane their necks to maintain eye contact with the participants on the far end. If the camera is set too high and participants are looking at the display, it will appear to the far-end participants that everyone in the call is looking down. Alternatively, if the camera is set too low and participants are looking at the display, the far-end participants get the “up-the-nose” view of whomever they are conversing with. Ideally, the monitor should be positioned so that the far-end participants are at eye-contact height with the participants displayed. The camera should be located just above the monitor and centered. This position creates a gaze angle that allows the participants in the room to look the far-end participants in the eye, or at the display, and still maintain eye contact with the far-end participants on the display. Figure 4-11 illustrates how this gaze angle should appear.

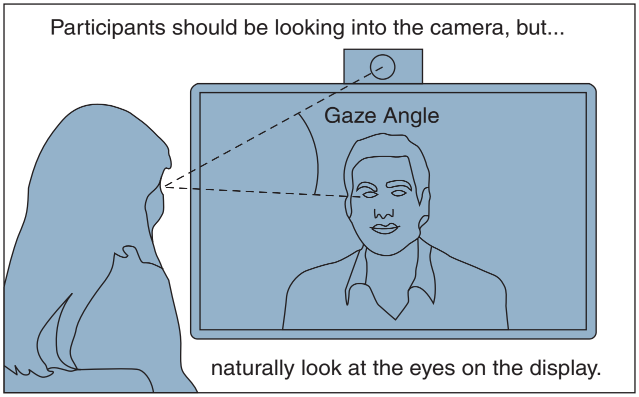

Participants should be looking into the camera, but...
Gaze Angle
naturally look at the eyes on the display.

Figure 4-11 *Gaze Angle*

The finer aesthetics of a meeting room can have just as much of an impact on video communication quality as the other aspects of room and environmental conditions that have been discussed thus far. The background seen through the camera’s eye should be carefully considered. We’ve already described how an endpoint will only update the part of a picture that has changed from frame to frame to conserve bandwidth. The more movement within a room, the more bandwidth needed to update the picture. It is best practice to eliminate any unnecessary motion in the background to minimize this issue; however, motion in the eye of a camera can be caused by more than just physical motion. Have you seen a picture such as a black-and-white spiral that appears to be moving even though you know in your mind it is not? This effect happens more frequently with a camera, especially when you’re trying to focus on a busy background. Cameras are constantly trying to find a single point to focus on. When there are numerous patterns in the camera’s field of view, the aperture of the camera is constantly adjusting to find that single focal point. The result seen on the far-end display is a false motion occurring in the background. Not only is this “motion” very distracting, but video quality is compromised because the video codec requires more bandwidth to update more of each frame. You should avoid a background that has busy wallpaper or many different objects. Pictures are always a nice touch in a room, but they should be hung outside the camera’s field of view. However, a simple company logo could be hung on the back wall of a meeting room, as long as it does not have a busy pattern.

Key Topic

Another best practice is to try to minimize contrasting colors. It is preferable to have one solid color as a background, preferably painted with a flat matte or eggshell finish. Equal to the importance of using a solid color, the actual color choice can affect video quality and bandwidth utilization. Cisco recommends using earth tones, such as beige, tan, brown, or forest green. All of these examples are safe colors to use, and they look really good over a video call, but some industrywide studies have been conducted, and the two highest recommended colors are not on Cisco's colors of choice. The color that takes the number-two spot is gray. The number one choice is blue—not just any shade of blue, but a shade that is consistent with Cisco blue. I believe that these colors did not make Cisco's list because most professional people do not want a gray or blue environment to work in. Therefore, Cisco's selections are softer tones that accommodate both video communications and day-to-day operations within an office environment. All industry experts are united on the worst wall color to use for video communications, and that color is white. It's interesting that white is the most widely used color within office environments because it is neutral. The problem with using white for video communication has to do with the way light and shadows react with white. Studies have shown that white walls use significantly more bandwidth than any other color in the spectrum. Therefore, the short answer to the question of what color a video meeting room should be painted is any color but white.

If you want to reference some of the color palettes Cisco recommends, check out the "Cisco Telepresence Room Design Palettes Quick Reference Guide": https://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration-endpoints/color_ref_guide_c07-642558.pdf.

One final note about room and environment conditions has to do with the very clothes a person wears during a video meeting. Striped, flowery, or any other patterned article of clothing worn by participants in a video call can have the same effect with the camera as a busy background. Although this topic overlaps a little bit into the last section on video etiquette, office employees should be encouraged to wear solid-color clothing on days when they know they will be participating in a video call.

Displays: Monitors and Projectors

Much of this section on light behavior has been dedicated to cameras, how light behaves around cameras, and how to position cameras in a meeting room used for video communication. Now the focus will turn to video output using monitors and projectors. Three different types of monitors can be used in a video communications room: CRT, plasma, and LCD. A fourth option is to use a projection system for display. The Cathode Ray Tube (CRT) option is never used in corporations and rarely seen even in consumer homes anymore. These old televisions were large and heavy, and the standard definition resolution they supported is far inferior to the higher-quality HD resolutions available everywhere today. Therefore, other than the honorable mention here, these types of displays will not be discussed further. As far as the other options are concerned, so many variables are involved in making decisions about projection versus monitors that we could spend a great deal of time on just this one topic. Solutions you might find yourself designing will require you to do your homework before deciding on what would be the best possible solution to use. The paragraphs that follow offer some brief descriptions about the differences between each of these options.

Plasma display panels (PDPs) are a type of flat-panel display that uses small cells containing plasma, which is ionized gas that responds to electric fields. When plasma screens first came out, the clarity of these screens was far superior to anything else on the market, including LCD displays. They range in size from 30 inches (diagonally) up to 150 inches. However, plasma displays had run their course by 2014 due to two main factors. Probably the most prominent factor was the price. Plasma displays were much more expensive than LCD displays. As more people bought LCDs, the prices dropped even more, to the point plasma displays could no longer compete. The second factor that led to the demise of plasma displays was the short life they lived. After about three years of use, plasma displays were prone to burn-in, which is where the images displayed on the screen would leave a permanent ghosting effect. This became a major deterrent away from this type of monitor.

Key Topic

Liquid crystal display (LCD) was a fierce competitor to the plasma display. Though they could not compete with plasma in quality at first, they could compete in price, which gave them an advantage. Plus, their quality was far superior to that of the CRT monitor, which was what the dominant market owned before they upgraded their older systems to this much-improved option. As time progressed, LCD displays began using LED back lighting to improve the image quality to that of plasma displays, putting the metaphorical nail in the coffin of plasma displays. LED monitors also reduce power consumption and space requirements. LCD displays are now reaching mammoth sizes, and prices continue to drop.

It would seem that LCD displays are the logical choice for video communication systems, but you should not rule out a fourth option just yet. Projection systems can now offer the same great quality of an LCD or plasma screen. Historically, there were three main issues with projection systems. First, more affordable projection systems had a lower quality, and the higher-resolution systems were priced too far out of reach. Second, the lumens on these projection systems were so low that room lights would have to be turned off before the display could be seen. This was not ideal for video communication because no one in the room would be seen if the lights were off. Third, the bulb in the projector had a finite number of burn hours before it went out. Then the cost of replacing the bulb was almost as high as the projector itself. Since those days of old, projectors have come a long way. You can now buy projectors that support full HD resolutions at about the same price as an LCD display. Both forward and rear projection systems are available, and they now use higher lumens to project on a screen in the daylight hours. Improvements have also been made to the bulbs in these projectors so that they last much longer, and they are not nearly as expensive to replace as they used to be. All of these factors make projectors a great alternative to an LCD display.

So, what is the best display to use in your video meeting room? For that answer, you will have to do your homework. Be aware of all the ways a display may be used, all the possible places a presenter might stand, and where viewers might sit or stand. Consider the angles of view, both horizontally and vertically. Look for possible sources of reflected light or ambient brightness on a nice day. Ask yourself a few probing questions to determine which display type is best for the solution you're designing:

- Will the display be on all the time?
- Will it show the same thing over and over?
- What type of content is most likely to be viewed: Excel spreadsheets or live video?

Here are a couple guidelines to help in your meeting room design. Don't use short-throw projectors with roll-up projection screens. The slightest air movement will cause the image on the screen to distort in a way that participants will find disturbing. LCDs are great for spaces with too much ambient light, but be aware of the potential for poor off-axis viewing angles.

Video Cables and Connectors

Just as with audio cables, two types of video cables can be used. Chapter 3 explained luminance, which establishes the brightness, or the light and dark portions of the picture, and chrominance, which establishes all the color information for the picture. Chrominance can be further broken down into the three main colors of the color spectrum, which are red, green, and blue components. These individual components are separated and combined in different manners depending on the connection method. Figure 4-12 illustrates the various composite and component video connectors.

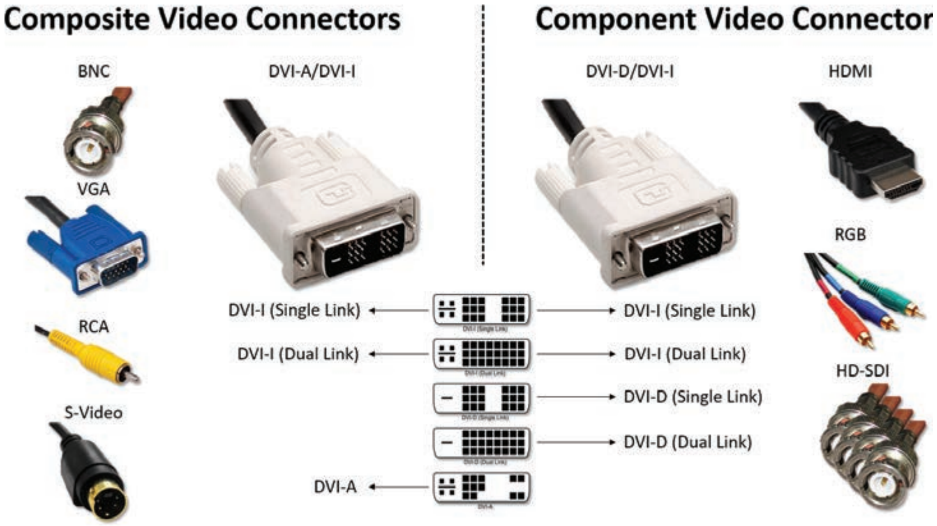


Figure 4-12 *Composite and Component Video Connectors*

Key Topic

Composite video is the simplest and lowest quality of all the varieties. All components that make up the video are combined and transmitted along a single cable. Video Graphics Array (VGA) is the most commonly used composite video connector. Each component is individually separated and given its own pin in the connector. Bayonet Neill-Concelman (BNC) is another composite video connector often found on the ends of coaxial cables. This type of connection is common with cable television, where a single coaxial cable runs into the back of your television set or cable service box. RCA connectors, which were discussed in the "Audio Cables and Connectors" section, often come with three connectors. The yellow connector offers composite video over a single wire, and the red and white connectors offer unbalanced audio for left and right speakers. These cables are commonly used when connecting a VHS or DVD player to a display. Y/C, also known as Separate Video (S-Video), is a connector that separates the Y, or luminance, and C, or chrominance components and transmits these signals individually. However, S-Video is still considered composite video because the chrominance components are not broken out into the three primary colors.

Key Topic

Component video improves on composite video quality by separating each of the color components of the chrominance portion of the signal, in addition to the luminance. Also known as YPbPr, the luminance (L) is integrated with the green portion of the signal. For a recap on how the green is calculated, refer to the "Chrominance and Luminance" section in Chapter 3, which discusses this procedure. RGB connector cable, pictured in Figure 4-12, is a type of RCA cable that will come with three or five connectors on each cable. The three video cables will be colored green for luminance, or Y; blue for primary blue, or Pb; and red for primary red, or Pr. Although BNC connectors can be used for a composite video connection, component video can also be achieved with three coax cables. This type of connection is frequently used in commercial applications with High Definition-Serial Digital Interface (HD-SDI) video formats. The most widely used component video connection globally is High-Definition Multimedia Interface (HDMI). HDMI is a fully digital standard that also has the added benefit of carrying balanced audio, power, and control on the same cable. HDMI uses YCbCr to calculate the color space for video, which allows a higher color depth. HDMI has evolved from version 1.0 to the recent update 2.1 standard, and now has a maximum supported resolution of 10k at 120 Hz.

The last video connector worth mentioning is Digital Visual Interface (DVI). I saved this particular connector till last because five different DVI connector types can support either analog composite video or digital component video. The Digital Visual Interface-Analog (DVI-A) connector is similar to the VGA connector. These connectors are not often found today due to the mass adoption of HD. More commonly found is the Digital Visual Interface-Digital (DVI-D) connectors. These digital-only connectors support HD resolutions comparable to HDMI. Digital Visual Interface-Integrated (DVI-I) allows either a DVI-A or DVI-D connector to join, thus supporting either analog or digital signals. There are two different connector types for DVI-D and DVI-I:

- Single-link DVI employs a single 165 MHz transmitter that supports resolutions up to 1920 × 1200 at 60 Hz, or 2560 × 1600 at 30 Hz.
- Dual-link DVI adds six pins, at the center of the connector, for a second transmitter, increasing the bandwidth and supporting resolutions up to 2560 × 1600 at 60 Hz, or 3840 × 2400 at 30 Hz.

As previously explained, the five connectors in the DVI category include DVI-A, DVI-D Single Link, DVI-D Dual Link, DVI-I Single Link, and DVI-I Dual Link.

Immersive Telepresence

Immersive Telepresence room systems represent the height of video communication today. They combine the best audio, video, and networking components available on the market to create an in-room experience that's as close to a face-to-face meeting as is possible with modern technology. Immersive Telepresence rooms of the past required strict implementation guidelines to create the environment to have a high-quality experience and allow the system to function at optimal levels. The legacy Tandberg T3 Immersive Telepresence room was quite literally a "room within a room" configuration that required the integrator to fully install the walls, ceiling, lighting, and flooring within an existing room to adequately control the conditions required to provide an exceptional video experience. In comparison, the legacy Cisco CTS 3000 was a standalone system that was installed into an already-completed room, but it still required extensive room remediation with proper lighting, temperatures, wall colors, and sound dampening in place before installation of the endpoint system and components was allowed.

Key Topic

The Cisco IX5000 was a game-changing, revolutionary Immersive Telepresence system that changed what was considered essential for room remediation with these types of systems. It is the first Immersive Video endpoint to require no room remediation prior to the installation, although some room remediation is still recommended. There are still recommendations and best practices that surround video communication, as mentioned earlier in the "Room and Environment Considerations" section of this chapter. For example, Cisco recommends lighting temperatures of 4000 K to 4100 K and a color rendering index of 82 or greater for best results with any telepresence endpoint. Also, the top-down lighting onto the subject's shoulders should not exceed two times the light value of the lighting that can be measured on the subject's face. The IX5000 was designed to operate with much wider room tolerances while still being able to control the customer experience. The IX5000 addresses the preceding two examples with built-in facial lighting elements mounted directly over the display monitors. This extra facial lighting, which can be adjusted manually, allows the illumination on the participants to be better balanced based on each room's needs.

In October 2019, the IX5000 endpoint was end-of-sale, marking the dawn of the next phase of Immersive Telepresence solutions. Cisco has launched a new endpoint called the Cisco Webex Room Panorama. This system now supports three simultaneous video streams using a single codec, just like the IX5000, plus two additional content video streams at the same time. What's more, this integrator system allows the room to be customized to the specific needs of the customer, taking Immersive Telepresence one step further. This endpoint is offered at a significantly lower price. Plus, all the furniture that was required with the IX5000 is no longer required with the Webex Room Panorama, and installation is much easier as well.

Video Etiquette

People communicate with more than just voices. One of the great advantages of video communication over audio-only communication is the ability to read someone's body language, see emotional responses, and share content. Communicating this way also opens the gate for other distractions. As our world and workplaces become more enriched with video solutions, we need to keep in mind basic etiquette for using video to communicate. Some of the etiquette suggestions that follow should already be familiar from more than a century's use of telephones, although others will be unique to video.

Prior to a scheduled meeting, you should try a test call to make sure there will be no connection issues at the scheduled time of the call. Enter the meeting room early to make sure it is clean and the chairs are all pushed under the table. Connect to the meeting early if you can and turn on self-view to see how the room and participants will appear to the far end of the call. Adjust the camera, if needed, so that all participants in the room can be seen clearly.

When using video communication devices, be aware of what the far-end participants are hearing from your end. This is especially true when tabletop microphones are used. Clicking the end of your pen, tapping on the table, or rustling papers can be very distracting because these noises are magnified over the communication systems. Placing papers surreptitiously over the microphone can have a reverse effect and muffle the audio of people speaking within the room. Most people have the common decency today to set their cellphones to vibrate during a meeting. However, placing mobile phones on a meeting room table will create vibrations that the mic will pick up when they inevitably go off. The general rule of thumb is to try eliminating external sounds as much as possible. Side conversations should be discouraged as well. A best practice during an audio or video meeting is to mute the audio altogether, but always assume the audio feed is active. You do not want to be caught complaining about your boss on the other end of the call because you thought the microphone was muted. This also goes for the beginning and end of a call. Audio channels always open before video channels, and audio channels are always the last to close. That means that you may be sending audio between endpoints even though you can't see video.

What you are wearing may affect the way people see you in more than one way when it comes to video communication. Stripes, plaids, and other multicolored designs can appear more pixelated on video or cause a false sense of motion. This effect can be distracting to people at the other end of the call, and their focus may be on the clothing rather than the person speaking. It is preferable to stick with solid colors. This suggestion should also be considered for the purpose of the background of a video call. Just as you would in a face-to-face conversation with someone, try to maintain eye contact. If the meeting room has been designed properly, doing so should be easy enough. Remember that the camera is the eyes of the participants at the far end of the call. Last to be mentioned, but certainly not the least to consider, try to avoid other distracting actions. Avoid eating food or chewing gum while using an endpoint, and don't swivel in your chair. Always try to maintain a professional presence for the duration of the call. There will be plenty of time to goof off when the call ends.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 4-3 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 4-3 Key Topics for Chapter 4

Key Topic Element	Description	Page Number
Paragraph	Physical Components of an Endpoint	55
Paragraph	How Reflections Affect Hearing	58
Paragraph	Dynamic Mics versus Condenser Mics	60
Table 4-2	Microphone Pickup Patterns	62
Paragraph	Balanced versus Unbalanced Audio Cables	64
Paragraph	AEC Operation	66
Paragraph	Microphone Placement	67
Paragraph	Speaker Placement	67
Paragraph	Audio Communication Etiquette	69
Paragraph	Field of View and Focal Length	70
List	Factors Controlling Depth of Field	70
Paragraph	White Balance for Color Temperature Correction	71
Section	Three-Point Light Technique	72
Paragraph	Gaze Angle	74
Paragraph	Wall Colors in Video Meeting Rooms	75
Paragraph	LCD and Projector Displays	77
Paragraph	Composite Video	78
Paragraph	Component Video	78
Paragraph	Immersive Telepresence Lighting Requirements	79

Define Key Terms

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

Absorption, ACG, AEC, Aperture, Balanced Audio Cable, Bidirectional, Cardioid, Clipping, Codec, Coherent Late Reflections, Condenser Mics, Critical Distance, CRT, Depth of Field, Diffusion, Direct Sound, Directional Mics, Distance Factor, Dynamic Range, Early Reflections, Endpoint, Field of View, Frequency Response, Gain, Gaze Angle, Good Levels, Headroom, Hypercardioid, LCD, Line Level, Mic Level, NRC Rating, Omnidirectional Mic, PDL, PoE, Polar Pattern, PTZ, Reflection, Reverb Time, Reverberations, Shotgun, Supercardioid, Unbalanced Audio Cable, White Balance, Zoom

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What are the six components that make up a video system?
2. What are the five functions of the menu settings on an endpoint?
3. What are the four categories of reflections?
4. List the three positions used in the three-point lighting technique.

This page intentionally left blank

CHAPTER 5

Communication Protocols

This chapter covers the following topics:

PSTN Communication: This topic will discuss the various PSTN connections options, including POTS, ISDN via BRI, and ISDN via PRI.

H.323 Communication: This topic will discuss the H.323 umbrella standard, H.323 gatekeeper registration, call flow without a gatekeeper, and call flow with a gatekeeper.

SIP Communication: This topic will cover the IETF SIP, discuss basic SIP registration, and address SIP call setup using early offer and delayed offer.

NAT and Firewall Traversal Solutions: This topic will discuss the different IETF NAT traversal protocols, including STUN, TURN, and ICE. This topic will also discuss the Cisco proprietary traversal protocol, ASSENT, and the ITU standard for traversal, H.460.

Up to this point, this book has focused on the intricate aspects of passing audio and video media between two nodes in an audio or video call. This chapter will turn the focus to the actual medium used to transport this data. Two mediums can be used for communication. Circuit-switching technology is the standard telephony mode of communication that has been used for over a century across the PSTN. Packet-switching is a relatively new technology that allows voice and video communication to travel across the digital network. Both modes of communication are incredibly complex, so this chapter will serve only as an introduction to each of these technologies. Topics discussed in this chapter include the following:

- PSTN Communication
- H.323 Communication
- H.323 Gatekeeper Registration
  - H.323 Call Flow without a Gatekeeper
  - H.323 Call Flow with a Gatekeeper
- SIP Communication
- SIP Registration
  - SIP Call Setup
  - Delayed Offer
  - Early Offer
- NAT and Firewall Traversal Solutions
  - STUN

- TURN
- ICE
- ASSENT and H.460

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

1.3 Configure these network components to support Cisco Collaboration solutions:

- 1.3.a DHCP
- 1.3.c CDP
- 1.3.d LLDP
- 1.3.e LDAP
- 1.3.f TFTP

“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
PSTN Communication	1–2
H.323 Communication	3–6
SIP Communication	7–10
NAT and Firewall Traversal Solutions	11–14

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. How many channels form an E1 link?
   a. 23
   b. 24
   c. 31
   d. 32

2. Which of the following control mechanisms uses IMUX to multiplex ISDN channels together?

a. H.221

b. H.460.19

c. BONDING

d. Assent

3. Which of the following are the minimum required standards for H.323 compliance? (Choose four.)

a. G.711

b. G.729

c. G.722

d. H.239

e. H.261

f. H.264

g. H.221

h. H.225

i. H.245

j. T.120

4. Which of the following RAS messages is used to broadcast communication for gatekeeper discovery?

a. ARQ

b. GRQ

c. BRQ

d. RRQ

5. Which of the following RAS messages is used to initiate an H.323 call when no gatekeeper is used?

a. GRQ

b. RRQ

c. ARQ

d. None of the above

6. Which of the following RAS messages is used to initiate an H.323 call through a gatekeeper?

a. GRQ

b. RRQ

c. ARQ

d. None of the above

7. Which of the following organizations is responsible for the management of SIP?

a. IEEE

b. IETF

c. ITU-T

d. ICANN

8. Once an endpoint has powered on and loaded the locally stored image, what is the next step for the endpoint to register to a CUCM?

   a. DHCP Discovery

   b. Send TFTP Get

   c. Send CDP

   d. Register to CUCM

9. Which protocol is responsible for exchanging capabilities during a SIP call setup?

   a. SIP

   b. SDP

   c. H.225

   d. H.245

10. In the call setup process, what SIP response does the destination endpoint use to send SDP information to the source endpoint?

    a. Invite

    b. Trying

    c. Ringing

    d. OK

11. In what private IP address class is the address 172.20.198.18 included?

    a. This is a public IP address, not a private IP address.

    b. Class A addresses

    c. Class B addresses

    d. Class C addresses

12. Which of the following network characteristics requires a STUN server to be used?

    a. Asymmetric network

    b. Symmetric network

    c. Both symmetric and asymmetric networks

    d. Neither symmetric nor asymmetric networks

13. What is the default listening port for TURN servers running on the Cisco Expressway?

    a. 5060

    b. 5061

    c. 3478

    d. 24000–29999

14. How many media ports need to be open for Assent to pass audio and video data through the firewall?

    a. 1

    b. 2

    c. 2400

    d. 30,000

Foundation Topics

PSTN Communication

The International Telecommunication Union, or ITU, is part of the United Nations. The purpose of the ITU is to help coordinate the use of information and communication technologies. Specifically, it coordinates global usage of the radio spectrum, facilitates cooperation between governments and corporations with assignment of satellite orbits, and most importantly for the purpose of this book, helps in the interconnection of networks and technology.

In particular, the sector most pertinent to this book is the ITU Telecommunication Standardization Sector, or ITU-T. The ITU-T is tasked with defining standards for any audio-visual communications on a circuit-switched or packet-switched network. Without a uniform standard, problems arise between systems that try to communicate but are using different formats to store and transmit data. Technically speaking, the main products of ITU-T are recommendations (ITU-T Recs)—standards defining how telecommunication networks operate and interwork. ITU-T Recs have nonmandatory status until they are adopted in national laws. The level of compliance is nonetheless high due to international applicability and the high quality guaranteed by ITU-T's secretariat and members from the world's foremost information and communication technology (ICT) companies and global administrations.

The ITU-T has created umbrella standards, which contain categorized lists of codecs that must be used to be able to communicate within a particular switching technology. The H.320 umbrella standard encompasses circuit-switched technologies, and the H.323 umbrella standard encompasses IP-based packet-switched technologies. Because the ITU-T has standardized how devices communicate, an H.320-supported device can communicate to any other H.320-supported device because they are all required to support the same minimum standards to be H.320 compliant. This is also true for H.323 devices. Defining what audio, video, data, and control codecs are being used in the conversation is crucial for devices being able to communicate.

Circuit switching is a method of implementing a telecommunications network in which two network nodes establish a dedicated communications channel, or circuit, through the network before the nodes may communicate. The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the communication session. The circuit-switched network was first implemented in the old analog telephone network. When a call is placed from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones for the entire duration of the call across the public switched telephone network, or PSTN.

Key Topic

For call setup and control, it is possible to use independent dedicated signaling channels from the phone to the network. Integrated Services Digital Network, or ISDN, is a type of circuit-switched networking service that uses an independent signaling channel while plain old telephone service, or POTS, does not. The method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line so that each signal appears on the line only a fraction of time in an alternating pattern is known as time-division multiplexing, or TDM. It is used when the bit rate of the transmission medium exceeds that of the signal to be transmitted. This form of signal multiplexing was developed in telecommunications for telegraphy systems in the late

19th century but found its most common application in digital telephony in the second half of the 20th century.

Key Topic

The two main types of ISDN to be familiar with are BRI and PRI. BRI, which stands for Basic Rate Interface, is primarily used for subscriber circuits similar to the same voice-grade telephony service that has been used for the last century. This allows BRI ISDN connections to use the same existing telephony exchange infrastructure at business locations. Each BRI ISDN circuit contains two Bearer channels, or B-channels, and one Delta channel, or D-channel. BRI Bearer channels support 64 kbps bandwidth and are used to carry the actual audio data. The BRI Delta channel supports 16 kbps and is used to send all the control signaling, such as call setup messaging, call teardown messaging, and timing for TMD. The Delta channel carries the address, informational, and supervisory signaling messages for all of the B-channels. By contrast, PRI, or Primary Rate Interface, circuits offer more B-channels.

Key Topic

PRI is primarily used for carrying multiple DS0 transmissions. PRI is the main standard used today for providing telecommunication services to businesses over a circuit-switched network. There are two different types of carriers for PRI ISDN services available globally. Throughout the United States, Canada, and Japan, the T-carrier is used, although Japan refers to its carrier as J-carrier. The T1 or J1 PRI ISDN circuit will carry 23 Bearer channels and one Delta channel. Although the purpose of these channels is the same as with BRI, they all support 64 kbps, including the D-channel. Multiple channels can be multiplexed together so that one T1 circuit can provide up to 1.544 Mbps of bandwidth for ISDN communication. Common throughout Europe, Australia, South America, and pretty much the rest of the world is the E-carrier. One E1 circuit consists of 30 Bearer channels and two Delta channels. Much like the T1 PRI circuit, each of these channels supports 64 kbps, including the two D-channels. Therefore, one E1 line can provide up to 2.048 Mbps of bandwidth for ISDN communication. Both T1 and E1 PRI ISDN lines can be leased from a telephone service provider, or TSP, with all channels available, or only a part of the channels available. These are called Fractional T1 or Fractional E1, and sometimes require special treatment when they are set up.

Audio communication has been available through ISDN since the H.320 standard was introduced in 1986. A single audio call required only 64 kbps bandwidth or less, so a single channel could easily be used to support an audio call. When video conferencing was first introduced, the medium was based on ISDN video endpoints that were connected via BRI or PRI circuits to the PSTN. Three BRI connections were common for low-resolution endpoints that supported up to 320 kbps for video and 64 kbps for audio. The common video format used was CIF. Higher-resolution endpoints could use fractional PRIs or a full PRI for up to 1.554 Mbps with T1 PRI and up to 2 Mbps with E1 PRI; however, this created a problem. The H.221 control standard, also referred to as Clear Channel Dialing, required the E.164 alias associated with each line to be dialed before the call could be placed. Therefore, to place a 384 Kbps call, up to six phone numbers had to be dialed at the same time.

An organization known as the Bandwidth On Demand Interoperability Group came up with a solution to this issue called BONDING. If two ISDN phones had a piece of software installed on them called an IMUX, then only one number needed to be dialed to initiate the call. The IMUX on the receiving phone would send a request for more channels to be opened. The IMUX on the source phone would proceed to place the remaining calls needed to support the bandwidth in the original call request. When all channels were opened, IMUX would allow the call setup to continue. This multiplexing of B-channels within ISDN based on BONDING was so effective that the ITU-T adopted BONDING into the H.320 umbrella standard. Figure 5-1 illustrates the difference between Clear Channel Dialing and BONDING.

The still-lingering issue with ISDN-based calling using video communication was that many calls were long distance or international. Each channel that was opened had a toll charge associated with it. This resulted in high PSTN costs, even for CIF-based video communication calls between two locations. Therefore, video communication was not widely accepted into the business world until the less-expensive IP-based packet-switched communication was available with the premiere of high-speed Internet.

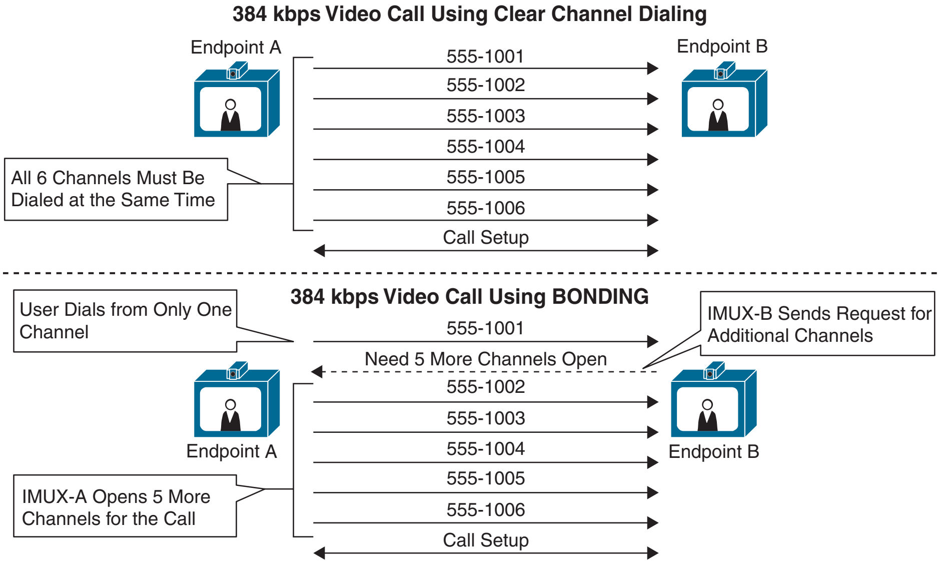

384 kbps Video Call Using Clear Channel Dialing
Endpoint A
Endpoint B
555-1001
555-1002
555-1003
555-1004
555-1005
555-1006
Call Setup
All 6 Channels Must Be Dialed at the Same Time
384 kbps Video Call Using BONDING
User Dials from Only One Channel
555-1001
Need 5 More Channels Open
IMUX-B Sends Request for Additional Channels
555-1002
555-1003
555-1004
555-1005
555-1006
Call Setup
Endpoint A
Endpoint B
IMUX-A Opens 5 More Channels for the Call

Figure 5-1 *Clear Channel Dialing vs. BONDING*

To be able to communicate with other devices that are using H.320, each endpoint must support certain minimum standards. Endpoints that support these minimum standards are referred to as being *standards compliant*. The minimum audio codec to support is G.711, but many other audio codecs can be supported as well, as outlined in Chapter 2, "Audio Basics." The minimum video codec that must be supported is H.261, although more video codecs are available as well. Refer to Chapter 3, "Video Basics," for more information on video codecs. The minimum control codec, which is the codec that controls call setup and call teardown and maintains the timing during the call, is H.221. A substandard under the H.221 standard is known as Q.931. This is the mechanism known for the initial handshake during call setup and for terminating the channels during call teardown. BONDING is also a control codec and is more commonly used today for video calls. These are the minimum codecs that must be supported to be H.320 compliant. However, other codecs used for other purposes are available under the H.320 umbrella standard, such as T.120 or H.239, which are both used for content sharing. Other codecs support features such as chair control during conferences, mute, call hold, call transfer, far-end camera control, and many more. Table 5-2 identifies the minimum standards for H.320 compliance.

Key Topic

Table 5-2 Minimum Standards for H.320 Compliance

Capability	Codec
Audio	G.711
Video	H.261
Data Sharing	T.120
Control	H.221

Private branch exchanges (PBXs), which were discussed in Chapter 1, "Introduction to Collaboration," were often used within enterprise environments. PBXs performed local call control for phones. They also allowed different enterprise locations to be connected via a leased service connection. This type of connection was usually less expensive than a connection through a telephony service provider via ISDN lines.

H.323 Communication

Key Topic

H.323 is an umbrella standard developed and maintained by the ITU-T for IP-based packet-switched communication. It is referred to as an *umbrella* standard because it encompasses many substandards. To be H.323 compliant, the device must support a minimum set of substandards, such as G.711 for audio, H.261 for video, and H.225 and H.245 for control. Many of the standards included in H.323 are taken from the H.320 umbrella standard for circuit-switched communication, such as Q.931, which is a substandard under H.225, all of the audio and video codecs, and the H.239 codec for content sharing.

H.323 devices can place calls without a central call control device by dialing the IP address of another system. However, a central call control device for H.323 endpoints, which is known as a *gatekeeper*, can be used to extend the management functions of an H.323 environment in three capacities: registration, security, and call control.

Key Topic

Registration allows the use of E.164 aliases, H.323 IDs, and prefixes in addition to IP address dialing. E.164 aliases are numeric-only values containing 1–15 digits that are assigned to an endpoint. They work in the same manner as any phone number would in a typical telephony environment. H.323 IDs can use any combination of numbers, letters, and/or special characters, but spaces are not allowed. Because of this ability, an H.323 ID can be in the form of a URI. However, an H.323 ID is not a URI because it is not dependent on the domain being a fully qualified domain name (FQDN). Prefixes are a feature of H.323 dial plan architecture that allows easy access to services such as Multipoint Conferencing Units (MCUs) and gateways.

Security regarding the gatekeeper does not refer to call encryption. That type of security is a function built into endpoints and can be used with or without a gatekeeper. Security within the context of a gatekeeper refers to the capability to determine which devices can and cannot register to the gatekeeper. This function helps secure access and control features within the communications network.

Call control is the ability to determine which devices can call each other and administer the bandwidth that can be utilized when calling between different devices and locations. More advanced call control policies can be configured, such as transforming the dialed aliases, redirecting call traffic, and restricting calls through ISDN gateways from an outside source, which is known as *hair-pinning*.

H.323 Gatekeeper Registration

Call Setup mode is an H.323 setting configured on an endpoint that can be set to either Direct or Gatekeeper. If Call Setup mode is set to Direct, the endpoint will never attempt to register to a gatekeeper and will only be able to dial by IP address. When Gatekeeper mode is used, the endpoint is completely subservient to a gatekeeper and will perform no function until it has registered. Once registration has occurred, the device must request permission from the gatekeeper before it will attempt any action including placing or answering calls. The ITU created the communication protocol known as RAS (Registration, Admission, and Status) that identifies all messaging schemes between any device and a gatekeeper. RAS is a substandard under the H.225 standard for call setup and is used only by endpoints that register to the gatekeeper.

Another setting on an endpoint that affects its registration is known as Discovery mode. Discovery mode determines how an endpoint will locate the gatekeeper to which it will attempt to register. Discovery mode can be configured to either Automatic or Manual. If Discovery mode is set to Automatic, the endpoint will broadcast a message that is known as a Gatekeeper ReQuest (GRQ) to the entire network broadcast domain to which the device belongs. The first gatekeeper to respond with a Gatekeeper ConFirm (GCF) is where that endpoint will send a Registration ReQuest (RRQ). If the Discovery mode is set to Manual, then the address of the gatekeeper must be entered into the device. This address becomes the address that the endpoint will direct the RRQ. The gatekeeper that receives the RRQ will respond with a Request In Progress (RIP). This message allows the gatekeeper to process though various security policies to assess whether the endpoint is allowed to register. If a security policy prohibits registration, the gatekeeper will respond to the device with a Registration ReJect (RRJ). If there are no configurations prohibiting the registration, the gatekeeper will respond with a Registration ConFirm (RCF). Figure 5-2 illustrates the H.323 registration process.

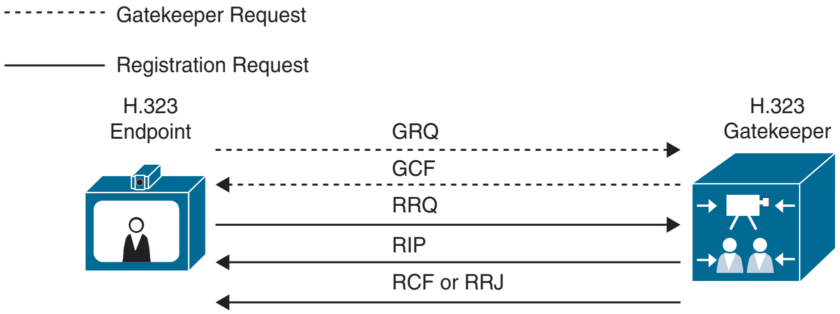


Figure 5-2 *H.323 Registration Process*

H.323 Call Flow without a Gatekeeper

Both H.323 and SIP use the three-way handshake method of the TCP/IP network for initial call setup. If you are not familiar with this method, this brief review should explain the purpose and process of the method appropriately. Assume that a client, such as a computer, is going to transfer files to an FTP server. It is vital that the information being shared is sent securely and completely, without any loss of data. Therefore, before the client will send any of the important information, a three-way handshake is used to establish a TCP connection with the server. The client initiates this process by sending a SYN message to the server. The server sends back a SYN/ACK message to the client acknowledging the receipt of the SYN, and then the client sends an ACK message to the server establishing a TCP connection. Now the client can begin sending the file packets to the server and will receive an acknowledgment on each packet sent as they are received. If any packets sent by the client do not receive an acknowledgment in return, the client knows to resend those packets. This process is the same for IP telephony calling. A TCP connection must be established between two endpoints before important call capability information is exchanged. In the IP telephony world, this three-way handshake is known as *call setup*. Figure 5-3 illustrates the three-way handshake method.

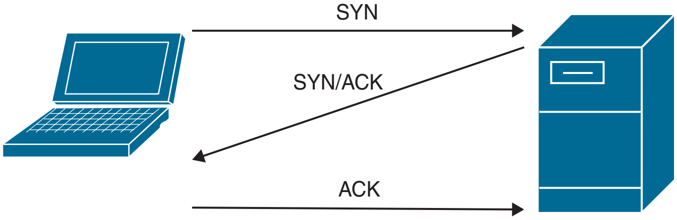


Figure 5-3 *Three-Way Handshake Method*

Key Topic

As mentioned before, H.323 devices can place calls without a central call control device by dialing an IP address of another system. The endpoint will not register to a gatekeeper, Call Setup mode should be set to Direct, and the endpoint will dial by IP address. The source endpoint will send a Q.931 call setup message to the destination endpoint. Q.931 contains the source and destination IP address, in hexadecimal format, and any crypto-hash token if the call is to be encrypted. Both Q.931 and RAS messaging are part of the H.225 control standard for call setup. Because a gatekeeper is not being used in this scenario, there is no RAS messaging either. H.225 performs the same function as the SYN message in a three-way handshake. The destination endpoint can now respond to the Q.931 call setup message it received. The first response this endpoint will send out is the Alerting message. This process allows the destination endpoint to ring and sends a ring-back tone to the source endpoint. The Alerting message is equivalent to the SYN/ACK message in a three-way handshake. Once the call is answered, either manually or automatically, a Connect message is sent to the source endpoint. The Connect message is equivalent to the ACK message in a three-way handshake. Both the Alerting and Connect messages are part of the Q.931 messaging system.

After the call setup messaging is complete, the two endpoints must now go through the H.245 negotiation process to ensure that the most appropriate codecs are selected and to identify the UDP ports that will be used for communications. This is the important data that the three-way handshake is used for to ensure all data is exchanged properly between two endpoints. First, each endpoint must send a Terminal Capabilities Set, sometimes called Capabilities Exchange or CapEx, containing all the codecs that each endpoint is capable of using. These codecs are the audio and video compression algorithms, such as G.711 and H.261, and other capabilities like dual video, far-end camera control, chair control, and so on. Because this communication is all TCP communication, there will be acknowledgments for each communication sent. Once this process is completed, the master/slave determination needs to be made. The master is simply the endpoint that will select the codecs to be used and allocate the UDP ports for RTP and RTCP communications. Based on several criteria, it can be either endpoint. Most often the endpoint that initiated the call will be the master, but that is not always true. In some instances, the endpoint with the most capabilities or the highest capabilities will be the master. In every call that involves a bridge, such as the Cisco Meeting Server, the bridge will be the master. Once the master is selected, that endpoint will initiate the next step in the process, opening logical channels. Obviously, actual channels are not being used for an IP-based call. This terminology was taken from the H.320 umbrella standard. The logical channels referred to here are the UDP ports that will be used for sending the media packets and signaling between each endpoint. Audio ports will always be opened first, then video, then ports for each additional capability. The master will also open the Real-time Transport Control Protocol (RTCP) ports used for signaling first, which will always be odd-numbered. Then the Real-time Transport Protocol (RTP) ports will open for the actual media, and they will always be even-numbered. Once each set of ports has been opened, the endpoints will begin to exchange media and the call will be set up. Figure 5-4 illustrates the H.323 call setup process without a gatekeeper.

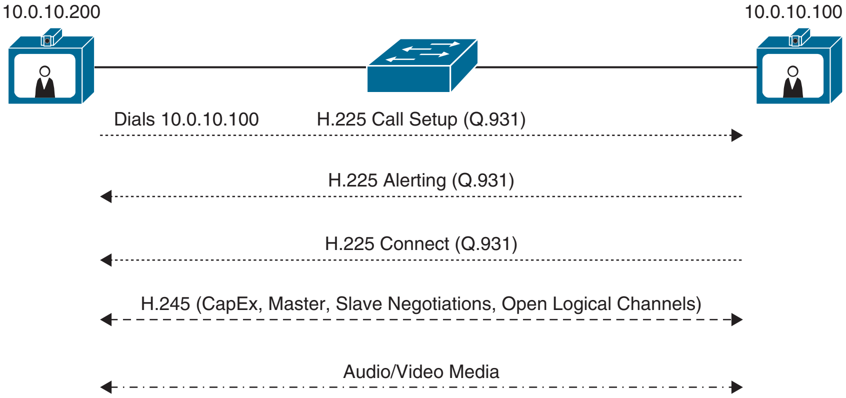


Figure 5-4 *H.323 Call Setup Process Without a Gatekeeper*

H.323 Call Flow with a Gatekeeper

Before I explain H.323 call flow with a gatekeeper, it is important to understand two methods that exist for H.323 call setup. These two methods are called *slow start* and *fast start*. In most cases on a Cisco Expressway running as an H.323 gatekeeper, slow start is used. Therefore, the explanations here are based on this method of call setup. Fast start simply combines some of the H.245 functions into the H.225 call setup process. Fast start goes beyond the scope of this book, but it is worth mentioning because it is still seen in Cisco Unified Communications Manager environments when H.323 gateways are being used.

Key Topic

Endpoints that are registered to a gatekeeper follow the same calling process as endpoints that do not register to a gatekeeper, but some extra messaging must take place between the endpoint and the gatekeeper first. This is where RAS messaging comes into play. RAS is commonly referred to as Registration, Admission, and Status. During an H.323 call setup involving a gatekeeper, a call admission process must occur. When the source endpoint dials the alias of the destination endpoint, it sends an Admission ReQuest (ARQ) to the gatekeeper. The gatekeeper responds with a RIP message because there may be call control policies that prohibit or restrict the call or certain aspects to the call. If the policies restrict access to the dialed alias, or the gatekeeper cannot locate the dialed alias, the return message will be an Admission ReJect (ARJ). Provided the destination endpoint is located and there are no restrictions prohibiting the call, the return message will be an Admission ConFirm (ACF), which also includes the IP address of the destination endpoint and the bandwidth that is allowed for this call.

The source endpoint then uses the preceding information to send a Q.931 call setup message to the destination endpoint. When the destination endpoint receives the call setup message, it must first request permission to answer the call from the gatekeeper. Therefore, the destination endpoint sends an ARQ message to the gatekeeper. The gatekeeper responds with a RIP message and proceeds to check whether there are any bandwidth restrictions. Provided there are no restrictions, the gatekeeper responds with an ACF. The destination endpoint can now respond to the Q.931 call setup message it received with the same Alerting and Connect message discussed previously.

After the call setup messaging is complete, the two endpoints must now go through the H.245 negotiation process to ensure that the most appropriate codecs are selected and to identify the UDP port that will be used for communications. As mentioned before, the communication sent using H.245 includes a terminal capabilities set, master/slave determination, and opening logical channels, or ports. Once each set of ports has been opened, the endpoints will begin to exchange media and the call will be set up. Figure 5-5 illustrates the H.323 call setup process with a gatekeeper.

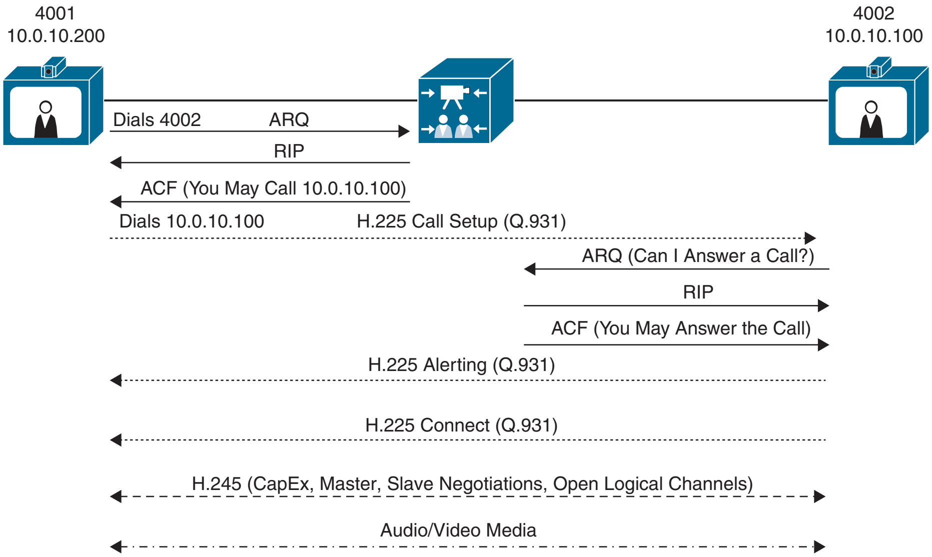


Figure 5-5 *H.323 Call Setup Process with a Gatekeeper*

SIP Communication

Key Topic

Session Initiation Protocol, or SIP, is a communication protocol that is created and managed by the Internet Engineering Task Force, or IETF. Unlike H.323, SIP endpoints cannot operate without a call control device. The SIP call control device is generically called a SIP server and functions at the center of all SIP-related call control activities. The SIP server performs two functions: Registrar and Proxy. The SIP Registrar maintains a table that is composed of IP addresses and Uniform Resource Identifier (URI) addresses taken from devices at the time of registration. URI addresses are the only type of alias SIP uses for communication other than IP addresses. Because a URI must be in the format Host@FQDN (fully qualified domain name), the domain must exist within the SIP Registrar for successful registration to occur. SIP addresses can also be in the form of Host@IP_Address. The SIP Proxy helps in locating and connecting two devices at the time of call setup. Cisco has two devices that fulfill the role of SIP server: the Cisco Unified Communications Manager and the Expressway.

When SIP was originally designed, the intention was not focused specifically on voice and video communication over IP. In fact, it would be a surprise if this use was even conceived at the time SIP was first drafted. SIP came out at a time when the Internet was young, and bandwidth rates were slow. Part of what caused data to lag so badly was the size of the payload data on each packet being sent. Therefore, the IETF drafted a proposal for how packets could be sent that would minimize the payloads and in effect reduce the time it took to send data. Because SIP was not written for one specific use, many vendors use SIP, even today, for various applications. By the late 1990s and early 2000s, many companies began using SIP for voice and video communication. It was used so heavily that the IETF amended some of the original RFCs to accommodate this specific application of use. Because RFCs are just recommendations for how the protocol should be used, they can be changed by independent vendors to accommodate their own proprietary brand of SIP. Now there are multiple variants with SIP, such as Microsoft. Microsoft released OCS, which was later changed to Lync, which was changed again to Skype for Business, and is now known as Microsoft Teams. Cisco also released a brand of SIP known as Skinny Client Control Protocol, or SCCP. SCCP is a very lightweight protocol that has a simplified message structure, whereas SIP has a range of different messages with each having a lot of additional data. Other vendors followed suit, and this did present a problem with cross-vendor compatibility in the beginning. However, interoperability between vendors is improving. Cisco has made a deliberate move away from SCCP since 2010 and supports SIP as the IETF recommends its use to encourage better interoperability using Cisco Collaboration products.

Basic SIP Registration

The SIP Registration process is very simple without a lot of complex messaging being sent back and forth. The endpoint sends an alias with its IP address to the SIP Registrar. The Registrar will reply with a "200 OK" message if the registration is accepted or an error message, such as "404," if it is not. However, the process to get to this point of registration is quite different depending on the type of SIP Registrar used. The Cisco Unified Communications Manager and the Expressway-C have a different process that leads to the endpoint trying to register.

The registration process on the Cisco Unified Communications Manager seems lengthy, but it actually makes deploying large quantities of phones and endpoints much easier. Every part of this process is automated using different tools on the Cisco routers, switches, and the Cisco Unified Communications Manager to enable phones to communicate and register with the Cisco Unified Communications Manager without any human interaction outside of plugging the patch cable into the back of the phone. The steps to this process are as follows:

Key Topic

1. The endpoint obtains power from the switch.
2. The endpoint loads the locally stored image (Phone-Load).
3. After the locally stored image is loaded, the first communication that the endpoint will send out is a Cisco Discovery Protocol (CDP) frame with a Voice VLAN query to

the switch. This CDP communication is used to obtain the Voice VLAN information if no local Voice VLAN ID (VVID) is configured already on the phone. If a non-Cisco phone or non-Cisco switch is used, then the LLDP-MED protocol can be used for the same purpose.

4. If the Cisco Catalyst switch has a Voice VLAN configured, it sends back a CDP frame with the VVID. Note that the VVID is used for both voice and video traffic.
5. When VLAN discovery is complete, the endpoint will send a DHCP discovery message to the DHCP server. Typically, the DHCP server is a router, but the Cisco Unified Communications Manager, as well as other DHCP server types, can also fulfill this role. A limitation in using the Cisco Unified Communications Manager is that it allows support for only up to 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. When the DHCP server receives the DHCP discovery, it responds with a DHCP offer. The DHCP offer includes an IP address, subnet mask, and default gateway address at a minimum. Additionally, a TFTP server address (with use of Option 150) and possibly one or more DNS addresses can also be provided. The endpoint responds to the DHCP offer with a DHCP request for the specific information sent in the DHCP offer. The DHCP server will then send a DHCP acknowledgment authorizing the use of the DHCP information exchanged and end the DHCP session.
6. 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. This message is typically sent over HTTP when using current endpoints, but TFTP signaling could be used as well. The communication that the endpoints sent to the TFTP server contains their MAC addresses because that is what the Cisco Unified Communications Manager uses to identify the endpoint's configuration file.
7. The Cisco Unified Communications Manager will first exchange a certificate trust list (CTL) file. The CTL file contains a set of certificates and is used only when Cisco Unified Communications Manager cluster security has been enabled. Next, the Cisco Unified Communications Manager will send the configuration files. After the configuration file has been downloaded, the endpoints will verify they are running the requested load, or firmware version. If the version they are running is different from the current version on the TFTP server, or different from a version specified in the configuration file, the Cisco Unified Communications Manager will send the current system load files and upgrade the firmware. Once upgraded, the endpoints will reboot. All information obtained up to this point will be retained.
8. The final step in the process is for the endpoints to register to the Cisco Unified Communications Manager. This is the SIP registration part of the process. The endpoint will send its IP address and alias information to the Cisco Unified Communications Manager and request registration.
9. The Cisco Unified Communications Manager will respond with the SIP message "200 OK." Now the registration process is complete.

Figure 5-6 illustrates the preceding steps when registering SIP endpoints to the Cisco Unified Communications Manager.

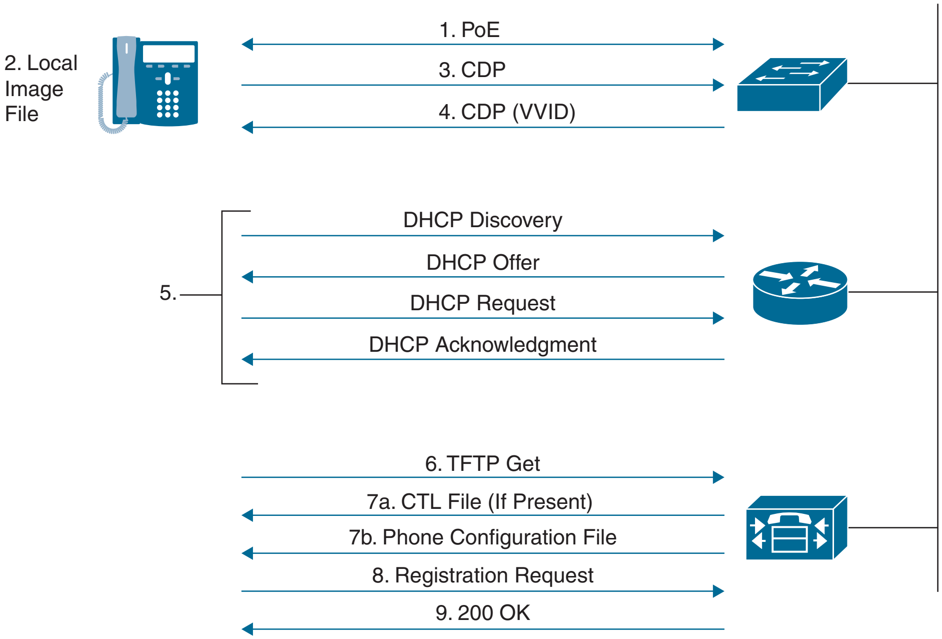


Figure 5-6 *SIP Registration Process to the Cisco Unified Communications Manager*

By contrast, the SIP registration process to a Cisco Expressway-C is not automated as it is when registering to the Cisco Unified Communications Manager. VLAN discovery through CDP is not essential for endpoints registering to the Expressway-C. Also, instead of configuration settings being sent to the endpoint using TFTP, these settings must be configured manually on the endpoint by an administrator. Therefore, there is no need for Option 150 to be configured on the DHCP server. The following steps outline the registration process on the Cisco Expressway-C:

Key Topic

1. Most Cisco Telepresence endpoints that register to the Cisco Expressway obtain local power from the power cube rather than through PoE. The exception would be the Cisco SX10 endpoint. Therefore, when an endpoint is going to register to the Cisco Expressway, it must first obtain power from the power cube.
2. As the endpoint is powering on, it will load the locally stored image, much like an endpoint would within a Cisco Unified Communications Manager environment.
3. Cisco CE software-based endpoints can use CDP for VLAN discovery, but VLAN discovery will not impact Expressway-C registration as long as the VLAN the device is on can route to the Expressway.
4. When VLAN discovery is complete, or if the endpoint does not use CDP, the endpoint will send a DHCP discovery message to the DHCP server. 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, and possibly one or more DNS

addresses. TFTP addresses are not used in an Expressway registration deployment. The endpoints respond to the DHCP offer with a DHCP request for the specific information that is sent in the DHCP offer. The DHCP server will then send a DHCP acknowledgment authorizing the use of the DHCP information that is exchanged and end the DHCP session.

5. The SIP URI and Expressway IP address are typically configured manually on the endpoint. These configurations can also be provisioned through Cisco TMS.
6. The final step in the process is for the endpoints to register to the Cisco Expressway. The endpoints will send their IP address and alias to the Cisco Expressway in the request registration. The alias must be in the form of a URI (name@FQDN), and the domain of the alias must match one of the domains configured in the domain database of the Expressway.
7. If there are no configured restrictions on the Expressway, it will respond with the SIP message "200 OK." The registration process is now complete.

Figure 5-7 illustrates the SIP registration process to an Expressway-C.

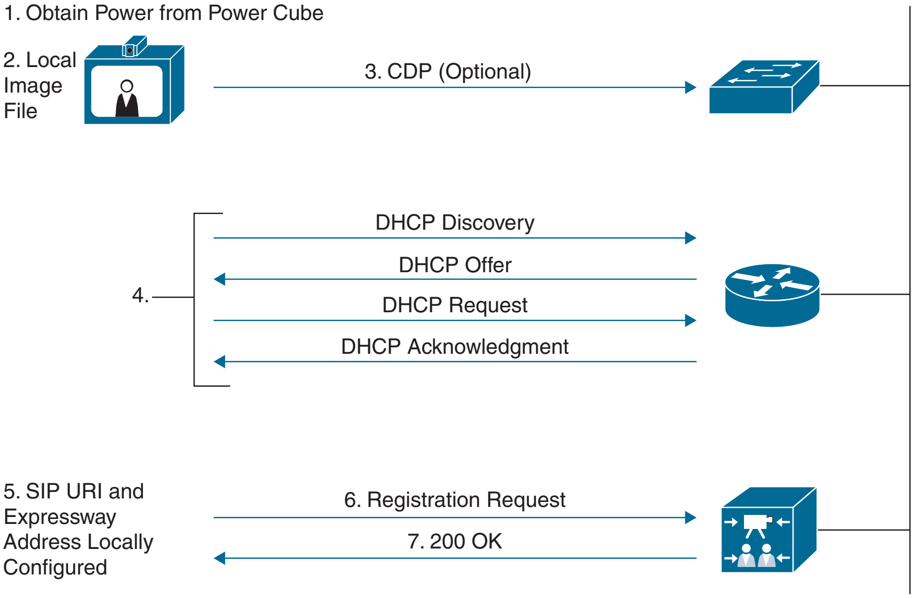


Figure 5-7 *SIP Registration Process to the Expressway Core*

SIP Call Setup

Both the Cisco Unified Communications Manager and the Cisco Expressway process SIP call 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 leveraged mark the differences between each call control server. There are two methods to process a SIP call: early offer and delayed offer. Both early offer and delayed offer use Session Description Protocol (SDP), which is the mechanism SIP uses to exchange codec capabilities and identify the UDP ports that are needed for RTP media. The Cisco Unified

Communication Manager can use either early offer or delayed offer, depending on certain settings and other configuration elements. Early offer is the only method that is used in the Cisco Expressway.

A third method of call setup is called early media. The early media feature is supported for SIP calls. Early media is the capability of two user agents to communicate before a call is actually established. Support for early media is important both for interoperability with the public switched telephone network (PSTN) and billing purposes. Early media is defined when media begins to flow before the call is officially connected. Media channels are set up prior to the call connection. These channels are used to provide the ring tone that the caller hears and are not generated by the caller's endpoint or other queuing services, such as Music-On-Hold. Early media is supported on Cisco IOS gateways.

Delayed Offer

SIP delayed offer begins when a source endpoint dials the destination alias using SIP, and an Invite message is sent to the SIP server. The SIP Proxy function of the SIP server examines the table that is created by the SIP Registrar to determine the destination endpoint's IP address using the alias that is dialed. The SIP server will then proxy the Invite message to the destination endpoint. At the same time the invite message is proxied, the SIP server will respond to the source endpoint with a Trying message. The Trying message contains the destination endpoint's IP information. After the Trying message is received, the source endpoint now possesses the source and destination IP addresses. The Invite message of the SIP call setup process is equivalent to the SYN message of the three-way handshake.

When the destination endpoint receives the Invite message, that endpoint now has the source and destination IP address information as well. The destination endpoint will then respond with two messages. The first message is the Ringing message, which tells the destination endpoint to ring and sends a ring-back tone to the source endpoint. The Ringing message is equivalent to the SYN/ACK message of the three-way handshake. When the user of the destination endpoint answers the call, an OK message is sent to the source endpoint. The OK message contains call connection status and is equivalent to the ACK message of the three-way handshake.

After the source endpoint receives the OK message from the destination endpoint, the SDP information can be sent to the destination endpoint. The destination endpoint is now aware of the ports specified by the source endpoint for the media communication, these ports are opened, and the destination endpoint can now receive audio and video media over these UDP ports. The destination endpoint will send back an acknowledgment that the SDP information was received, followed by that endpoint's SDP information. The source endpoint will open the ports specified by the received SDP communication and return an acknowledgment to the destination endpoint, and the call will be set up.

As you can see, a lot of back-and-forth communication occurs when delayed offer is used. For this reason, early offer is the preferred method to use. The whole purpose of SIP is to simplify the data messages sent between two nodes. Figure 5-8 illustrates the SIP delayed offer call setup process.

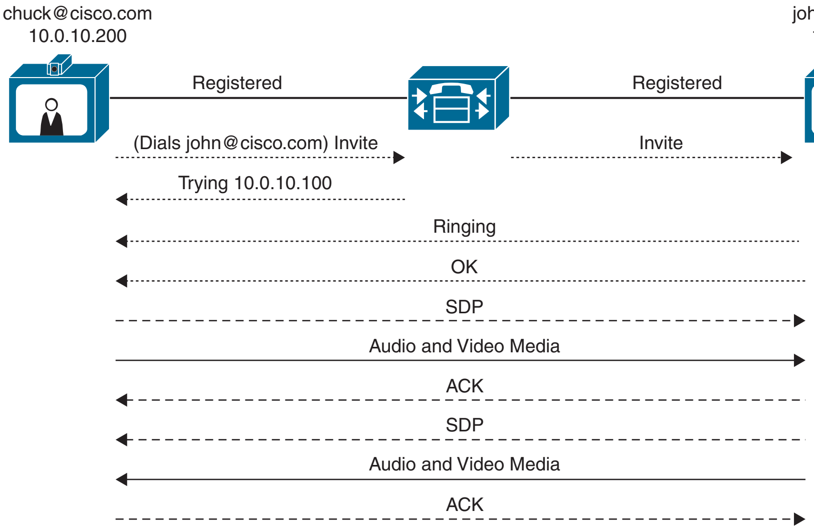


Figure 5-8 *SIP Delayed Offer Call Setup Process*

Early Offer

The big differentiator between delayed offer and early offer happens when the SDP information is sent. The SIP early offer begins when a source endpoint dials the destination alias using SIP, and an Invite message is sent to the SIP server along with the SDP information of the source endpoint. The SIP proxy function of the SIP server examines the table that is created by the SIP Registrar to determine the destination endpoint's IP address using the alias that is dialed. The SIP server will then proxy the Invite message with the SDP packets to the destination endpoint. At the same time the invite message is proxied, the SIP server will respond to the source endpoint with a Trying message. The Trying message contains the destination endpoint's IP information. After 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 will have the source and destination IP address information as well. The destination endpoint will then respond with two messages. The first message is the Ringing message, which 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 to the source endpoint. The OK message contains call connection status, acknowledgment that SDP information has been received, and the destination endpoint's SDP information. Since the destination endpoint is now aware of the ports specified by the source endpoint for the media communication, these ports are opened, and the destination endpoint can now receive audio and video media over these UDP ports. Once the source endpoint receives the OK message from the destination endpoint, the UDP ports that are specified from that communication will be opened so that audio and video media can be received from the destination endpoint. An acknowledgment will be sent to the destination endpoint and the call will be set up. Figure 5-9 illustrates the SIP early offer call setup process.

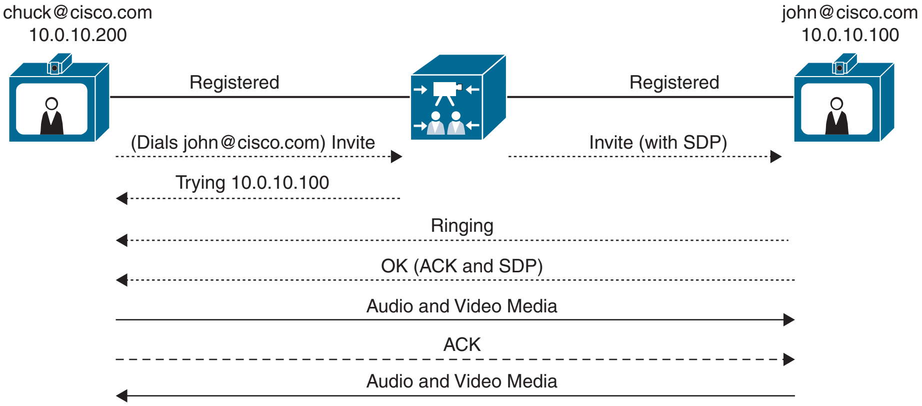


Figure 5-9 *SIP Early Offer Call Setup Process*

NAT and Firewall Traversal Solutions

Communication over IP has come a long way in a short time. One huge obstacle that had to be overcome before companies could really start migrating away from PSTN-based communication to IP-based communication was how to securely route network traffic through firewalls and across NAT servers.

The purpose of a firewall is to control IP traffic entering your network. Firewalls generally block unsolicited incoming requests, meaning that any communication originating from outside your network will be prevented. However, firewalls can be configured to allow outgoing requests to certain trusted destinations and to allow responses from those destinations. Allowing traffic in both directions prevents the firewall from doing its job. Therefore, a firewall exists to protect the inside of a corporate network from outside attack.

Most firewall ports are set to allow traffic to be sent from inside the network to an outside destination and accept a reply on the same port. This means that any communication must be started by an internal system. An example of this type of communication could be when a user within an enterprise network browses to Google.com from a web browser. A TCP communication is sent through the firewall, which marks the packets, and then forwards the request to the Google web server. When the Google server sends back the response, the firewall is already expecting this response, so the communication is allowed to come in and is redirected to the requesting application.

Key Topic

In a similar manner, a video call made from an endpoint inside a network through a firewall to an outside endpoint begins with a TCP communication. The firewall will allow the exchange of TCP call setup information and allow UDP media packets originating from an inside endpoint to be sent to an outside endpoint. However, the media traffic in the opposite direction does not come back on the same ports. The firewall observes these communication packets as originating from outside the network and blocks those packets from ever reaching the internal endpoint. This is a common issue, and it is referred to as *one-way audio* and *one-way video*. Notice also that to even get to this point, the call had to originate from inside the network. Inbound calls originating from outside the network are out of the question. Two endpoints located behind two different firewalls would never be able to call each other. The seeming resolution to this issue would be to open the ports needed for two-way communication, but this will not work for two reasons. First, opening the ports on the firewall will leave the network vulnerable to attacks from outside the network. This is never a good idea. Second, there is a second issue with NAT that could prevent endpoints from communicating with each other.

The Institute of Electrical and Electronics Engineers (IEEE) first introduced communication using packet-switched technology in 1974. They experimented with several Internet Protocol versions (IPv1-3) until the predominant protocol called IPv4 was established circa 1981. At that time, engineers couldn't 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 required an IP address greatly increased, and the World Wide Web began to expand, they 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, such as how to migrate hundreds of millions of devices that are already established under IPv4 over to an IPv6 network.

Another resolution that came about around the same time as IPv6 was Network Address Translation (NAT). The 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 Corporation 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, but are not routable across the public Internet. The ranges for private IP addresses are

Key Topic

- Class A addresses 10.0.0.0–10.255.255.255 have 16,777,216 available addresses.
- Class B addresses 172.16.0.0–172.31.255.255 have 1,048,576 available addresses.
- Class C addresses 192.168.0.0–192.168.255.255 have 65,536 available addresses.

Public IP addresses are routable across the public Internet and can be leased from an Internet service provider. Today different versions of NAT can be used based on many different factors. 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 routing return traffic that comes back from the desired destination. For example, if a computer assigned a private IP address of 10.10.1.14 tries to navigate to Google.com, the edge router will masquerade that private IP address with its assigned public IP address of 209.165.201.1:12345. When the Google server returns communication to the computer, return traffic goes to the public-facing port of the router, but the port :12345 tagged at the end of the IP address 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 sent from Google to the computer that initiated the communication. Similar to NAT is another protocol called Port Address Translation (PAT). Sometimes NAT and PAT can be used together.

NAT becomes an issue with collaboration devices for two reasons. First, NAT doesn't 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 wanted to communicate, one would never be able to discover the other. For example, if a device were to try routing 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 tried to route to the public IP address of the far-end router, after the packets arrived, the far-end router wouldn't know to which device the packets should be routed.

The second issue that comes with NAT has to do with User Datagram Protocol (UDP) 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. Since each UDP packet sent is essentially a new transmission, a different virtual port is used, and transmissions will never reach their targeted destination.

The IETF, which came up with the SIP communications protocol and NAT, also came up with the first solution that allowed communication between private networks through a NAT server. That protocol is known as STUN, which stands for Session Traversal Utilities for NAT. After creating the RFC for STUN, the IETF came up with two other RFC protocols known as TURN (Traversals Using Relays around NAT) and ICE (Interactive Connectivity Establishment).

STUN, TURN, and ICE are methods that assume certain behavior from the NAT/firewall and do not work in all scenarios. The control is removed from the firewall, which has to be sufficiently opened to allow users to create the pinholes needed to let the communication through. Therefore, STUN, TURN, and ICE offer only a NAT traversal solution and are not firewall traversal solutions at all. Also, these solutions can only operate within the SIP communications protocol, so they offer no solution for H.323 communications.

STUN

STUN requires a STUN client, which could be the phone or some other device, which sends packets to a STUN server on the Internet. The STUN server replies with information about the IP address and ports from which the packets were received and detects the type of NAT device through which the packets were sent. The STUN client can then use the public IP and assigned port in constructing its headers so that external contacts can reach the client without the need for any other device or technique. Once the STUN server assigns a port, it is no longer involved in the line of communication.

STUN requires that the NAT server allow all traffic that is directed to a particular port be forwarded to the client on the inside. This means that STUN works only with less-secure NATs, so-called full-cone NATs exposing the internal client to an attack from anyone who can capture the STUN traffic. STUN may be useful within asymmetric network environments but is generally not considered a viable solution for enterprise networks. In addition, STUN cannot be used with symmetric NATs. This may be a drawback in many situations because most enterprise-class firewalls are symmetric. For more information about STUN, see RFC 5389. Figure 5-10 illustrates how STUN works within a network.

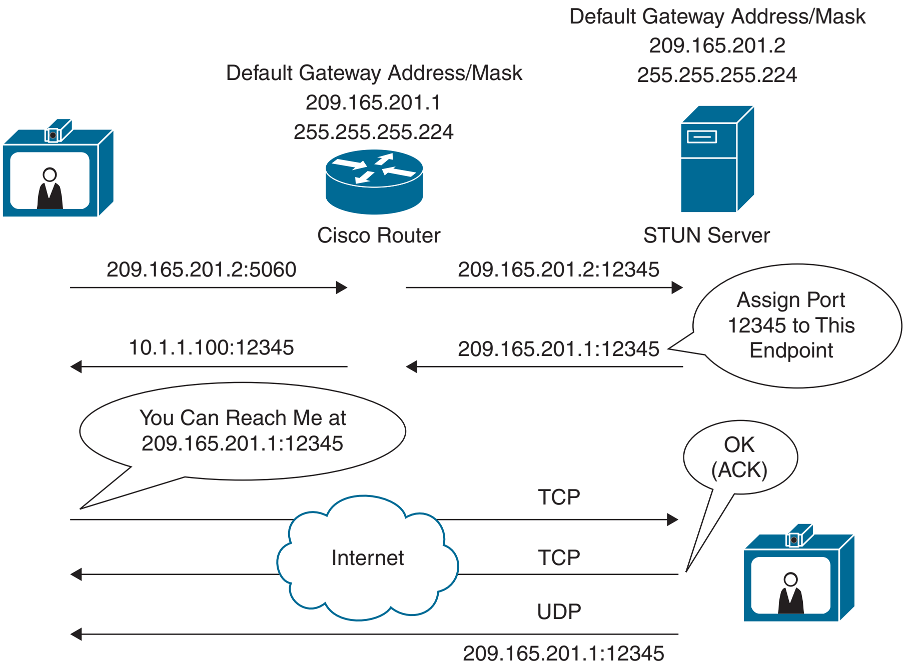


Figure 5-10 *STUN Operation Within an Asymmetric Network*

TURN

Key Topic

TURN operates similarly to STUN, but it allows an endpoint behind a firewall to receive SIP traffic on either TCP or UDP ports. This solves the problems of clients behind symmetric NATs, which cannot rely on STUN to solve the NAT traversal issue. TURN connects clients behind a NAT to a single peer. Its purpose is to provide the same protection as that created by symmetric NATs and firewalls. Symmetric NATs use dynamic ports that often change. Therefore, the TURN server acts as a relay so that any data received is forwarded on to the client, and port allocation can be updated on the fly. The client on the inside can also be on the receiving end, rather than the sending end, of a connection that is requested by a client on the outside.

This method is appropriate in some situations, but since it essentially allows inbound traffic through a firewall, with only the client in control, it has limited applicability for enterprise environments. It also scales poorly since the media must traverse through the TURN server. Also, since all media must traverse the TURN server, the server supporting TURN must be robust enough to handle high volumes of traffic. For more information about TURN, see RFC 5766. Figure 5-11 illustrates how TURN works within a network.

TURN relay services are the only IETF services available on the Expressway-E. To use TURN services, you need the TURN Relay option key. This controls the number of TURN relays that can be simultaneously allocated by the TURN server. The TURN page found under the **Configuration > Traversal > TURN** menu is used to configure the Expressway-E's TURN settings. Table 5-3 identifies the configurable options for TURN on the Cisco Expressway.

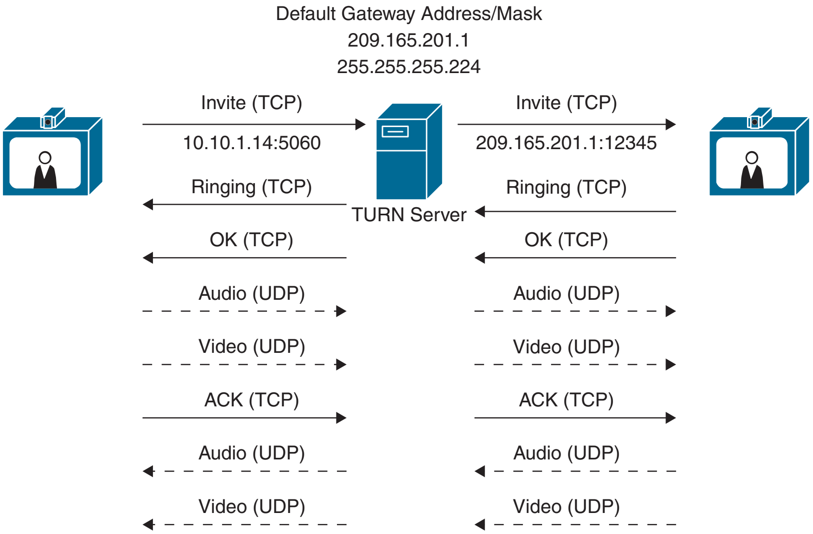


Figure 5-11 *TURN Operation Within a Symmetric Network*

Key Topic

Table 5-3 Configurable Options for TURN on the Cisco Expressway

Field	Description	Usage Tips
TURN Services	Determines whether the Expressway offers TURN Services to traversal clients.	
TURN Requests Port	The listening port for TURN requests. The default is 3478. On large VM deployments, you can configure a range of TURN request listening ports. The default range is 3478–3483.	To allow endpoints to discover TURN Services, you need to set up DNS SRV records for _turn._udp. and _turn._tcp. (either for the single port or a range of ports as appropriate). If you need to change the TURN requests port (or range, for large systems) while the TURN Services are already On, do the following: **1.** Change TURN Services to Off and click Save. **2.** Edit the port number/range. **3.** Change TURN Services to On and click Save. The reason is that changes to the port numbers do not take effect until the TURN Services are restarted.
Authentication Realm	This is the realm sent by the server in its authentication challenges.	Ensure that the client's credentials are stored in the local authentication database.

Field	Description	Usage Tips
Media Port Range Start/End	The lower and upper port in the range used for the allocation of TURN relays. The default TURN relay media port range is 24000–29999.	

A summary of the TURN server status is displayed at the bottom of the TURN page. When the TURN server is active, the summary also displays the number of active TURN clients and the number of active relays. Click the active relay links to access the TURN relay usage page, which lists all the currently active TURN relays on the Expressway. Further details of each TURN relay can be reviewed, including permissions, channel bindings, and counters.

ICE

ICE provides a mechanism for SIP client NAT traversal. ICE is not a protocol, but a framework that pulls together a number of different techniques such as TURN and STUN. It allows clients residing behind NAT devices to discover paths through which they can pass media, verify peer-to-peer connectivity via each of these paths, and then select the optimum media connection path. The available paths typically depend on any inbound and outbound connection restrictions that have been configured on the NAT device. Such behavior is described in RFC 4787. ICE essentially incorporates all of the methods proposed for NAT traversal of SIP that do not rely on the firewall or NAT device. ICE is a complex solution to the problem of NAT traversal, but because it encompasses multiple solutions, it is regarded as one that will always enable the connection, regardless of the number of NATs involved. However, ICE still relies on client/server-based approaches and removes control from the enterprise. Due to its complexity, there is very limited client support for ICE today.

When a client reaches out to the ICE server, it can determine what type of NAT is being used; whether it’s in an asymmetric or symmetric network environment. The ICE server will then establish a connection with the client using STUN or TURN, depending on what the situation calls for. If STUN is used, then the ICE server will assign a port to the client and step out of the line of communication. If TURN is used, then the ICE server will act as the relay between client communications. For more information about ICE, see RFC 5245. Figure 5-12 illustrates how ICE works within a network.

ASSENT and H.460

Although the IETF overcame many problems, there were still many more to overcome. Their solutions, although good, were incomplete. Tandberg was a company that had been a leader in video telepresence for many years prior to its acquisition by Cisco. Tandberg climbed this ladder to success much the same way as Cisco, by acquiring key companies that possessed the technology it needed for the time. In 2004 Tandberg acquired Ridgeway Systems and Software, which was a UK-based software company specializing in firewall and NAT traversal. Ridgeway had developed a unique proprietary solution that is known today as Assent. This protocol has revolutionized the way IP communication traverses firewalls and NATs and has become the standard the ITU followed for an open standard all companies can use.

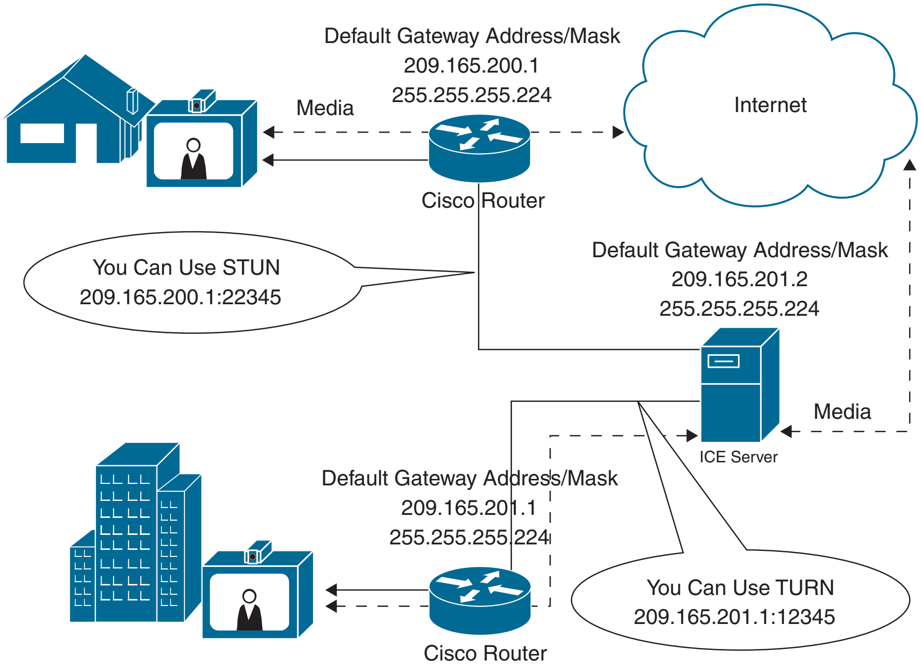


Figure 5-12 *ICE Operation Within Asymmetric and Symmetric Networks*

Key Topic

Assent requires two components to work: 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 was initiated from inside the firewall with the keepalive message. Now the ports allocated to this solution can be used after 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 RTP traffic uses one port and all RTCP traffic uses a second port. In addition to the firewall traversal capabilities of Assent, NAT traversal is built into the protocol as well. Also, Assent can be used with both the SIP and H.323 communication standards.

Key Topic

Assent is such a powerful tool that the ITU used it as the basis to develop H.323 Traversal standards. By the summer of 2005, the standards were completed and in full use. H.460.17 was the traversal standard used prior to the Assent-based standards. 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 requires demultiplexed ports 50000 to 52400 to be opened on the firewall. H.460.19 works as a layer on H.460.18 to allow multiplexing 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. It is important to note that the ITU standards for firewall traversal only support the H.323 communication standard.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 5-4 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 5-4 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
Paragraph	TDM	88
Paragraph	BRI	89
Paragraph	PRI	89
Table 5-2	Minimum Standards for H.320 Compliance	91
Paragraph	Minimum Standards for H.323 Compliance	91
Paragraph	H.323 Aliases	91
Paragraph	Q.931 and H.245	93
Paragraph	H.323 Call Setup with RAS Messaging	94
Paragraph	Functions of SIP Server	95
List	CUCM Registration Process for SIP	96
List	Expressway Registration Process for SIP	98
Paragraph	Differentiator Between Early Offer and Delayed Offer	99
Paragraph	Firewall Dilemma	102
List	Private IP Address Classes	103
Paragraph	NAT Dilemma	104
Section	STUN	104
Section	TURN	105
Table 5-3	Configurable Options for TURN on the Cisco Expressway	106
Section	ICE	107
Paragraph	Assent Operation for H.323 and SIP	108
Paragraph	H.460 Operation for H.323	108

Define Key Terms

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

Assent, BRI, CAC, Call Setup Mode, CDP, CTL, DHCP, Discovery Mode, E.164 Alias, Firewall, FQDN, Gatekeeper, GRQ, H.239, H.245, H.320, H.323, H.323 ID, H.460.17, H.460.18, H.460.19, HTTP, ICANN, ICE, IEEE, IETF, ITU, LLDP-MED, NAT, Option 150, PAT, Prefix, PRI, Q.931, RAS, RFC, RIP, RRQ, SCCP, SDP, SIP, SIP Proxy, SIP Registrar, SIP Server, STUN, TCP, TDM, TFTP, TURN, UDP

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the two main types of ISDN with the channels supported, carrier types, and bandwidth supported on each channel.
2. List and define the three types of aliases that can be used with H.323 registered endpoints.
3. What are the nine steps in the SIP registration process to a CUCM?
4. List the three IETF NAT traversal solutions, the Cisco firewall, and NAT traversal solution and the three ITU firewall and NAT traversal solutions.

This page intentionally left blank

CHAPTER 6

Cisco Solution for Converged Collaboration

This chapter covers the following topics:

Introduction to Cisco Endpoints: This topic will introduce the various Cisco voice and video endpoints available on the market today, including UC phones, soft clients, and Telepresence endpoints.

Introduction to Cisco Call Control: This topic will introduce the Cisco infrastructure that can be used for call control in a Collaboration solution, including the Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco Expressways, and Webex Control Hub.

Introduction to Cisco Applications: This topic will introduce common Cisco infrastructure applications that enhance the user experience in a collaboration deployment, including Cisco Unity Connection Server, Cisco IM and Presence Service, Cisco Meeting Server, and Management software.

Designing a Cisco Collaboration Solution: This topic will overview the various aspects to designing a Cisco Collaboration solution, including licensing, sizing, bandwidth management, high availability, disaster recovery, dial plan, security, and quality of service.

Establishing a foundation for audio and video communication up to this point has been important. We will revisit key information shared through the first five chapters of this book throughout the rest of the chapters ahead. This chapter, as well as the rest of this book, will focus on specific products in the Cisco Collaboration product portfolio. This chapter will not cover an exhaustive list of all Cisco Collaboration products, and not every product mentioned in this chapter will be covered in later chapters. The purpose of this chapter is merely to provide a high-level overview of the main components available in a Cisco Collaboration solution. Topics discussed in this chapter include the following:

- Introduction to Cisco Endpoints
  - UC Phones
  - Soft Clients
  - Telepresence Endpoints
- Introduction to Cisco Call Control
  - Cisco Unified Communications Manager
  - Cisco Unified Communications Manager Express

    - Cisco Expressways
    - Webex Control Hub
- Introduction to Cisco Applications
    - Cisco Unity Connection Server
    - Cisco IM and Presence Service
    - Cisco Meeting Server
    - Management Software
- Designing a Cisco Collaboration Solution
    - Licensing
    - Sizing
    - Bandwidth
    - High Availability
    - Disaster Recovery
    - Dial Plan
    - Security
    - QoS

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

1.1 Describe the Cisco on-premises, hybrid, and cloud collaboration solution design elements described in the SRND/PA:

- 1.1.a Licensing (Smart, Flex)

1.3 Configure these network components to support Cisco Collaboration solutions:

- 1.3.a DHCP
- 1.3.b NTP
- 1.3.c CDP
- 1.3.d LLDP
- 1.3.e LDAP
- 1.3.f TFTP
- 1.3.g Certificates

1.6 Describe Webex Control Hub Features

2.5 Describe SIP OAuth on Cisco UCM

"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
Introduction to Cisco Endpoints	1–2
Introduction to Call Control	3–6
Introduction to Cisco Applications	7–9
Designing a Cisco Collaboration Solution	10–14

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 soft clients does Cisco offer in its current product portfolio? (Choose three.)
   a. Jabber Client
   b. Jabber Video for Telepresence
   c. Webex (Meet, Team, Call)
   d. CMS
   e. WebRTC
   f. CMA
2. Which of the following Cisco Telepresence endpoint category markings is used for personal endpoints?
   a. DX
   b. MX
   c. SX
   d. IX
   e. Webex endpoint
3. What is the maximum number of DHCP addresses that can be delivered and managed by a CUCM?
   a. 10
   b. 100
   c. 1000
   d. 10,000

4. What is the maximum user capacity on the Cisco Unified Communications Manager Express?
   a. 150
   b. 250
   c. 350
   d. 450
5. What is the primary difference between a Cisco VCS and a Cisco Expressway Server?
   a. Cisco VCS has user-based licenses, but an Expressway has device-based licenses.
   b. Cisco VCS has device-based licenses, but an Expressway has user-based licenses.
   c. VCS is used autonomously, and the Expressway is used with CUCM exclusively.
   d. VCS is used exclusively with the CUCM, and the Expressway is autonomously.
6. Which Webex tool can be used to call into a Webex Meeting?
   a. Webex Meeting application
   b. Webex Teams application
   c. Webex Calling application
   d. All the above
7. Which of the following applications can offer voicemail services to UC phones? (Choose two.)
   a. CUCCE
   b. CUCCX
   c. CUC
   d. CUE
   e. IMP
   f. CUCM
   g. CMS
   h. Expressway
8. Which of the following is a service offered through CMS?
   a. Voicemail integration
   b. Manual creation of users
   c. Microsoft Skype for Business Integration
   d. Direct endpoint registration to the server
9. Which of the following management tools allows conference meetings to be scheduled?
   a. Telepresence Management Suite
   b. Prime Collaboration Provisioning
   c. Prime Collaboration Assurance
   d. Prime Collaboration Analytics
   e. Telepresence Management Suite and Prime Collaboration Provisioning

10. Which of the following options is included with a CUCL Enhanced license?
    a. Unity Connection
    b. Expressway Firewall Traversal
    c. PMP Basic
    d. Webex Conferencing
11. How many endpoints can a BE6000H server that is running CUCM support?
    a. 1000
    b. 1200
    c. 2500
    d. 5000
12. What is the maximum number of peers supported in an Expressway Cluster?
    a. 4
    b. 6
    c. 8
    d. 10
13. What protocol is used to secure SIP signaling across the CUCM?
    a. HTTPS
    b. SSL
    c. TLS
    d. AES128
14. What is Layer 2 QoS called?
    a. Cost of service
    b. Class of service
    c. DiffServ
    d. IntServ

Foundation Topics

Introduction to Cisco Endpoints

Cisco has spent the last several years restructuring its Collaboration endpoint portfolio to bring out a line of endpoints that offer cutting-edge technology in a sleek design at a reasonable price. All Cisco Collaboration endpoints can be divided into two main categories: Unified Communications (UC) endpoints and Telepresence endpoints. Some UC endpoints are voice-only, and others support high-definition (HD) video. Some of the soft clients available fall into the UC category as well. All Telepresence endpoints are HD video-capable and offer more features for the end user. The Cisco Unified Communications Manager treats these two types of collaboration endpoints differently in regard to QoS.

UC Phones

Cisco voice over IP (VoIP) phones are user-friendly and full-featured to meet the needs of entire organizations. They range from a company lobby phone to the desks of the busiest managers and C-level employees. Cisco's VoIP phones provide all the features companies use from their office desk phones, such as speakerphone, transfer, hold, and voicemail access, as well as interactive video collaboration and the capability for a PC to use the same network connection as the phone. Some different models support Bluetooth, USB, Wi-Fi, and other advanced features. Some phones have a built-in camera with HD capabilities. Each phone connects back to the Cisco UCM using the Session Initiation Protocol (SIP) and comes equipped for Power over Ethernet (PoE), which can be supplied by many Cisco switches. Alternatively, a power supply can be used in conjunction with the phone. Cisco has narrowed its VoIP phone product portfolio to three categories of phones: the 6800 series, 7800 series, and 8800 series phones.

Soft Clients

Key Topic

Although the Cisco Jabber client is another product in the Cisco UC phone category, Cisco has announced the end of life for Jabber. Software maintenance and support ended July 31, 2023, but the product can continue to be used and even upgraded to the latest version, 12.7. Cisco recommends companies that use Jabber currently migrate to the Webex app instead. The Webex app will register to the Cisco Unified Communications Manager and support presence, messaging, meeting, and calling, just as Jabber does. No changes need to be made to the on-premises calling solution when switching apps.

The Jabber software phone or Webex app can be installed on any Microsoft Windows or Apple Mac computer. An app version is also available on Android and Apple IOS devices, including phones and tablets. The Jabber client phone or Webex app can be configured in the Cisco Unified Communications Manager using the Cisco Unified Client Services Framework (CSF) for PC clients. These two client applications provide instant messaging (IM), presence, voice and video communication, voice messaging, desktop sharing, and other collaborative workspace capabilities that support 1080p30 high-definition video interoperability. The CPU must be Intel Core i5 or later, with a bandwidth of between 2 and 4 Mbps, and the client must be running version 12.6 or later. The Cisco Jabber client uses the Cisco Precision Video Engine and ClearPath technology to optimize video media. The Cisco Precision Video Engine uses fast video-rate adaptation to negotiate optimum video quality, based on network conditions. Similar technologies exist in the Webex client as well. These clients can be used on premises or through a Hosted Collaboration Solution (HCS) in the cloud. No matter what platform you choose to operate this client from, Cisco Jabber clients and the Webex app provide a consistent experience across devices.

Cisco Unified Client Services Framework is a software application that combines several services into an integrated client. An underlying framework is provided for integration of Cisco UC services, including audio, video, web collaboration, visual voicemail, and more, into an IM and Presence application. As mentioned previously, Cisco Jabber is based on the Cisco Unified Client Services Framework and combines advanced collaborative media features with Cisco UC. Cisco Jabber uses SIP for call control, XMPP for IM and Presence, and Computer Telephony Integration (CTI) for desktop IP phone control. You can use CTI to take advantage of computer-processing functions while making, receiving, and managing telephone calls. CTI applications allow you to perform such tasks as retrieving customer information from a database using a caller ID, or working with the information gathered by an interactive voice response (IVR) system to route a customer's call, along with that caller's information, to the appropriate customer service representative.

Key Topic

Cisco Jabber operates in one of two modes: deskphone mode or softphone mode. In deskphone mode, the Cisco Jabber client controls the Cisco IP phone of the user. Should a call be placed from the Jabber soft client, the video phone connected will actually launch the call and use its own resources for audio and video. The same thing is true for answering incoming calls using Jabber in deskphone mode. For an IP phone without a camera, the video input and output are processed on the Cisco Jabber client platform, but the voice input and output are processed on the IP phone. A protocol known as Cisco Audio Session Tunnel (CAST) is used to split the audio and video media between the two destinations. In softphone mode, the Cisco Jabber client behaves like any other IP phone and originates and terminates all audio and video communication interactions using the computer resources upon which it is running.

The Cisco Meeting Application, or CMA, is another soft client application that can run on a computer, smartphone, or tablet. CMA is built on the WebRTC protocol and is dependent on the Cisco Meeting Server, or CMS. CMA is capable of audio-only calling, HD video calling, and instant messaging. Through proper integrations configured on the Cisco Meeting Server, CMA is completely interoperable with Microsoft Skype for Business. Cisco is no longer developing CMA, but development and support of WebRTC will continue. Cisco has been bolstering the Cisco Jabber application to replace CMA. For more information on these added capabilities to Jabber, see Chapter 26, "Webex Calling Using a Local Gateway."

Key Topic

The Webex app is a cloud-based application that can be installed as an application on a computer, smartphone, or tablet. Originally, the Webex app was called Cisco Spark, but Cisco decided to combine Spark and Webex into a single and more powerful cloud-based solution to bring more control and capabilities into the hands of users. Cisco Spark was then renamed Webex Teams and supported both messaging and calling. Cisco later incorporated a new calling solution into Webex, which meant there were three now different Webex applications: Webex Meetings, Webex Calling, and Webex Teams. In an effort to consolidate and simplify how users consume Webex, Cisco eventually came out with one app to rule them all, which we know today as the Webex app. This new Webex application supports persistent group and point-to-point messaging, is capable of voice and video calling, and can be used to schedule and join meetings.

Telepresence Endpoints

The categorization of Cisco Telepresence endpoints has changed many times over the years Cisco has been developing these products. Currently, Cisco Telepresence endpoints are divided into four categories. The Webex Room Kit Series endpoints are intended for integrators to customize meeting rooms for businesses. The Webex Room Series endpoints are Meeting Experience endpoints and are all-in-one meeting room solutions that don't require room remediation or integration. These endpoints offer a simple plug-and-play setup that anyone can accomplish. The Webex Board Series endpoints are exactly the same as the Webex Room Series, with one extra capability. The Webex Board has an annotation function that allows whiteboarding capabilities. This feature can be used whether you are in a meeting or not. Users can draw on a blank canvas or annotate over a projected graphic. The Webex Desk Series endpoints are Desktop Experience endpoints that offer a more personal user experience during meetings. All of these endpoints share a common base code known as Cisco Telepresence Collaboration Endpoint (CE) software; therefore, no matter what endpoint is used within an enterprise solution, configuration of each endpoint and the user experience are the same.

Table 6-2 outlines all of the current endpoints in each of these categories.

Key Topic

Table 6-2 Cisco Telepresence Endpoint Product Portfolio

Webex Desk	Webex Room	Webex Room Kit	Webex Board
Webex Desk Mini	Webex Room 55 Single	Webex Room Kit USB	Webex Board 55
Webex Desk	Webex Room 55 Dual	Webex Room Kit Mini	Webex Board 70
Webex Desk Pro	Webex Room 70 Single G2	Webex Room Kit	Webex Board 85
Webex Desk Camera	Webex Room 70 Dual G2	Webex Room Kit Plus	Webex Board Pro
Webex Desk Hub	Webex Room Panorama	Webex Room Kit Plus P60	
		Webex Room Kit Pro	
		Webex Room Kit Pro P60	

Introduction to Cisco Call Control

What good are all these endpoints without a call control system to register to? The Cisco Collaboration solution is a complete end-to-end solution. Cisco is the only solution on the market today that can offer all the switching and routing needs, along with the call control and premium endpoints to connect users regardless of their location. Just as the endpoint portfolio is robust enough to meet the needs of any size company, the Collaboration infrastructure also is a robust and extensive solution with many facets to suit the needs of any customer. On-premises solutions offer call control through the Cisco Unified Communications Manager, the Cisco Expressway series, and the Cisco Unified Communications Manager Express (CME). The on-premises deployment can be extended with additional supporting infrastructure. Unity Connection provides unified messaging services to remote and on-premises endpoints through the Cisco Unified Communications Manager. Unity Express is a unified messaging service that runs on the Cisco Integrated Services Routers (ISRs). The Cisco Unified Communications Manager IM and Presence Service provide native standards-based, dual-protocol, enterprise instant messaging and network-based presence as part of Cisco Unified Communications. For small to medium-sized businesses, Cisco offers subscription-based cloud call control and services. Through partners of Cisco, customers can choose a Hosted Collaboration Solution (HCS), which offers the same on-premises products outlined previously, except hosted in the cloud. Alternatively, Cisco has the Cisco Webex Cloud solution, which supports calling, meeting, and messaging capabilities, all hosted and managed from the cloud. Webex can also be integrated in a hybrid deployment with the Cisco Unified Communications Manager.

Cisco Unified Communications Manager

Cisco Unified Communications Manager extends enterprise telephony features and functions to packet telephony network devices. These packet telephony network devices include Cisco IP phones, media-processing devices, VoIP gateways, and multimedia applications. Additional data, voice, and video services, such as converged messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact with the IP telephony solution through the Cisco Unified Communications Manager API. Cisco Unified Communications Manager provides call processing. Call processing refers to the complete process of routing, originating, and terminating calls, including any billing and statistical collection processes. Cisco Unified Communications Manager sets up all the signaling connections between endpoints and directs devices such as phones, gateways, and conference bridges to establish and tear down streaming connections. The dial plan is a set of configurable lists that Cisco Unified Communications Manager uses to determine call routing. Cisco Unified Communications Manager provides the ability to create scalable dial plans for users. Cisco Unified Communications Manager also extends services such as hold, transfer, forward, conference, speed dial, last-number redial, call park, and other features to IP phones and gateways. Cisco Unified Communications Manager uses its own database to store user information. You can authenticate users either locally or against an external directory. You also can provision users by directory synchronization. With directory synchronization, you can automatically add users from the directory to the local database. Cisco Unified Communications Manager allows synchronization from the following directories to the database:

- Microsoft Active Directory 2003 R1/R2(32-bit)
- Microsoft Active Directory 2008 R1(32-bit)/R2(64-bit)
- Microsoft Active Directory Application Mode 2003 R1/R2 (32-bit)
- Microsoft Active Directory 2012
- Microsoft Lightweight Directory Services 2008 R1(32-bit)/R2(64-bit)
- Microsoft Lightweight Directory Services 2012
- Sun ONE Directory Server 7.0
- OpenLDAP 2.3.39
- OpenLDAP 2.4
- Oracle Directory Server Enterprise Edition 11gR1

Cisco Unified Communications Manager provides a programming interface to external applications such as Cisco Jabber, Cisco Unified IP IVR, Cisco Personal Assistant, and Cisco Unified Communications Manager Attendant Console.

Cisco Unified Communications Manager uses different signaling protocols to communicate with Cisco IP phones for call setup and maintenance tasks, including SIP, SCCP, or even H.323 gateway services. When a calling endpoint dials the number of a called endpoint, dialed digits are sent to Cisco Unified Communications Manager, which performs its main function of call processing. Cisco Unified Communications Manager finds the IP address of the called endpoint and determines where to route the call. Using SCCP or SIP, Cisco Unified Communications Manager checks the current status of the called party. If Cisco Unified Communications Manager is ready to accept the call, it sends the called party details and signals, via ring back, to the calling party to indicate that the destination is ringing. Cisco IP phones require no further communication with Cisco Unified Communications Manager until either the calling or called endpoint invokes a feature, such as call transfer, call conferencing, or call termination. After the call setup is finished, media exchange normally occurs directly between Cisco IP phones using RTP to carry the audio and potentially video stream.

Cisco Unified Communications Manager depends on some additional network elements. In particular, the Cisco Unified Communications Manager cluster uses external NTP and DNS servers plus DHCP and TFTP services that are used by the endpoints. NTP is a protocol for synchronizing computer system clocks over IP networks. NTP has a hierarchical organization that is based on clock strata. Stratum 0 is an extremely precise clock source, such as an atomic clock or radio clock. A stratum 1 server is directly connected to a stratum 0 clock and can provide time information to other (stratum 2) devices, which in turn serve stratum 3 devices. Cisco Unified Communications Manager typically uses stratum 1 NTP to obtain time information from a time server. Only the publisher sends NTP requests to the external NTP server or servers. Subscribers synchronize their time with the publisher. NTP must be enabled and configured during installation of Cisco Unified Communications Manager. At least one external NTP reference must be reachable and functioning when installing the Cisco Unified Communications Manager publisher to complete the installation. Cisco recommends using a minimum of three external NTP servers in a production environment.

It is extremely important that all network devices have accurate time information because the system time of Cisco Unified Communications Manager is relevant in the following situations:

- Cisco IP phones display date and time information. This information is obtained from the device pool on the Cisco Unified Communications Manager.
- CDR and CMR, which are used for call reporting, analysis, and billing, include date and time information.
- Alarms and events in log files, as well as trace information in trace files, include time information. Troubleshooting a problem requires correlation of information that is created by different system components (Cisco Unified Communications Manager, Cisco IOS gateway, and so on). This problem solving is possible only if all devices in the network have the same correct time information.
- Some Cisco Unified Communications Manager features are date-based or time-based and therefore rely on the correct date and time. These features include time-of-day routing and certificate-based security features.

To ensure that all network devices have the correct date and time, it is recommended that all network devices use NTP for time synchronization.

The Cisco Unified Communications Manager DHCP server is designed to serve IP phones in small deployments with a maximum of 1000 devices. It provides a subset of Windows, Linux, or Cisco IOS DHCP server functionality that is sufficient for IP phones, but it should not be used for other network devices, such as PCs. The DHCP server of Cisco Unified Communications Manager must not be used with deployments of more than 1000 registered devices. Even if there are fewer devices, the CPU load of the services must be watched closely. If high CPU load is experienced, the DHCP service should be provided by other devices, such as a dedicated DHCP server, switch, router, or another server. Multiple DHCP services can be configured per Cisco Unified Communications Manager cluster. Each Cisco Unified Communications Manager DHCP server can be configured with multiple subnets. In nonattached subnets, DHCP relay must be enabled so that the DHCP requests that were sent out by the clients are forwarded to the DHCP server.

Cisco Unified Communications Manager can use IP addresses or names to refer to other IP devices in application settings. When names are used, they need to be resolved to IP addresses by DNS. Both methods have some advantages. The system does not depend on a DNS server, which prevents loss of service when the DNS server cannot be reached. When a device initiates a connection for the first time, the time that is required to establish the connection is shorter because a DNS lookup sent to the DNS server and a DNS reply sent back from the server are not required. By eliminating the need for DNS, there is no danger of errors caused by DNS misconfiguration. Troubleshooting is simplified because there is no need to verify proper name resolution.

When DNS is used, management is simplified because logical names are simpler to manage than 32-bit addresses. If IP addresses change, there is no need to modify the application settings because they can still use the same names; only the DNS server configuration has to be modified in this case. IP addresses of Cisco Unified Communications Manager servers can be translated toward IP phones because the IP phone configuration files include server names, not the original server IP address, which should appear differently to the IP phone. As long as these names are resolved to the correct address when IP phones send out DNS requests, the NAT is not a problem. If certificates are being used to secure the communications environment, DNS will be required because the DNS FQDN is an integral part of certificates. Although historically Cisco has recommended that DNS not be used, with the increasing need for secure connections, it is best practice to use DNS throughout a Cisco Collaboration environment.

The Cisco Unified Communications Manager is a very powerful tool with many call features to offer to companies of any size. Volumes of books have been dedicated to the many facets the Cisco Unified Communications Manager has to offer. Chapters 15 through 19 of this book will delve into these features, including initial setup considerations, LDAP integrations, registration methods, CAC, and globalized call routing through the Cisco Unified Communications Manager.

Cisco Unified Communications Manager Express

Cisco Unified Communications Manager Express (CME) provides call processing to Cisco Unified IP phones for distributed enterprise branch-office environments. Even branch offices within the same enterprise can have different needs and requirements when it comes to unified communications. Cisco Unified CME delivers on this need by providing localized call control, mobility, and conferencing alongside data applications on Cisco Integrated Services Routers (ISRs). Because the solution is Cisco IOS software-based, Cisco Unified CME is easy to configure and can be tailored to individual site needs. It is feature-rich and can be combined with Cisco Unity Express and other services on the Cisco ISR to provide an all-in-one branch-office solution that saves valuable real estate space. Cisco Unified CME is ideal if you are looking for an integrated, reliable, feature-rich unified communications system for up to 450 users.

Cisco Expressway

The Cisco Expressway Series call control components are based on the Cisco Telepresence Video Communication Server (VCS). In April 2010, Cisco closed on the acquisition of a company called Tandberg, which had a call control solution called the VCS. This call control system is different from the Cisco Unified Communications Manager in many ways; namely, the VCS provides call control only for video devices, whereas the Cisco Unified Communications Manager provides call control for both voice and video endpoints. However, the VCS solution possesses a capability that does not exist in the Cisco Unified Communications Manager. The VCS is capable of true firewall and NAT traversal between the internal network and the public Internet. In an effort to capitalize on this capability, Cisco released the Expressway series that is built on the same operating system (OS) as the VCS. The difference was that endpoints could not register directly to the Expressway series servers. The Expressway series existed to secure proxy registration requests from endpoints outside of the corporate network to the Cisco Unified Communications Manager inside the network without the use of a VPN. This function is known as Mobile and Remote Access (MRA).

Key Topic

In August 2016, Cisco announced that the Expressway series servers would support device registration directly to the Expressway with appropriate licenses. At this point, this announcement confused a lot of people as to what the distinction was between an Expressway and a VCS. The menus were already identical, and the only distinction before was the registration capabilities. This is still the distinction between these two servers. Although registration is allowed on both products, the Cisco VCS allows for device-based licensing, whereas the Expressway allows for user-based licensing. Endpoints can register directly to the Cisco VCS Control or the Cisco VCS Expressway via SIP or H.323. The Expressway Core and Expressway Edge can now also support endpoint registrations directly via SIP or H.323, but the Expressway Edge can also proxy registration requests to the Expressway Core or the Cisco Unified Communications Manager. However, it can only proxy SIP registration requests, not H.323. Table 6-3 compares the differences between the Cisco Expressway and the Cisco VCS.

Key Topic

Table 6-3 Comparison of the Cisco Expressway and the Cisco VCS

Feature	Cisco Expressway	Cisco VCS
Server Components	Expressway Core Expressway Edge	VCS Control VCS Expressway
Registration Licensing	Included with CUCL and CUWL user licenses (Registration supported on X8.9 or later)	Device Registration Licenses required (2500 max per server)
Call Licensing	Internal and mobile calling included Rich Media Session (RMS) Licenses required for B2B and B2C calling	Nontraversal Call Licenses required Traversal Call Licenses required
Microsoft Interop License	Requires RMS licenses	Requires Option Key
FindMe License	Available	Requires Option Key
Device Provisioning License	Requires Option Key (Free)	Requires Option Key (Free)
Clustering Capabilities	Up to 6 servers	Up to 6 servers

I do not know what Cisco's future plans are for these products. At the time this book was written, Cisco had not announced any plans to make either of these products end of sale, and they are both marketed as viable solutions for customers.

Webex Control Hub

Cisco has a cloud-based call control solution for customers as well. Webex by Cisco is a multifaceted cloud-based solution that warrants a deeper explanation on each of the Webex solutions Cisco has to offer. The Cisco Webex solution can be divided into three categories: meeting, messaging, and calling.

Webex Meetings is the same powerful tool that has been used for years to allow multipoint conferencing in the cloud. Participants can join via the Webex app, through a browser, or by using a phone or Telepresence endpoint. All the same tools that have traditionally been used with Webex Meetings are still available; plus, Cisco has added a few more enhancements. Webex Meetings allows for high-quality voice and HD video communication, content sharing, polling, annotation, and many more supported features. Webex Meetings is a full cloud platform, but it can be extended to a hybrid meeting deployment using the Video Mesh Node.

Webex messaging allows for point-to-point messaging or group messaging in Spaces. This highly secure messaging solution allows conversations to be escalated to a voice or video meeting where content can be shared, and a whiteboard application can be leveraged. All whiteboard notations can be saved into a Webex Space so that collaboration can continue after the meeting ends. Webex messaging also supports the uploading and downloading of documents, and many other integrations and bots can be leveraged through this application.

Webex Calling is a tool that has always been available with the Webex solution since the inception of Spark; however, since Cisco acquired BroadSoft, it has worked diligently to bring the BroadSoft calling features into Webex. Webex Calling allows certain phones to register to the Webex Control Hub, and from those phones, users can call out over IP or through the public switched telephone network (PSTN). Alternatively, the Webex application can be used from any Windows or Mac computer, tablet, or smartphone. Additionally, this newer Webex Calling solution offers many more calling features than were previously available with Spark Calling.

The Webex Control Hub is the centralized, cloud-based management tool for all Cisco Webex-related products. Calling features, such as endpoint and phone registration, and voicemail, are all managed through the Webex Control Hub. Users are also managed from here. Users can be imported through an LDAP integration, and single sign-on can be set up as well. User privileges can be assigned as needed, including additional administrators and security compliance officers. All Webex meeting, messaging, and calling features can be configured and managed on an individual basis, based on location, or as an organization as a whole. Many different hybrid integrations are available between an on-premises deployment of Cisco Collaboration and the Webex cloud, which are all initiated through the Webex Control Hub. The following list is a summation of the hybrid integrations available with Webex at the writing of this book:

- **Hybrid Directory Service:** Simplify the administrative experience by automatically synchronizing Microsoft Active Directory users with Webex user management (creating, updating, and deleting) so that users are always current in Webex. This requires Cisco Directory Connector installation.

- **Hybrid Calendar Service:** Integrate your Microsoft Exchange, Office 365, or Google Calendar with Webex capabilities. Hybrid Calendar Service makes it easier to schedule meetings, especially from a mobile device. Depending on which calendar you are integrating, this may require a Calendar Connector installation.
- **Hybrid Calling for Webex Devices:** Hybrid Calling for Webex Devices provides hybrid call functionality for Room, Desk, and Cisco Webex Board devices that are added to Workspaces or associated with users in Control Hub. Webex devices are registered to the cloud, and when they are enabled with Hybrid Calling, they also connect to the enterprise. Webex devices in the Workspace become a part of your existing on-premises dial plan, allowing these devices to call user extensions or the PSTN and to receive incoming calls.
- **Webex Video Mesh:** The Webex Video Mesh node is media processing software installed on a Cisco Unified Computing System (UCS) server that registers and is managed by the Control Hub. It allows local Webex meeting participants to use the local media resource for processing participant streams to lower latency and provide bandwidth savings. Webex Video Mesh will choose the best resource for the participant based on node placement and call volume.
- **Hybrid Data Security:** By default, all Webex customers get end-to-end encryption with dynamic keys stored in the cloud Key Management Service (KMS), Cisco's security realm. Hybrid Data Security moves the KMS and other security-related functions to your enterprise data center so that nobody but you holds the keys to your encrypted content.
- **Hybrid Message Service:** Hybrid Message Service enables exchange of one-to-one instant messages between the Cisco Webex app client and the Cisco Jabber client registered to the Unified Communications Manager IM and Presence service. Hybrid Message Service enables Cisco Jabber users to see the presence status of Cisco Webex users based on their Webex app activity.
- **Groups Integration:** When you create a team in the Webex app, you can automatically create and connect the team to a Microsoft 365 group. You can then manage people in the team from Microsoft 365 and use Microsoft SharePoint folders to save your files.
- **Serviceability Service:** You can ease the collection of logs with the Webex Serviceability Service, which automates the tasks of finding, retrieving, and storing diagnostic logs and information. The service also triggers analysis against diagnostic signatures so that TAC (Technical Assistance Center) can identify problems and resolve cases faster. This capability uses the *Serviceability Connector* deployed on-premises. When you open a case with TAC, TAC engineers can retrieve relevant logs as they perform the diagnosis of the problem. TAC can collect the needed logs without coming back to you each time.
- **Video integration (with Microsoft Teams):** This integration enables your video devices to join Microsoft Teams meetings. The integration applies to Webex devices and other SIP-capable video devices, whether they register to Webex or to your on-premises infrastructure.

- **Webex Monitoring Service:** You can collect baseline data on your organization's network when using Webex services with the Webex Monitoring Service. The data can help you troubleshoot issues that your users run into, such as identifying if a low-quality meeting is caused by a network problem.

One last capability of the Webex Control Hub worth mentioning is the many analytics and troubleshooting tools. They allow administrators to track, manage, and control the Cisco cloud collaboration solution. Cisco Webex is not just for small and medium-sized businesses; it is for any sized business that wants to extend and enhance its global collaboration efforts.

Introduction to Cisco Applications

UC applications are used to unify your voice, video, data, and mobile applications for collaboration within the Cisco Collaboration solutions. Applications include communication gateways, voicemail, and unified IM and Presence services. Other customer collaboration applications, which will not be discussed in this book beyond this chapter, are used to create the foundation for strong customer relationships. These products include contact center and voice self-service products. Media service applications are used to enable collaboration anywhere with more security and high-quality integrated voice, video, and content sharing. These applications include video conferencing products, web conferencing applications, and conferencing management tools.

Cisco Unity Connection Server

Cisco Unity Connection (CUC) is a robust unified messaging and voicemail solution that accelerates collaboration by providing users with flexible message access options and the IT department with management simplicity. You can access and manage messages from your email inbox, web browser, Cisco Jabber, Cisco IP phone, smartphone, or tablet with Cisco Unity Connection. You also can easily prioritize messages and respond quickly to colleagues, partners, and customers. Mobile users, or anyone who simply prefers to do so, can use the speech-activated tools for hands-free message retrieval.

For IT, CUC is an "integrated by design" extension of Cisco Unified Communications Manager. It is easy to manage using Cisco Prime Collaboration, Cisco's single application for unified management of the entire voice and video deployment. Cisco Prime Collaboration simplifies deployment, provisioning, monitoring, and system management. Chapter 23, "Adding Users and Devices in the Webex Control Hub," will delve much deeper into CUC.

Cisco Unity Express (CUE) offers industry-leading integrated messaging, voicemail, fax, automated attendant, interactive voice response (IVR), time-card management, and a rich set of other messaging features on the Cisco Integrated Services Router (ISR) platform. It provides these integrated services specifically designed for small and medium-sized office environments or enterprise branch offices. With Cisco Unity Express, you can easily and conveniently manage your voice messages and greetings right through your web browser using Web Inbox, traditional intuitive telephone prompts, an easy-to-use visual voicemail interface (which is called the Cisco Unity Express VoiceView Express application), email access to messages, and a straightforward GUI that allows simple administration and management.

Cisco Unity Express is an essential component of either a Cisco Unified Communications Manager or Cisco Unified CME Solution. In a Cisco Unified Communications Manager environment, Cisco Unity Express provides local storage and processing of integrated messaging, voicemail, fax, automated attendant, and IVR for branch offices with limited WAN connectivity, thereby alleviating concerns about WAN bandwidth and quality of service (QoS). Additionally, Cisco Unified Communications Manager customers with Cisco Unity Connection unified messaging solutions at their larger locations can use Cisco Unity Express at their branch-office locations and network the solutions so that employees can easily send messages between locations. In a Cisco Unified CME environment, customers deploy a single Cisco ISR platform with Cisco Unity Express installed to meet their office telephony and messaging needs, as well as their other business communications needs.

Cisco IM and Presence Service

Cisco Unified Communications Manager IM and Presence Service, or IMP, provides native standards-based, dual-protocol, enterprise instant messaging and network-based presence as part of Cisco Unified Communications. This secure, scalable, and easy-to-manage service within Cisco Unified Communications Manager offers feature-rich communications capabilities both within and external to the enterprise.

IM and Presence Service is tightly integrated with Cisco and third-party-compatible desktop and mobile presence and IM clients, including the Cisco Jabber platform, Cisco Webex Social, and Cisco Jabber SDK. It enables these clients to perform numerous functions such as instant messaging, presence, click-to-call, phone control, voice, video, visual voicemail, and web collaboration. IM and Presence Service offers customers and partners the flexibility of rich, open interfaces that enable IM and Cisco's rich network-based presence, as well as IM and presence federation for a wide variety of business applications. Chapter 25, "Webex Calling Features," will delve much deeper into the Cisco IM and Presence Service.

Cisco Meeting Server

Conferencing is an essential component of any collaboration solution, especially when serving remote users or a large user base. Cisco Rich Media Conferencing offers features such as instant, permanent, and scheduled audio and video conferencing, as well as content sharing. Conference bridges provide the conferencing function. A conference bridge is a resource that joins multiple participants into a single call. It can accept any number of connections for a given conference, up to the maximum capacity allowed for a single conference on that device. The output display for a given party shows all connected parties minus the viewer's own input. Cisco Rich Media Conferencing solutions utilize various infrastructures to provide audio and video conferencing capabilities and content sharing. The conferencing infrastructure can be Cisco Unified Communications Manager using software or DSP resources, Cisco Meeting Server, or Cisco Webex Collaboration Cloud. Cisco Rich Media Conferencing solutions are available as on-premises, cloud, or hybrid deployments. This allows organizations to integrate with the Collaboration solution in which they have already invested or, alternatively, to implement a service that is hosted in the cloud. This is one of the more important distinctions between the various solutions, and it is the first decision point when determining which solution is the best fit for an organization. Cisco Webex Software as a Service (SaaS) offers a completely off-premises solution, while Cisco Collaboration Meeting Rooms (CMR) Hybrid is a solution with a mix of on-premises and off-premises equipment. Organizations that have deployed Cisco Collaboration Systems Releases (CSRs) will benefit most from leveraging an on-premises solution. This section focuses specifically on introducing the CMS product.

Cisco Meeting Server (CMS) is a Rich Media Conferencing product for on-premises deployments only. It cannot be part of a CRM-Hybrid deployment. This robust CMR solution can be deployed as an appliance server or as a virtual machine. Virtual deployments use VMware ESXi hypervisors for deployment. The Cisco Meeting Server appliance server has several options available. Customers who purchased the Acano solution before the Cisco acquisition can still use the Acano-X appliance server. Newer customers who wish to deploy the Cisco Meeting Server as an appliance can use the Cisco UCS platforms CMS1000 or CMS2000.

CMS offers a consistent one-meeting experience with many features available. However, exactly what features are available may depend on the device that is used to connect to the meeting. Calls can be made using the Cisco Meeting app, a physical endpoint, or through a third-party application. CMS supports both Telepresence Interoperability Protocol (TIP) and non-TIP supported devices. Once connected to a Space, which is what a virtual meeting room is called on CMS, users can set camera and microphone settings, mute or activate a personal microphone, share a screen or an application, chat, change devices, change screen layout, and see caller information to name a few. Bring your own device (BYOD) allows users to use their own devices to see presentations, chat with other participants, or even transfer a call from an endpoint to a smartphone or tablet using CMA.

Additional features of CMS include a seamless integration with Microsoft Skype for Business (S4B), support for WebRTC, and clustering the Database and Call Bridge services for a scalable and resilient deployment. CMS is a rich and robust CMR solution for on-premises deployments. Cisco Meeting Server is a topic that goes outside the scope of this book, so I will not go any deeper into this topic.

Management Software

Management software is a suite of tools that are used to unburden the IT administrator from some of the overwhelming day-to-day maintenance tasks of managing a collaboration network. Management tools are not essential for collaboration solutions to function, but as a network grows, these management tools do ease the stress among the people responsible for keeping all the components of the network functional. Think of what kind of car you need to take a long road trip. You don't need the comforts of leather seats, air conditioning, XM radio, or fine-tuned suspension. All you "need" is something that can get you from point A to point B. However, all those extra amenities sure do make that journey a lot more comfortable. You may even find yourself quite refreshed upon reaching your destination. Management software simply adds extra comforts to the management side of collaboration. There are two management products available in the Cisco Collaboration product portfolio: Telepresence Management Suite (TMS) and Prime Collaboration.

Cisco TMS offers everything from complete control and management of multiparty conferencing, infrastructure, and endpoints, to centralized management of the telepresence network. Flexible scheduling tools are designed to meet the needs of basic users for quick conference creation, including integration with Microsoft Exchange for scheduling through Outlook clients, and to provide advanced conference booking options for IT administrators. This includes One-Button-to-Push meeting access, which is supported in Cisco TMS Version 13.1 and later. Phonebooks can be created and pushed out to all Cisco Collaboration endpoints, and each phonebook can contain a multitiered layer of directories within it. Additional services provided by TMS include backup and restore features, scheduled system upgrades, configuration templates, dial-plan management, and many troubleshooting tools and reports.

Cisco TMS is provided as a software-based application for installation on a customer-provided Microsoft Windows Server with a SQL back end. Any physical server running an appropriate version of Microsoft Windows Server can run TMS, but Cisco recommends using the Cisco UCS server. The Cisco TMS user interface is a web browser-based application that uses Microsoft Internet Information Services running on the .NET framework. The caveat to using TMS is that it only supports Telepresence products. UC phones and services are not supported through TMS. However, third-party Telepresence endpoints can be managed by TMS. Cisco Prime Collaboration is the management software to use for support of UC services and phones.

Cisco Prime Collaboration helps enterprises address the continuous transformation of their networks as they invest in next-generation collaboration technologies with integrated video and voice deployments. It empowers IT departments to effectively manage this transformation and the video network lifecycle as they meet demands from end users for high-quality solutions everywhere and at all times. At the same time, it addresses the need to reduce operating expenses and optimize limited resources. Prime Collaboration provides simplified, unified management for video and voice networks. This management solution helps ensure superior quality experiences for end users and lower operating expenses for supporting video and voice communication. Prime Collaboration removes management complexity and provides automated, accelerated provisioning, real-time monitoring, proactive troubleshooting, and long-term trending and analytics in one integrated product. This solution delivers a premier operations experience through an intuitive user interface and automated workflows that ease implementation and ongoing administration. Self-Provisioning and Self-Care features allow users to provision their own phones, like the 7800 and 8800 series phones, and change phone settings such as names, directories, and speed-dials. The three modules to contribute to an enhanced management experience from Prime Collaboration include

- Prime Collaboration Provisioning
- Prime Collaboration Assurance
- Prime Collaboration Analytics

As mentioned earlier, Cisco Prime Collaboration Provisioning unifies administration of your UC environment to one interface, including Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco Unified Communications Manager IM and Presence service, Unity Connection, and Unity Express. It provides one interface for provisioning video, call control, messaging, and presence for a single cluster implementation. It has an intuitive interface that provides a single view of a user and the user's services, as well as a consolidated view of users across the organization. With these capabilities, Cisco Prime Collaboration significantly accelerates site rollouts and dramatically reduces the time required for ongoing moves, adds, and changes by facilitating the delegation of these tasks. This allows organizations to optimize IT resources, resulting in exceptional productivity gains and lowered operating expenses. Prime Collaboration Provisioning comes in Standard and Advanced versions. The Advanced version comes with everything in the Standard version and also includes multicluster and multiversion support for Cisco Unified Communications Manager and Unity Connection, advanced RBAC, ordering workflow, templates, and API support.

Prime Collaboration Assurance provides additional monitoring tools for the Cisco Unified Communications environment, including Cisco Unified Communications Manager, Unity Connection, and Video. It can continuously monitor in real time and do advanced troubleshooting of the environment, sending a notification when a problem arises so that issues can be proactively resolved. For video, it allows viewing of the end-to-end session paths including jitter and packet loss, with a web-enabled interface for fault monitoring of video components, including a dashboard view. Prime Collaboration Assurance provides efficient, integrated service assurance management through a single, consolidated view of the Cisco video and voice collaboration environment and is offered in Standard and Advanced versions. The Advanced version includes all the components of the Standard version, plus diagnostics, reporting features, multiple cluster management, five access levels, and higher levels of discovery, inventory, fault management, and dashboards.

Cisco Prime Analytics enables network managers to maximize the value of the massive amounts of information available about their network traffic by

- Continuously monitoring live data
- Instantaneously processing queries
- Providing real-time analysis and action
- Efficiently using compute resources

The Analytics module provides historical reporting of key performance indicators and helps enable IT network managers to analyze trends for capacity planning, resource optimization, and quality of service. The solution helps track collaboration technology adoption rates in the network and provides metrics to help analyze how users are actually using the collaboration endpoints on a daily basis. It also provides insights into key collaboration network resource usage trends. With historical data and many reporting options with easy customization, IT managers have access to actionable information, simplifying the long-term planning process contributing to ongoing technology investment decisions, and helping to optimize the network configuration for an improved experience quality for end users. Cisco Prime Collaboration Analytics provides real-time monitoring and support capabilities for real-time communication.

Designing a Cisco Collaboration Solution

There are many factors to consider when designing a Cisco Collaboration solution for a customer. The Collaboration solution could be an on-premises solution, a cloud-based solution, or a hybrid of the two. The type of Collaboration solution being designed will directly impact the licensing used for that solution. The types of services offered to the customer will also impact the licensing model. Then there are sizing considerations that have to be taken into account. When sizing a solution, you should not forget to leave room for expected growth within the customer organization. Bandwidth allocations and CAC need to be planned so that call loads during peak hours do not overtax the network. Sometimes systems break. Therefore, high availability needs to be designed into the Collaboration solution so that appropriate redundancies are in place in the event of key system failures. When systems fail, data can be lost. Disaster recovery components will help ensure data retention during these outages. Then there's the dial plan, which may be one of the most important aspects to designing a Collaboration solution. The dial plan is used during every call, and the complexity of the dial plan will impact many aspects of the overall implementation and usability of the solution. Security is a growing concern in any networked solution. Designing appropriate security measures into the Collaboration solution is equally important. Finally, there is the quality of service design that will coincide with the Collaboration solution. QoS controls how data traffic is routed through the network during high congestion times. As you can see, there are many aspects to designing a Collaboration solution that must be taken into consideration. Although each one of these topics could fill a chapter or more on its own, the following sections will dip into each one of them to provide a roadmap of the various aspects to consider when designing a Cisco Collaboration solution.

Licensing

Businesses today are as diverse as two snowflakes. These differences bring with them different needs in a workplace that is constantly changing. Layer this complication with a multitude of products ranging from call control devices such as the Cisco Unified Communications Manager, to conferencing applications, such as the Cisco Meeting Server, to cloud solutions, such as Cisco Webex, and contriving a singular license plan that covers the many needs of a business becomes a colossal task. Cisco rose to this charge and devised a licensing solution that can be tailored to any company's needs, regardless of the size of the organization, the solution it's using, or the components needed to meet its needs. As with any Cisco product, understanding the requirements for licensing your product at the time of installation is important.

A great example of the licensing obstacles Cisco has had to overcome, due in part to acquisitions, is the licensing differences between the Cisco VCS and the Cisco Unified Communications Manager. Historically, the Cisco VCS used "device-based" licenses, where licenses were purchased based on the number of devices that were allowed to register. Then additional call licenses were required based on the number of concurrent calls the VCS would allow, complicated even more by the type of call, and traversal or nontraversal call licenses. Cisco devised the Cisco Expressway series that could perform all the functions of the VCS because it is essentially a VCS and uses the same user-based licenses as the Cisco Unified Communications Manager. These licenses are the Cisco Unified Workspace Licensing, or CUWL.

CUWL licenses are broken down into two varieties, with a third possibility being the Cisco User Connect Licensing, or CUCL, which are designed for voice-only solutions in the Cisco Collaboration suite of devices. This program is based on users rather than devices and allows customers to simply purchase licenses based on the number of users they wish to service, with each user having access to multiple devices or services as part of the program. Table 6-4 identifies the CUWL and CUCL licenses and the capabilities included with each license as well as the purchasable options available for each license.

Key Topic

Table 6-4 CUWL and CUCL Licensing Model

	CUCL Essentials	CUCL Basic	CUCL Enhanced	CUWL Standard	CUWL Professional
Number of Devices Supported	One	One	One or Two	Multiple	Multiple
Cisco Prime Collaboration	Included	Included	Included	Included	Included
Jabber/IMP	Included	Included	Included	Included	Included

	CUCL Essentials	CUCL Basic	CUCL Enhanced	CUWL Standard	CUWL Professional
Jabber UC	N/A	N/A	Included	Included	Included
Expressway Firewall Traversal	N/A	N/A	Included	Included	Included
Unity Connection	Optional	Optional	Optional	Included	Included
Webex Conferencing	Optional	Optional	Optional	Optional	Included
PMP Basic	N/A	N/A	Optional	Optional	Included
PMP Advanced	N/A	N/A	Optional	Optional	Optional

Table 6-4 displays nine different components that can come with different licensing levels. Cisco Prime Collaboration is a Prime Collaboration Provisioning standard license that is included with the Cisco Unified Communications Manager. The difference between Jabber/IMP and Jabber UC is that Jabber/IMP refers to the desktop client on Microsoft Windows or Apple Mac computers, and Jabber UC refers to the Jabber application on smartphones and tablets. Expressway Firewall Traversal allows for firewall traversal licenses through the Expressway Core and Expressway Edge servers. This includes MRA capabilities and one RMS license per user. Unity Connection allows voicemail and other services that come with Unity Connection. Webex Conferencing includes one named user license for both Webex Meeting Center and Webex Meeting Server. Webex can be used for cloud-based meeting or Hybrid meetings using the Video Mesh server installed on-premises.

Key Topic

To use the on-premises Cisco Meeting Server for multipoint conferences, multiparty licenses are required. Two types of multiparty licenses are available: Shared Multiparty Plus (SMP) and Personal Multiparty Plus (PMP). With the Cisco licensing model outlines in Table 6-4, PMP licenses can be purchased as Basic or Advanced. PMP Basic provides one PMP license per user that will support host meetings on the Cisco Meeting Server for up to four participants in each meeting. PMP Advanced provides one PMP license per user that will support host meetings on the Cisco Meeting Server for an undefined number of participants in each meeting. The number of participants for PMP Advanced licenses is limited only by the infrastructure that has been installed. A huge advantage to PMP licenses is the amount of security and control they offer to the meeting. Other users cannot join personal meeting spaces that have been assigned to each user on the Cisco Meeting Server unless the host to whom the space belongs has joined the meeting. Once the host drops out of a meeting hosted in that space, all other participants will be dropped as well. This feature prevents the meeting resources from being abused by other people. SMP licenses are not part of the licensing model outlined in the table because they are not assigned to any one user. When SMP licenses are added to the Cisco Meeting Server, any user can create and join a meeting using this license. Because SMP does not share the same level of control that PMP licenses do, they should be purchased and used sparingly.

There are some other differences between CUWL and CUCL licenses that should be noted. CUWL standard and professional licenses support multiple endpoints. For example, this license allows for two desktop endpoints for a single user license, allowing for a single user to have an endpoint both at the office and at home. CUCL packages are designed for voice-only solutions, whereas the Expressway series is only used to provide VPN-less traversal services for voice endpoints. Video can be used over CUCL using Jabber or video UC phones, such as 8845 or 8865, but this is not the designed purpose of these licenses. Telepresence endpoints cannot register under the CUCL model. Notice that CUCL supports only one or two devices per user. The idea here is that a user may need to register a VoIP phone and Jabber, or that user may just use a VoIP phone.

Cisco has been using CUWL and CUCL licenses for many years because it has led the market in on-premises infrastructure. In more recent years, a new market has opened up in cloud-based offerings, and Cisco has been working diligently to dominate this market as well. With the need to be able to deliver collaboration services cost-effectively, using on-premises infrastructure or cloud-based services, depending on the needs of employees, Cisco has devised a new layer to its licensing model known as Flex.

The Cisco Collaboration Flex Plan entitles people to use Cisco's industry-leading collaboration tools with one simple subscription-based offer. It helps with transitions to the cloud, and investment protection, by including cloud, premises, hosted, and hybrid deployments, with the flexibility to use them all. Companies can choose to equip employees with meetings, calling, or both, and add more licenses at the time they're needed. Companies can also easily add Contact Center capabilities, which are also included in the Collaboration Flex Plan. One agreement covers software, entitlements, and technical support for cloud-based and on-premises services. Companies simply choose the services they need today and grow at their own pace. There is no need to manage complex agreements. And you can mix and match meetings and calling subscriptions for flexibility and value. With the Flex Plan, you can choose the right subscription based on your business size and needs. Each option includes technical support. Choose from the following purchasing models:

Key Topic

- For enterprisewide deployment, Cisco Enterprise Agreement customers can purchase via the Cisco Collaboration Flex Plan. You can gain maximum value by enabling services for everyone in your organization for meetings or calling or both.
- To purchase meetings according to usage: Cisco Collaboration Flex Plan—Active User Meetings: Anyone can host a meeting, and you pay only for those who use the entitlement.
- To provide meetings and/or calling services to individuals, teams, or departments: Cisco Collaboration Flex Plan–Named User: Your purchase is based on the number of people who need services. You can grow at your own pace.
- To provide contact center services to your service agents: Cisco Collaboration Flex Plan—Concurrent Agent: Your purchase is based on the number of agents simultaneously using services at your peak busy hour. Again, you can grow at your own pace.

At the same time, you can seamlessly drive enhanced team collaboration with Cisco Webex Teams, which is included at no additional charge. Cisco Webex Teams is a great tool to collaborate with other coworkers for ongoing work. Teams can be used on every device, in every place, to move work forward. You can enable services for selected individuals, teams, or departments, or for your entire organization. And you have the flexibility to add services as adoption grows. To learn more about the Cisco Collaboration Flex Plan, visit

https://cisco.com/go/collaborationflexplan

Cisco introduced a new way to add licenses to on-premises collaboration products called Smart Licensing. Smart Licensing was introduced as an option with Cisco Unified Communication product version 11.5, but it is required for licensing products from version 12.0 onward. Cisco is transforming the end-to-end software lifecycle to make the customers' experience better and easier. A major part of this change is a move away from Product Activation Key (PAK) licenses to Smart Licensing to make the license registration process faster and more flexible. At the heart of the transformation is Smart Licensing and Smart Accounts, which offer streamlined purchasing and software administration. Smart Licensing is a flexible software licensing model that simplifies the way you activate and manage licenses across your organization. The Smart Licensing model makes it easier for you to procure, deploy, and manage your Cisco software licenses. To use Smart Licensing, you must first set up a Smart Account.

A Smart Account is a central repository where you can view, store, and manage licenses across the entire organization. Comprehensively, you can get access to your software licenses, hardware, and subscriptions through your Smart Account. Smart Accounts are required to access and manage Smart License–enabled products. Creating a Smart Account is easy and takes less than five minutes. You can create a Smart Account on cisco.com. Smart Accounts offer a simple-to-use, centralized, and organized solution to license management. With a Smart Account, you get full visibility and insight into all of your Cisco software assets deposited into the Smart Account, including PAK licenses and Enterprise Agreements. When Smart Accounts are used with Smart Licenses, the benefits include

- **Real-Time Visibility:** You can view all of your software licenses, entitlements, and users across the organization.
- **Centralized Management:** A single location enables authorized users to see all license entitlements and move licenses freely through the network as needed.
- **Cost-Effectiveness:** You can drive down the cost of license management with reduced overhead, better utilization management, and more efficient planning.
- **Organization:** Virtual Accounts provide the flexibility to organize licenses by department, product, geography, or other designation, whatever makes the most sense for your company.

Sizing

Capacity planning involves sizing a solution to meet all of the current needs of an organization and have room to scale based on projected growth. This will determine the type of server that should be used for the installation. To illustrate how a server can be selected based on the capacity needed, this chapter will go into some of the Cisco UCS servers to a limited degree. The two primary questions that should be asked when sizing a solution are, "What is the maximum number of users who will utilize these services?" and "What is the maximum number of endpoints that will be used?"

For small and medium-sized businesses (SMB) that need only voice services, Cisco offers a great product to meet these needs. The Cisco Business Edition 4000 (BE4K) is a cloud-managed system that can support up to 200 VoIP phones. It can be preconfigured for the customer by the Cisco partner reseller through the cloud management portal and can be managed by the partner or customer after it has been installed and provisioned. This system will support the 7800 and 88X1 series phones and comes equipped with support for 120 hours of voicemail messages. You can add a 1-, 2-, or 4-port T1/E1 PRI card, or a 2- or 4-port BRI card for digital PSTN connections. You can add a 2- or 4-port FXO card, a 2- or 4-port FXS card, or a 2-port FXS with 4-port FXO combination card for analog PSTN connections. Alternatively, you can build a SIP trunk to your service provider for SIP-to-PSTN connections using the built-in CUBE gateway services.

Another UCS server Cisco offers is the Business Edition 6000 (BE6K), which comes in a Medium density (BE6000M) or High density (BE6000H) platform. The BE6K servers come preloaded with VMware ESXi and all the OVAs and ISOs needed to complete an installation of the VMs once the server has been installed and powered on. The BE6000M has a max capacity of 1000 users per cluster and 1200 endpoints per cluster. The BE6000H has a max capacity of 1000 users per cluster and 2500 endpoints per cluster. Extra nodes can be added for redundancy, but the capacity limits do not change. One of the great benefits to using a BE6K server is that the sizing tool is not needed because capacity limits are preset.

If higher capacity is needed than what the BE4K or BE6K can offer, Cisco has made available a third option called the Business Edition 7000 (BE7K). Like the BE6K, the BE7K comes preloaded with VMware ESXi and all the OVAs and ISOs needed to complete an installation of the VMs after the server has been installed and powered on. The BE7K can be purchased in a Medium density (BE7000M) or High density (BE7000H) platform. It is sized using the sizing tool, and capacity limits increase when extra nodes are added to this server. The BE7K can support up to 10,000 users per node and up to 40,000 users per cluster. It can also support up to 10,000 endpoints per node and up to 40,000 endpoints per cluster.

It should be plain to see that as the complexity of installing the server increases, the capabilities of the server increase as well. Installing the BE4K server is very easy, but it has a limited calling capability, whereas installing the BE7K is much more complex, but it has a significantly higher calling capability. What has not been mentioned before is that in the progression of each server, an increase in features is also supported. The link for the sizing tool is https://tools.cisco.com/cucst. You will have to log in with a CCO account and be associated with a Cisco partner company to access the sizing tool.

Bandwidth

Three main aspects to bandwidth must be considered when designing a Collaboration solution. First, you must consider the audio and video components being used. This includes everything discussed in Chapters 3–5 and much more. Codecs used, scan rate, compression algorithms, environmental conditions, and many other aspects can positively or negatively impact bandwidth. Second, QoS can affect bandwidth utilization. This topic will be discussed later in this chapter and in more depth in Chapter 12, “Cisco Core Network Components.” Third, provisioning and admission control allow you to set up parameters within the collaboration environment so that you can more closely observe and manage bandwidth.

Provisioning bandwidth and ensuring that the correct bit rate is negotiated between various groups of endpoints are important aspects of bandwidth management. In a Cisco Unified Communications Manager environment, bit rate is negotiated via Cisco Unified Communications Manager, which uses a concept of regions to set the maximum audio and maximum video bit rates for any given call flow. Cisco Unified Communications Manager locations work in conjunction with regions to define the characteristics of a call flow. Regions define the type of compression or bit rate that is used between any two devices. Location links define the amount of available bandwidth for the path between devices. Each device and trunk in the system is assigned to a region, by means of a device pool, and a location, by means of a device pool or by direct configuration on the device itself.

Key Topic

- Regions allow you to set the per-call bandwidth of voice and video calls. The audio limit on the region can result in filtering out codecs with higher bit rates. However, for video calls, the video limit constrains the quality (resolution and transmission rate) of the video.
- Locations define the amount of total bandwidth available for all calls to another location. When a call is made on a link, the regional value for that call must be subtracted from the total bandwidth allowed for that link.

Building a region matrix to manage maximum voice and video bit rate (video resolution) for groups of devices can assist in ensuring that certain groups of devices do not oversaturate the network bandwidth. When creating a region matrix, you should group devices into maximum video bit rate categories. The smaller the number of groups, the easier it is to calculate bandwidth requirements. Also, you should consider the default region settings to simplify the matrix and provide intra-region and inter-region defaults. There are other region considerations for bandwidth provisioning. The first consideration is whether to have different intra-region settings versus inter-region settings. This will determine whether per-site regions are required or not. The concept here is that if intra- and inter-regional audio or video bit rates are to be different, per-site regions will be required. This augments the configuration of regions to the number of sites (N) multiplied by the number of video groups (X): N*X = number of regions required on average. If intra- and inter-regional audio and video bit rates will be the same, only the regions for the video groups are required (X).

Another consideration is to reuse regions configured for audio-only IP phones when possible. Audio codec configuration is shared, so if video calls need to use different audio codecs, you need to configure new regions. For example, if voice-only devices use the G.729 audio codec over the WAN and G.711 or G.722 on the LAN while video devices always use G.711 or G.722, the voice-only and video endpoints cannot share a region. Thus, each site would require a region per group of devices. Sites = N, and video region groups = 4 + voice-only region group; then N*4 is the number of regions required. You can use the Prime Collaboration Provisioning tool or the Bulk Administration Tool as configuration aids. Per-site regions might not be needed if a single audio codec is used for both intra-region and inter-region calls as well as voice-only calls. If both audio and video endpoints use G.711 or G.722 over the WAN and LAN for voice-only or video calls, voice-only IP phones and video endpoints could use the same region. You should consider the default region settings to simplify the matrix.

The Call Admission Control (CAC) function can be an important component of a Collaboration system, especially when multiple sites are connected through an IP WAN and limited bandwidth resources are available for audio and video calls. Consider for a moment that traditional TDM-based PBXs operate within circuit-switched networks, where a circuit is established each time a call is set up. As a consequence, when a legacy PBX is connected to the PSTN or to another PBX, a certain number of physical trunks must be provisioned. When calls have to be set up to the PSTN or to another PBX, the PBX selects a trunk from those that are available. If no trunks are available, the call is rejected by the PBX and the caller hears a network-busy signal.

Now consider an IP-connected Unified Communications system. Because it is based on a packet-switched IP network, no circuits are established to set up an IP telephony call. Instead, the IP packets containing the voice samples are simply routed across the IP network together with other types of data packets. Quality of service (QoS) is used to differentiate the voice packets from the data packets, but bandwidth resources, especially on IP WAN links, are not infinite. Therefore, network administrators dedicate a certain amount of "priority" bandwidth to voice traffic on each IP WAN link. However, after the provisioned bandwidth has been fully utilized, the IP telephony system must reject subsequent calls to avoid oversubscription of the priority queue on the IP WAN link, which would cause quality degradation for all voice or video calls. This function is known as Call Admission Control, and it is essential to guarantee good voice and video quality in a multisite deployment involving an IP WAN. To preserve a satisfactory end-user experience, the CAC function should always be performed during the call setup phase so that, if network resources are not available, a message can be presented to the end user, or the call can be rerouted across a different network (such as the PSTN).

High Availability

The next consideration when planning a call processing deployment should be high availability and redundancy within the solution. This involves planning clusters of the call agents being used and configuring proper redundancy. This also involves planning redundancy in power being supplied to the hosting servers along with uninterruptible power supply (UPS) sources. Finally, this involves planning high availability in the network connectivity.

As it pertains to call processing, clustering is a grouping of call agents that work together as a single call processing entity with higher capacity. Multiple Cisco Unified Communications Managers can be clustered together, multiple VCSs can be clustered together, and multiple Cisco Expressways can be clustered together. However, there is no cross-cluster between different call agents, such as the VCS and Cisco Expressway, the VCS and Cisco Unified Communications Manager, or the Expressway and the Cisco Unified Communications Manager. However, different call agent clusters can be trunked together in order to unify communications. The Cisco Unified Communications Manager cluster can be trunked to a VCS cluster, Cisco Expressway cluster, and another Cisco Unified Communications Manager cluster.

Key Topic

The Cisco Expressways and VCSs can support up to six peers in a cluster. One of the peers in the cluster is designated as the master, and all settings under the Configuration menu on the master are replicated to each of the other peers in the cluster. If any of these configuration settings are changed from any peer in the cluster that is not the master, those changes will immediately be overwritten by the master of the cluster. Settings under the Applications menu can be configured from any peer in the cluster, and these settings will be replicated to all other peers in the cluster. Therefore, a round-trip delay time between any peer in the cluster should not exceed 30 ms, or 15 ms each one-way direction. In the event the master goes down, the next subsequent peer listed will assume the role of the master. When configuring a cluster of Cisco Expressways or VCSs, you need to configure each peer with a unique IP address, URL, and system name, but they should share the same cluster name, which should be in the form of a URL. The system URL should resolve to a DNS A-record for that particular call agent. The cluster URL should resolve to all call agents in the cluster using round-robin for distribution and load balancing.

Key Topic

Clusters in the Cisco Unified Communications Manager behave differently than those of the VCSs or Cisco Expressways. A Cisco Unified Communications Manager cluster is made up of two different service node types: the publisher and the subscriber. The publisher is essentially the master of the cluster, and each cluster can have only one publisher. Each subsequent node in a cluster is referred to as a subscriber. If you are installing a Cisco Unified Communications Manager for the first time, and you do not plan to establish a cluster, the one node is still designated as the publisher. You can then establish a cluster at a later time by setting up the required number of subscriber nodes. The publisher node is the only node in a cluster with full read-write access to the configuration database. Should the publisher go down, all services will continue to operate normally, and user-facing configuration changes to the database can be made during a publisher outage. Information is then synced to the publisher when connectivity is re-established. No other services can be written to the database when the publisher is down. Peers in a Cisco Unified Communications Manager cluster are referred to as *service nodes* because they can be grouped based on services they offer. Common service groupings include Call Processing, TFTP, Media Resources, Computer Telephony Integration (CTI) Manager, and Unified CM Applications. Figure 6-1 illustrates a Cisco Unified Communications Manager cluster with various service nodes grouped together.

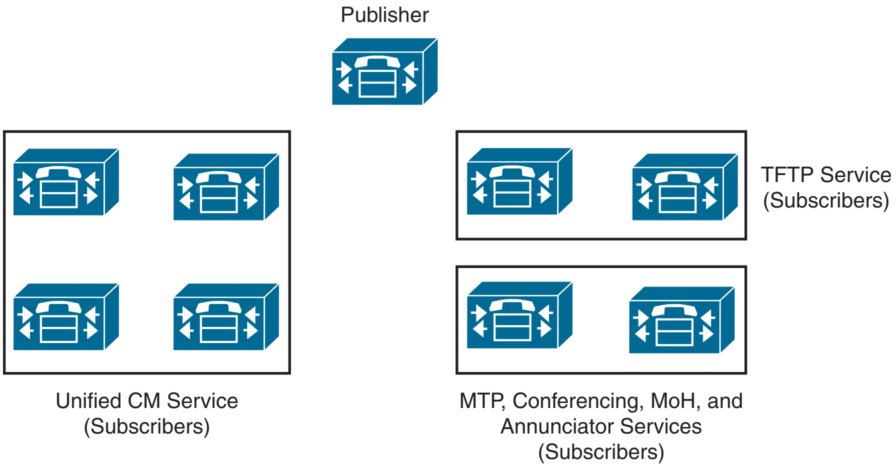


Figure 6-1 *CUCM Cluster with Service Nodes*

Key Topic

In addition to establishing service groups within a Cisco Unified Communications Manager cluster, you can also configure redundancy groups for call processing failover in the event a Cisco Unified Communications Manager within the cluster crashes. There are two options for configuring redundancy groups: a two-to-one (2:1) option and a one-to-one (1:1) option. With the 2:1 option, there is one shared backup call processing subscriber for every two primary call processing subscribers. In the event one of the primary call processing subscribers crashes, the backup will immediately assume the role until such time as the failed subscriber can be restored. However, should both primary call processing subscribers fail, the backup will be able to assume the role of only one of the primary call processing subscribers; therefore, a loss in call processing capabilities will be encountered. When the cluster is being upgraded, these redundancy groups can help maintain call processing while each primary subscriber is being rebooted. The upgrade order of sequence is to fully upgrade and reboot one of the primary subscribers first, then do the same for the second primary subscriber, and last should be the backup subscriber. Figure 6-2 illustrates how a 2:1 group of call processing subscribers can be used within the Cisco Unified Communications Manager dependent on the size of the deployment. Only two examples are provided, but many combinations exist based on the capacity of the cluster being deployed.

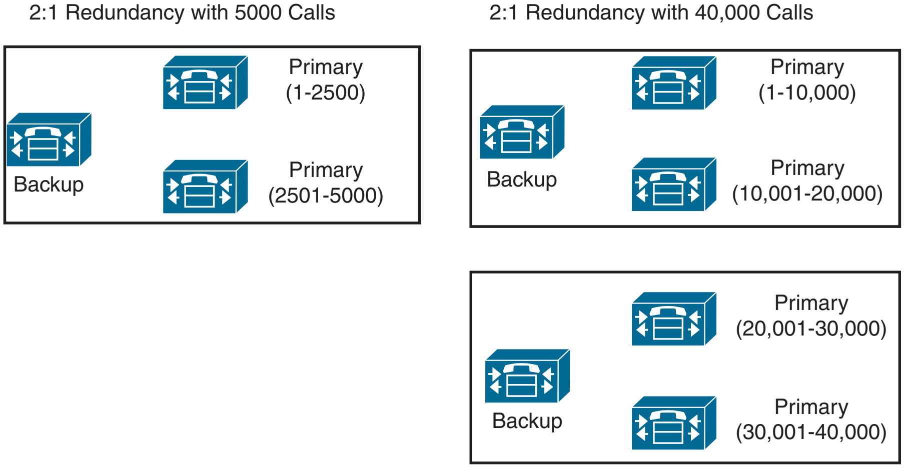


Figure 6-2 *Call Processing Subscriber Groups in a 2:1 Deployment*

With the 1:1 option, there is a single backup call processing subscriber for each primary call processing subscriber. This does require more server space and processing because more Cisco Unified Communications Manager deployments are needed. However, in the event any of the primary call processing subscribers crashes, the backup will immediately assume the role until such time as the failed subscriber can be restored. This is a more robust solution that helps mitigate the prospect of downtime in your call center. In a 2:1 group, device registration and call processing services are available only on the primary subscribers unless a subscriber crashes; then the backup will kick in. However, in a 1:1 group, registration and call processing can be load-balanced between the primary and backup subscriber. Figure 6-3 illustrates how a 1:1 group of call processing subscribers can be used within the Cisco Unified Communications Manager dependent on the size of the deployment. Only two examples are provided, but many combinations exist based on the capacity of the cluster being deployed.

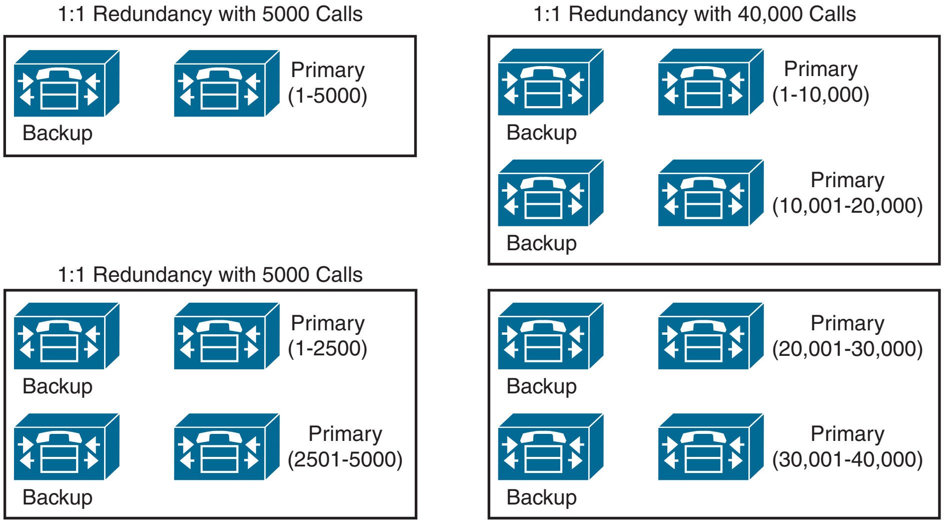


Figure 6-3 *Call Processing Subscriber Groups in a 1:1 Deployment*

When you are choosing the server(s) that will host the call agent VMs, it is best practice to choose a platform that supports dual power supplies. You should plug each power supply into different power sources so that in the event one of the power circuits fails, there is still constant power being supplied to the hosting server. Extra measures can be taken when combining dual power supplies with an UPS source. Should a power outage occur at the facility where the server is located, constant power will continue to be provided to the server, whereby phone services will also continue.

Several measures can be taken to provide high availability in the network connectivity. The speed and duplex used for network connectivity are essential to ensuring high availability. Many devices will be communicating with the call agent and will require a lot of bandwidth. Cisco recommends using a 1 Gbps or 10 Gbps throughput rate on the NIC the server is connected to. Voice and video communications should always use full duplex. If 1 Gbps or 10 Gbps throughput is used, full duplex is automatic. If a lower throughput is used, you should check the duplex configuration to ensure that it is set to full duplex, and not automatic or half duplex. Auto duplex on a Cisco switch will default to half duplex. Network redundancy can be achieved by using two Ethernet connections at the server. Each connection should be connected to a different switch so that in the event one of the switches fails, network connectivity will be maintained. This same redundancy can be implemented between switches within the network by physically distributing the network connections between different physical network switches within the same location. On the server, within the hypervisor there is a virtual switch with multiple uplinks. Therefore, a single virtual NIC defined in the call agent OVA settings is sufficient. In the VMware vSphere virtual switch, you can configure NIC teaming for the switch uplink.

Disaster Recovery

The Cisco Webex Global Site Backup architecture handles power outages, natural disaster outages, service capacity overload, network capacity overload, and other types of service interruptions. Global Site Backup supports both manual and automatic failover. The manual failover mode is typically used during maintenance windows. The automatic failover mode is used in case of real-time failover due to a service interruption.

Global Site Backup is automatic and transparent to the end users, it is available for all users, and it imposes no limits on the number of users who can fail over. Global Site Backup consists of the following main components:

- **Global Site Service:** Is responsible for monitoring and switching traffic at the network level
- **Database Replication:** Ensures that the data transactions occurring on the primary site are transferred to the backup site
- **File Replication:** Ensures that any file changes are maintained in synchronization between the primary and the backup site

For disaster recovery, you can configure a cold-standby system in a second data center. If the primary system is configured for high availability, you can optionally choose to configure high availability for the disaster recovery system. Cisco Prime Collaboration Deployment does a direct migration, whereas previous migration methods involved more steps with a “server recovery” Disaster Recovery System relying on an initial upgrade followed by a restore from backup.

Dial Plan

The dial plan is one of the key elements of a Unified Communications and Collaboration system, and it is an integral part of all call processing agents. Generally, the dial plan is responsible for instructing the call processing agent on how to route calls. The dial plan performs many functions.

Key Topic

Endpoint addressing is one of the main functions of a dial plan. For destinations registered with the call processing agent, addresses are assigned to provide reachability. These internal destinations include all endpoints, such as IP phones, video endpoints, soft clients, and analog endpoints, as well as applications, such as voicemail systems, auto attendants, and conferencing systems. Path selection is another function of a dial plan. Depending on the calling device and the destination dialed, a path to the dialed destination is selected. If a secondary path is available, this path will also be considered if the primary path fails. Calling privileges is a third function of the dial plan. Different groups of devices can be assigned to different classes of service, by granting or denying access to certain destinations. For example, lobby phones might be allowed to reach only internal and local PSTN destinations, whereas executive phones could have unrestricted PSTN access. Dial plans can affect the manipulation of dialed destinations. On the path from the dialing device to the dialed destination, the dial plan can apply manipulations to the dialed destination. For example, users in the United States might dial 9011496901234 to reach a destination in the PSTN in Germany, while a user in France might be able to reach the same destination by dialing 000496901234. This dialed destination would need to be presented as 011496901234 to a PSTN trunk on a gateway in the U.S. and as 00496901234 to a PSTN trunk on a gateway in France. The dial plan can also affect calling numbers; for example, calls across the WAN may display a caller ID as 4111, but when the call is routed across the PSTN, it may appear as 3055554111. Presentation of information about identities involved in the call is also part of a dial plan. During session establishment and also while in the call, on both the calling and the called device, information about the other device is displayed. Depending on call state and direction, this includes calling, diverting, alerting, and connected party information. The dial plan can define mappings that influence the format and content of information displayed.

Dial plan and number normalization considerations must be taken into account when deploying software-based endpoints. Jabber desktop clients typically use the directory for searching, resolving, and adding contacts. The number that is associated with those contacts must be in a form that the client can recognize, resolve, and dial.

Deployments may vary, depending on the configuration of the directory and Cisco Unified Communications Manager. In cases where the directory contains E.164 numbering, such as +18005551212, for business, mobile, and home telephone numbers, and Cisco Unified Communications Manager also contains an E.164 dial plan, the need for additional dial rules is minimized because every lookup, resolution, and dialed event results in an E.164-formatted dial string. If a Cisco Unified Communications Manager deployment has implemented a private dial plan, such as 5551212, then translation of the E.164 number to a private directory number needs to occur on Cisco Unified Communications Manager and possibly on the IOS gateways as well. Outbound calls can be translated by Cisco Unified Communications Manager translation patterns that allow the number being dialed, such as +18005551212, to be presented to the endpoint as the private number 5551212. Inbound calls can be translated by means of directory lookup rules. This allows an incoming number of 5551212 to be presented for reverse number lookup caller identification as 18005551212.

Private numbering plan deployments may arise, where the dial plan used for the company and the telephone number information stored in the LDAP directory may require the configuration of translation patterns and directory lookup rules in Cisco Unified Communications Manager to manage number format differences. Directory lookup rules define how to reformat the inbound call ID to be used as a directory lookup key. Translation patterns define how to transform a phone number retrieved from the LDAP directory for outbound dialing.

Cisco Unified Communications Manager uses translation patterns to manipulate both the calling and called numbers before a call is routed, and they are handled strictly by Cisco Unified Communications Manager. Application dialing rules can be used as an alternative to translation patterns to manipulate numbers that are dialed. Application dialing rules can automatically strip numbers from or add numbers to phone numbers that the user dials. Application dial rules are configured in Cisco Unified Communications Manager and are downloaded to the client from Cisco Unified Communications Manager. Translation patterns are the recommended method for manipulating dialed numbers.

Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory. A directory lookup rule specifies which numbers to transform based on the initial digits and the length of the number. Directory lookup rules are configured in Cisco Unified Communications Manager and are downloaded to the client from Cisco Unified Communications Manager. Before a call is placed through contact information, the client application removes everything from the phone number to be dialed, except for letters and digits. The application transforms the letters to digits and applies the dialing rules. The letter-to-digit mapping is locale-specific and corresponds to the letters found on a standard telephone keypad for that locale. Users cannot view or modify the client transformed numbers before the application places the call.

Security

Key Topic

Firewalls and ACLs are security capabilities that exist on the router to help secure your network by providing a first line of defense from attacks outside your network trying to access data inside. Unfortunately, that is not always enough to protect information inside the network from malicious attacks. If a user were to log in to his bank account across the public Internet, what is to stop a hacker from obtaining that user's login credentials and emptying the bank account? If that communication were sent over a nonsecure connection, the login information is in plain text. All the hacker would need is a packet sniffer to capture and view that information, and then would have access. To hide important information, the data needs to be encrypted. Think "Da Vinci Code" with text ciphers, only for a digital world. As long as your computer and your bank's server are the only two devices with the text ciphers, no other device will be able to read your information. Two security mechanisms can provide this level of encryption. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communications security over a computer network for TCP and UDP traffic. Although SSL is rarely used anymore, the TLS protocol aims primarily to provide privacy and data integrity between two communicating hosts or applications.

Client/server applications such as web browsers, email, and VoIP commonly use the TLS protocol to prevent eavesdropping and tampering of information. The easiest way to segregate the information is to use different port numbers for unencrypted traffic and encrypted traffic, such as port 80 for HTTP or port 443 for HTTPS. The connection is secure because symmetric cryptography is used to encrypt the transmitted data. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiation at the start of the session. The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. Identification is usually in the form of digital "certificates" that contain the server name, the trusted certificate authority (CA), and the server's public encryption key. The identity of the communicating parties can be authenticated using this public-key cryptography (asymmetric cryptography) to ensure only the intended recipient can decrypt the traffic. The negotiation of a shared secret is both secure and reliable against eavesdroppers and attacks, including man-in-the-middle attacks. The connection ensures integrity because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

After the client and server have agreed to use TLS, they negotiate a stateful connection by using a handshake procedure. Figure 6-4 shows a general overview of how a TLS handshake takes place.

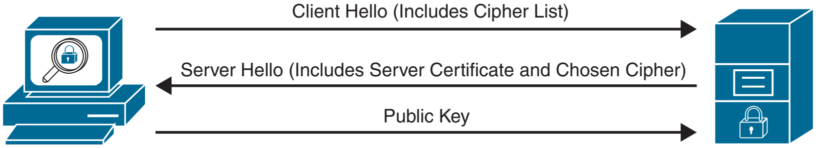

Client Hello (Includes Cipher List)
Server Hello (Includes Server Certificate and Chosen Cipher)
Public Key

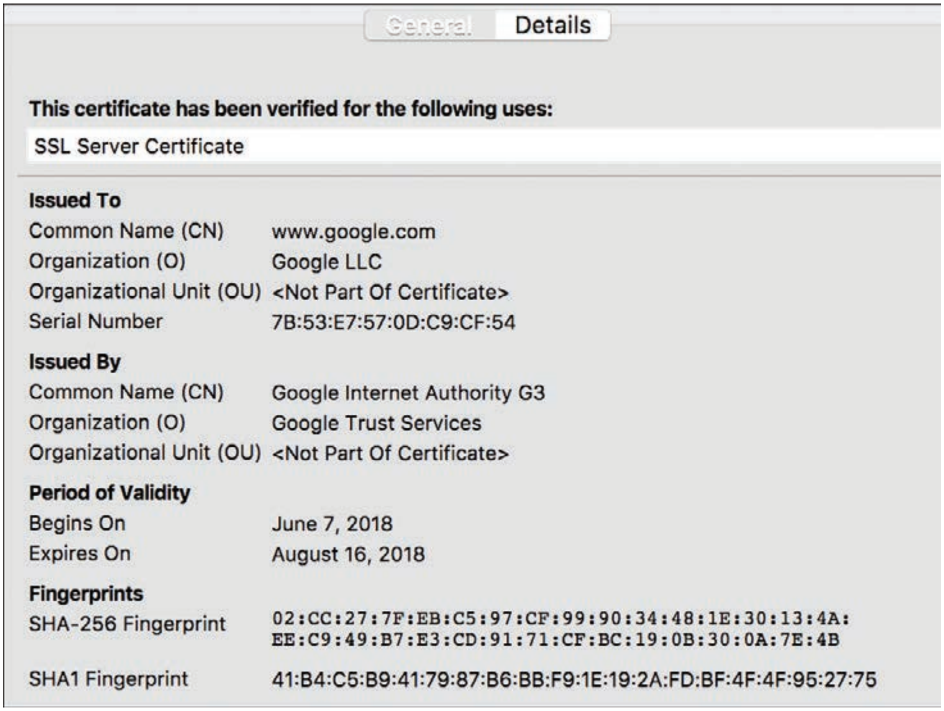
Figure 6-4 *TLS Handshake Overview*

The handshake begins when a client connects to a TLS-enabled server requesting a secure connection and presents a list of supported ciphers and hash functions. From this list, the server picks a cipher and hash function that it also supports and informs the client of the decision. The server then identifies itself with its digital certificate, which can contain the server name, the trusted certificate authority, and the server's public encryption key. The client then validates the certificate before proceeding. Public-key encryption is used to share the pre-master secret via the use of RSA or Diffie-Hellman key exchange. This process generates a random and unique session key for encryption and decryption that has the additional property of forward secrecy, which protects past sessions against future compromises of secret keys or passwords.

Remember that the server is validated because the client initiates the secure connection. The client side confirms that the server is who it claims to be and whether it can be trusted with the use of certificates. Figure 6-5 illustrates the elements contained within a certificate that can be used to verify the certificate holder is authentic.

Key Topic

The client receives the digital certificate from the server side of the TLS negotiation, but the identity must be verified before proceeding. As seen in Figure 6-5, when Google's server sends its certificate, it contains the name of the certificate holder. This name is checked against the Common Name (CN) or the Subject Alternative Name (SAN), which is www.google.com in this instance. Also, it contains additional information like a serial number, expiration dates or Period of Validity, revocation status (not applicable in this figure), a copy of the certificate holder's public key (SHA-256 Fingerprint used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority (SHA1 Fingerprint). If you trust this certificate authority, you can verify (using the CA's public key) that it really did sign the server's certificate. To sign a certificate yourself, you need the private key, which is known only to the CA of your choice. This way, an attacker cannot falsely sign a certificate and claim to be Google.com. When the certificate has been modified, the signature will be incorrect, and the client will reject it.



General | Details

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To	
Common Name (CN)	www.google.com
Organization (O)	Google LLC
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	7B:53:E7:57:0D:C9:CF:54
Issued By	
Common Name (CN)	Google Internet Authority G3
Organization (O)	Google Trust Services
Organizational Unit (OU)	<Not Part Of Certificate>
Period of Validity	
Begins On	June 7, 2018
Expires On	August 16, 2018
Fingerprints	
SHA-256 Fingerprint	02:CC:27:7F:EB:C5:97:CF:99:90:34:48:1E:30:13:4A: EE:C9:49:B7:E3:CD:91:71:CF:BC:19:0B:30:0A:7E:4B
SHA1 Fingerprint	41:B4:C5:B9:41:79:87:B6:BB:F9:1E:19:2A:FD:BF:4F:4F:95:27:75

Figure 6-5 *Elements of a Certificate*

Although this form of TLS encryption is very secure, you can still take additional measures to ensure an even higher level of security. This is known as Mutual TLS, which is synonymous with TLS Verify. In Mutual TLS authentication, both parties authenticate each other through verifying the provided digital certificate so that both parties are assured of the others' identity. Mutual TLS is similar to the normal process of the client handling the verification of the server's certification but includes the additional step of the client providing a certificate to the server for verification. This process allows the server side to authenticate the client, allowing both parties to trust each other. Figure 6-6 illustrates how a Mutual TLS negotiation would take place.

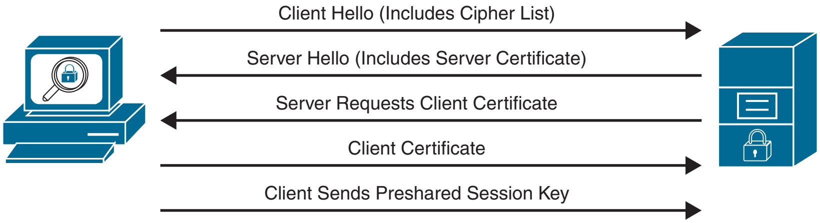

Client Hello (Includes Cipher List)
Server Hello (Includes Server Certificate)
Server Requests Client Certificate
Client Certificate
Client Sends Preshared Session Key

Figure 6-6 *Mutual TLS Negotiation*

Server-to-server connections rely on Mutual TLS for mutual authentication. In the Cisco Collaboration infrastructure, some examples would be a secure connection between endpoints and the Cisco Unified Communications Manager, referred to as TLS Verify, Cisco Unified Communications Manager intercluster trunks to other clusters, and even

Cisco Unified Communications Manager SIP trunks to a Cisco Expressway or a Video Communication Server (VCS).

Another form of security called OAuth 2 can be used within a Cisco collaboration solution. TLS, as it has been described up to this point, is what's known as an authentication protocol. OAuth 2 is known as an authorization protocol. It is an open standard defined by the IETF OAuth working group, which was originally released in 2007. In 2010, OAuth 2.0 was released as RFC 6749, which is the current version of the standard.

Have you ever noticed when trying to log in to a site on the Internet, such as a pizza delivery website, that the login screen prompts you to use an application like Facebook or Google instead? That alternative option of using Facebook or Google is an OAuth authentication. OAuth allows an end user to authorize an application to gain access to a third-party service without sharing their credentials with the application. In the example provided, a user could log in to the pizza delivery app using Facebook without ever having to enter a username or password. If authentication *is* required, it would only be required by the social media application that's providing the authorization.

To grant access to a third-party service, a user authorizes an OAuth server via authentication to issue OAuth tokens to the third-party application. The application can now present the OAuth token to access a protected resource rather than user credentials. OAuth tokens will expire after a period of time, thus limiting the time the third-party application can access the resource. In some implementations, OAuth can provide a method to refresh an expired token to provide continued access to information or a service. The key benefit here is that the user never gave their authentication credentials to the third party. These were kept secret between the social media site and the user. The token can be defined so that it has a limited scope; for example, it can be used to view contacts on the social media site but doesn't allow for the posting of information. Finally, the token can be valid for a predefined duration.

QoS

Key Topic

QoS is a marking system for network traffic that allows packets to be prioritized during high congestion times, so that drop-sensitive packets can be sent first and drop-insensitive packets are sent last. For example, an email is sent using TCP, which will resend the packets in the event they are not received at the destination. Voice and video packets are sent over UDP and will not be resent if they are dropped, which could cause media issues at the receiving end of the call. Therefore, voice and video traffic should be provided with a higher priority than email traffic. When it comes to QoS, it is best practice to mark packets as close to the source as possible. Most devices, such as computers and servers, cannot mark their own packets and should not be trusted even if they can. Cisco phones, however, can mark their own packets and can be trusted with the QoS markings they provide. Therefore, QoS trust boundaries should be set up so that the switch will trust the QoS markings that phones place on their own packets. Layer 2 QoS uses a mechanism called class of service (CoS), which operates on the 802.1q VLAN. Unlike Layer 3 QoS mechanisms, CoS does not ensure network performance or guarantee priority in packets being delivered. Therefore, after packets are marked with CoS, they will need to be converted to DSCP using the cos-to-dscp map, which is built into all Cisco switches. By default, QoS on a Cisco access switch is disabled. Once QoS is enabled, the switch does not trust QoS settings from a phone. Two simple commands can be entered under the global menu on a switch to enable QoS and change the trust boundary. Once QoS is enabled, you can use a **show** command to verify these settings.

Example 6-1 illustrates the QoS Enable and Trust Boundary Commands and the **show** verification command.

Example 6-1 *QoS Enable and Trust Boundary Commands*

```
Switch(config)# mls qos
Switch(config)# interface fastethernet 0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# end
Switch# show mls qos interface fastethernet 0/1
FastEthernet0/1
trust state: trust cos
trust mode: trust cos
cos override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
```

Obviously, this is the simplest design, and there are many other concerns to consider, along with many other settings that can be configured. This example is intended to provide a basic understanding of QoS at the Layer 2 level. For more information on QoS, refer to the *Enterprise QoS Solution Reference Network Design Guide*.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 6-5 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 6-5 Key Topics for Chapter 6

Key Topic Element	Description	Page Number
Paragraph	Framework for Cisco Jabber	117
Paragraph	Deskphone Mode and Softphone Mode for Jabber	118
Paragraph	Webex app	118
Table 6-2	Cisco Telepresence Endpoint Product Portfolio	119
List	Databases Supported for Directory Synchronization	120
Paragraph	Signaling Protocols Supported Through the CUCM	120
Paragraph	NTP Used by CUCM	121
Paragraph	DHCP from CUCM	121
Paragraph	Licensing Differences Between the VCS and Expressway Products	123

Key Topic Element	Description	Page Number
Table 6-3	Comparison of the Cisco Expressway and the Cisco VCS	123
Paragraph	CUC	126
Paragraph	CUE	126
Paragraph	IM and Presence service	127
Paragraph	CMS	128
Paragraph	Additional Features Supported on CMS	128
Paragraph	TMS Features	129
List	Three Models of Prime Collaboration	129
Paragraph	Prime Collaboration Provisioning	129
Paragraph	Prime Collaboration Assurance	130
List	Prime Collaboration Analytics	130
Table 6-4	CUWL and CUCL Licensing Model	131
Paragraph	PMP and SMP Licenses	132
List	Purchasing Models for Flex Licensing	133
List	Benefits of Smart Accounts	134
Paragraph	Business Edition Series UCS Servers	134
List	Regions and Locations	136
Paragraph	Expressway Cluster Requirements	137
Paragraph	CUCM Cluster Behavior	137
Paragraph	2:1 Redundancy Group in CUCM	138
Paragraph	1:1 Redundancy Group in CUCM	139
Paragraph	Functions of a Dial Plan	141
Paragraph	TLS and SSL Comparison	142
Paragraph	Certificate Checking Process	143
Paragraph	QoS Best Practice for L2 Marking	145

Define Key Terms

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

CAST, CE, CMA, CME, CMS, CTI, CUBE, CUC, CUCL, CUCM, CUCSF, CUE, CUWL, DNS, DX, Flex, FXO, FXS, HCS, IM, IMP, IX, Locations, MRA, MTLS, MX, NTP, PMP, PoE, Regions, RMS, SMP, SSL, SX, TC, TIP, TLS, UC, URI, URL, VCS, VoIP, VPN, Webex Endpoints, WebRTC, XMPP

Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. It might not be necessary to memorize the complete syntax of every command, but you should be able to remember the basic keywords that are needed.

To test your memory of the commands, cover the right side of Table 6-6 with a piece of paper, read the description on the left side, and then see how much of the command you can remember.

The CLCOR (350-801) exam focuses on practical, hands-on skills that are used by a networking professional. Therefore, you should be able to identify the commands needed to configure and test QoS settings on a switch.

Table 6-6 Cisco Meeting Server MMP Commands

Task	Command Syntax
Enables the multilayer switching quality of service	Switch(config)# **mls qos**
Enters the configuration field if fast Ethernet switch port 1	Switch(config)# **interface fastethernet 0/1**
Configures the switch to trust all ingress traffic	Switch(config-if)# **mls qos trust cos**
Takes the admin out of global configuration mode in the switch	Switch(config-if)# **end**
Displays the QoS settings configured on the switch from above	Switch# **show mls qos interface fastethernet 0/1**
Displays output from the previous show command	FastEthernet0/1 Trust state: **trust cos** Trust mode: **trust cos** CoS override: **dis** Default COS: **0** DSCP Mutation Map: Default DSCP Mutation Map Trust device: **none**

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the four main categories of Webex endpoints in the Telepresence product portfolio.
2. List the licensing differences between an Expressway and a VCS.
3. List the three models of Prime Collaboration.
4. List the switch commands to enable QoS at Layer 2.

This page intentionally left blank

This part covers the following topics:

- **Chapter 7, Cisco Unified Communications Phones:** This chapter will introduce the current Cisco UC phones available and discuss the features and capabilities of these phones. Specifically, the focus of this chapter will center around the 7800 series and 8800 series phones. As companies begin migrating to the cloud, the software running on the phones changes as well. This chapter will explain the differences between Enterprise software and Multiplatform Phone (MPP) software.
- **Chapter 8, Cisco Telepresence Endpoints:** This chapter will introduce the current Cisco Telepresence endpoint portfolio. All of the endpoints discussed in this chapter support the CE software operating system. Cisco has introduced many new endpoints and omitted a few from its product line. Therefore, the focus of this chapter will be on the current Cisco Telepresence endpoints at the time this book was written.
- **Chapter 9, Endpoint Registration:** This chapter will delve into the registration and call setup settings that exist on Cisco Telepresence endpoints. UC endpoints are controlled entirely from the Cisco Unified Communications manager, so they will not be discussed in this capacity. However, Cisco Telepresence endpoints have so much intelligence built into them that many features are available to the users from the interface of the endpoint itself. Unlike UC endpoints, Telepresence endpoints can register to the Cisco Unified Communications Manager, or the Cisco Expressway, or even a third-party call control system. This chapter will help you understand the differences in registering to these different call control systems.
- **Chapter 10, Call Settings on Cisco CE Software-Based Endpoints:** This chapter will describe how to access and configure various call settings on Cisco CE software-based endpoints, such as calling options, content sharing options, and several other options.
- **Chapter 11, Maintaining Cisco Endpoints:** This chapter will explain how to perform various maintenance tasks from the Cisco Telepresence endpoints. These maintenance tasks include upgrading the endpoint software, performing a backup and restore of the endpoint configurations, and accessing logs on Telepresence endpoints. Although the main focus of this chapter is on Telepresence endpoints, a short discussion of how to access logs on UC endpoints will also be included in this chapter.

Part II

Endpoints

Chapter 7: Cisco Unified Communications Phones

Chapter 8: Cisco Telepresence Endpoints

Chapter 9: Endpoint Registration

Chapter 10: Call Settings on Cisco CE Software-Based Endpoints

Chapter 11: Maintaining Cisco Endpoints

CHAPTER 7

Cisco Unified Communications Phones

This chapter covers the following topics:

7800 Series Phones: This topic will introduce the Cisco 7800 series VoIP phones along with features and capabilities.

8800 Series Phones: This topic will introduce the Cisco 8800 series VoIP and video phones along with features and capabilities.

Software Versions for Phones: This topic will explain the differences between the Enterprise software for phones and the Multiplatform Phone (MPP) software available on Cisco UC phones.

Cisco Unified Communications (UC) phones are closer to what would normally be referred to as business phones. These are voice over IP (VoIP) phones that reflect the typical image of a phone with a handset and numeric dial pad. They operate entirely on an IP network and depend on an intelligent IP PBX in order to function. In the Cisco world of collaboration, that PBX is the Cisco Unified Communications Manager (or CUCM). Cisco offers three main series of phones to customers: the 6800 series, 7800 series, and the 8800 series. The 6800 series will only register to the Webex Control Hub, so they will not be discussed in this chapter. The other two phone models can operate using two distinct operating systems. This chapter will introduce you to the current Cisco Unified Communications phones and the software versions they support. Topics discussed in this chapter include the following:

- 7800 Series Phones
- 8800 Series Phones
- Software Versions for Phones

“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
7800 Series Phones	1–2
8800 Series Phones	3–6
Software Versions for Phones	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 size is the screen on the Cisco IP Phone 7811?
   - **a.** 3.28”
   - **b.** 3.5”
   - **c.** 4.78”
   - **d.** 5.0”
2. How many lines does the Cisco IP Phone 7861 support?
   - **a.** 8
   - **b.** 10
   - **c.** 12
   - **d.** 16
3. Which of the following is a difference between the Cisco IP Phone 8811 and 8841?
   - **a.** 8841 supports Bluetooth; 8811 does not.
   - **b.** 8841 supports a color display; 8811 does not.
   - **c.** 8841 supports Intelligent Proximity; 8811 does not.
   - **d.** 8841 comes with one USB port; 8811 comes with none.
4. Which of the following comes with an 8851 phone but not with the 8851NR?
   - **a.** USB Port
   - **b.** Bluetooth
   - **c.** Touchscreen
   - **d.** Wi-Fi
5. Which of the following phones comes with video support and Wi-Fi?
   - **a.** 8845
   - **b.** 8865
   - **c.** 8865NR
   - **d.** Both B and C

6. What video resolution is supported on the Cisco IP Phone 8800 series, which supports video communication?
   a. 360p30
   b. 480p30
   c. 720p30
   d. 1080p30
7. Which Cisco IP video phone model supports the MPP firmware load?
   a. 7861
   b. 8845
   c. 8861
   d. All of these answers are correct.

Foundation Topics

7800 Series Phones

Cisco IP 7800 series VoIP phones are a lower-cost option for customers who are setting up a new UC solution and are not concerned about the features their phones offer to end users. The Cisco IP 7800 series phones are all voice-only and support a Class 1 Power over Ethernet (PoE), as well as other basic phone features, such as hold, call forward, and call transfer. The Cisco IP 7800 series phones can be used in an on-premises deployment and register to the Cisco Unified Communications Manager, or they can register to the Webex Control Hub in the cloud. These phones can also register to the Cisco Unified Communications Manager from a remote location without a VPN by using the Mobile and Remote Access (MRA) option through the Expressway Series servers. Table 7-2 identifies some of the features supported on the Cisco IP 7800 series phones.

Key Topic

Table 7-2 Cisco IP 7800 Series Phone Models and Features

Feature	7811	7821	7832	7841	7861
Screen	3.28”	3.5”	3.4”	3.5”	3.5”
Ethernet Switch	10/100	10/100	10/100	10/100/1000	10/100/1000
Line Keys	1	2	1	4	16
Backlit	No	Yes	Yes	Yes	Yes
Wideband Audio	Optional	Yes	Yes	Yes	Yes
Field-Replaceable bezel	No	Yes	No	Yes	Yes
PoE	Class 1	Class 1	Class 2	Class 1	Class 1
Cloud Ready	Yes	Yes	Yes	Yes	Yes
Power Save Plus	No	Yes	No	Yes	Yes

Key Topic

The line keys on each model are fully programmable. You can set up keys to support either lines, such as directory numbers, or call features, such as speed dialing. You can also boost productivity by handling multiple calls for each directory number, using the multi-call-per-line appearance feature. Tri-color LEDs on the line keys support this feature and make the phone simpler and easy to use. The Cisco IP Phone 7811 and the 7832 speakerphone support one line, and these phones are available only in a charcoal gray color. All other phone models in this series are available in either charcoal gray or white. The Cisco IP Phone 7821 supports two lines, the Cisco IP Phone 7841 supports four lines, and the Cisco IP Phone 7861 supports 16 lines. None of the Cisco IP 7800 series phones support the Key Expansion Module (KEM). Fixed function keys on all models give you one-touch access to services, messaging, directory, hold and resume, transfer, and conference features. The full-duplex Cisco 7832 speakerphone lets you set up clear multiparty conferences for flexible, productive collaboration.

The Cisco IP 7800 series phones set a new standard in usability and deliver a context-sensitive user experience. This series features a high-resolution 3.5” (396 × 162) grayscale display with white backlighting on IP Phones 7821, 7841, and 7861, and a 3.2” (384 × 106) display without backlighting on IP Phone 7811, for easy reading. The 7832 speakerphone features a 3.4” backlit, monochrome, pixel-based display with an antiglare bezel to make viewing and interaction easier. Localized language support, including right-to-left onscreen text, meets the needs of global users. In fact, 38 different languages are supported on the Cisco IP 7800 series phones. Refer to the “Cisco IP Phone 7800 Series Data Sheet” at Cisco.com for a specific language support listing.

The Cisco IP Phone 7800 series is also more energy efficient and eco-friendly, to support your green initiatives. Each phone supports PoE Class 1, Cisco’s EnergyWise, and is Energy Star certified. A standard power-save option is available on Cisco IP Phones 7821, 7841, and 7861 to reduce power consumption during off hours, save money, and maximize energy efficiency.

The Cisco IP 7800 series phones portfolio is ideal for any mid-sized to large enterprise company that wants to update its phone system from a traditional analog or digital-based system to an IP communications system. It’s also an excellent choice if you’re seeking to expand your voice communications support with your current Cisco Unified Communications solution. Small businesses that have interest in the Cisco IP 7800 series phones but have investment in or are considering third-party hosted call control services are also candidates for the Cisco IP 7800 series phones. Figure 7-1 illustrates the different key options available on the Cisco IP Phone 7841 model.

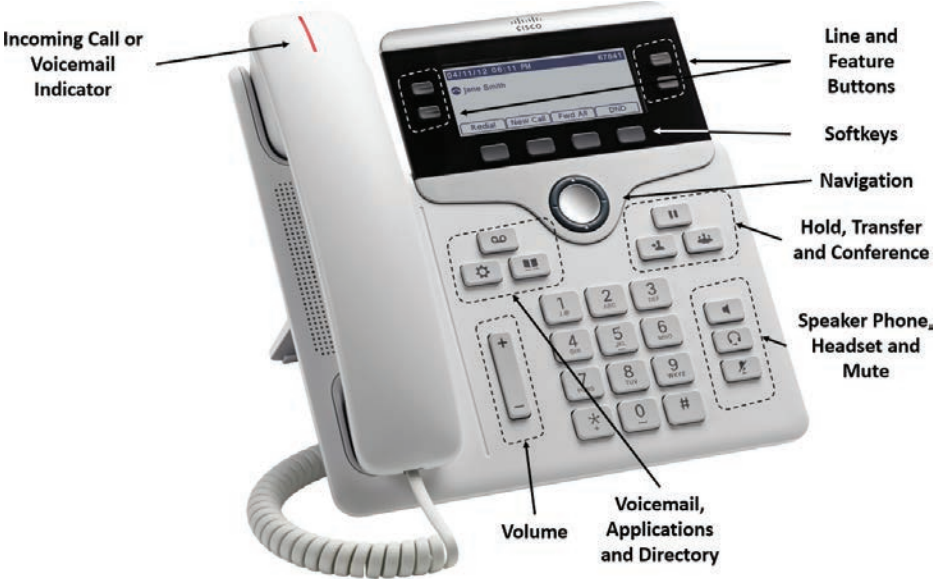

Incoming Call or Voicemail Indicator
Line and Feature Buttons
Softkeys
Navigation
Hold, Transfer and Conference
Speaker Phone, Headset and Mute
Volume
Voicemail, Applications and Directory

Figure 7-1 *Key Options on the Cisco IP Phone 7841 Model*

The feature and line buttons may light up in three different colors—green, amber, or red—and may be steady or flashing. A steady green LED indicates an active call or two-way intercom call. A flashing green LED indicates a call on hold. A steady amber LED indicates privacy is in use, a one-way intercom call is in use, or that line is logged into a hunt group. A flashing amber LED indicates an incoming call or reverting call. A steady red LED indicates a remote line is in use, such as a shared line, or Do Not Disturb (DND) has been activated. A flashing red LED indicates that a remote line has been placed on hold. The phone screen shows information about your phone, such as directory number, active call and line status, softkeys, speed dials, placed calls, and phone menu listings. The screen is made up of three sections: the header row, the middle section, and the footer row. Figure 7-2 illustrates the three sections of the Cisco IP 7800 Series Phone Screen.

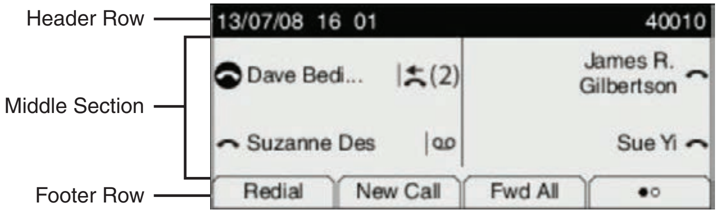


Figure 7-2 *Three Sections of the Cisco IP 7800 Series Phone Screen*

At the top of the screen is the header row. The header row displays the phone number, current date and time, and a number of icons. The icons displayed indicate when certain features are active. The middle of the phone screen displays the information associated with the line and feature buttons on the phone. The bottom row of the screen contains the softkey labels. Each label indicates the action for the softkey button directly below the indicated place on the screen. An administrator can reduce the amount of power a phone screen uses when the phone is not being used. Two energy-saving levels can be set up on a Cisco IP 7800 series phone:

- **Power Save:** The backlight or screen turns off when the phone is inactive for a set interval. The backlight can be managed.
- **Power Save Plus:** The phone screen turns on and off at times that are based on the employee's work schedule. If that employee's work hours or work days change, an administrator can reconfigure the phone.

For example, a Cisco IP 7800 phone can be set to alert the user 10 minutes before it turns off. The user will see the Select button light up and receive a message on the screen that the phone is turning off soon. Notifications can be set up at the following intervals:

- Four rings at 10 minutes before power off
- Four rings at 7 minutes before power off
- Four rings at 4 minutes before power off
- Fifteen rings at 30 seconds before power off

When a phone is active, it waits until it has been inactive for a set interval before it notifies the user of the pending power shutdown. Note that the Cisco IP Phone 7811 doesn't support Power Save or Power Save Plus. When a phone does turns off to save energy, the phone screen goes blank, and the Navigation button lights up. A user simply needs to press this button to turn the phone back on.

8800 Series Phones

A step up from the 7800 series phones are the 8800 series phones. These phones are the latest and greatest in the Cisco UC Phone product portfolio and offer a more feature-rich experience for end users. The 8800 series phones can be used in an on-premises deployment and register to the Cisco Unified Communications Manager, or they can register to the Webex cloud. These phones can also use MRA from remote locations to register back to the Cisco Unified Communications Manager at a central office location so that a VPN does not need to be utilized. Table 7-3 identifies some of the features supported on the 8800 series phones.

Table 7-3 8800 Series Phone Models and Features

Feature	8811	8841	8851	8851NR	8861	8845	8865	8865NR
Screen	Grayscale	Color	Color	Color	Color	Color	Color	Color
HD Video 720p	No	No	No	No	No	Yes	Yes	Yes
Bluetooth	No	No	Yes	No	Yes	Yes	Yes	No
Cisco Intelligent Proximity (MV)	No	No	Yes	No	Yes	Yes	Yes	No
USB Ports	0	0	1	1	2	0	2	2
KEM	0	0	2	2	3	0	3	3
Wi-Fi	No	No	No	No	Yes	No	Yes	No

With the Cisco IP Phone 8811, you can increase personal productivity through an engaging user experience that is both powerful and easy to use. The Cisco IP Phone 8811 combines an attractive new ergonomic design with wideband audio for crystal clear voice communications, "always-on" reliability, encrypted voice communications to enhance security, and access to a comprehensive suite of unified communications features from Cisco on-premises and hosted infrastructure platforms and third-party hosted call control. The Cisco IP Phone 8811 supports five programmable line keys. You can configure keys to support either multiple directory numbers or calling features such as speed dial. You can also boost productivity by handling multiple calls for each directory number, using the multi-call-per-line feature. Fixed-function keys give you one-touch access to applications, messaging, directory, and often-used calling features such as hold/resume, transfer, and conference. Backlit acoustic keys provide flexibility for audio path selection and switching. The Cisco IP Phone 8811 offers a 5" high-resolution (800 × 480) widescreen backlit grayscale display. Localized language support, including right-to-left onscreen text, meets the needs of global users. This phone supports a built-in Gigabit Ethernet switch for your PC connection. Support for Cisco EnergyWise technology makes the Cisco IP Phone 8811 more energy efficient and eco-friendly; the phone is qualified by the Energy Star organization. The Cisco IP Phone 8841 supports all the same features and capabilities as the Cisco IP Phone 8811, except that this phone offers a 5" high-resolution (800 × 480) widescreen VGA backlit color display.

Key Topic

The Cisco IP Phone 8851 supports all the same features as the Cisco IP Phones 8811 and 8841, plus some additional features and capabilities. Cisco Intelligent Proximity for Mobile Voice (MV) brings the worlds of desk and mobile together for you when you are using your mobile device at the desk for your work. You can move the audio path over to the Cisco IP Phone 8851 during active mobile calls to take advantage of its superior audio acoustics. An example would be to share a conversation with a colleague you want to listen in on the call. This capability gives you greater flexibility and a superior user experience when at your desk. The Cisco IP Phone 8851 also comes standard with one USB port, so you can connect a headset or charge your smartphone while at your desk. The Cisco IP Phone 8851 offers a 5” high-resolution (800 × 480) widescreen VGA backlit color display. Up to two optional IP Phone 8800 Key Expansion Modules with up to 56 additional line and feature keys are supported. The Cisco IP Phone 8851NR is a No Radio variant of the 8851 model that can be used in secure environments such as government and military buildings. There are some feature differences between the 8851 and the 8851NR; for example, the Cisco IP Phone 8851NR does not support Bluetooth or Intelligent Proximity. All other features and settings are the same, however. The Cisco IP Phone 8861 adds four extra capabilities beyond those of the Cisco IP Phone 8851. First, the 8861 phone offers two USB ports, one on the side just like the 8851 offers, plus an additional port on the back of the phone. Second, this phone supports a wireless network connection with 802.11a/b/g/n/ac WLAN enabled. Third, this phone offers up to three optional IP Phone Key Expansion Modules supporting up to 108 additional line and feature keys. Finally, the Cisco IP Phone 8861 offers a 5” high-resolution (800 × 480) widescreen VGA backlit color *touchscreen* display.

Key Topic

The three IP phones Cisco offers with video capability are the Cisco IP Phones 8845, 8865, and the 8865NR. The Cisco IP Phone 8845 can help users increase personal productivity through powerful and easy user experiences. It combines an attractive ergonomic design with 720p30 HD video capabilities in addition to the wideband audio for crystal-clear video and voice communications. The 8845 encrypts video and voice communications for security and offers access to a comprehensive suite of unified communications features. Offering capabilities above the Cisco IP Phone 8841 beyond just video, the 8845 also supports Cisco Intelligent Proximity MV and Bluetooth. The Cisco IP Phone 8865 offers all the same great features as the Cisco IP Phone 8861, plus the HD 720p30 video capabilities. The Cisco IP Phone 8865NR offers the same features as the 8865, except the Cisco IP Phone 8865NR does not support Bluetooth, Wi-Fi, or Intelligent Proximity. All phones in the Cisco IP Phone 8800 series are available in two color options: charcoal gray and white.

The phone buttons on the Cisco IP Phone 8800 series are similar to the Cisco IP Phone 7800 series, with some minor differences. All Cisco IP Phones in the 8800 series have identical buttons to one another. Based on the preceding descriptions, there are obviously two hardware types available in the Cisco IP Phone 8800 series. The Cisco IP Phones 8811, 8841, 8851, 8851NR, and the 8861 do not have a camera. The Cisco IP Phones 8845, 8865, and 8865NR do have cameras. The cameras can be manually tilted but have no pan or zoom capabilities. A shutter on the end of the camera can be closed for those people who fear being watched even when a call is not in session. (You know who you are.) Figure 7-3 illustrates the different key options available on the Cisco IP Phone 8865.

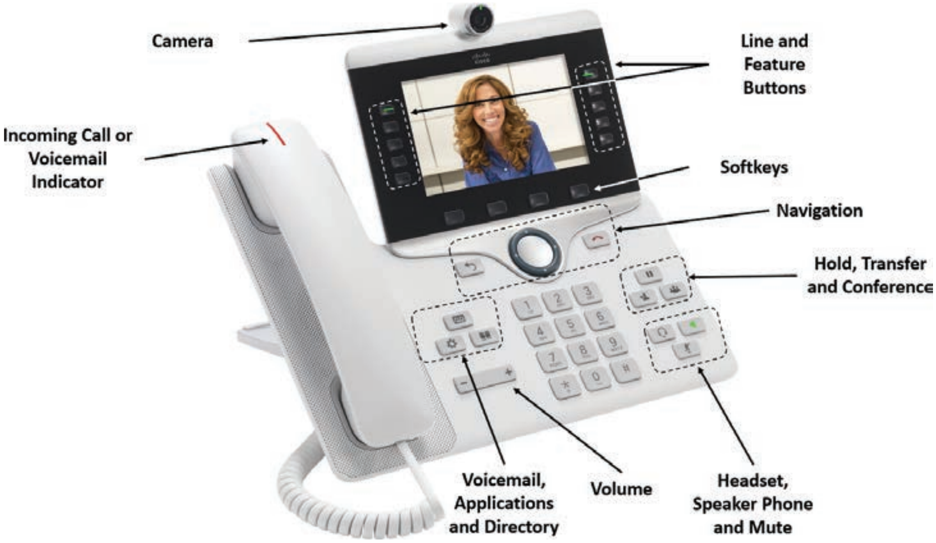
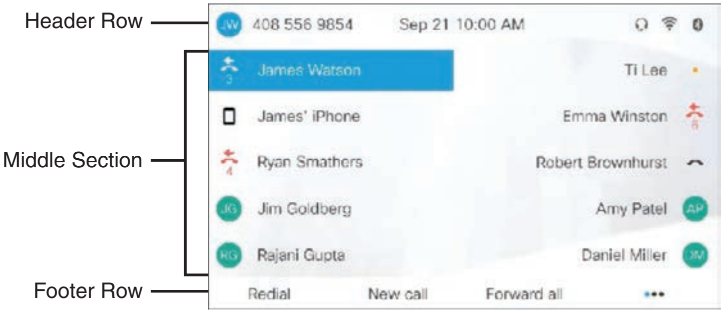

Camera
Line and Feature Buttons
Incoming Call or Voicemail Indicator
Softkeys
Navigation
Hold, Transfer and Conference
Voicemail, Applications and Directory
Volume
Headset, Speaker Phone and Mute

Figure 7-3 *Key Options on the Cisco IP Phone 8865*

The Cisco IP Phone 8800 series and the Cisco IP Phone 7800 series have many similar characteristics. All phones in the 8800 series support Power Save and Power Save Plus. The LED colored lighting on the 8800 series phones is the same as it is on the 7800 series phones. The phone screen on the Cisco IP Phone 8800 series shows the same basic information about your phone as the Cisco IP Phone 7800 series, such as directory number, active call and line status, softkeys, speed dials, placed calls, and phone menu listings. The screen is made up of the same three sections: the header row, the middle section, and the footer row. The difference between these two phones is the size of the screen and the feel of the phone. Also, the screen on the 8845, 8865, and 8865NR phones will display the video communication from the far-end endpoint during a call. Figure 7-4 illustrates the three sections of the Cisco IP 8800 series phone screen.



JW 408 556 9854 Sep 21 10:00 AM

James Watson Ti Lee

James' iPhone Emma Winston

Ryan Smathers Robert Brownhurst

JG Jim Goldberg Amy Patel AP

RG Rajani Gupta Daniel Miller DM

Redial New call Forward all •••

Figure 7-4 *Three Sections of the Cisco IP 8800 Series Phone Screen*

Three other phones in the 8800 series are worth mentioning. The Cisco Unified IP speakerphones 8831 and 8832 are audio-only phones with a single programable line key; they use the DECT microphones. These devices are great for smaller huddle rooms where small teams can place audio calls to clients. The main difference between these two speakerphones is that the 8831 has a dial pad in a separate device that is attached to the speakers with a cable, whereas the 8832 is a redesigned speakerphone with a new look that includes an all-in-one unit between the speaker and the dial pad. Additionally, the 8832 has a physical USB port.

The last model worth mentioning is the Cisco Wireless IP Phone 8821. This phone is a ruggedized, resilient, and secure 802.11 wireless LAN handset that delivers cost-effective, on-premises, comprehensive voice over Wireless LAN (VoWLAN) communications for the highly mobile in-campus worker. While the 8821 is sleek and lightweight, the design is hardened for users. It is Ingress Protection standard (IP54) rated and is sealed for protection against dust, splashes, and water. The device is also MIL-STD-810G tested, with a dozen drops onto concrete from heights of up to 5 feet (1.5 m), to help ensure shock resistance and avoid breakage if dropped. The 8821 enhances security and simplifies configuration management. Stronger encryption is supported for certificate management and policy enablement with the support of Secure Hash Algorithm 2 (SHA-2). Simple Certificate Enrollment Protocol (SCEP) eases IT administration by enabling automatic certificate management on the device.

Software Versions for Phones

Currently, two different types of firmware can be used on the Cisco IP phones in the 7800 and 8800 series. Phones that register to the Webex Control Hub must be running the Multiplatform Phone, or MPP, firmware. Phones that register to the Cisco Unified Communications Manager must be running the Enterprise firmware. Cisco IP phones can be ordered with the desired firmware already installed, which is ideal for greenfield deployments. Alternatively, the software can be migrated to the needed platform on existing phones used in an enterprise, which is ideal for brownfield deployments.

For partners who provide voice and video services to end customers registering to third-party call control platforms, Cisco offers MPP firmware loads that support these platforms. The platforms that support the MPP firmware include Asterisk, Webex Calling (formerly Broadcloud), Broadworks, Centile, and Metaswitch. The feature set provided by this firmware is not identical to that of the Enterprise firmware designed and built for use with Cisco Unified Communications Manager, but there are many similarities. The features and information about the Cisco IP phones shared up to this point in this chapter have been based on the Enterprise firmware. For more information on specific feature support using Enterprise firmware, refer to the data sheet on the Cisco phone model you wish to inquire about. Table 7-4 identifies some of the features supported on phones running the MPP firmware.

Table 7-4 MPP Firmware Feature Support

Security	Applications	Call Control and Audio Features	Directory	Management
802.1x authentication	Cisco XML Services Interface (XSI)	Busy Lamp Field (BLF)	Local phonebook	Configuration: Browser Phone Auto Provision
Media encryption via SRTP	UC-One Presences	Call forwarding	XML/LDAP remote directory	Auto Provision via TFTP/HTTP/HTTPs for mass deployment

Security	Applications	Call Control and Audio Features	Directory	Management
Transport Layer Security (TLS)		Call hold	Intelligent search	Encrypted HTTP data in plain HTTP transmissions
Encrypted configuration files		Call pickup	Call history	Packet Capture, Problem Reporting Tool (PRT), and upload of PRT
Digest authentication		Call park	Reverse address lookup in all directories	Remote generation and upload of PRT data
Password login		Call transfer	Intelligent Proximity MV	Configuration report to provisioning server
HTTPs secure provisioning		Call waiting		
Mandatory/ Optional Secure Call		Do Not Disturb (DND) Extension Mobility/Hot Desking Intercom Music on Hold		

Many more call control and audio features are available with the MPP firmware, but this table should be sufficient to provide an understanding of the types of features that are available. In addition to the many features supported though this firmware, there is also support for 24 different languages. By enabling phones to support both the Enterprise firmware and the MPP firmware, Cisco is extending its reach to companies of every size, shape, and purpose.

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 35, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 7-5 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 7-5 Key Topics for Chapter 7

Key Topic Element	Description	Page Number
Table 7-2	Cisco IP 7800 Series Phone Models and Features	154
Paragraph	Lines Supported on Different 7800 Series Phone Models	154
Paragraph	Color Indicator LED Reference	156
List	Power Save and Power Save Plus on 7800 Series Phones	156
Table 7-3	8800 Series Phone Model Features	157
Paragraph	Difference Between 8811 and 8841 Phones	157
Paragraph	Difference Between 8851, 8851NR, and 8861	158
Paragraph	Difference Between 8841 and 8845	158
Paragraph	Enterprise and MPP Phone Firmware	160
Table 7-4	MPP Firmware Feature Support	160

Define Key Terms

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

Intelligent Proximity MV, KEM, LED, MPP, NR, PoE, Power Save, Power Save Plus, USB, WLAN

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the number of lines supported on each of the 7800 series phones.
2. List the number of KEMs supported on each of the Cisco IP Phone 8800 series models.
3. List five of the call control audio features supported through the MPP firmware.

This page intentionally left blank

CHAPTER 8

Cisco Telepresence Endpoints

This chapter covers the following topics:

CE Software: This topic will discuss the back-end software that runs on all the Cisco Telepresence endpoints mentioned in this chapter.

DX Series: This topic will introduce the DX series endpoint that is intended to be used as a personal desktop video communications device.

SX Series: This topic will introduce the SX series integrator endpoints that are intended to be used by professional integrators in multipurpose rooms.

MX Series: This topic will introduce the MX series all-in-one meeting room endpoints that are an easy installation option for meeting rooms where multiple participants will gather for local meetings as well as video call meetings with a remote location.

Webex Series: This topic will introduce the most recent endpoints in the Cisco product portfolio, the Webex series endpoints. These endpoints overlap with the SX and MX series but offer cutting-edge technology in the cameras, displays, speakers, microphones, and processing endpoints to deliver the best user experience in a video call that is available in the market today.

IX Series: This topic will introduce the only immersive product in the Cisco Telepresence endpoint portfolio, the IX5000. This room-within-a-room system offers best-in-class audio, video, and overall user experience.

Cisco has made its mission to be the top company in the IT industry that delivers the best products available in the market. It has not failed its mission with the development of the Cisco Telepresence endpoint product portfolio. These endpoints possess such advanced technology that they continually create a “wow” factor for anyone who has the chance to use them and see them perform. At the same time, Cisco has managed to keep the everyday end user in mind by complementing these endpoints with an easy-to-use touch controller that offers a seamless and consistent user experience no matter which of these endpoints is used. With Cisco Telepresence endpoints, the power is truly in the hands of the user. Topics discussed in this chapter include the following:

- CE Software
- DX Series
- SX Series
- MX Series
- Webex Series

    - Cisco Webex Room Kit Mini
    - Cisco Webex Room Kit
    - Cisco Webex Room Kit Plus
    - Cisco Webex Room Kit Pro
    - Cisco Webex 55 (Single and Dual)
    - Cisco Webex 70 (Single and Dual)
    - Cisco Webex Board
- IX Series

"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
CE Software	1
DX Series	2
SX Series	3
MX Series	4
Webex Series	5–11
IX Series	12

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 CE9.7.1 Cisco has added a graphical equalizer in the Audio Console to simplify usage and modification. How many different equalizer setups can be configured and attached to audio inputs and outputs?

a. 1

b. 2

c. 4

d. 8

2. Which of the following is a feature that comes with the Cisco DX80 endpoint?
   a. Touch 10 controller
   b. Document camera
   c. TRC 5 remote control
   d. IEEE 802.11AC wireless capability
3. Which of the following SX series endpoints supports the H.265HEVC codec?
   a. SX10
   b. SX20
   c. SX80
   d. All of these answers are correct.
4. What is the maximum number of multisite participants that can be supported on the MX700 endpoint at 1080p30 resolution?
   a. 2+1
   b. 3+1
   c. 4+1
   d. Multisite is not supported on these endpoints.
5. What is the horizontal field of view on the Cisco Webex Room Kit Mini?
   a. 120°
   b. 150°
   c. 170°
   d. 83°
6. How many participants does Cisco recommend in a space using the Webex Room Kit endpoint?
   a. 5
   b. 7
   c. 10
   d. 14
7. What is the zoom capability on the Cisco Webex Room Kit Plus cameras?
   a. 3x zoom
   b. 4x zoom
   c. 5x zoom
   d. 6x zoom
8. What type of audio input connectors exist in the back of the Cisco Webex Room Kit Pro for microphones?
   a. XLR
   b. Mini-jack
   c. USB
   d. Euroblock

9. Which of the following is a new technology that exists on the Cisco Webex Room 55 and not on the MX300G2?
    a. Touch 10 controller
    b. Multisite capabilities
    c. SIP and H.323 support
    d. Speaker tracking

10. How many participants are recommended in a space using the Cisco Webex 70 G2 endpoint?
    a. 24
    b. 12
    c. 28
    d. 14

11. Which of the following statements about the Cisco Webex Board is true?
    a. The Cisco Webex Board can now register to the CUCM and share whiteboarding during calls.
    b. The Webex Board cannot register to the CUCM but can be used for whiteboarding locally.
    c. The Webex Board can be used for whiteboarding locally or during a call only if it is registered to the Webex Control Hub.
    d. The Cisco Webex Board can now register to the CUCM but can share whiteboarding only during local meetings.

12. The Cisco IX5000 endpoint comes with two three-headed dongles. Which of the following are connections supported on these dongles? (Choose three.)
    a. Mini Display Port
    b. USB
    c. Thunderbolt
    d. HDMI
    e. Display Port
    f. VGA

Foundation Topics

CE Software

Tandberg was a leader in the video communication market for many years. The MXP endpoint product line the company offered was feature rich and simple to use; plus, it supported the best quality in video communications during that time. However, technology is always changing, and improvements were needed to continue leading the industry. Tandberg achieved a key asset when it acquired Codian. Although the main product behind this acquisition was the media resources Codian offered, Tandberg quickly used its technology to produce a new product line called the C-Series, which ran on the Tandberg/Codian (TC) software. After Cisco acquired Tandberg, it was not difficult for the company to see the value it had in these endpoints. Cisco continued to develop the software, eventually replacing its own CTS software-based endpoints and has since come out with new endpoints based on this software code. Prior to developing the current product line of endpoints, Cisco made some improvements to the TC software so that when it launched the upgrade version to the eighth major adaptation, it also changed the name of the code to Collaboration Endpoint, or CE. With the vision of a new suite of products that would support this software, Cisco announced a lot of its video endpoints to go end of sale. At the time this chapter was written, the current CE software version is CE9.10, which was released on January 8, 2020. To see the current versions of Cisco Collaboration equipment, go to https://software.cisco.com.

If you have older equipment running TC software, and you want to upgrade, you must first make sure the endpoints are upgraded to TC7.3.6. From this TC version, you can proceed to upgrade to CE8.x or CE9.x. You can also downgrade from CE9 directly to CE8.x or TC7.3.6. The Cisco Room Kit Mini is initially shipped running version CE9.6, which is a special release for this system only; however, you can upgrade the software on this system, which Cisco does recommend. If you are using the Audio Console, which is a feature introduced with CE9.5, and you are upgrading to CE9.6.1 or later, you should make a note of the Audio Console setup because these settings will not transfer over to the newer versions, and a backup under TC9.5 cannot be restored after the upgrade is complete. You can manually configure Audio Console settings on one endpoint that has been upgraded and use a backup of that endpoint on other endpoints after they are upgraded.

Key Topic

With CE9.7.1 Cisco has introduced several new features, including added support for accessing the xAPI using a WebSocket. A WebSocket is a bidirectional persistent connection between a client and the server where information can flow back and forth without the overhead of initiating a new TCP connection or authentication for every request. From CE9.7.1 the room device will act as a WebSocket server with direct access to the xAPI using JSON RPC 2.0 as the data transport. After establishing a WebSocket connection to the room device, you can register feedback, execute configurations and commands, or get the status of the device by sending JSON documents over the WebSocket connection. The client will also receive unsolicited data from the server, such as feedback events if registered. This feature mainly targets integrators and is a modern alternative to access the xAPI compared to SSH or serial. For more information on how to get started with xAPI over WebSocket, refer to the official xAPI over WebSocket guide found at www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/products-command-reference-list.html.

Ambient noise reporting is another new feature that uses the device microphones to estimate the ambient or background noise. The value is an A-weighted decibel value of the ambient noise level (dBa). Note that the value is not a calibrated sound pressure level (SPL), so it has to be evaluated as a relative value of the ambient sound level in the room. The feature is disabled by default and can be enabled by setting the ambient noise reporting to On in the xAPI using the command **xConfiguration RoomAnalytics AmbientNoiseEstimation Mode: On**. The estimated value is accessible via the xAPI with the command **xStatus RoomAnalytics AmbientNoise Level.**

Some other added features include Privacy mode, Room Kit Mini support for 1080p video, and editing favorites in the on-screen display (OSD). Privacy mode is a feature that adds a new button on the Touch 10 or in the on-screen UI, allowing you to disable video while in a call. The far-end participants will see only a placeholder image indicating that you have disabled the video on your device. On the local end, an icon will be displayed on the screen, indicating that you are currently not sending video. With CE9.7.1, the Room Kit Mini will now support 1080p video while used as a USB camera. In previous versions, only 720p video resolution was supported. The DX70 and DX80 endpoints can now edit favorites from the OSD. This feature allows users to edit the contact information in their local favorites from the OSD interface of the DX70 and DX80 in the same way that was introduced for the Touch 10 in CE9.6.1. Note that this feature is not available when using the TRC6 remote control.

Key Topic

Audio Equalizer is available in previous software versions via the xAPI only. Since CE9.7.1, Cisco has added a graphical equalizer in the Audio Console to simplify usage and modifications. The graphical equalizer setup is available in the Audio Console app on the room device web interface. This new graphical equalizer allows you to create up to eight different equalizer setups and attach them to an output or a microphone input. For example, an equalizer can be used in scenarios where users want to tweak the audio experience on microphone inputs or if the output equipment is expressing too much bass or treble. The graphic equalizer makes it easier for users to customize the overall audio experience on the analog line inputs and outputs. Figure 8-1 illustrates the Audio Console for CE software-based endpoints.

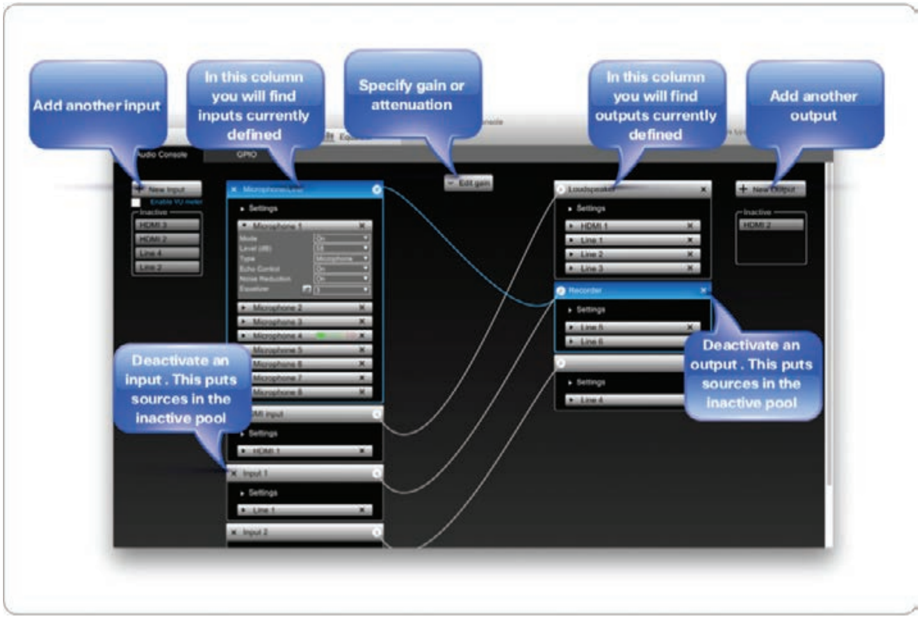

Add another input
In this column you will find inputs currently defined
Specify gain or attenuation
In this column you will find outputs currently defined
Add another output
Deactivate an input . This puts sources in the inactive pool
Deactivate an output . This puts sources in the inactive pool
Audio Console
GPIO
New input
Edit gain
Loudspeaker
New Output
Settings
Microphone 1
HDMI 1
Line 1
Line 2
Line 3
Recorder
Input 1
Input 2
Inactive
HDMI 2

Figure 8-1 *Audio Console for CE Software-Based Endpoints*

Key Topic

One last feature worth mentioning that CE software supports is Intelligent Proximity for Content Sharing, which should not be confused with Intelligent Proximity for Mobile Voice. Intelligent Proximity for Content Sharing is a Cisco proprietary protocol that uses an ultrasonic audio tone, unheard by the human ear, that pairs the endpoint with the Intelligent Proximity application. This application can be installed on a smartphone, tablet, Mac computer, or Windows computer. Once paired, the application will use a Wi-Fi signal, which must be on the same network as the endpoint to establish communication. Then the

Intelligent Proximity app can be used to view and select participants to call from the directories on the endpoint, launch calls, answer incoming calls, and view content being shared during a call. You can scroll back and view previously shared information even when the presenter is sharing something different, and you can take snapshots of the content to peruse after the call ends. When using Intelligent Proximity from a Mac or Windows computer, you can also share content through the application. This bring-your-own-device (BYOD) application has revolutionized collaboration as we know it, putting the power of information into the hands of the users within their own devices. Figure 8-2 illustrates how the Intelligent Proximity app can be used on a smartphone.

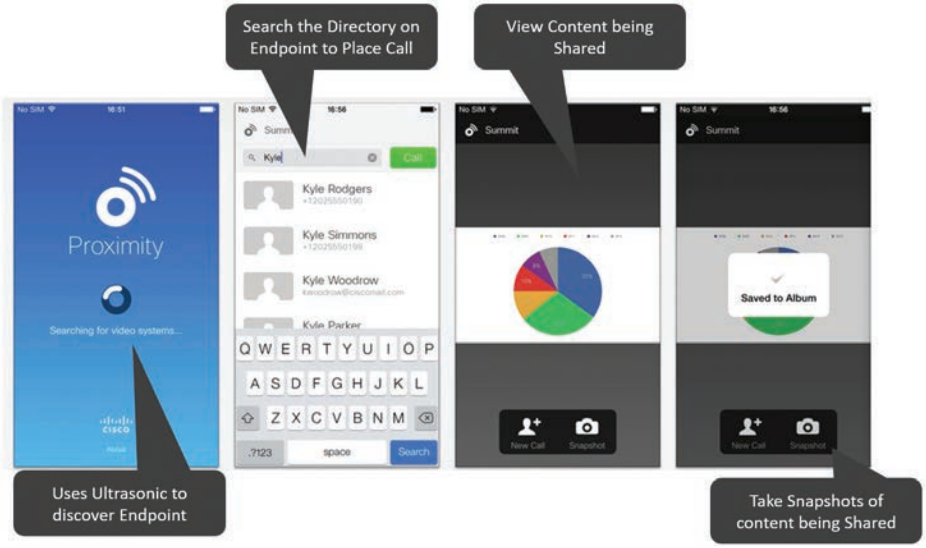

Search the Directory on Endpoint to Place Call
View Content being Shared
Proximity
Searching for video systems...
Kyle
Call
Kyle Rodgers
Kyle Simmons
Kyle Woodrow
Kyle Parker
Summit
Saved to Album
New Call
Snapshot
Uses Ultrasonic to discover Endpoint
Take Snapshots of content being Shared

Figure 8-2 *Intelligent Proximity for Content Sharing on a Smartphone*

Cisco Telepresence is all about the user experience. It allows users to virtually be in two or more places at once while leveraging full-spatial audio, high-definition video, and interactive desktop communication. This life-like experience allows for face-to-face communication between users regardless of their location. The Cisco Telepresence product portfolio offers several platforms of products to meet the needs of any company, regardless of the number of participants or room size. Chapter 6, “Cisco Solution for Converged Collaboration,” provided an introduction to the Cisco Telepresence product portfolio. This chapter will provide a more detailed explanation for each of the Cisco Telepresence endpoints. All of the Telepresence endpoints mentioned in this chapter have recently been announced as end of sale and replaced by the Webex endpoints. Because these announcements were fairly recent, and some people are still using these endpoints in production environments, they will still be mentioned in their related sections. Also, these endpoints are not end of life, so they can still be under service contracts. Since CE software is being used, it doesn’t matter which product is used; the experience will be consistent with great audio and video quality.

DX Series

There are two products in the Desktop Experience (DX) portfolio from which companies can choose. These endpoints are targeted at management personnel and typically have one participant in the camera field of view. The endpoints in this portfolio include the Cisco DX70 and the Cisco DX80. At the time this chapter was written, the Cisco DX70 and DX80 have become end of sale, but they are still under Cisco support. When these endpoints first came out, they supported an Android operating system (OS), would only register to the Cisco Unified Communications Manager, and were treated as a Cisco UC phone. On April 20, 2017, Cisco announced the end of sale for the Android OS and encouraged companies to migrate the OS on these DX endpoints to CE software. With the CE software running on the DX endpoints, they are treated as a Telepresence endpoint on the Cisco Unified Communications Manager, will register to the Webex Control Hub via SIP, and will register to the Expressway via SIP or H.323.

Key Topic

The DX70 endpoint is a midsized personal desktop endpoint with a 14-inch multitouch capacitive display that supports a 1920×1080 resolution. The DX80 endpoint is a large personal desktop endpoint with a 23-inch multitouch capacitive display that supports a 1920×1080 resolution. Because both endpoints support the multitouch capacitive display, neither of them requires a Touch 10 or TRC remote; however, the menus on the display resemble the menus on the Touch 10, so user adoption should be easy and transferable to other CE software-based endpoints. These endpoints can double as a second monitor for a computer using the HDMI-in port, which helps reduce the number of devices on an office desktop. This same connection can be used to easily share content with far-end participants during a call through the simple touch of a button on the screen. They also support the Intelligent Proximity for Content Sharing application for easy synchronization of a person's smartphone, tablet, or computer. The manual HD camera attached to the system has a privacy shutter that can be opened or closed when needed. It also has manual tilt capability for positioning the camera, but no pan or zoom capability. If you point the camera straight down at your desktop, it will become a document camera that inverts the image so that it can be presented as content. Figure 8-3 illustrates the Cisco DX80 endpoint.

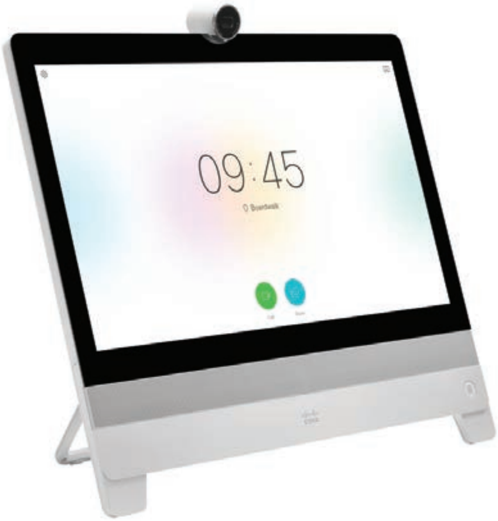


Figure 8-3 *Cisco DX80*

The Cisco Telepresence DX70 endpoint supports full HD resolutions up to 1080p30, and up to 48 kHz sampling rate for audio. It also includes a built-in acoustic echo canceller, automatic gain control, automatic noise reduction, and support for Bluetooth headsets using Bluetooth 3.0 (HFP, A2DP). Video codecs supported on the DX70 include H.263, H.263+, H.264, and H.264AVC. Audio codecs supported on the DX70 include AAC-LD, OPUS, G.722, G.722.1, G.711mu, G.711a, G.729ab, and G.729. Lip synchronization is a feature built into H.323 but not SIP. However, the DX70 endpoints have active lip synchronization built into the endpoint. Content can be shared up to 1080p15 using H.239 over H.323, or BFCP over SIP. When the DX70 is registered to the Webex Control Hub, a whiteboard feature can be used to illustrate concepts or annotate on content being shared. This feature also works outside of a call no matter where the endpoint is registered. Additional features include +E.164 dialing support, adjustable ring and volume controls, adjustable display brightness, auto-answer, headset autodetection, call forward, caller ID, corporate directory with call history lists, ad hoc conferencing capabilities (conferencing services required through Cisco Unified Communications Manager), DND, Extension Mobility, hold, MWI, audio and video mute, self-view, OBTP, shared line, SNR, call transfer, and voicemail.

The Cisco Telepresence DX80 supports all the same features as the DX70, but the DX80 endpoint offers some added benefits. The DX80 supports a larger screen at 23 inches with high-contrast LED backlighting for a better user experience. The Automatic Wake-up feature is one of the added benefits to the DX80. This Collaboration endpoint can automatically detect when someone enters a room. It will wake up, say hello, and provide guided instructions, making it effortless for users to start using the device. The multisite feature on the DX80 allows multipoint meeting to be hosted directly on the endpoint itself without the use of an external bridge. The multisite feature supports connections to three participants—this system plus two others, or 2 +1. Table 8-2 identifies some of the feature differences between the DX70 and DX80 endpoints.

Key Topic

Table 8-2 DX70 and DX80 Feature Differences

	DX70	DX80
Screen Resolution	14" 1920×1080	23" 1920×1080
Multisite	No	2+1
Contrast Ratio	700:1	1000:1
Wi-Fi Capable	802.11a, b, g, n	802.11a, b, g, n
EoS	August 16, 2018	January 30, 2021

SX Series

The Cisco Telepresence Solutions Experience (SX) products are integrator solutions that come with the codec, microphone, camera, and cables. The customer needs to supply the monitor and speakers. These products allow meeting environments to be customized to the specific needs of the customer. The extent to how extensive an environment can be customized depends on the product within the SX series that is being used, and there are three SX products from which to choose: SX10, SX20, or SX80.

The Cisco Telepresence SX10 Quick Set is a low-cost high-quality endpoint. The endpoint comes with the codec, internal microphone, and camera in compact packaging that is mountable on the top of most flat-screen displays. The Cisco SX10 is designed for a small meeting room with up to six participants. At the same price as roughly that of a computer, the SX10 is a low-cost entry point for organizations looking to purchase their first Telepresence devices or to extend their current topology. These endpoints can register to the Cisco Unified Communications Manager, the Cisco Expressway Core, or to the Webex cloud using SIP only. Included with the purchase of the Cisco SX10 is the TRC6 remote to navigate the physical interface and cables for a basic installation. Alternatively, the Intelligent Proximity for Content Sharing application can be used to control the SX10. A microphone is built into the endpoint, but an external Cisco Telepresence Precision MIC 20 can be used in addition to the built-in microphone of the SX10. The camera for the SX10 is integrated directly into the unit as well. The camera has an optical zoom of 2.65x and a total zoom of 5x.

Key Topic

There are two choices in regard to powering the SX10. Either an external power cube, which is included with the system, or Power over Ethernet (PoE) can be used to supply the 12 watts needed for operation. This is the only Cisco Telepresence endpoint that can be powered by PoE currently. Therefore, one of the nice benefits of the Cisco Telepresence SX10 Quick Set is that a single Ethernet cable can be used for both power and Ethernet connectivity. Add in a single HDMI cable to the monitor of your choice, and only two cables are needed to complete the installation of this endpoint. The Cisco Telepresence SX10 Quick Set supports high-definition video with up to 1080p30 resolution at up to 3 Mbps. Figure 8-4 illustrates all the components that come with the Cisco Telepresence SX10 Quick Set endpoint.

Key Topic

The Cisco Telepresence SX20 Quick Set is a low-price multipurpose set for simple and flexible meeting room installations that will accommodate up to 12 participants. This device comes standard with the Cisco Telepresence SX20 codec, a Cisco Telepresence Precision Camera, a Cisco Telepresence Precision MIC 20 (which can be connected through a mini-jack port), a Cisco Telepresence TRC5 remote control, and basic cables with power supply. Optional hardware that can be ordered with this endpoint includes a Cisco Touch 10 control pad, wall-mount kit, one additional Cisco Telepresence Precision MIC 20, camera-mount bracket, or a spare TRC5 remote control. The codec is based on video-conferencing standards and can register to the Cisco Unified Communications Manager, Expressway, or Webex Control Hub via SIP, or to the Cisco Expressway or a third-party call control system via H.323. Video resolutions up to 1080p60 are supported on the SX20 endpoint using H.264AVC up to 6 Mbps per call. The Cisco Telepresence SX20 Quick Set has three camera options: The Cisco Telepresence PrecisionHD camera comes in 4x or 12x zoom-capable models, or the Precision 40 Camera with 8x zoom and 4x optical plus digital capable model. The Cisco Telepresence SX20 Quick Set also supports the option for dual-display and support for a four-way (3+1) multipoint call using the Multisite option key. The Cisco Telepresence SX20 codec supports an HDMI video input with VISCA far-end camera control to connect the Cisco Telepresence PrecisionHD Camera. A DVI-I input and an HDMI input are available for the connection to a PC for presentation sharing. The Cisco Telepresence SX20 codec supports audio on the HDMI output port for the monitor, but a one-line audio output is available for external speakers if the speakers in the monitor are not adequate. The network connection on the Cisco Telepresence SX20 supports Gigabit Ethernet. Figure 8-5 illustrates all the components that come with the Cisco Telepresence SX20 Quick Set endpoint.

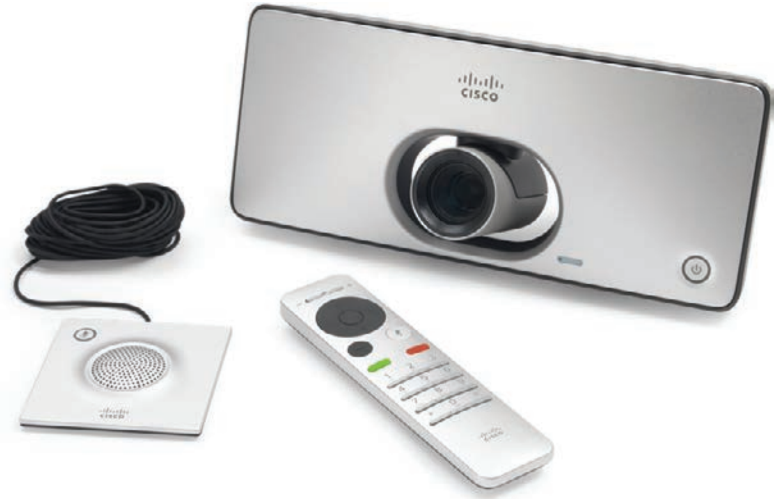


Figure 8-4 *Cisco Telepresence SX10 Quick Set*

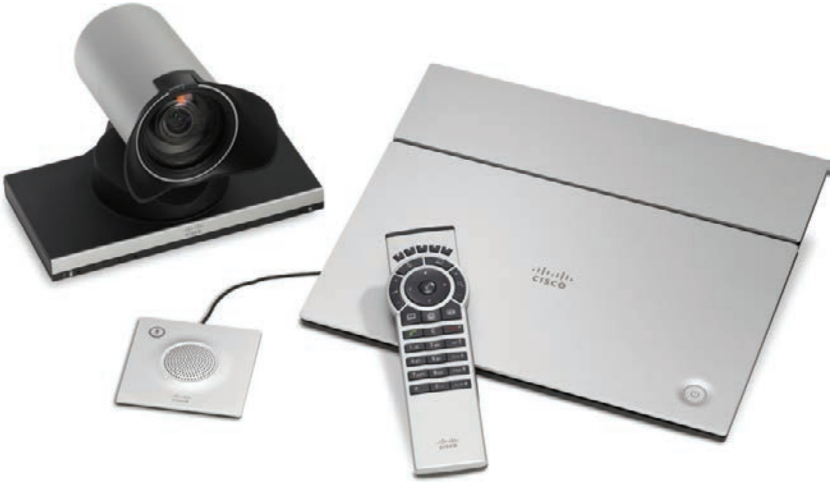


Figure 8-5 *Cisco Telepresence SX20 Quick Set*

Key Topic

The Cisco Telepresence SX80 is a flexible integrator video endpoint for medium to large meeting rooms and boardrooms. It could also be used in larger auditorium-style rooms. The SX80 is sold with three different integration packages. For small deployments, the SX80 is sold with the Precision HD 1080p 4x camera. For larger rooms, the SX80 can be sold with the Precision 60 camera or the Speaker Track 60 dual-camera system, which is the same Speaker Track system sold with the MX700 and MX800 endpoints. The SX80 supports either H.323 or SIP single-stack call registration, meaning it supports either the H.323 or SIP protocols for registration, but not both concurrently. The SX80 supports the multisite conferencing option key with capacity to support five participants (4+1) in a single multipoint conference. All current Cisco Telepresence devices support the H.264 video standard. The SX80 is the first Telepresence endpoint to be able to support the H.265 High Efficiency

Video Codec (HEVC) video standard. Because the MX700 and MX800 are built using the SX80 codec, they too can support the H.265 HEVC video codec. The SX80 codec is a powerful audio and video engine. It incorporates high-definition video collaboration applications into large meeting rooms, boardrooms, and purpose-built or vertical application rooms such as training, briefing, demo rooms, and auditoriums. The SX80 delivers up to 1080p60 end-to-end high-definition video. It offers industry-first support for H.265, which lays the foundation for future bandwidth efficiencies that the new standard makes possible. The codec offers a rich input and output set and flexible media engine. It supports three screens to help enable various use cases that are adaptable to your specific needs. The SX80 can support up to four HD cameras and eight microphones directly connected to the codec. It has an eight-port audio mixer and eight separate acoustic echo cancellers for each microphone connection. Figure 8-6 illustrates the front and back views of the Cisco Telepresence SX80 endpoint.

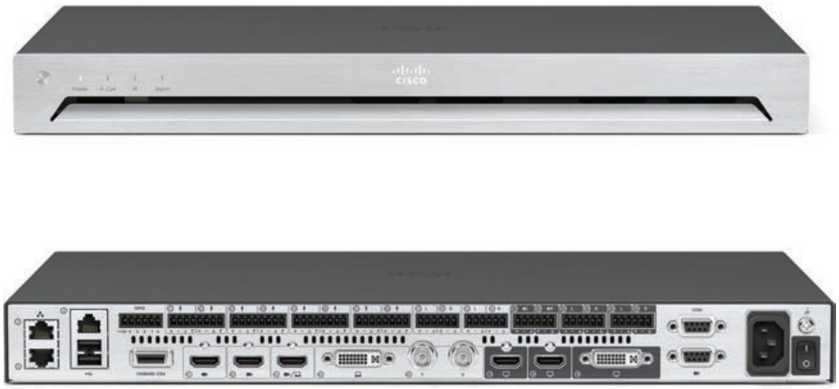


Figure 8-6 *Cisco Telepresence SX80*

Based on the preceding descriptions, there are some pretty obvious and significant differences between these three integrator solutions. The SX10 is a small but easy-to-install solution that brings powerful HD video capabilities to small meeting rooms for businesses. The SX20 is a little bit more complex to set up but brings with it more powerful tools to enhance the meeting experience and extend the number of participants to a medium-sized meeting space. The SX80 extends the level of room customization to astronomical levels. With extensive tools built into the SX80 endpoint, the reach of local and far-end participants goes beyond what either of the previous products can provide. Due to the introduction of several integrator Webex endpoints, which will be discussed later in this chapter, the SX20 and SX80 endpoints were scheduled to go end of sale in October 2019. The SX10 reached end of sale in January 2020; however, Cisco will continue to support these powerful products for five years beyond the EoS date. Table 8-3 illustrates some of the differences between these three SX integrator products.

Key Topic

Table 8-3 SX Endpoint Feature Differences

	SX10	SX20	SX80
Video Resolution	1080p30	1080p60	1080p60
Protocol Support	SIP	SIP/H.323	SIP/H.323

	SX10	SX20	SX80
Multisite	N/A	2+1 at 720p30 3+1 at 576p30	4+1 at 720p30 3+1 at 1080p30
Video Codec	H.264AVC	H.264AVC	H.265HEVC
Display Support	1	2	3
Bandwidth Support	3Mbps point-to-point	6Mbps point-to-point or multipoint	6Mbps point-to-point 10Mbps multipoint
EoS	January 28, 2020	October 29, 2019	October 29, 2019

MX Series

The Multipurpose Experience (MX) portfolio is made up of four main products that can be deployed quickly and easily in any multipurpose conference room. These units can be leveraged to support local meetings or conference calls out to remote locations. Because these units are an all-in-one system, installation is as simple as removing the unit from the box; setting up the mounting option you chose; and connecting the power, Ethernet, microphone, and touch controller. No other cables need to be connected. Which unit should be installed depends on the size and dimensions of the room within which it will be utilized.

The Cisco Telepresence MX 200G2 endpoints come with a 42-inch display that supports resolutions up to 1920×1080. The Cisco Telepresence MX 300G2 endpoints come with a 55-inch display that supports resolutions up to 1920×1080. Both systems support a DVI-I connected device and an HDMI-connected device for content sharing and support of PC-input resolutions from SVGA (800×600) to 1080p (1920×1080). These endpoints also support an embedded four-way multisite conferencing option (3+1). The Cisco Telepresence MX200G2 and MX300G2 endpoints have one integrated full-range microphone and an integrated full-range speaker system. The system also supports up to two instances of the Cisco Telepresence Precision MIC 20 so that the audio input range can be extended. One Cisco Telepresence Precision MIC 20 microphone is included with the MX200G2, and a second mic can be purchased as an add-on option. Two Cisco Telepresence Precision MIC 20 microphones are included with the Cisco Telepresence MX300G2.

The following mounting options are available for these endpoint solutions:

Key Topic

- Floor stand
- Table stand (Cisco Telepresence MX200G2 only)
- Wall mount (which doubles as a bracket for VESA mount systems; VESA is a standard for video-display mount systems)
- Wheel base

The Cisco Telepresence MX200G2 and MX300G2 endpoints are easy to install. Each purchase includes an all-in-one monitor, codec and camera unit, and cables, plus your choice of mounting option. These endpoints can register to the Cisco Unified Communications Manager using SIP. They can register to the Cisco Expressway Core using either SIP or H.323.

They can also register to the Webex cloud using SIP. The MX200G2 and the MX300G2 endpoints were announced to be end of sale on May 2, 2018. The replacement product is the Cisco Webex Room 55. Figure 8-7 illustrates the MX300G2 with mounting options.

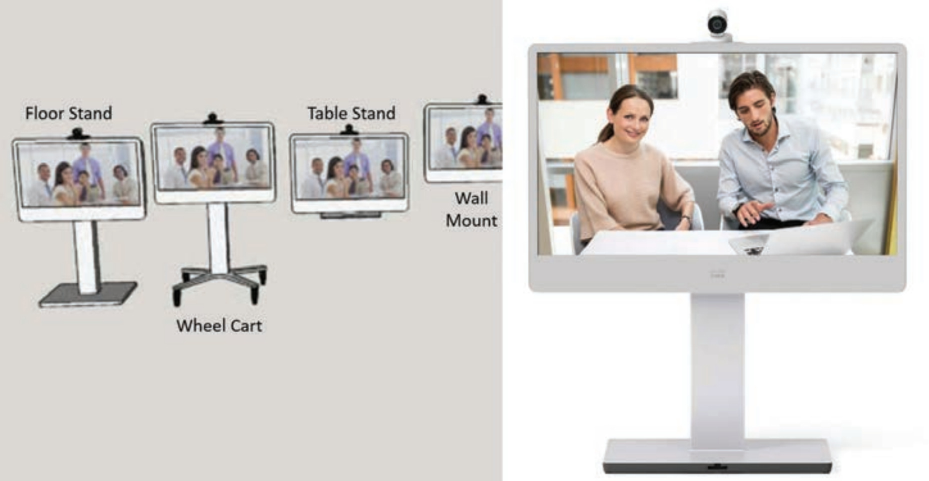


Figure 8-7 *Cisco Telepresence MX300G2 with Mounting Options*

Key Topic

The Cisco Telepresence MX700 and MX800 represent the performance line in the Cisco integrated video collaboration room systems. The MX700 and MX800 systems come standard with a built-in amplifier and speaker system for high-fidelity sound. You can choose from a powerful single camera or an intelligent dual-camera speaker-tracking solution. Both cameras provide 1080p60 resolution and support 20x total zoom (10x optical, 2x digital zoom.) The MX700 and MX800 are driven by the SX80 codec integrated into the system. Should an engineer need to access the connectors on this codec, such as to connect an external display, the cover on the left side of the system can be removed. The cover is fastened with magnets. Premium resolution and dual display are also standard features on the MX700 and MX800. The intuitive Cisco Telepresence Touch 10 provides an easy-to-use interface for both MX700 and MX800 systems. The Cisco Telepresence MX700 has the options of one or two 55-inch (1.4m) TFT-LCD monitors. The Cisco Telepresence MX800 has the options of one or two 70-inch TFT-LCD monitors. The displays on both systems have a resolution of 1920×1080 (16:9) with a contrast ratio of 4000:1. Both systems also have 3 HDMI and 1 DVI-I video inputs and 15 audio inputs. Mounting options include either a wall-mounted solution or a floor-stand mounting solution. The options for the monitors, camera, and mounting must all be selected at the time of purchase because these units are customized on a per-order basis. These endpoints can register to the Cisco Unified Communications Manager using SIP. They can register to the Cisco Expressway Core using either SIP or H.323. They can also register to the Webex cloud using SIP. Figure 8-8 illustrates the single-screen and dual-screen options, as well as the single camera and dual camera with speaker-tracking options on the Cisco Telepresence MX800 endpoint.

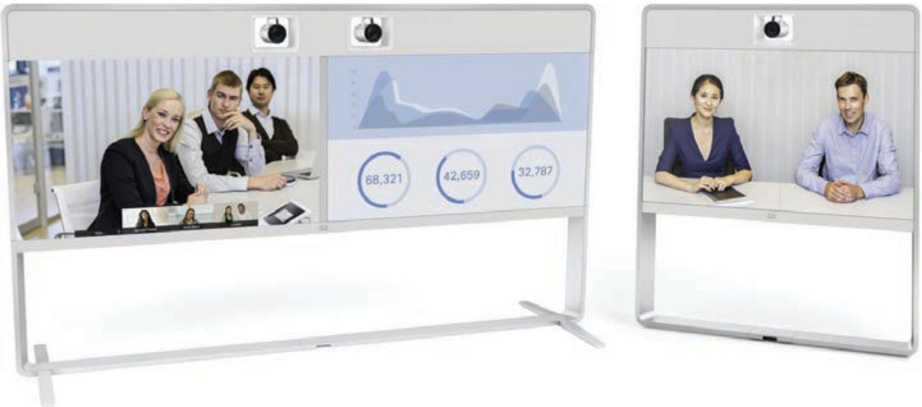


Figure 8-8 *Cisco Telepresence MX800 with Display and Camera Options*

As with other Cisco endpoint product portfolios, there are some significant differences between the MX series endpoints mentioned in this section. The first endpoint that Cisco released after the Tandberg merger was the MX200 (G1), which was quickly followed by the MX300 (G1). These two endpoint systems were all-in-one contained units that allowed companies to deploy a room system in 10 minutes or less. Just take them out of the box, attach the mounting system, plug in the cables, and you were ready to use the systems. Improving on the display and codec capabilities of these two endpoints, a few years later Cisco released the MX200G2 and MX300G2. They were followed shortly by the MX700 and MX800, which bring 4K display and H.265HEVC video compression along with them. The MX700 and MX800 also have higher multisite capability, the Speaker Track 60 dual-camera option, and the option for a built-in second display for content sharing. They offer a more uniform look to room integration and offer much higher capabilities to enhance the user experience. Table 8-4 illustrates some of the feature differences between the MX series endpoints.

Key Topic

Table 8-4 Cisco Telepresence MX Series Feature Differences

	MX200G2	MX300G2	MX700	MX800 (Single or Dual)
Display Size	42″ 1920×1080 with 1300 contrast ratio	55″ 1920×1080 with 4000:1 contrast ratio	55″ 1920×1080 with 4000:1 contrast ratio	70″ 1920×1080 with 4000:1 contrast ratio
Mounting Options	Floor stand, wheel base, table stand, wall mount	Floor stand, wheel base, table stand, wall mount	Floor stand, wall mount	Floor stand, wall mount
Multisite	2+1 at 720p30 3+1 at 576p30	2+1 at 720p30 3+1 at 576p30	4+1 at 720p30 3+1 at 1080p30	4+1 at 720p30 3+1 at 1080p30
Video Codec	H.264AVC	H.264AVC	H.265HEVC	H.265HEVC
Camera	2.5× optical zoom (5× with digital)	4× optical zoom (8× with digital)	20× total zoom (10× optical, 2× digital)	20× total zoom (10× optical, 2× digital)

	MX200G2	MX300G2	MX700	MX800 (Single or Dual)
Bandwidth Support	6Mbps point-to-point or multipoint	6Mbps point-to-point or multipoint	6Mbps point-to-point 10Mbps multipoint	6Mbps point-to-point 10Mbps multipoint
EoS	May 2, 2018	May 2, 2018	April 1, 2019	April 1, 2019

Webex Series

When Cisco released the cloud solution called Cisco Spark, it began developing a line of endpoints with cloud support in mind. The first product it released was the Spark Board, which brought whiteboarding capabilities into the video meeting, along with annotation capabilities. The original Spark Board had a unique OS built specifically for its intended purpose; therefore, the Spark Board would only register to Cisco Spark in the cloud. Shortly after the Spark Board came out, Cisco began changing the current endpoints in its portfolio so that CE software-based endpoints could register to on-premises infrastructure or to the cloud. This brought about the development of the Spark Room Kit, which is based on the same CE software. When Cisco changed its cloud collaboration solution from Spark to Webex, the name changed on the endpoints as well, but the functions all stayed the same. Since then, Cisco has continued to develop a whole line of products called the Collaboration Room Endpoints, some of which have already replaced the Cisco Telepresence products discussed earlier in this chapter. For the record, all Cisco CE software-based endpoints can register to the Webex Control Hub in the cloud or to on-premises infrastructure, such as the Cisco Unified Communications Manager, Expressway, or other standards-based third-party call control systems. The following subsections of this Webex Series topic will delve into the more recent Collaboration Room Endpoints Cisco has developed.

Cisco Webex Room Kit Endpoints

Webex Room Kit endpoints are integrator endpoints that can be customized to a room's specifications. They typically come equipped with the codec, speakers, microphone(s), cables for a basic setup, and a touch control pad. Everything else is provided by the customer. Deciding which type of room kit to use is determined by several factors, such as room size, microphone type and number of microphones being used, type of speakers and number of speakers being used, and type of displays and the number of displays being used. Other room elements could be considered for the integration, too, such as automated shades over windows, content-sharing connection points, and many more.

The Webex Room Kit USB is a lighter version of the Webex Room Kit Mini. It is a smart videoconferencing solution for huddle spaces and is compatible with any collaboration vendor. With a simple user interface, the Cisco Room USB is controlled with a remote control device or directly through your software client. When not in use, it makes your screens come alive with digital signage of your choice. You can experience Cisco quality in your smallest spaces at an affordable price.

The Cisco Webex Room Kit Mini is an artificial intelligence–powered videoconferencing system custom-designed for the huddle workstyle, and it's easy to use, deploy, and manage. It combines codec, camera, microphones, and speakers into a single device that integrates with a 4K display supplied by the customer to bring more intelligence and usability to all of your huddle rooms and spaces. Room Kit Mini is rich in functionality and experience, while priced and designed to be easily scalable. The Room Kit Mini is ideal for huddle spaces with three to five people because of its wide 120-degree field of view, which allows everyone in a huddle space to be seen. It also offers the flexibility to connect to laptop-based videoconferencing software via USB. The Mini is tightly integrated with the industry-leading Cisco Webex platform for continuous workflow and can register on premises to the Cisco Unified Communications Manager via SIP, the Expressway via SIP or H.323, or to Cisco Webex in the cloud. Figure 8-9 illustrates the Cisco Webex Room Kit Mini.

Figure 8-9 *Cisco Webex Room Kit Mini*

Key Topic

The Cisco Webex Room Kit Mini brings intelligent views to smaller rooms with a discreet, integrated camera. The system will "wake up" automatically when someone walks into the room and will recognize who entered the room through their mobile device syncing with Intelligent Proximity or Webex Teams enabled. The system can be easily controlled with the Cisco Touch 10 controller as well. When the meeting begins, the camera will automatically detect meeting participants and provide an ideal framing base on their location within the room. The integrated microphones and speakers provide a great audio experience during the meeting as well. Add to that the automatic noise suppression, which reduces disruptive sounds coming from the meeting room, such as typing, paper rustling, pencil tapping, or other such noises. Not only are meetings smarter, but presentations are smarter too. Content can be shared using a wired or wireless connection to your PC or other device, and you can share clearer content with 4K content-sharing capabilities. The AI integrations bring a smarter room all around. There are built-in metrics that count people in the room, enabling analytics for better resource planning. The system can connect to the network using Wi-Fi, and it supports Bluetooth as well. In-room controls are also built into the system so that peripherals, such as lights and blinds, can be controlled through the Touch 10 controller. Table 8-5 outlines some of the features supported on the Webex Room Kit Mini.

Key Topic

Table 8-5 Webex Room Kit USB and Room Kit Mini Features

Feature	Webex Room Kit USB	Webex Room Kit Mini
Bandwidth	Up to 6Mbps point-to-point	Up to 6Mbps point-to-point
Resolution	Live video resolutions (encode and decode) up to 1920×1080p30 and p60 (HD1080p)	Up to 4K video input and output at 30 fps or 1080p60
Audio features	High-quality 20 kHz audio Automatic gain control Automatic noise reduction Active lip synchronization	High-quality 20 kHz audio Automatic gain control Automatic noise reduction Active lip synchronization

Feature	Webex Room Kit USB	Webex Room Kit Mini
Content sharing	One HDMI input supports formats up to a maximum 4K (3840×2160) at 30 fps, including HD1080p60	H.239 and BFCP up to 3840×2160p5
Wireless sharing	Webex app Intelligent Proximity	Webex app Intelligent Proximity
Multipoint support	No	2+1 up to 1080p30 3+1 up to 720p30
Protocols	SIP, H.323, and Webex	SIP, H.323, and Webex
Camera	4K UltraHD 2× zoom, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity	4K UltraHD 2× zoom, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity

Key Topic

The Cisco Webex Room Kit was one of the first products created in the Cisco Webex endpoint portfolio, and many of the advanced features included in the Room Kit Mini were first incorporated in the Cisco Webex Room Kit, such as the AI functionality. Like the Cisco Telepresence SX80 endpoint, the Webex Room Kit endpoint supports the H.265 HEVC standard. The Cisco Webex Room Kit delivers the unmatched video and audio experience customers have come to expect from Cisco. In addition, new capabilities enable even smarter meetings, smarter presentation capabilities, and smarter room and device integrations—further removing the barriers to usage and deployment of video in small to medium-sized rooms. The Room Kit includes camera, codec, speakers, and microphones integrated in a single device. It also comes with a Touch 10 controller, but the monitor and speakers are not provided. It is ideal for rooms that seat up to seven people. It offers sophisticated camera technologies that bring speaker-tracking capabilities to smaller rooms. The product is rich in functionality and experience but is priced and designed to be easily scalable to all of your small conference rooms and spaces. Although the Room Kit was built to enhance the user experience in the cloud, it can be registered on the premises to the Cisco Unified Communications Manager using SIP, or to the Cisco Expressway Core using SIP or H.323, or to Cisco Webex in the cloud using SIP. The OS used by this system is the same CE software found on all the aforementioned Cisco Telepresence endpoints. Figure 8-10 illustrates the Cisco Webex Room Kit bottom and front views.

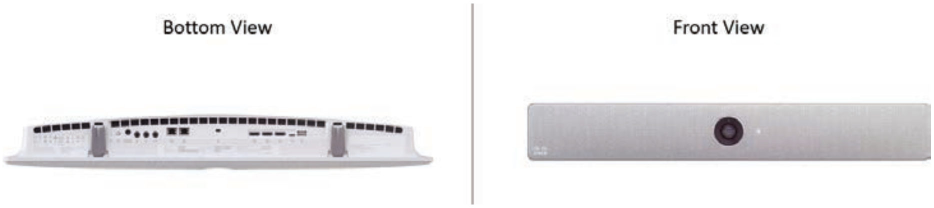


Figure 8-10 *Cisco Webex Room Kit*

The camera on the Cisco Webex Room Kit is a 4K Ultra HD camera with 3x digital zoom and an 83-degree horizontal field of view and a 51.5-degree vertical field of view. It supports resolutions up to 1080p60 and features autoframing by speech detection and facial recognition, autofocus, autobrightness, and autowhite-balancing. The connectors on the back of the Room Kit allow for one or two displays to be connected; the second display is used for content. Content can be shared over an HDMI cable through the video input, wirelessly through Intelligent Proximity, or wirelessly through the Webex Teams app when registered to the Webex Control Hub. The Cisco Webex Room Kit does have a built-in microphone with a six-element microphone array to provide accurate speaker tracking; plus, there are two 4-pin mini-jack audio inputs for table mics to be added. Five integrated high-quality speakers in balance have a frequency response from 70 Hz to 20 kHz, 24 W of amplifier power, and a max output level of 86 dB. This all translates to best-in-the-industry audio and video quality. Table 8-6 outlines some of the features supported on the Webex Room Kit.

Table 8-6 Webex Room Kit Features

Feature	Description
Bandwidth	Up to 6Mbps point-to-point
Resolution	Up to 4K video input and output at 30 fps or 1080p60
Audio features	High-quality 20 kHz audio Subwoofer line out Automatic gain control Automatic noise reduction Active lip synchronization
Content sharing	H.239 and BFCP up to 3840×2160p5 or 1080p30
Wireless sharing	Webex Teams app Webex Meetings app Intelligent Proximity
Multipoint support	2+1 up to 1080p30 3+1 up to 720p30
Protocols	SIP, H.323, and Webex
Camera	5K UltraHD 3× zoom, 15.1 MP image sensor, 1/1.7 CMOS, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity

The Cisco Telepresence Room Kit Plus was released at the same time as the Cisco Webex Room Kit and is similar in nature to the Room Kit but supports a quad-camera bar with integrated speakers and microphones, making it ideal for rooms that seat up to 14 people. It offers sophisticated camera technologies that bring speaker-tracking and autoframing capabilities to medium or large-sized rooms. Because the video capabilities of the Room Kit Plus are much more advanced than the Room Kit, the codec is external to the rest of the unit itself. The product is rich in functionality and experience but is priced and designed to be easily scalable to all of your conference rooms and spaces—whether registered on the premises or to Cisco Webex in the cloud. Figure 8-11 illustrates the Cisco Webex Room Kit Plus.

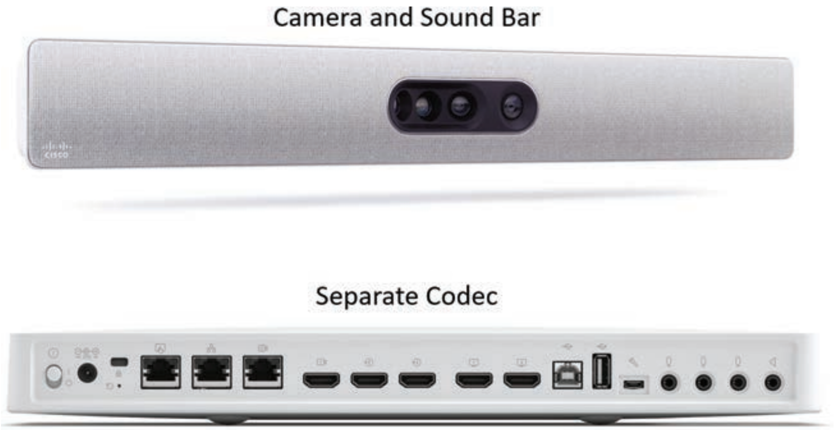


Figure 8-11 *Cisco Webex Room Kit Plus*

One of the prominent differentiators between the Room Kit Plus from the Room Kit or the Room Kit Mini is the quad-camera capabilities and the separate codec system that brings more processing power to this particular solution. However, the Room Kit Plus still brings the same intelligence to medium- and large-sized meeting rooms. While other companies are still struggling to insert advanced features such as speaker tracking, wireless sharing, and 4K content into their high-end products, Cisco is already delivering these innovations to meeting rooms of all sizes in a cost-effective and simple way. With the Room Kit Plus, Cisco is helping customers experience smarter meetings, enable smarter presentations, and create smarter room and device integrations. These features were previously the domain of higher-end video-conferencing rooms but can now be brought to every room and every team. And when registered to Cisco Webex, additional cloud-based functionalities are enabled that enhance the user experience and team workflow and further simplify deployment. The Cisco Webex Room Kit Plus comes standard with the Cisco Webex Codec Plus, the Cisco Webex Quad Camera and Sound Bar, a Cisco Touch 10 controller, and a wall-mount kit for the quad camera. It supports the H.265 High Efficiency Video Codec, and two HDMI video outputs for 4K video up to 30 frames per second or 1080p60. A third HDMI output will support 1080p60 for content sharing. Because the Cisco Webex Room Kit Plus was designed for larger meeting rooms, there are three 4-pin mini-jacks for external microphones in addition to the six-element microphone array built into the system. Table 8-7 outlines some of the features supported on the Webex Room Kit.

Key Topic

Table 8-7 Webex Room Kit Plus Features

Feature	Description
Bandwidth	Up to 6Mbps point-to-point
Resolution	Up to 4K video input and output at 30 fps or 1080p60
Audio features	High-quality 20 kHz audio Subwoofer line out Prepared for inductive loop (line out) Automatic gain control Automatic noise reduction Active lip synchronization

Feature	Description
Content sharing	H.239 and BFCP up to 3840×2160p5 or 1080p30
Wireless sharing	Webex Teams app Webex Meetings app Intelligent Proximity
Multipoint support	2+1 up to 1080p30 3+1 up to 720p30
Protocols	SIP, H.323, and Webex
Camera	5K UltraHD 5× zoom, 15.1 MP image sensor, 1/1.7 CMOS, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity

The Cisco Webex Room Kit Pro provides a powerful and flexible platform for creating the ultimate video collaboration experience. Similar to the SX80, the Room Kit Pro can be integrated in large custom video rooms, including boardrooms, auditoriums, and purpose-built rooms for vertical applications. The Room Kit Pro is built with integrators in mind and enables flexibility and creativity for customized video collaboration rooms that delight customers. The Room Kit Pro acts as the audio and video engine for UltraHD video collaboration applications and AV integrations in which up to three screens, multiple cameras, and multiple content sources can be leveraged. Camera options include the Cisco Webex Quad Camera used with the Cisco Webex Room Kit Plus, Precision 60 camera, or SpeakerTrack 60 dual camera. The codec that drives this system is the component that sets it apart from the rest. The Room Kit Pro continues with the same artificial intelligence capabilities already offered on the rest of the Cisco Webex Room Series, including intelligent views, noise suppression, voice commands, and people count. Figure 8-12 illustrates the Cisco Webex Room Kit Pro codec connection ports.

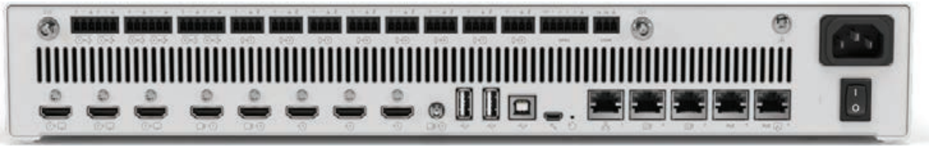


Figure 8-12 *Cisco Webex Room Kit Pro*

The Room Kit Pro delivers up to 2160p60 end-to-end UHD video. The codec's rich set of video and audio inputs, flexible media engine, and support for up to three screens enable a variety of use cases, adaptable to your specific needs. The Room Kit Pro can register on premises or to Cisco Webex in the cloud. The Room Kit Pro supports intelligent cameras and functionality to enable dynamic viewing capabilities in video meetings. The Cisco Webex Quad Camera system with four embedded digital cameras enables the best overview and speaker-tracking capabilities. With the quad camera, the Room Kit Pro can also deliver analytics such as people count. The Cisco SpeakerTrack 60 dual-camera system features a unique direct fast-switching approach for speaker tracking with two Precision 60 cameras. Cisco PresenterTrack makes it easier for presenters to move around the front of the room, using the Precision 60 camera to follow a presenter within a defined zone. With its powerful media engine, the Room Kit Pro lets you build the video collaboration room of your dreams. Cisco offers three options to purchase the Cisco Webex Room Kit Pro:

- **Room Kit Pro:** Codec Pro, Quad Camera, and Touch 10
- **Room Kit Pro Precision 60:** Codec Pro, Precision 60 camera, and Touch 10
- **Codec Pro:** Codec only

The Cisco Webex Room Kit Pro is video innovation in a box, bringing more intelligence and usability to your large specialized collaboration rooms and spaces. The Room Kit Pro supports up to six simultaneous video inputs: three 4K and three 1080p. It will also support up to eight microphones directly connected to the endpoint. More can be added by changing the audio input from mic level to line level and adding an external equalizer or amplifier. All microphone connections use the Euroblock port so that cable lengths can be more easily customized. Table 8-8 identifies some of the features supported on the Webex Room Kit Pro.

Table 8-8 Webex Room Kit Pro Features

Feature	Description
Bandwidth	Up to 6Mbps point-to-point up to 15Mbps multisite
Resolution	Up to 4K video input and output at 30 fps or 1080p60
Video inputs	2 HDMI up to 1080p60 3 HDMI up to 3840×2160p30 1 3G-SDI/HD-SDI up to 1080p60
Video outputs	2 HDMI up to 3840×2160p60 1 HDMI up to 3840×2160p30
Audio features	High-quality 20 kHz audio 8 separate acoustic echo cancellers 8-port audio mixer 8 assignable equalizers Automatic gain control Automatic noise reduction Active lip synchronization
Audio inputs	8 microphones, 48V phantom powered, Euroblock connector, mic level or balanced line level 3 HDMI outputs
Audio outputs	6 balanced line-level outputs, Euroblock connector 3 HDMI outputs HDMI Input #1 supports Audio Return Channel (ARC) audio output to Cisco Webex Quad Camera 1 Line out for Subwoofer (Cisco Webex Quad Camera)

Feature	Description
Multipoint support	2+1 up to 1080p30 3+1 up to 720p30 4+1 up to 720p30
Network interfaces	1 Ethernet 10/100/1000 for LAN 2 Ethernet 10/100/1000 for direct pairing with camera 2 Ethernet 10/100/1000 with PoE, 1 dedicated for direct pairing with Touch 10 Wi-Fi 802.11a/b/g/n/ac 2.4 GHz and 5 GHz for LAN 2×2 Multiple Input and Multiple Output (MIMO) Bluetooth 4.0 LE

Cisco Webex Room Endpoints

Key Topic

The Webex Room 55 is the replacement product for the Cisco Telepresence MX200G2 and MX300G2 endpoints. The Room 55 includes camera, codec, display, speaker system, and microphones integrated in a single device and is optimized for rooms that seat up to seven people. It is an all-in-one, integrated system that's easy to install, use, deploy, and manage. It's crafted with high-quality components: professional 4K display for longevity and minimal latency, powerful digital zoom camera for discreet tracking, and sophisticated speaker system and amplifier that deliver rich sound. The light industrial design combines aluminum and fabric for a sustainable and humanizing effect. The Cisco Webex Room 55 has the Cisco Webex Room Kit as its base technology, bringing new capabilities such as speaker tracking, best overview, automatic wake-up, and people count to enable even smarter meetings, smarter presentation capabilities, and smarter room and device integrations. The Room 55 is rich in functionality and experience but is priced and designed to be easily scalable to all of your meeting rooms and spaces, whether registered on-premises to the Cisco Unified Communications Manager via SIP, or the Cisco Expressway Core via SIP or H.323, or to Cisco Webex cloud via SIP. Figure 8-13 illustrates a Cisco Webex Room 55.

Figure 8-13 *Cisco Webex Room 55 Dual*

The Cisco Webex Room 55 was granted the Red Dot award for innovation in design in 2017. This unit utilized the same 5k UltraHD camera as the Cisco Webex Room Kit and a 4K display to provide powerful and clear video up to 4Kp30. This H.265-compliant system can be ordered with a single display or with a dual display. The integrated Room Kit is located above the display for better camera angles and for better audio distribution throughout the meeting room. The integrated speakers offer stereo quality with a dedicated center speaker for optimal voice pick-up, and there is a built-in amplifier that delivers rich sound. The speakers are covered in a fabric for a more natural and inviting feel. The frame of the system is built using aluminum for a lighter design and sustainability. The height is increased over the MX300G2 to accommodate taller tables. The Webex Room 55 continues to support the same mounting options as the MX300G2 endpoints with your choice between a floor stand, wheel base, or wall mount. All three of these order options come with a Touch 10 controller, two additional table mics, and all the other cables needed to initially set up the system.

Key Topic

The Cisco Webex Room 70 G2 is similar to the Cisco Telepresence MX800. They both present a 70-inch display, they both support H.265HEVC, and they can both be ordered with a single or dual display on a floor stand or wall mount. However, there are some distinct differences between the two as well. Where the MX800 is equipped with the Precision 60 or SpeakerTrack 60 cameras, the Cisco Webex Room 70 G2 is built off the Cisco Webex Room Kit Plus. This system offers a powerful codec, a quad camera, and 70-inch single or dual 4K display(s) with integrated speakers and microphones, making it ideal for rooms that seat up to 14 people. It offers sophisticated camera technologies that bring speaker-tracking and auto-framing capabilities to medium and large-sized rooms, plus all of the AI integrations offered with the Cisco Webex Room Kit series of endpoints. The product is rich in functionality and experience but is priced and designed to be easily scalable to all of your conference rooms and spaces—whether registered on the premises to the Cisco Unified Communications Manager via SIP, or the Cisco Expressway Core via SIP or H.323, or to Cisco Webex in the cloud. Figure 8-14 illustrates the Cisco Webex Room 70 G2 product.

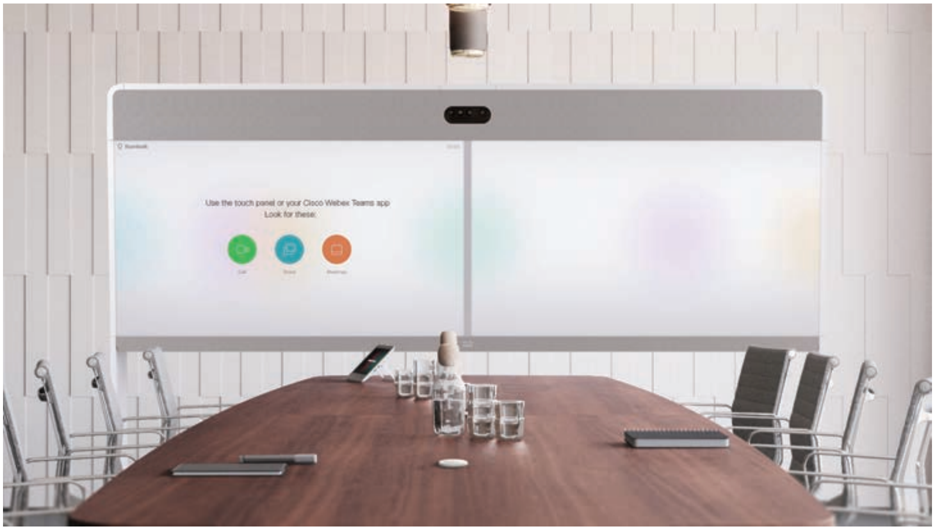


Figure 8-14 *Cisco Webex Room 70 G2*

The Cisco Webex Room Panorama is basically a Webex Room Kit Pro with a software key that unlocks some additional capabilities. In fact, if you have a Webex Room Kit Pro, you can order the key to upgrade the system to a Webex Room Panorama. It runs on the same CE software that the other Webex endpoints use, allowing this executive room system to register via SIP to Webex in the cloud, or on-premises to the Cisco Unified Communications Manager or Expressway. It also supports H.323 for registration to the Expressway. The powerful, integrated cameras deliver intelligent view capabilities, such as panorama video, automatic framing, and speaker tracking. Automatic noise suppression reduces meeting disruptions. Room Panorama supports up to three screens, dual-content sources, wireless sharing, and 4K content for great presentations. The people count feature offers usage metrics and resource allocation. Tight integrations with screens enhance user interactions, and APIs and macros allow for meeting personalization. With the enhanced capabilities and extensive registration options, there is no wonder this solution is the next generation to replace the IX5000.

Cisco Webex Board Endpoints

With the Cisco Webex Board, you can wirelessly present, whiteboard, video- or audio-conference, and even annotate shared content. It has everything you need for team collaboration at the touch of a finger. You can use the Cisco Webex Teams app to connect with virtual team members through the devices of their choice. This product comes in three models: the Cisco Webex Board 55s, the Cisco Webex Board 70s, or the new Cisco Webex Board 85. The Cisco Webex Board 55s is a fully self-contained system on a high-resolution 4K 55-inch LED screen with an integrated 4K camera, embedded microphones, and a capacitive touch interface. The Cisco Webex Board 70s is a fully self-contained system on a high-resolution 4K 70-inch LED screen with an integrated 4K camera, embedded microphones, and a capacitive touch interface. The Cisco Webex Board 85 is a fully self-contained system on a high-resolution 4K 85-inch LED screen with an integrated 4K camera, embedded microphones, and a capacitive touch interface. Figure 8-15 illustrates the three Webex Boards available for use today.

Figure 8-15 *Cisco Webex Board 85, 70s, and 55s*

Key Topic

With the original release of the Cisco Spark Board, which was later changed to the Cisco Webex Board, this series would only register to Cisco Webex in the cloud and required activation and registration to use the features available on these systems. This was due to the operating system that drove this endpoint. Since then, Cisco has changed the OS to the CE software so that the Webex Board will now register to the Cisco Unified Communications Manager via SIP or to the Cisco Expressway via SIP or H.323. You can also still register the Webex Board to the Webex Control Hub in the cloud. There are some limitations to registering the Webex Board on premises. At the time this chapter was written, the Webex Board can only be used for whiteboarding and annotation during local meetings when registered on premises. These whiteboard sessions cannot be saved, and whiteboarding and annotation are not supported during a call from the Webex Board. This capability is roadmapped for an undefined time in the future. However, you no longer have to unlock the whiteboarding functionality to use it, and these functions still work the same when registered to the Webex Control Hub. Table 8-9 illustrates some of the feature differences and commonalities between the three different models of the Cisco Webex Board.

Key Topic

Table 8-9 Cisco Webex Board Features

	Webex Board 55s	Webex Board 70s	Webex Board 85
Display	55" LED LCD 4K	70" LED LCD 4K	85" LED LCD 4K
Camera	Fixed lens Infinite focus 4kp60 resolution 83° horizontal field of view 55° vertical field of view	Fixed lens Infinite focus 4kp60 resolution 83° horizontal field of view 55° vertical field of view	Fixed lens Infinite focus 4kp60 resolution 83° horizontal field of view 55° vertical field of view
Participants	Up to 5 people	Up to 7 people	Up to 14 people
Dimensions (H×W×D)	36.2×55.7×7.5 in (919×1416×191 mm)	47.5×73.8×9.6 in (1207×1875×245 mm)	48.1×77.4×3 in (1221×1966×76 mm)
Audio Features	High-quality 20 kHz audio Acoustic echo cancellation Automatic gain control Autonoise reduction Active lip synchronization Mic array with voice tracking	High-quality 20 kHz audio Acoustic echo cancellation Automatic gain control Autonoise reduction Active lip synchronization Mic array with voice tracking	High-quality 20 kHz audio Acoustic echo cancellation Automatic gain control Autonoise reduction Active lip synchronization Mic array with voice tracking

Webex Desk Series Endpoints

Cisco developed a whole new line of video telepresence endpoints for the individual called Webex Desk Series endpoints. The three main Webex Desk endpoints come in three sizes: 15-inch, 24-inch, and 27-inch. Any of them can be used as a second screen for your laptop, which makes sharing content while in a meeting even easier. Figure 8-16 illustrates the three Webex Desk endpoints available in this series.

The Webex Desk Mini is designed with an integrated handle that makes it easy to move around from one room to another. It also comes equipped with privacy features such as noise removal, video backgrounds, and easy access to in-meeting controls. It provides everything you need to work. With its USB-C connection, you can double up your screen real estate, interact with any laptop content and applications, as well as join any conference app running on your laptop. It's the perfect work companion to your laptop. With a 64-degree, 8 MP camera, intelligent microphone array for focused sound pickup, and a powerful speaker system, you get a high-quality video and audio experience every time. Webex Desk Mini is an all-in-one collaboration device optimized to serve your needs to meet, work, and flex your inner creativity. It's a versatile, compact, and affordable device, designed to be your hybrid and remote work companion.

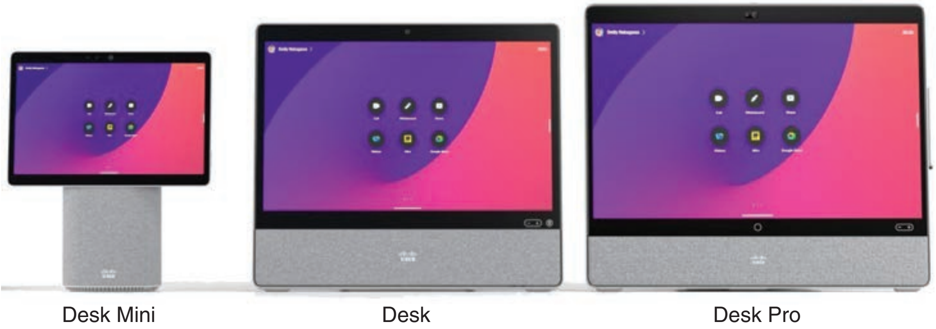


Figure 8-16 *Webex Desk Series*

The Webex Desk is the all-in-one collaboration and productivity device for your desk, whether you are at home, in the office, or in a shared space. It is purpose-built for collaborating, whether you're in a meeting, sharing your laptop screen, or brainstorming with a teammate. The Webex Desk device features a 24-inch, interactive 1080p display, 64-degree 8MP camera, full-range speaker, and a mic array with AI-powered background noise removal. This powerful device creates a clutter-free desk space, enabling you to be organized and productive. You can manage your workday with dynamic layouts and custom views, take the strain off your laptop, and optimize your meetings—all from a single system. You can meet without distractions or background noise as well as rock a presentation with immersive sharing. You can also co-create with digital whiteboarding and live content annotations. Easy setup and management capabilities allow customers to deploy and support thousands of devices at once. Also, with Control Hub, you'll gain insight into environmental health and device usage with the ability to triage issues from anywhere.

The Cisco Webex Desk Pro is an AI-powered collaboration device for the desk. It is purpose-built for collaboration, and it features a stunning 4K display, advanced cognitive collaboration capabilities such as Webex Assistant and facial recognition, and creative applications such as digital whiteboarding. You can easily pair your device wirelessly or dock your laptop and quickly join or start your meeting with one button to push. With a USB-C connection, the Webex Desk Pro becomes an all-in-one primary monitor and collaboration device that supports your videoconferencing software of choice. The Webex Desk Pro is designed for personal desk-based collaboration and focus rooms that accommodate one or two people. Packed with all the workplace and workflow capabilities included within Cisco's larger meeting room devices, the Webex Desk Pro is the ultimate desk-based collaboration device. At the time the Cisco Webex Desk Pro was announced, Cisco stated that it did not intend to replace the DX80 endpoint with this new addition. Table 8-10 compares the differences between each of the Webex Desk endpoints.

Key Topic

Table 8-10 Webex Desk Series Endpoints Features

Feature	Webex Desk Mini	Webex Desk	Webex Desk Pro
Display	15-inch	24-inch	27-inch
Camera	64° horizontal field of view, 50° vertical field of view 8MP image sensor, supports up to 30 fps	64° horizontal field of view, 50° vertical field of view 8MP image sensor, supports up to 30 fps	4K Ultra HD camera 71° horizontal field of view, 59° vertical field of view 12 MP image sensor, supports up to 30 fps
Multisite	No	3-way resolution up to 1080p30 + content up to 1080p15 4-way resolution up to 720p30 + content up to 1080p15	Adaptive SIP/H.323 MultiSite: 3-way, resolution up to 1080 at 30 fps, plus content up to 4K at 15 fps 4-way, resolution up to 720 at 30 fps, plus content up to 4K at 15 fps 5-way, resolution up to 720 at 30 fps, plus content up to 4K at 10 fps
Dimensions (H×W×D)	Width: 14.6 in (37.1 cm) Height: 16.25 in (41.3 cm) Depth: 5.3 in (13.5 cm) Weight: 8.5 lb (3.9 kg)	Width: 22.2 in (56.5 cm) Height: 18.7 in (47.4 cm) Depth: 2.8 in (7.0 cm) Weight: 19.2 lb (8.7 kg)	Width: 24.8 in (63 cm) Height: 20.1 in (51 cm) Depth: 3 in (7.5 cm) without desk stand, 7.1 in (18 cm) with desk stand attached Weight: 24.4 lb (11.6 kg)
Audio features	Acoustic Echo Cancellation (AEC) Active Lip Synchronization Automatic Gain Control (AGC) Focused sound pickup	High-quality full-band audio Automatic Gain Control (AGC) AI-powered noise removal	High-quality 20 kHz audio Automatic gain control Automatic noise reduction Active lip synchronization Keyclick suppression

Feature	Webex Desk Mini	Webex Desk	Webex Desk Pro
	De-reverberation Full duplex Full-band audio Music mode Noise reduction Noise removal Optimize for my voice Self-hear Third-party integration Ultrasound technology	Active lip synchronization Focused microphone pickup Music mode	

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 8-11 lists a reference of these key topics and the page numbers on which each is found.

Table 8-11 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Paragraph	xAPI and WebSockets	168
Paragraph	Audio Console with Graphical Equalizer	169
Paragraph	Intelligent Proximity for Content Sharing	169
Paragraph	DX80 Endpoint Overview	171
Table 8-2	DX70 and DX80 Feature Differences	172
Paragraph	SX10 Cabling	173
Paragraph	SX20 Camera Options	173
Paragraph	SX80 Capabilities	174
Table 8-3	SX Endpoint Feature Differences	175
List	Mounting Options for MX200 and MX300	176
Paragraph	MX700 and MX800 Displays	177
Table 8-4	Cisco Telepresence MX Series Feature Differences	178

Key Topic Element	Description	Page Number
Paragraph	Room Kit Mini AI Capabilities	180
Table 8-5	Webex Room Kit Mini Features	180
Paragraph	Webex Room Kit Components	181
Table 8-6	Webex Room Kit Features	182
Paragraph	Room Kit Plus Components	182
Table 8-7	Webex Room Kit Plus Features	183
Paragraph	Webex Room Kit Pro Components	184
List	Purchase Options for Webex Room Kit Pro	185
Table 8-8	Webex Room Kit Pro Features	185
Paragraph	Webex Room 55 Components	186
Paragraph	Webex Room 70 Components	187
Paragraph	Webex Board Registration	188
Table 8-9	Cisco Webex Board Features	189
Table 8-10	Webex Desk Series Endpoints	191

Define Key Terms

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

3G-SDI, AI, Autoframing, BFCP, CE, DND, DX, Euroblock, H.239, HD-SDI, Inductive Loop, Intelligent Proximity for Content Sharing, JSON, MIMO, MWI, MX, OBTP, OS, OSD, PoE, Precision Camera, PrecisionHD Camera, Precision MIC 20, SNR, Speaker Track 60, SX, Touch 10, TRC, UltraHD, VISCA, Webex Meeting App, Webex Teams App, WebSocket, xAPI

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List all of the endpoints in the DX, SX, and MX product lines.
2. List the mounting options for the MX300 G2 endpoint.
3. List all of the endpoints in the Webex endpoint product line.
4. What are the three purchase options for the Cisco Webex Room Kit Pro?
5. List all the system components that make up the IX5000 endpoint room system.

CHAPTER 9

Endpoint Registration

This chapter covers the following topics:

SIP Registration to the Cisco Unified Communications Manager: This topic will explain how to configure settings on UC phones and Telepresence endpoints for SIP registration to the Cisco Unified Communications Manager.

SIP Registration to the Cisco Expressway Core: This topic will explain how to configure settings on Telepresence endpoints for SIP registration to the Cisco Expressway Core.

H.323 Registration to the Expressway Core: This topic will explain how to configure settings on Telepresence endpoints for H.323 registration to the Cisco Expressway Core.

For any old-school voice engineers who might be reading this book, and to the general audience of people who may or may not understand this simple truth, the Cisco Unified Communications approach to provisioning and controlling phones has been to keep the intelligence in the call control systems, such as the Cisco Unified Communications Manager, and keep the phones dumb. This is a practice taken from tradition telephony over analog or digital circuit-switched systems and continues to be practiced cross-vendor in the IP telephony world. Cisco has added some intelligence to its UC phones, such as with Dial Rules, but on the norm, it continues to keep the intelligence at the hub of the call control systems. This idea has changed with Telepresence endpoints. There is a shared intelligence between the endpoint and the call control system, both in function and capabilities. What you will discover throughout this chapter is the much more advanced configuration options that exist on Telepresence endpoints versus their counterparts, UC phones. Topics discussed in this chapter include the following:

- SIP Registration to the Cisco Unified Communications Manager
- PoE
  - CDP and LLDP-MED
  - DHCP
  - TFTP
  - SIP Registration
  - ITL, CTL, and CAPF
- SIP Registration to the Expressway Core
- DHCP versus Static IP

- Manual Configuration of SIP Settings

- H.323 Registration to the Expressway Core
  - H.323 Aliases
  - Manual Configuration of H.323 Settings

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 1.1.g Security (certificates, SRTP, TLS)
- 1.3.g Certificates
- 2.3 Deploy SIP 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 9-1 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
SIP Registration to the Cisco Unified Communications Manager	1–6
SIP Registration to the Expressway Core	7–8
H.323 Registration to the Expressway Core	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. How much power can be supplied to a phone using Cisco prestandard PoE?

a. 5.5W

b. 7W

c. 14.5W

d. 15W

2. When you are configuring a VLAN on a switchport, which of the following commands will configure the phone to use IEEE priority tagging for voice traffic and to use the default native VLAN to carry all traffic?
   a. 802.11n
   b. 802.1q
   c. 802.1p
   d. 802.3af
3. When the CUCM is used as the DHCP server, how many devices can it support?
   a. 100
   b. 500
   c. 1000
   d. 10,000
4. The Maximum Serving Count service parameter specifies the maximum number of requests that can be concurrently handled by the TFTP server on the CUCM. What is the default value of this parameter?
   a. 2500
   b. 5000
   c. 7500
   d. 10,000
5. Which SIP registration header field contains the address of record of the person responsible for the registration?
   a. Request URI
   b. To
   c. From
   d. Call-ID
6. Which of the following are considered Security By Default mechanisms on the CUCM? (Choose two.)
   a. ITL
   b. CTL
   c. CAPF
   d. TLS
   e. TLS Verify
   f. TVS
7. Which of the following is a required setting when configuring static network information on an endpoint?
   a. Gatekeeper address
   b. DNS
   c. TFTP
   d. Default gateway address
8. Which of the following commands is required before the SIP endpoint can register to the Cisco Expressway when configuring the CE endpoint using CLI?

- **a.** **xConfiguration NetworkServices SIP Mode: On**
- **b.** **xConfiguration Provisioning Mode: VCS**
- **c.** **xConfiguration Provisioning Mode: TMS**
- **d.** **xConfiguration SIP DisplayName:** *name*

9. Which of the following aliases is acceptable as an H.323ID?

- **a.** 555 - 1212
- **b.** John Hancock
- **c.** John 1212
- **d.** John@Hancock

10. An administrator is using the CLI to configure a DX80 endpoint to register to a Cisco Expressway Core. While configuring the alias, the administrator configures an H.323 ID when it should not have been. How can the administrator remove the H.323 ID using the CLI?

- **a.** **xconfiguration h323 h323alias remove all**
- **b.** **xconfiguration h323 h323alias id:** *leave blank*
- **c.** **xconfiguration h323 h323alias id: delete**
- **d.** **xconfiguration h323 h323alias id: ""**

Foundation Topics

SIP Registration to the Cisco Unified Communications Manager

Chapter 5, "Communication Protocols," provided a high-level overview of the SIP registration process to the Cisco Unified Communications Manager. The basic elements of the whole SIP registration process can be summarized in the following order:

1. The endpoint obtains power.
2. The endpoint loads the locally stored image file.
3. The endpoint communicates with the switch using CDP or LLDP-MED.
4. The endpoint negotiates DHCP with the DHCP server.
5. The endpoint is issued CTL (optional) and ITL certificates from the Cisco Unified Communications Manager.
6. The endpoint communicates with the TFTP server.
7. The endpoint registers to the CUCM.

Although many moving parts must be configured for this registration process to work, after each component is configured, very little must be done on the end user's part for devices to register to the Cisco Unified Communications Manager. This process is designed to ease the registration process and also allow engineers to mass-deploy tens of thousands of endpoints at the same time. When the components involved with this process are deployed properly, little to no configuration needs to be set up on the endpoint itself. You can just power the system on and let these services provision all the various settings on the phones.

The following sections describe how to configure these various components so that this provisioning process will operate correctly.

PoE

An endpoint can receive power in two ways: Power over Ethernet (PoE) or through a power cube, which is the traditional cable you plug into the system and the wall outlet. All Telepresence endpoints require a power cube to be used, with the one exception of the Cisco Telepresence SX10. All of the Cisco UC phones can support either a power cube or PoE. Because PoE is the expected form of power, none of the UC phones come standard with a power cube; this component must be ordered separately. A big difference between some of the phones as related to PoE is the type or class of PoE supported.

PoE, also referred to as *inline power*, is the capability for the LAN switching infrastructure to provide power over a copper Ethernet cable to an endpoint or powered device. Cisco developed and first delivered this capability in 2000 to support the emerging IP telephony deployments. IP telephones, such as desktop PBX phones, need power for their operation, and PoE enables scalable and manageable power delivery and simplifies deployments of IP telephony. Because these early PoE-capable devices were basic phones without a lot of features added to them, the power requirements were pretty low. Cisco's prestandard PoE, which was called inline power, supported only 7 watts (7W) of power. The IEEE quickly recognized the contribution Cisco made to the IT industry and began working on a standardization for PoE. The first standard for PoE that could be used industrywide and applicationwide was 802.3af. With the advent of 802.3af came many more devices that could support PoE, including wireless access points, video cameras, point-of-sale devices, security access control devices such as card scanners, building automation, and industry automation, to name a few.

The IEEE 802.3 standard outlines two types of devices: power sourcing equipment (PSE) and powered devices (PDs). Power sourcing equipment provides power to the powered devices. A PSE can support power delivery Type A, Type B, or both. Type A involves sending power over two unused pairs or wires on a CAT3, CAT5, or CAT5E cable. This works well for links up to 100 Mbps, but Gigabit Ethernet uses all the copper pairs in a CAT5E cable. Therefore, Type B uses a "phantom power" technique to send power and data over the same pairs. When an Ethernet device is connected to a PSE, the PSE initially applies a low voltage (2–10 volts) to sense whether the device is a PoE PD. If it is, the PD will send a return current back to the PSE, and 48 volts will be supplied so the device can power on and load its locally stored image file. If no return current is sent back to the PSE, the device connected is not a PD, such as a computer connected over Ethernet, and no power will be supplied. The maximum power that a PSE will supply down an Ethernet cable using 802.3af is 15 watts; however, due to possible losses on a long cable, the maximum power that a PD can receive down an Ethernet cable using 802.3af is 12.95 watts.

The IEEE 802.3at standard, also known as PoE+, supports up to 25.5W of power on the ports, allowing devices that require more than 15.4W to power on when connected to the PoE+ ports. Several Cisco switches support 802.3at PoE, including the Meraki MS series switches. Based on the classification currently used by the device, the Meraki MS switch will classify the device as a Class 0, 1, 2, 3, or 4 type device and apply the proper standards-defined behaviors to the port. Table 9-2 describes these five classifications on Meraki switches.

Table 9-2 Meraki Switch PoE Classifications

Class	Usage	Classification Current [mA]	Power Range [watt]	Class Description
0	Default	0–4	0.44–12.94	Classification unimplemented
1	Optional	9–12	0.44–3.84	Very low power
2	Optional	17–20	3.84–6.49	Low power
3	Optional	26–30	6.49–12.95	Mid power
4	Valid for 802.3at (Type 2) devices, not allowed for 802.3af devices	36–44	12.95–25.50	High power

When a PD is connected to an 802.3at switch port, a lower power voltage can be supplied because 802.at is backward compatible. There is a limit to how much power may be drawn across wires before electrical damage occurs due to overheating within connectors and cable bundles. There is also a concern over signaling interference with this protocol. Some of these issues are resolved by using multiple pairs to deliver the necessary power. At the moment, 802.3at limits the number of pairs that can carry power to two. A current limit of 720mA is being considered, allowing 29.5W per pair; however, the IEEE is working on Draft 3.0 to reduce this to 600mA giving 25W per pair, or 50W per device. The IEEE is also looking at mandating Category 5 cables and later to be used with 802.3at so that you do not have to worry about supporting Category 3 cabling. With 802.3at the maximum power that can be delivered to the application is 50W. The first detection pulse, or *classification pulse*, from the PSE will be the same as 802.3af, to which the 802.3af PDs will respond normally. A second PoE Plus pulse then will cause an 802.3at PD to respond as a Class 4 device and draw the Class 4 current. After this has happened, there will be a data exchange where information such as duty-cycle, peak, and average power needs will be shared. Other features to be catered for in 802.3at include dynamic power assignment, leading to more efficient power supply designs and consequent power saving.

For a Cisco UC phone to receive PoE from a switch, it is essential to connect the patch cable coming from the switch into the appropriate port on the phone. You should be aware of three switch ports in Cisco phones. There are two physical switch ports on the back of each phone. One of the switch ports is called a *network port*, and this is the port to which the patch cable that connects back to the switch should be connected. The second physical port on the back of a Cisco phone is called the *PC port*, and it is the port that a computer can be connected to in order to receive network access. PoE will not be supplied to the phone if the network cable from the switch is connected to the PC port, nor will the phone be able to communicate with the switch. These two physical interfaces are easy to recognize because there is a graphic below each port to describe that port's purpose. The computer port has the graphic of a computer monitor, and the network port graphic displays three squares interconnected with lines, signifying the network. The third port on a Cisco phone that you should be aware of is a virtual port located in the phone's software, which bridges between the computer port and the network port. The phone uses this port to control how packets are marked for the purpose of quality of service (QoS) before they are sent to the switch. PoE promises to create a new world of networked appliances as it provides power and data connectivity over existing Ethernet cables. Table 9-3 identifies the three PoE types discussed in this section. Bear in mind that Cisco has not created or sold prestandard PoE devices since the late 2000s. The information on prestandard PoE is for comparison purposes only.

Table 9-3 Three PoE Types Supported on Cisco Switches

Prestandard Inline PoE	802.3af PoE	802.3at PoE+
Cisco Proprietary	IEEE standard	Backward compatible with 802.3af; PoE+ just adds an additional class of power to the 802.3af standard
10/100 only	15.4W per port	30W per port
7W per port	Compatible with Gigabit Ethernet	Relatively new; currently only Cisco is shipping PoE+ phones
Incompatible with all non-Cisco devices that accept Power over Ethernet	PoE devices are not compatible with Cisco prestandard PoE; the power negotiation process is completely different	
	Cisco PoE switches are backward compatible with prestandard PoE	
	Enough power for most IP phones and wireless access points from all manufacturers	

No settings need to be configured on a Cisco phone to enable PoE. These settings are hardcoded into the phone itself. Most Cisco PoE-capable switches come preconfigured to support PoE as well; however, some settings on a Cisco switch can be configured to disable or enable PoE on certain ports and even boost the power capabilities on specific ports. The following examples illustrate how to configure PoE on a Cisco Catalyst 4500 series switch. Depending on the model number you are configuring, the commands you use might vary slightly. You can enter the following commands into a Cisco switch to enter configuration mode and configure PoE on a specific switchport:

```
Switch# configure terminal

Switch(config)# interface {fastethernet|gigabitethernet} (slot/
port)

Switch(config-if)# power inline {auto[max milli-watts] | never
| static [max milli-watts]}

Switch(config-if)# end

Switch# show power inline {fastethernet|gigabitethernet} slot/
port
```

An example of the preceding configuration could be as follows:

```
Switch# configure terminal
```

```
Switch(config)# interface fastethernet 0/1

Switch(config-if)# power inline auto 15.4

Switch(config-if)# end

Switch# show power inline fastethernet 0/1
```

As you can see from the preceding example, you can configure three settings on a switchport for PoE: auto, static, and never. The auto setting is the default value, and this setting allows the supervisor engine on the switch to direct the switching module to power up the interface only if the switching module discovers the phone and the switch has enough power. This mode has no effect if the interface is not capable of providing PoE. The static setting is recommended on high-priority PoE interfaces. The supervisor engine will pre-allocate power to the interface, even when nothing is connected, guaranteeing that there will be power for the interface. If the switch does not have enough power for the allocation, the command will fail. The supervisor engine directs the switching module to power up the interface only if the switching module discovers the powered device. Both of these modes allow you to specify the maximum wattage that is allowed on the interface. If you do not specify a wattage, the switch will deliver no more than the PSE hardware-supported maximum value. The never setting will disable PoE on that particular switchport. This setting is typically used when the interface is intended to be used only as a data interface. The supervisor engine never powers up the interface, even if an unpowered phone is connected. This mode is needed only when you want to make sure power is never applied to a PoE-capable interface. The switch can measure the actual PoE consumption for an 802.3af-compliant PoE module and displays this in the **show power inline** *module* command from the privileged EXEC mode.

One other command worth knowing can boost the power on a specific PoE port if not enough power is available: **power inline delay shutdown**. You might use this command when a prestandard PoE switch is being used to try powering up an 802.3af phone. You also can use this command on an 802.3af switch trying to power up an 802.3at device. However, it is important to understand that when this command is used, you are essentially "borrowing from Peter to pay Paul," as the saying goes. Power is being taken from another switchport to supply extra power to that particular port being configured. If you use this command, you will not be able to support as many phones on that switch as it was originally designed to support. The command you can use from the configuration mode prompt is as follows:

```
Switch(config-if)# power inline delay shutdown 20 initial 300
```

The **power inline delay shutdown** command configures the port to delay shutting down. This command is useful when a phone requesting more power than the port is originally designed to support would normally go into a cyclical reboot. The initial time period—in this example, 20 seconds—begins when the IEEE-compliant powered device is detected by the switch. If link-down occurs on the connected device during the initial time period, the shutdown time, **initial 300**, determines how long the switch continues to provide power to the device.

CDP and LLDP-MED

The next step in the registration process to the Cisco Unified Communications Manager, after the phone has powered on and loaded the locally stored image file, is to communicate with the switch. Two protocols can be used for this type of communication: Cisco

Discovery Protocol (CDP) and Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED).

CDP is a proprietary protocol that will work only when a Cisco device is communicating to a Cisco device, such as a Cisco phone communicating with a Cisco switch.

If either one of the devices, the phone or the switch, is not a Cisco product, the LLDP-MED protocol will need to be used instead. Several LLDP protocols are available, but LLDP-MED is specifically designed for voice and video communication. Now that it has been established that communication must occur between the phone and the switch, exactly what information is being exchanged is equally important to understand.

A PSE has a PoE “power budget,” which is simply the total power the switch can supply down Ethernet cables. Each time a PD is plugged into the PSE, the PSE subtracts the PD’s maximum power usage from its power budget. If the power budget is all used up, and another PD is connected, that PD will not receive any power. To avoid this problem, 802.3af specifies a method whereby a PD can indicate to the PSE what its maximum power usage will be, by indicating that it complies with one of four “power classes” specified in the standard. For example, if a PD indicates that it complies with power class 2, the PSE knows that it only has to subtract 3.84 watts from its power budget for that PD, thus leaving more power budget for other PDs. In this manner, after the phone powers on, the phone is capable of sending to the switch the required amount of power needed to sustain its core systems. CDP, or LLDP-MED, is the mechanism used to communicate these power adjustments to the switch.

Before the phone obtains its IP address, the phone must also determine which VLAN it should be in by means of the CDP communication that takes place between the phone and the switch. This communication allows the phone to send packets with 802.1Q tags to the switch in a “voice VLAN” so that the voice data and all other data coming from the PC behind the phone are separated from each other at Layer 2. Voice VLANs are not required for the phones to operate, but they provide additional separation from other data on the network. Voice VLANs can be assigned automatically from the switch to the phone, thus allowing for Layer 2 and Layer 3 separations between voice data and all other data on a network. A voice VLAN also allows for a different IP addressing scheme because the separate VLAN can have a separate IP scope at the Dynamic Host Configuration Protocol (DHCP) server. Applications use CDP messaging from the phones to assist in locating phones during an emergency call. The location of the phone will be much more difficult to determine if CDP is not enabled on the access port to which that phone is attached. There is a possibility that information could be gathered from the CDP messaging that would normally go to the phone, and that information could be used to discover some of the network. As mentioned before, not all devices that can be used for voice or video with Cisco Unified Communications Manager are able to use CDP to assist in discovering the voice VLAN. Third-party endpoints do not support CDP. To allow device discovery when third-party devices are involved, you can use LLDP-MED. This protocol defines how a switch port transitions from LLDP to LLDP-MED if it detects an LLDP-MED-capable endpoint. Support for both LLDP and LLDP-MED on IP phones and LAN switches depends on the firmware and device models. To determine if LLDP-MED is supported on a particular phone or switch model, you can check the specific product documentation, release notes, and whitepapers.

VLANS can be configured on specific switchports as a Voice VLAN ID (VVID) or as a data VLAN, or both as a voice and data VLAN. Video will typically use the VVID along with audio. It is not necessary to create a separate voice and video VLAN. Because VLANs will be used to communicate the Layer 2 class of service (CoS) to the phone, it is important to also set up CoS tagging on the switch for specific VLANs. CoS and QoS will be discussed in more depth in Chapter 13, "Layer 2 and Layer 3 QoS Parameters." The following commands outline how to configure VLANs on the switchports and enable CoS. There are several ways this can be done, and the commands may vary depending on the switch being used. These examples are based on current Cisco Catalyst Switch series.

```
Switch# configure terminal

Switch(config)# vlan number

Switch(config-vlan)# name name

Switch(config-vlan)# exit

Switch(config)# interface {fastethernet|gigabitethernet} (slot/
port)

Switch(config-if)# mls qos trust cos

Switch(config-if)# switchport voice {detect cisco-phone [full-
duplex] | vlan {vlan-id | dot1p | none | untagged}}

Switch(config-if)# end

Switch# show vlan
```

Issuing the **configure terminal** command allows you to enter the configuration mode.

Next, you can create a VLAN using the **vlan** *number* command and assign a **name** to the VLAN for a description.

After exiting VLAN configuration mode, you issue the **interface {fastethernet|gigabitethernet}** (*slot/port*) command to enter the interface configuration mode. Next, you issue the **mls qos trust cos** command so that this switchport will trust the CoS-to-QoS mapping embedded in the switch. Then you enter the **switchport voice {detect cisco-phone [full-duplex] | vlan {***vlan-id* **| dot1p | none | untagged}}** command. The **detect** part of the command will configure the interface to detect and recognize a Cisco IP phone. The **cisco-phone** is the only option allowed when you initially implement the **switchport voice detect** command. The default is **no switchport voice detect cisco-phone [full-duplex]**. The **full-duplex** command is optional. You can configure the switch to accept only a full-duplex Cisco IP phone. This setting is highly recommended because you do not want voice or video traffic to use half-duplex. Calls will consume twice the bandwidth, and connections will be spotty at best. The **vlan** *vlan-id* command will configure the phone to forward all voice traffic through the specified VLAN. By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5. Valid VLAN IDs are 1 to 4094. The **dot1p** command will configure the phone to use IEEE 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Alternatively, the **none** command will allow the phone to use its own configuration to send untagged voice traffic. Another alternative is the **untagged** command, which will configure the phone to send untagged voice traffic. Using **none** or **untagged** is not recommended for voice traffic.

You type **end** to exit configuration mode and then issue the **show vlan** command to verify the VLAN configuration. The following example shows how these commands should appear:

```
SW1(config)# vlan 200
SW1(config-vlan)# name VVID
SW1(config-vlan)# exit
SW1(config)# Interface fastethernet 0/1
SW1(config-if)# mls qos trust cos
SW1(config-if)# switchport voice vlan 200
SW1(config-if)# end
```

As an alternative to the **switchport voice vlan 200** command, you could use **switchport voice detect cisco-phone full-duplex** or **switchport voice vlan 802.1p**. The 802.1p will tag voice traffic with a CoS priority of 5 but use the default VLAN to send traffic. The **detect** command will send untagged traffic to the switch. Neither one of these options is ideal in a voice or video deployment, which is why the example uses the **voice vlan** command. In the preceding example, only the voice VLAN was applied to the switchport. Both the voice VLAN and the data VLAN can be applied to the switchport as another option for VLAN configuration. The phone will then use these VLANs to tag all communication originating from the phone with the voice VLAN, and all information originating from a connected computer with the data VLAN. The following example demonstrates how this might look on a switchport:

```
SW1(config)# vlan 200
SW1(config-vlan)# name VVID
SW1(config-vlan)# exit
SW1(config)# vlan 100
SW1(config-vlan)# name Data
SW1(config-vlan)# exit
SW1(config)# Interface fastethernet 0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 100
SW1(config-if)# switchport voice vlan 200
SW1(config-if)# end
```

Key Topic

A computer connected to the phone will normally send packets as untagged. The command **switchport mode access** will force the port into access mode. The phone will tag computer traffic as data and will tag phone traffic as voice (or video when applicable). Then the command **switchport access vlan 100** is used to identify that vlan100 should be used for access tagging of all data traffic originating from the computer. The command **switchport voice**

vlan 200 is used to identify that vlan200 should be used for tagging all voice and video traffic originating from the phone. If CoS Priority 5 should be used for Layer 2 QoS, you will still need to add the command **mls qos trust cos**, as mentioned previously. When third-party phones are being used, two VLANs on a single switchport may not work for appropriate tagging. LLDP-MED and most other vendor phones do not support this feature.

VLAN discovery is automatic on all Cisco IP phones and Telepresence endpoints, so no settings have to be configured on these devices for VLAN tagging to occur. However, some circumstances may prevent the phone or endpoint from discovering the VLAN. Therefore, you can manually configure a VLAN on a phone or endpoint. The following information on how to configure VLAN settings manually on a Cisco phone is applicable to the 7800 and 8800 series phones. These settings also are available on other Cisco phones, but the menu options to get to these settings may be different.

Key Topic

Step 1. Press the **Settings** button on your phone. This is the button with the gear icon.

Step 2. Use the circular navigation button on the phone to choose the **Admin Settings** menu option, or select the number associated with the menu option using the numeric keypad on the phone.

Step 3. Choose the **Network Setup** menu option in the same manner as above.

Step 4. In the next set of menus that appear, choose **Ethernet Setup**. There are several menu options under Ethernet Setup.

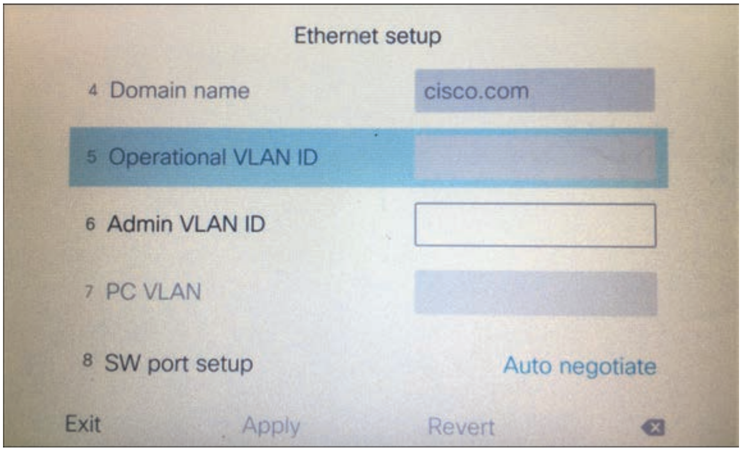
Step 5. Scroll down to the Operational VLAN ID field. This field is not configurable from the user interface but will display the Voice VLAN ID if one was provided from the switch.

Step 6. If the Operational VLAN ID field is blank, you will need to configure the Admin VLAN ID field with the appropriate VLAN ID.

Step 7. The PC VLAN field is another field that is not configurable from the user interface, unless the Admin VLAN ID was configured first. It will display the data VLAN ID if one was provided from the user interface. Otherwise, you will need to configure one.

Step 8. Press the **Apply** softkey to save the configured settings. Figure 9-1 illustrates these menu options under the Ethernet Configuration menu.

VLAN settings can also be configured on a Cisco CE software-based endpoint. It is important to note here that CE software-based endpoints have auto VLAN discovery enabled by default, but TC software-based endpoints do not. When CE endpoints are registering to a Cisco Unified Communications Manager, no settings have to be preconfigured on the endpoint for that endpoint to register. However, with legacy TC endpoints, you may have to preconfigure some settings on the endpoint before the endpoint can register to the Cisco Unified Communications Manager. The instructions that follow outline how to configure VLAN settings on a Telepresence endpoint and are based on CE software. Some menus may be different if you are configuring a Telepresence endpoint running the TC software. Also note that if the **NetworkServices > CDP Mode** is set to **Off**, VLAN discovery will not work, even though Auto Discovery may be enabled.



Ethernet setup

4 Domain name cisco.com

5 Operational VLAN ID

6 Admin VLAN ID

7 PC VLAN

8 SW port setup Auto negotiate

Figure 9-1 *Ethernet Configuration Menu Options on Cisco 7800 and 8800 Series Phones*

Step 1. Log in to the web interface for the CE endpoint you want to configure.

Step 2. Navigate to **Setup > Configuration > NetworkServices** and verify the CDP Mode is set to **On**. This setting should be on by default. Notice that LLDP-MED is not supported on CE software-based endpoints.

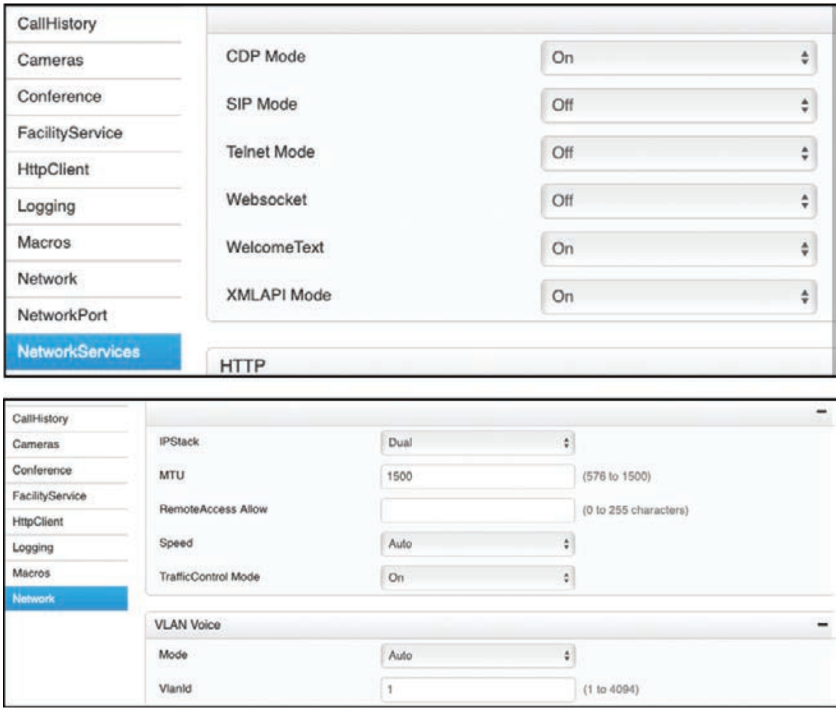
Step 3. In the left column, click the **Network** menu and scroll to the bottom of the page. Under the VLAN Voice section, you can set the VLAN Mode to **Auto**, **Manual**, or **Off**.

Step 4. Below the Mode setting is the VlanId setting. This will default to the value 1, and can be set between 1 and 4094. This field does not apply if the Mode is set to Auto. If you change the Mode to Manual, you will also need to enter the VlanId value that is appropriate to the voice VLAN configured on the switch.

Figure 9-2 illustrates how to configure CDP and VLAN settings on a Cisco CE software-based endpoint.

DHCP

After a phone has adjusted the power consumption from the switch and requested the VLAN information, the next step in the process is to establish appropriate network information through the DHCP process. The minimum amount of network information any device must possess in order to communicate across a network is an IP address, subnet mask, and default router address, also called a *default gateway address*. Additional network information that can be obtained using DHCP includes Domain Name System (DNS) addresses and Trivial File Transfer Protocol (TFTP) server addresses. The TFTP server address can be obtained by configuring Option 66 or Option 150. Option 66 is an open standard that will operate on any vendor's DHCP server. Option 150 is a Cisco proprietary protocol that will operate only on Cisco's and a few other vendors' DHCP servers. Additionally, Option 66 will support only one TFTP address, whereas Option 150 will support up to two addresses, making it a more redundant option to Option 66. There are many pros and cons to using DNS, but one great advantage in this context is that the TFTP server address can be configured as the URL of the Cisco Unified Communications Manager cluster so that more than one address can be delivered to the device trying to register.



CDP Mode On
SIP Mode Off
Telnet Mode Off
Websocket Off
WelcomeText On
XMLAPI Mode On

IPStack Dual
MTU 1500 (576 to 1500)
RemoteAccess Allow (0 to 255 characters)
Speed Auto
TrafficControl Mode On

VLAN Voice
Mode Auto
VlanId 1 (1 to 4094)

Figure 9-2 *CDP and VLAN Settings on a Cisco CE Software-Based Endpoint*

Many types of DHCP services can be used. The Cisco Unified Communications Manager has a built-in DHCP service, but there are limitations to using this option. It is recommended to use the DHCP service only for phones and Telepresence endpoints, but not for computers or other such devices. There is a capacity limit of 1000 devices that can receive DHCP information, and it is more complex to set up the DHCP service on the CUCM as opposed to another device because a helper address needs to be configured and certain devices will need to be restricted from using this service. A commonly used DHCP service is on the router itself. There, a greater pool of addresses can be set up, it can be used for all devices communicating on the network, and it is relatively easy to set up. The following example demonstrates how to set up DHCP on a router to support IP addressing, along with DNS address and TFTP address distribution. You should understand that this is not the only way to configure DHCP on a router, but one possible way it can be configured.

Key Topic

```
Router# configure terminal
Router(config)# ip dhcp pool caret&stic
Router(dhcp-config)# network 10.0.0.0 255.255.255.0
Router(dhcp-config)# default-router 10.0.0.1
Router(dhcp-config)# option 150 ip cucm-cluster.caret&STIC.com
Router(dhcp-config)# dns-server 8.8.4.4
Router(dhcp-config)# domain-name caret&STIC.com
Router(dhcp-config)# lease 7
Router(dhcp-config)# exit
```

The **ip dhcp pool** *name* command creates a pool from which IP addresses can be issued to devices that send a DHCP request. The *name* field can be any name you want to give to the pool. In the preceding example, **caret&STIC** is a fictitious company name that has also been assigned to the DHCP pool. The next command, **network** *IP address subnet mask*, establishes all the available addresses within a pool that can be used for DHCP assignment. This is where you will need to be careful. Servers will often be assigned static IP addresses, which should not be included in the pool. You can either configure a smaller subnet of addresses here, or you can go back and issue an exclusion range of addresses that will not be used in DHCP assignments. An example of how to issue a range of excluded addresses is as follows:

```
Router(config)# ip dhcp excluded-address 10.0.0.1 10.0.0.99
```

In this example, all the IP addresses from 10.0.0.1 to 10.0.0.99 are excluded from the DHCP pool. The first IP address that will be provided to a device that sends a DHCP request will be 10.0.0.100. The **default-router** *IP address* command establishes the default gateway address that will be assigned to devices. Devices trying to route data to another part of the network will send that data to this router address, and the default router will forward that traffic toward the intended destination across the network. The **option 150 ip** *TFTP server address* command will assign the TFTP server address to the endpoint. If DNS is used, the TFTP server address could be the URL address of the destination TFTP server. Otherwise, the IP address of the TFTP server can also be used. You could also use the **option 66 ip** *address* command here, but Cisco recommends using Option 150 when Cisco routers and phones are being leveraged. The **dns-server** *IP address* command allows up to three DNS server addresses to be listed. All addresses will be sent to devices in the order listed here, and they must be in the form of an IP address. To enter more than one DNS address, you must use a space between the different addresses. The **domain-name** *name* command will assign the domain to devices through DHCP. This allows for easier searching within a domain, such as registering Jabber to the IM and Presence server. When a user signs into Jabber with *user_name@domain*, the Jabber client will search for a *cup_login* SRV record associated with the *domain*. When DNS returns the address of the IM and Presence server, the Jabber client will try to register with the *user_name* part of the URI. Jabber will be covered in more depth in Chapter 26, "Users and Cisco Jabber Soft Clients." Finally, the **lease** *n* command determines how long a leased address can be used by a device before a new lease has to be requested. By default, the duration of a lease is one day. When you enter the **lease** *n* command, this duration will be extended to that number *n* of days. Actually, three values can be entered here to extend the duration to days, hours, and minutes. For example, if you wanted leased addresses to be available for 8 hours and 30 minutes, you could enter the command **lease 0 8 30**. This establishes DHCP leases to 0 days, 8 hours, and 30 minutes.

DHCP can be enabled or disabled on Cisco UC phones, but this setting is enabled by default. If the setting is disabled, static IP settings must be configured manually on the Cisco phone. The following steps outline how to disable DHCP and configure static IP settings on Cisco 7800 and 8800 series phones. If you are configuring a different phone model, the menus to configure these settings may be different.

Key Topic

Step 1. Press the **Settings** button on your phone. This is the button with the gear icon.

Step 2. Use the circular navigation button on the phone to choose the **Admin Settings** menu option, or select the number associated with the menu option using the numeric keypad on the phone.

Step 3. Choose the **Network Setup** menu option in the same manner as above.

Step 4. In the next set of menus that appear, choose **Ethernet Setup**. There are several menu options under Ethernet Setup.

Step 5. Choose **IPv4 Setup** to enter into the IPv4 menu options.

Step 6. The DHCP field is set to On by default. Change this field to **Off** to manually configure the IP information.

Step 7. Enter the IP Address, Subnet Mask, and Default Router information in the appropriate fields.

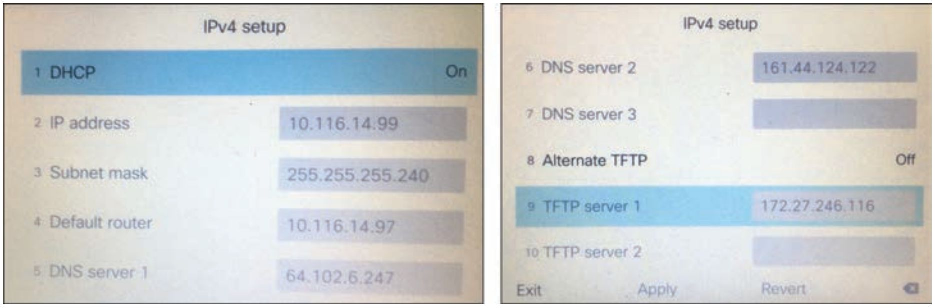
Step 8. The DNS Server 1, DNS Server 2, and DNS Server 3 fields allow you to enter up to three DNS addresses.

Step 9. The Alternate TFTP field indicates whether the phone is using an alternate TFTP server address. If this setting is set to Off, which is the default value, the phone is expecting the TFTP server address to come from Option 150 (or Option 66). If you change the value to **On**, you must manually enter a TFTP server address.

Step 10. The TFTP Server 1 and TFTP Server 2 fields allow you to enter a primary (1) and backup (2) TFTP server address.

Step 11. Click the **Apply** soft key to save these changed settings. The phone must be reset for the new network information to bind to the phone.

Figure 9-3 illustrates how to configure these network options on a Cisco 8865 phone.



IPv4 setup

1 DHCP On
2 IP address 10.116.14.99
3 Subnet mask 255.255.255.240
4 Default router 10.116.14.97
5 DNS server 1 64.102.6.247

IPv4 setup

6 DNS server 2 161.44.124.122
7 DNS server 3
8 Alternate TFTP Off
9 TFTP server 1 172.27.246.116
10 TFTP server 2

Figure 9-3 *Network Configuration Option on a Cisco 8865 Phone*

DHCP can be enabled or disabled on Cisco CE software-based endpoints, but this setting is enabled by default. If the setting is disabled, then static IP settings must be configured manually on the CE endpoint. The steps that follow describe how to disable DHCP and configure static IP settings on Cisco Telepresence CE software-based endpoints. If your endpoint is running the legacy TC software, the menus to configure these settings might be different.

Key Topic

Step 1. Log in to the web interface for the CE endpoint you want to configure.

Step 2. Navigate to **Setup > Configuration > Network** and locate the DNS section (second section down from the top).

Step 3. Enter the Domain in the Domain Name field. Enter up to three DNS addresses in the Server 1 Address, Server 2 Address, and Server 3 Address fields.

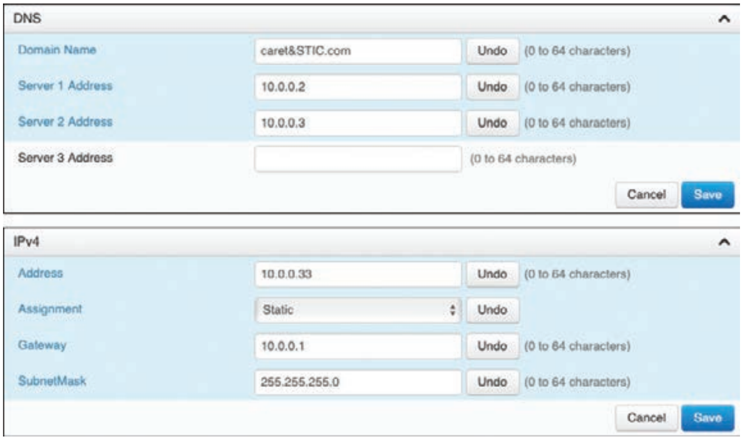
Step 4. Choose **Save** in the bottom-right corner of this section, and then scroll down to the IPv4 section.

Step 5. Change the Assignment field from DHCP to **Static**.

Step 6. Enter an IP address for the endpoint in the Address field. Enter the Default Router address in the Gateway field and enter the Subnet Mask address in the SubnetMask field.

Step 7. Choose **Save** in the bottom-right corner of this section. You will have to restart the endpoint before these changes will take effect.

Figure 9-4 illustrates the network setting menus on a CE software-based endpoint.



DNS

Domain Name	caret&STIC.com	Undo	(0 to 64 characters)
Server 1 Address	10.0.0.2	Undo	(0 to 64 characters)
Server 2 Address	10.0.0.3	Undo	(0 to 64 characters)
Server 3 Address			(0 to 64 characters)

IPv4

Address	10.0.0.33	Undo	(0 to 64 characters)
Assignment	Static	Undo	
Gateway	10.0.0.1	Undo	(0 to 64 characters)
SubnetMask	255.255.255.0	Undo	(0 to 64 characters)

Figure 9-4 *Network Setting Menus on a CE Software-Based Endpoint*

Step 8. To configure the TFTP server address, choose the **Provisioning** menu in the left column.

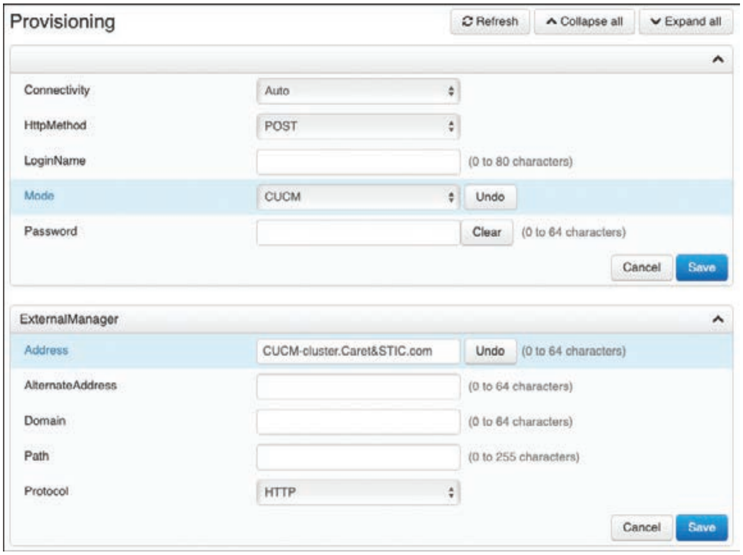
Step 9. In the top section, ensure the Connectivity field is set to Auto, and then change the Mode to **CUCM**.

Step 10. Choose **Save** in the bottom-right corner of this section.

Step 11. In the ExternalManager section, enter the address of the TFTP server in the Address field. You can enter a second AlternateAddress as well, or just use a URL address for the Cisco TFTP Server cluster in the first Address field.

Step 12. Ensure the Protocol field is set to **HTTP**, and then choose the **Save** button in the bottom-right corner of that section.

Figure 9-5 illustrates how to configure the Provisioning settings on a CE software-based endpoint.



Connectivity	Auto	
HttpMethod	POST	
LoginName		(0 to 80 characters)
Mode	CUCM	Undo
Password		Clear (0 to 64 characters)

Address	CUCM-cluster.Caret&STIC.com	Undo (0 to 64 characters)
AlternateAddress		(0 to 64 characters)
Domain		(0 to 64 characters)
Path		(0 to 255 characters)
Protocol	HTTP	

Figure 9-5 *Configure Provisioning Settings on a CE Software-Based Endpoint*

TFTP

IP phones and Telepresence endpoints rely on a TFTP-based process to acquire configuration files, software images, and other endpoint-specific information. The Cisco Unified Communications Manager runs a TFTP service as a file serving system, and this service can run on one or more Cisco Unified Communications Manager servers. It builds configuration files and serves firmware files, ringer files, device configuration files, and so forth, to endpoints. The TFTP file systems can hold several file types, such as the following:

Key Topic

- Phone configuration files
- Phone firmware files
- Certificate trust list (CTL) files
- Identity trust list (ITL) files
- Tone localization files
- User interface (UI) localization and dictionary files
- Ringer files

- Softkey files
- Dial plan files for SIP phones

The TFTP server manages and serves two types of files: those that are not modifiable, such as firmware files for phones, and those that can be modified, such as configuration files. A typical configuration file contains a prioritized list of Cisco Unified Communications Managers for a device, the TCP ports on which the device connects to those Cisco Unified Communications Managers, and an executable load identifier. Configuration files for selected devices contain locale information and URLs for the messages, directories, services, and information buttons on the phone. When a device's configuration changes, the TFTP server rebuilds the configuration files by pulling the relevant information from the Cisco Unified Communications Manager database. The new file is then downloaded to the phone after the phone has been reset. An example of a file being downloaded to a phone again could be if a single phone's configuration file is modified, such as during Extension Mobility login or logout. Only that file is rebuilt and downloaded to the phone. However, if the configuration details of a device pool are changed, such as if the primary Cisco Unified Communications Manager server is changed, all devices in that device pool need to have their configuration files rebuilt and downloaded. For device pools that contain large numbers of devices, this file rebuilding process can impact server performance.

The TFTP server can also perform a local database read from the database on its co-resident subscriber server. A local database read not only provides benefits such as the preservation of user-facing features when the publisher is unavailable but also allows multiple TFTP servers to be distributed by means of clustering over the WAN. The same latency rules for clustering over the WAN apply to TFTP servers as apply to servers with registered phones. This configuration brings the TFTP service closer to the endpoints, thus reducing latency and ensuring failure isolation between the sites.

When a device requests a configuration file from the TFTP server, the TFTP server searches for the configuration file in its internal caches, the disk, and then remote Cisco TFTP servers, if specified. If the TFTP server finds the configuration file, it sends the file to the device. If the configuration file provides Cisco Unified Communications Manager names, the device resolves the names by using DNS and opens a connection to the Cisco Unified Communications Manager. If the device does not receive an IP address or name, it uses the TFTP server name or IP address to attempt a registration connection. If the TFTP server cannot find the configuration file, it sends a "file not found" message to the device.

A device that requests a configuration file while the TFTP server is processing the maximum number of requests will receive a message from the TFTP server that causes the device to request the configuration file later. The Maximum Serving Count service parameter, which is configurable, specifies the maximum number of requests that can be concurrently handled by the TFTP server. You can use the default value of 2500 requests if the TFTP service is run along with other Cisco CallManager services on the same server. For a dedicated TFTP server, you should use the following suggested values for the Maximum Serving Count: 2500 for a single-processor system or 3000 for a dual-processor system. The Cisco Unified IP Phones 7800 series and 8800 series request their TFTP configuration files over the HTTP protocol (port 6970), which is much faster than using the TFTP protocol.

Key Topic

Every time an endpoint reboots, an angel gets his wings. Not really; just wanted to make sure you're still paying attention. Every time an endpoint reboots, the endpoint will send a TFTP

GET message for a file whose name is based on the requesting endpoint's MAC address. For a Cisco Unified IP Phone 8861 with a MAC address of abcdef123456, the filename would be SEPabcdef123456.cnf.xml. The received configuration file includes the version of software that the phone must run and a list of Cisco Unified Communications Manager servers with which the phone should register. The endpoint might also download ringer files, softkey templates, and other miscellaneous files to acquire the necessary configuration information before becoming operational. If the configuration file includes software file version numbers that are different from those the phone is currently using, the phone will also download the new software files from the TFTP server in order to upgrade the firmware on the phone or endpoint. The number of files an endpoint must download to upgrade its software varies based on the type of endpoint and the differences between the phone's current software and the new software.

Option 150 allows up to two IP addresses to be returned to phones as part of the DHCP scope. The phone tries the first address in the list, and it tries the subsequent address only if it cannot establish communications with the first TFTP server. This address list provides a redundancy mechanism that enables phones to obtain TFTP services from another server even if their primary TFTP server has failed. Cisco recommends that you grant different ordered lists of TFTP servers to different subnets to allow for load balancing. An example of how this might look could be as follows:

- In subnet 10.0.0.0/24: Option 150: TFTP1_Primary, TFTP1_Secondary
- In subnet 10.1.1.0/24: Option 150: TFTP1_Secondary, TFTP1_Primary

Under normal operations, a phone in subnet 10.0.0.0/24 will request TFTP services from TFTP1_Primary, while a phone in subnet 10.1.2.0/24 will request TFTP services from TFTP1_Secondary. If TFTP1_Primary fails, phones from both subnets will request TFTP services from TFTP1_Secondary. Load balancing avoids having a single point of failure, where all phones from multiple clusters rely on the same server for TFTP service. TFTP load balancing is especially important when phone software loads are transferred, such as during a Cisco Unified Communications Manager upgrade, because more files of larger size are being transferred, thus imposing a bigger load on the TFTP server and on the network.

SIP Registration

As mentioned in Chapter 5, everything discussed up to this point in this chapter is not actually part of the SIP registration process; however, these processes had to transpire in order for SIP registration to the Cisco Unified Communications Manager to occur successfully. After the TFTP process has completed and the endpoint or phone has obtained all the system configuration information, SIP registration can occur. SIP endpoints must send a REGISTER request to a SIP server with a URI and a Call-ID, which is the IP of the endpoint registering. According to the IETF RFC 3621, a URI is made up of a host portion and a fully qualified domain name (FQDN) portion separated by an @ symbol, such as andy.dwyer@caret&stic.com. This is important to understand because the SIP registrar function of the SIP server breaks down these components individually to successfully process the REGISTER request. Each component is broken down as follows:

Key Topic

- **Request-URI:** The Request-URI names the domain of the location service for which the registration is meant, such as *sip:caret&stic.com*. The *userinfo* and @

components of the SIP URI must not be present. The domain in the URI must be qualified by the SIP server for registration to occur.

- **To:** The To header field contains the address of record whose registration is to be created, queried, or modified. The To header field and the Request-URI field typically differ because the former contains a username. This address of record must be a SIP URI or SIPS URI. Based on the preceding example, the request URI would be sip:andy.dwyer@caret&stic.com.
- **From:** The From header field contains the address of record of the person responsible for the registration. The value is the same as the To header field unless the request is a third-party registration. Therefore, the From header will also be sip:andy.dwyer@caret&stic.com.
- **Call-ID:** All registrations from a user agent client (UAC) should use the same Call-ID header field value for registrations sent to a particular registrar. If the same client were to use different Call-ID values, a registrar could not detect whether a delayed REGISTER request might have arrived out of order.
- **CSeq:** The CSeq value guarantees proper ordering of REGISTER requests. A user agent (UA) must increment the CSeq value by one for each REGISTER request with the same Call-ID.
- **Contact:** REGISTER requests may contain a Contact header field with zero or more values containing address bindings.

If you are already familiar with the Cisco Unified Communications Manager, you might see an issue here based on the IETF components needed for registering to the SIP registrar. The Cisco Unified Communications Manager uses directory numbers (DNs) for endpoint registration, not URIs. First, it's important to understand that the IETF RFCs are just guidelines for how SIP should operate. They are not hard-set boundaries you have to follow. If you want to "color outside the lines with SIP, you can certainly do so. Second, a DN on the Cisco Unified Communications Manager is essentially a URI in its base form.

Suppose you have a phone you were trying to register to a Cisco Unified Communications Manager at 10.0.0.30 with the DN 2001. The "domain" would be the IP address of the Cisco Unified Communications Manager, so the DN would actually be 2001@10.0.0.30. If DNS were used in a Cisco Unified Communications Manager environment, and the URL for the Cisco Unified Communications Manager was cucm1.caret&stic.com, the DN would actually be 2001@caret&stic.com.

When calls are placed between the Cisco Unified Communications Manager and the Expressway Core, incoming requests will use this format and so must be changed accordingly. The Expressway will be discussed further in Part IV. What is different within a Cisco Unified Communications Manager environment is the dialing behavior on the back end. The Cisco Unified Communications Manager will treat DNs dialed differently than URIs dialed within the same cluster. Bringing the subject back to registration, even though DNs are technically used on the Cisco Unified Communications Manager, for the purpose of registration they are treated the same as any other URI. Consider how the Cisco Unified Communications Manager will separate the different components of a REGISTER request from an endpoint with the DN 2001:

- **Request URI:** 10.0.0.30
- **To:** sip:2001@10.0.0.30
- **From:** sip:2001@10.0.0.30
- **CallID:** aef12b80-d1e1367c-2b2f-db8512c6@10.0.0.30
- **CSeq:** (101 REFER, 101 NOTIFY OR 101 SUBSCRIBE)
- **Contact:** N/A

Verifying phone registration from the Cisco IP phone is quite simple. The easiest way to verify that a phone is registered is to look on the display screen. If you see a message across the top of the screen and a spooling circle, the phone is not registered. If you see the assigned phone DN, such as 2001, beside Line 1 and at the top of the screen, the phone is registered. You can verify other registration information by pressing the Settings button and then selecting the Phone Information menu. On this screen, you can see the following information:

- **Model Number**, such as *CP8845*
- **IPv4 Address**, such as *10.0.0.100*
- **Host Name**, which is the *SEP<MAC Address>*
- **Active Load**, which is the Enterprise phone load version, such as *sip8845_65.11-7-1-17*
- **Last Upgrade**, such as *07/04/2019 2:34pm*
- **Active Server**, such as *ucm-sub1.caret&stic.com*
- **Stand-by Server**, such as *ucm-pub.caret&stic.com*

The last two options shown here signify that the phone is registered. These fields will be blank if the phone is not registered. Figure 9-6 illustrates an 8845 phone that has been registered to the Cisco Unified Communications Manager.

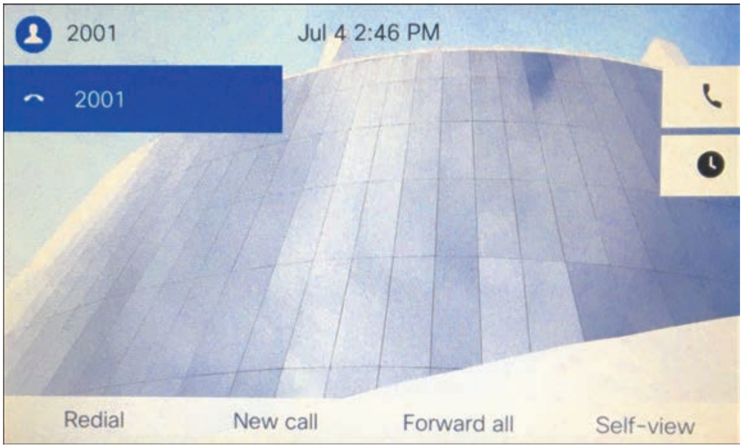


Figure 9-6 *Home Screen of an 8845 Phone Registered to the CUCM*

Verifying SIP registration on Cisco CE software-based endpoints is just as simple as verifying registration on Cisco IP phones. If you see a “Not Registered” message in the top-left corner of the screen, that is the indicator the phone is not registered. If you see the assigned phone DN, such as 2002, in the center of the screen or the Touch 10 controller, the phone is registered. You can verify other registration information by pressing the Settings button in the top-left corner of the screen and then selecting the System Information menu. On this screen, you can see the following information:

- **Video Address**, such as *2002@caret&stic.com*
- **IP Address**, such as *10.0.0.101*
- **MAC Address**, such as *AB:CD:EF:12:34:56*
- **SIP Proxy**, such as *10.0.0.30 (Registered)*
- **Software**, such as *ce 9.1.5 d1c67fb 2017-11-16*
- **Device**, such as *Cisco Telepresence DX80 TANDBERG*

The SIP Proxy setting is another identifier that the endpoint is registered. For one thing, it says Registered. For another, this field will be blank or show Not Registered if there is an issue or if the phone has never been provisioned. Figure 9-7 illustrates a Cisco Telepresence DX80 that has been registered to the Cisco Unified Communications Manager.

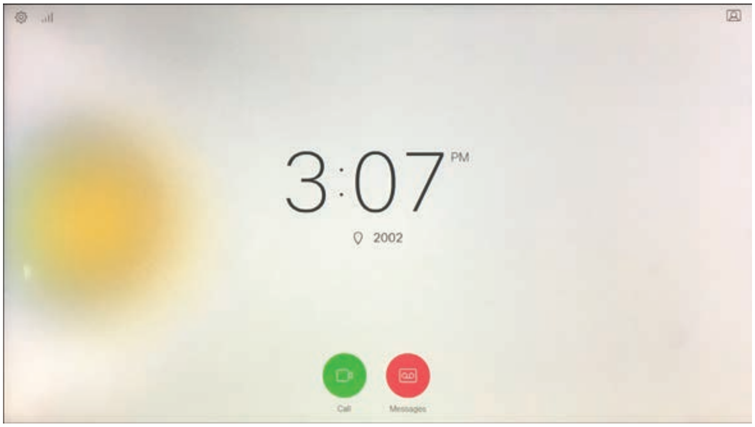


Figure 9-7 *Home Screen of DX80 Endpoint Registered to the CUCM*

ITL, CTL, and CAPF

Even though both an endpoint and the Cisco Unified Communications Manager might be located on the same LAN or WAN, it is still important to secure communications between these two products. Cisco offers several security measures, depending on what level of security you desire for the network you’re managing. The lowest level of security available on the Cisco Unified Communications Manager for endpoint registration is the identity trust list (ITL). A step above this option is the certificate trust list (CTL). The highest level of security available is the Certificate Authority Proxy Function, or CAPF. In order to better understand each of these types of security on the Cisco Unified Communications Manager, it is important to formulate a basic understanding of how secure communication over IP works in its base form. If security certificates is an unfamiliar topic to you, review the “Security” subsection under the “Designing a Cisco Collaboration Solution” section in Chapter 6.

Key Topic

Returning to the topic of securing communications between an endpoint or phone and the call control system, a Security By Default (SBD) mechanism called ITL and Trust Verification Service (TVS) is enabled on all Cisco Unified Communications Manager installments. IP phones contain a limited amount of memory, and there can also be a large number of phones to manage in a network. The Cisco Unified Communications Manager acts as a remote trust store via TVS so that a full certificate trust store does not have to be placed on each IP phone. Any time the phone cannot verify a signature or certificate via the CTL or ITL files, it asks the TVS server for verification. This central trust store is easier to manage than if the trust store were present on all IP phones. A number of files must be present on the Cisco Unified Communications Manager itself. The most important piece is the TFTP certificate and the TFTP private key. The TFTP certificate is located under **OS Administration > Security > Certificate Management > CallManager.pem**. The Cisco Unified Communications Manager uses the CallManager.pem certificate’s private and public keys for the TFTP service, as well as for the Cisco CallManager (CCM) service. All phones can use the TFTP public key in the CallManager.pem certificate to decrypt any file encrypted with the TFTP private key and to verify any file signed with the TFTP private key.

The presence of an ITL file will direct the phone to request a signed TFTP configuration file from the Cisco Unified Communications Manager TFTP server. The ITL file allows the phone to verify that the configuration file came from a trusted source. After the phone boots and obtains an IP address and the address of a TFTP server, it asks for the ITL files first. After the ITL file is downloaded, it must be verified. Several permutations could transpire here, including the following possibilities:

- The phone has no ITL file present. In this state, the phone blindly trusts the next ITL file downloaded and uses this signature henceforth.
- The phone already has an ITL file. In this state, the phone verifies that the recently downloaded files match the signature in either the ITL or TVS server.

After the signed configuration file is downloaded, the phone must authenticate it against the function for CCM+TFTP inside the ITL. After the phone receives the ITL files from TFTP successfully and they have been authenticated, the phone asks for a signed configuration file. This is the TFTP Get message discussed previously. With ITL files present on phones, configuration files must be signed by a trusted TFTP server. The file is plain text on the network while it is transmitted but comes with a special verification signature. The phone requests SEP<*MAC Address*>.cnf.xml.sgn to receive the configuration file with the special signature. This configuration file is signed by the TFTP private key that corresponds to CallManager.pem on the Operating System Administration Certificate Management page.

9

ITL is a leaner version of a CTL file. The CTL file contains a server certificate, public key, serial number, signature, issuer name, subject name, server function, DNS name, and IP address for each server. The CTL file can also contain entries for the following servers or security tokens:

- System Administrator Security Token (SAST)
- Cisco CallManager and Cisco TFTP services that are running on the same server

- Certificate Authority Proxy Function (CAPF)
- TFTP server(s)
- ASA firewall

After you create the CTL file, you must restart the Cisco CallManager and Cisco TFTP services in Cisco Unified Serviceability on all nodes that run these services. The next time that the phone initializes, it will download the CTL file from the TFTP server. If the CTL file contains a TFTP server entry that has a self-signed certificate, the phone requests a signed configuration file in .sgn format. If no TFTP server contains a certificate, the phone requests an unsigned file. After the Cisco CTL client adds a server certificate to the CTL file, you can display the certificate in the CTL client GUI. When you configure a firewall in the CTL file, you can secure a Cisco ASA firewall as part of a secure Cisco Unified Communications Manager system. The Cisco CTL client displays the firewall certificate as a CCM certificate. Cisco Unified Communications Manager Administration uses an e-token to authenticate the TLS connection between the Cisco CTL client and Cisco CTL provider. The process of obtaining a CTL file is the same as with an ITL file, except that the CTL request must occur first. The CTL file is then used to verify the ITL when it is requested. If the phone already has a CTL but no ITL, the phone trusts an ITL only if it can be verified by the CCM+TFTP function in the CTL file.

Key Topic

The Certificate Authority Proxy Function, which automatically installs with the Cisco Unified Communications Manager, performs several tasks depending on your configuration. It can be used to authenticate via an existing manufacturing installed certificate (MIC), locally significant certificate (LSC), randomly generated authentication string, or optional less secure "null" authentication. It issues locally significant certificates to supported Cisco Unified IP phones. It upgrades existing locally significant certificates on the phones. CAPF also retrieves phone certificates for viewing and troubleshooting. During installation, a certificate that is specific for CAPF gets generated. This CAPF certificate, which the Cisco CTL client copies to all Cisco Unified Communications Manager servers in the cluster, uses the .0 extension.

When the phone interacts with CAPF, the phone authenticates itself to CAPF by using an authentication string, existing MIC or LSC, or "null"; generates its public key and private key pair; and then forwards its public key to the CAPF server in a signed message. The private key remains in the phone and never gets exposed externally. CAPF signs the phone certificate and then sends the certificate back to the phone in a signed message. Before you use CAPF, ensure that you have performed all necessary tasks to install and configure the Cisco CTL client. To use CAPF, you must activate the Cisco Certificate Authority Proxy Function service on the first node.

SIP Registration to Expressway Core

Up to this point, we've discussed the registration process to the Cisco Unified Communications Manager using both the Cisco Unified IP phones and the Cisco Telepresence endpoints. Throughout the rest of this chapter, the focus will be on the Cisco Telepresence endpoints because the Cisco Unified IP phones cannot register to the Cisco Expressway. A proxy registration function using Mobile and Remote Access (MRA) allows Cisco Unified IP phones to register to the Cisco Unified Communications Manager through the Expressway Core and Edge, but in this type of deployment, the registration is still to the Cisco Unified

Communications Manager. This section of the chapter will focus on direct registration to the Cisco Expressway, which is intended for Cisco Telepresence endpoints and third-party endpoints.

Unlike the Cisco Unified Communications Manager, the Cisco Expressway does not have an easy provisioning mode available natively through which endpoints can register. There is a way to provision registration to a Cisco Expressway through another application called the Cisco Telepresence Management Suite (TMS), but TMS will not be discussed in this book. Therefore, endpoints that will register to the Cisco Expressway must be manually configured before they can register. This is one of the reasons the Cisco Unified Communications Manager is a preferred call control system. However, some circumstances require endpoints to register to the Expressway. A company may be using legacy Tandberg endpoints or third-party endpoints that cannot register to the Cisco Unified Communications Manager. Another reason could be that a company is already using a legacy VCS call control system and wants to upgrade to Expressway and continue to use the same system. Whatever the reason, this section will describe how to register SIP endpoints to the Cisco Expressway.

DHCP versus Static IP

Chapter 5 discussed the registration process to an Expressway using SIP. The following is a summation of that process for a quick review:

1. An endpoint obtains local power from the power cube and loads the locally stored image file. The exception is the SX10, which could obtain power from a power cube or PoE.
2. Cisco CE software-based endpoints can use CDP for VLAN discovery, but VLAN discovery will not impact Expressway-C registration.
3. When VLAN discovery is complete, or if the endpoint does not discover the VLAN, the endpoint will send a DHCP discovery message to the DHCP server. Alternatively, the endpoint may be configured with static network settings.
4. The SIP URI and Expressway IP address are configured manually on the endpoints.
5. The final step in the process is for the endpoints to register to the Cisco Expressway. The endpoints will send an IP address and alias to the Cisco Expressway in the REGISTER request. The alias must be in the form of a URI (name@FQDN), and the domain of the alias must match one of the domains configured in the Domain database of the Expressway.
6. If there are no configured restrictions on the Expressway, it will respond with the SIP message “200 OK.” The registration process is now complete.

Key Topic

The SIP registration process to the Cisco Expressway is much easier to explain because there are not as many moving parts. As is evident in the preceding steps, no PoE settings need to be configured because most of the endpoints do not support PoE. No VLAN settings have to be configured because the default VLAN can be used to register to the Cisco Expressway. The Expressway will tag voice and video packets, so the voice VLAN can be used but is not required for QoS purposes. This brings the process to the network addressing step. DHCP can be used on Telepresence endpoints, but it is recommended to use static IP addressing for several reasons. First, there is always the possibility that the IP address can change when DHCP is being used. This can negatively impact several aspects of Telepresence endpoint registration. The Expressway identifies endpoints registered by the IP address, not the MAC address, as does the Cisco Unified Communications Manager. Therefore, if the IP address changes, there could be duplicate registration entries for a single endpoint on the Cisco Expressway, causing call-routing issues. The IP address changing will also prevent, or at least slow down, an administrator from accessing the Telepresence endpoint remotely, which brings up the second reason static addresses should be used. The Cisco Telepresence endpoints support a high-functioning web interface and a command-line interface that can be accessed via the IP address. Cisco Unified IP phones do not have as robust of an interface; therefore, administrators do not need constant access to those addresses. All of the features a unified IP phone can support are managed through the Cisco Unified Communications Manager. A Cisco Telepresence endpoint, on the other hand, has many features supported directly on the endpoint itself, and accessing many of those features requires an IP address to access the Web interface of the endpoint, or access it through the CLI. Another reason static IP addressing is recommended on Cisco Telepresence endpoints is the newer API integrations that can be configured on newer versions of the CE software-based endpoints. There may be many more reasons why static addressing should be used over DHCP, but at the end of the day, you should use whatever method works best for your environment. Both methods will work in the end.

If you choose to use static IP addressing, the following instructions will provide some direction to change the default DHCP value to Static and configure all the necessary settings to render the Cisco Telepresence endpoint functional. Note that changing the IP address on a Cisco Telepresence endpoint will not impact access until after the system has been rebooted. A binding process must take place between the new IP address and the endpoint while the old address is purged from the system, which can occur only during a reboot. Therefore, you can make all the necessary changes over the web interface or CLI without losing the connection to the endpoint. However, after the reboot process has started, you will need to use the "new" IP address to regain access to the system. This first set of instructions will guide you through changing the IP settings using the web interface. This process is similar to the previously described process under the "DHCP" section.

Step 1. Log in to the web interface for the CE endpoint you want to configure.

Step 2. Navigate to **Setup > Configuration > Network** and locate the DNS section (second section down from the top).

DNS settings are not required for SIP registration to the Cisco Expressway. There may be reasons you may or may not want to configure these settings, so they are included for you to decide whether to use them.

Step 1. Enter the Domain in the Domain Name field. Enter up to three DNS addresses in the Server 1 Address, Server 2 Address, and Server 3 Address fields.

Step 2. Choose **Save** in the bottom-right corner of this section, and then scroll down to the IPv4 section.

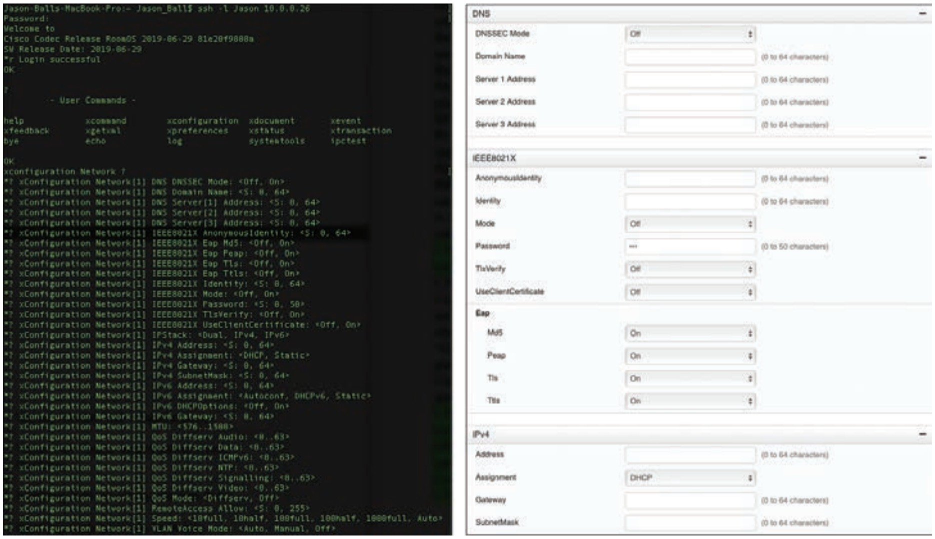
Step 3. Change the Assignment field from DHCP to **Static**.

Step 4. Enter an IP address for the endpoint in the Address field. Enter the Default Router address in the Gateway field, and enter the Subnet Mask address in the SubnetMask field. All three of these fields are required for proper routing across the network.

Step 5. Choose **Save** in the bottom-right corner of this section.

Step 6. You will have to restart the endpoint before these changes will take effect. To restart the endpoint, choose **Maintenance > Restart**. Click the blue **Restart Device** button. When a popup window appears, click the red **Restart** button, and the system will go through a restart process. This will take about 60 seconds to complete.

One of the nice aspects to the design of the Cisco Telepresence CE software-based endpoints is the continuity between the web interface menu structure and the CLI command structure. To access the configuration menus from the web interface, you were instructed previously to choose **Setup > Configuration.** To access the configuration menus from the CLI, you need to enter the command **xConfiguration.** By the way, you can use abbreviations, such as **xconfig**, and you can use the Tab key to finish commands. Also, if you are not sure of what the next command should be, use the question mark and press Enter. A list of possible commands will be displayed. The next menu on the web interface to select is the Network menu from the left column. In the CLI, the next word to enter after **xConfiguration** is **Network.** On the web interface, if you wanted to configure the domain name, you would scroll down to the DNS section and find the Domain Name field. From the CLI, if you wanted to configure the domain name, you would enter the command **xConfiguration Network 1 DNS Domain Name:** followed by the domain name you want to configure. Figure 9-8 illustrates the continuity of these two interfaces with a side-by-side comparison between the CLI and the web interface configuration options for the network settings.



```
Jason-Balls-MacBook-Pro:~ Jason_Ball$ ssh -l Jason 10.0.0.26
Password:
Welcome to
Cisco Codec Release RoomOS 2019-06-29 81e20f9888a
SW Release Date: 2019-06-29
*r Login successful
OK

?
          - User Commands -

help                xcommand            xconfiguration  xdocument       xevent
xfeedback           xgetxml             xpreferences    xstatus         xtransaction
bye                 echo                log             systemtools     ipctest

OK
xconfiguration Network ?
*? xConfiguration Network[1] DNS DNSSEC Mode: <Off, On>
*? xConfiguration Network[1] DNS Domain Name: <S: 0, 64>
*? xConfiguration Network[1] DNS Server[1] Address: <S: 0, 64>
*? xConfiguration Network[1] DNS Server[2] Address: <S: 0, 64>
*? xConfiguration Network[1] DNS Server[3] Address: <S: 0, 64>
*? xConfiguration Network[1] IEEE8021X AnonymousIdentity: <S: 0, 64>
*? xConfiguration Network[1] IEEE8021X Eap Md5: <Off, On>
*? xConfiguration Network[1] IEEE8021X Eap Peap: <Off, On>
*? xConfiguration Network[1] IEEE8021X Eap Tls: <Off, On>
*? xConfiguration Network[1] IEEE8021X Eap Ttls: <Off, On>
*? xConfiguration Network[1] IEEE8021X Identity: <S: 0, 64>
*? xConfiguration Network[1] IEEE8021X Mode: <Off, On>
*? xConfiguration Network[1] IEEE8021X Password: <S: 0, 50>
*? xConfiguration Network[1] IEEE8021X TlsVerify: <Off, On>
*? xConfiguration Network[1] IEEE8021X UseClientCertificate: <Off, On>
*? xConfiguration Network[1] IPStack: <Dual, IPv4, IPv6>
*? xConfiguration Network[1] IPv4 Address: <S: 0, 64>
*? xConfiguration Network[1] IPv4 Assignment: <DHCP, Static>
*? xConfiguration Network[1] IPv4 Gateway: <S: 0, 64>
*? xConfiguration Network[1] IPv4 SubnetMask: <S: 0, 64>
*? xConfiguration Network[1] IPv6 Address: <S: 0, 64>
*? xConfiguration Network[1] IPv6 Assignment: <Autoconf, DHCPv6, Static>
*? xConfiguration Network[1] IPv6 DHCPOptions: <Off, On>
*? xConfiguration Network[1] IPv6 Gateway: <S: 0, 64>
*? xConfiguration Network[1] MTU: <576..1500>
*? xConfiguration Network[1] QoS Diffserv Audio: <0..63>
*? xConfiguration Network[1] QoS Diffserv Data: <0..63>
*? xConfiguration Network[1] QoS Diffserv ICMPv6: <0..63>
*? xConfiguration Network[1] QoS Diffserv NTP: <0..63>
*? xConfiguration Network[1] QoS Diffserv Signalling: <0..63>
*? xConfiguration Network[1] QoS Diffserv Video: <0..63>
*? xConfiguration Network[1] QoS Mode: <Diffserv, Off>
*? xConfiguration Network[1] RemoteAccess Allow: <S: 0, 255>
*? xConfiguration Network[1] Speed: <10full, 10half, 100full, 100half, 1000full, Auto>
*? xConfiguration Network[1] VLAN Voice Mode: <Auto, Manual, Off>
```

DNS –

DNSSEC Mode: Off

Domain Name: (0 to 64 characters)

Server 1 Address: (0 to 64 characters)

Server 2 Address: (0 to 64 characters)

Server 3 Address: (0 to 64 characters)

IEEE8021X –

AnonymousIdentity: (0 to 64 characters)

Identity: (0 to 64 characters)

Mode: Off

Password: ••• (0 to 50 characters)

TlsVerify: Off

UseClientCertificate: Off

Eap

Md5: On

Peap: On

Tls: On

Ttls: On

IPv4 –

Address: (0 to 64 characters)

Assignment: DHCP

Gateway: (0 to 64 characters)

SubnetMask: (0 to 64 characters)

Figure 9-8 *CLI and Web Interface Comparison for Network Configuration*

To access the CLI of a CE software-based endpoint, you can open the terminal emulator of your choosing. PuTTY is a popular tool to use from Windows-based computers, and it is free to download. The preceding example is taken from Terminal, which comes with Apple Mac computers. You also can use other emulator tools, so do your homework if you do not already have a preference. Some will be free, and others you will have to pay for. You will need to use SSH to access the endpoint's CLI. Telnet is supported, but it is disabled by default. For security reasons, it is recommended to leave Telnet disabled. From PuTTY, open the emulator and enter the IP address in the Host Name (or IP address) field. Choose the SSH radio button below that field, and then click the Open button. From Terminal, enter the command **ssh -l admin** *IP address* and then press Enter. Both tools will prompt you to validate the certificate and then prompt you to log in. With Terminal, the username is already added to the access command, so you will only need to enter the password. With PuTTY, you will need to enter the username first followed by the password. After you are logged in, you can enter the commands to configure the endpoint. The following is a list of network commands that can be entered through the CLI. Use the up-arrow key to recall the last command entered. Commands in the CLI are not case sensitive.

Key Topic

- **xConfiguration Network 1 DNS Domain Name**: *domain*
- **xConfiguration Network 1 DNS Server [1-3] address**: *IP of DNS*
- **xConfiguration Network 1 IPv4 Assignment**: [**DHCP** | **Static**]
- **xConfiguration Network 1 IPv4 Address**: *IP address for endpoint*
- **xConfiguration Network 1 IPv4 Gateway**: *default gateway IP address*
- **xConfiguration Network 1 IPv4 SubnetMask**: *subnet mask IP address*
- **xCommand Boot**

Because the last command does not configure any settings on the endpoint, it does not use the **xConfiguration** level of command. **xCommand** is the structure level that tells the system to execute a function. In this case, the endpoint must go through a reboot process to bind the IP address with the endpoint. After the reboot process begins, the connection to the emulator will terminate. You will need to use the new IP address to access the system remotely again.

Manual Configuration of SIP Settings

After the network settings have been configured on the CE software-based endpoint, you can configure the SIP settings so that the endpoint can try registering to the Cisco Expressway. When a CE software-based endpoint is first booted, a setup wizard runs on the endpoint. You can choose whether the endpoint will register to Cisco Webex or to Other Services. After you select Other Services, the options presented are Cisco UCM, Cisco UCM via Expressway, VCS (VCS can also be an Expressway Core), or Advanced Setup. When you select the Cisco UCM option, a field called Enter Server Address will populate so that you can configure the TFTP server address. When you select the Cisco UCM via Expressway option, three fields will be populated: Username, Passphrase, and Domain. When you select the VCS option, four fields will be populated: Host Server Address, Username, Passphrase, and Domain. When you select the Advanced Setup option, the next screen will provide a warning: "Advanced setup is an option for administrators to directly set up the system with their own software. If you continue you will not be able to call until you register with a service." The steps outlined here assume Advanced Setup is the option you chose on the endpoint. Two methods can be used to manually configure a CE software-based endpoint to an Expressway Core. The administrator can use the web interface or the CLI, as mentioned previously with the network settings options. This section will first examine the web interface options for configuring the SIP registration settings on a CE endpoint.

First, you need to obtain the IP address from the endpoint and enter this address in the address bar on a web browser. You can use either HTTP or HTTPS to access the endpoint by default, although you may want to disable HTTP for security reasons. When the login screen appears, enter the Username admin and leave the Passphrase field blank. CE software-based endpoints do not have a password set on them by default. The administrator will need to set this password. If you want to go ahead and set a password on the endpoint, click the Admin link in the top-right corner of the screen and select the Change Passphrase menu option. You can also navigate to **Security > Users** and select the Admin user account to gain access to this screen. You will be prompted to enter the Current Passphrase, Passphrase, and Repeat Passphrase. Here, leave the first field blank, enter a password in the second and third fields, and then click the Change Passphrase button. Now you are ready to configure the SIP registration settings to the Expressway Control. Navigate to **Setup > Configuration** and follow these steps:

Key Topic

Step 1. Choose **NetworkServices** from the menu column on the left of the screen, and ensure the SIP Mode setting is set to On. This is the default setting.

Step 2. Choose **Provisioning** from the menu on the left and change the Mode to **VCS**. This is an optional step because registration to the Expressway Core will occur whether this setting is changed or not. The mode could also be set to TMS or Auto and still register to the Expressway Core. Click **Save** after changing the setting.

Step 3. Choose **SIP** from the menu column on the left. You can configure several settings under this menu. Some of those settings are as follows:

a. **DefaultTransport:** This setting defines the default mechanism used when SIP communications are sent. The values can be set to Auto, TCP, TLS, or UDP. The default value is Auto. You can leave this setting as Auto or change it to another value. For security reasons, you may want to change this setting to TLS.

b. **DisplayName:** This is an optional setting. If the display name is set, when a call is placed from or to this endpoint, this name will be displayed to the participants on the other end of the call. If this value is not configured, the URI address will be displayed as the name.

c. **Proxy 1 Address:** This is a required field to be configured. This is where you will need to enter the address of the Expressway Core. If DNS is configured on this endpoint, you can enter the URL of the Expressway Core. If DNS is not being used, you will need to enter the IP address of the Expressway Core. In either case, some setting must be configured in this field.

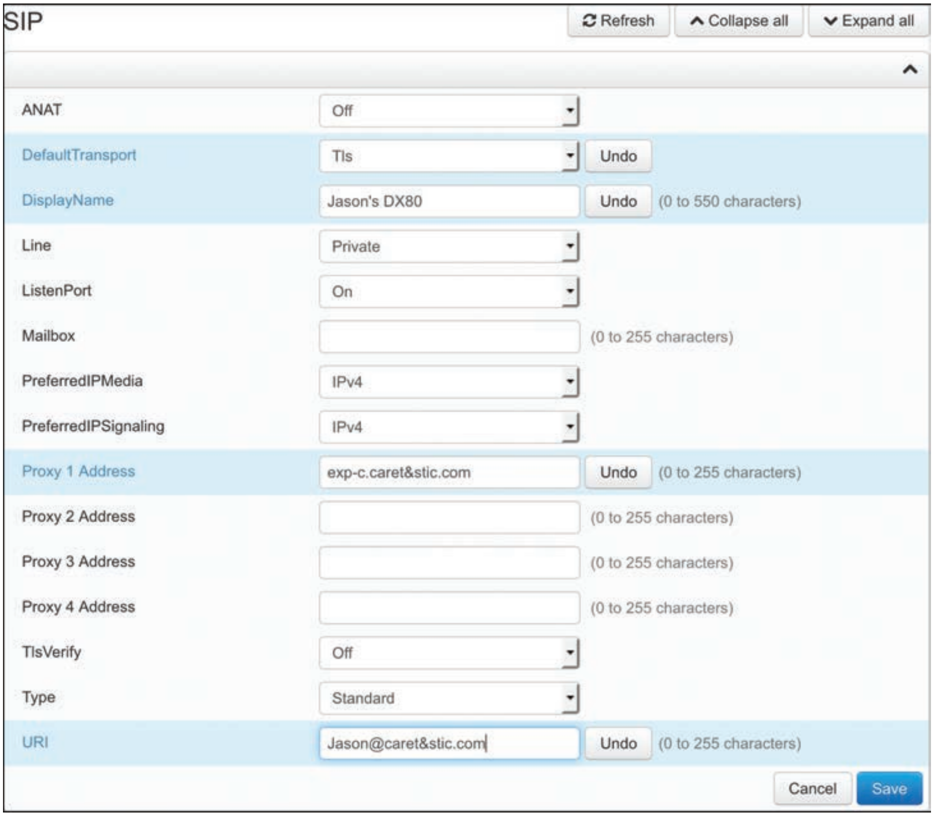
d. **TLS Verify:** This setting should be enabled only if TLS Verified is being used. You will first need to upload a signed certificate to this endpoint, DNS will have to be enabled, and the Proxy 1 Address will have to be a URI. The default value for this setting is Off.

e. **Type:** Two types of SIPs can be used on CE software-based endpoints. Standard is the default value, and the value that should be selected when registering to the Expressway Core. Cisco is the other value option and should be used only when registering to the Cisco Unified Communications Manager. When the **Provisioning > Mode** is set to CUCM, this value will change automatically to Cisco.

f. **URI:** This is the URI address assigned to this endpoint. This is a required field because the Expressway Core will check the domain portion of the URI address against a domain database within the Expressway before allowing registration. The URI should be in the form of Host@FQDN.

Step 4. After you configure all the settings under this section, click the **Save** button.

Registration should occur instantaneously. To verify the endpoint has registered successfully, choose Home from the menus at the top of the screen. On the right side of the screen under the SIP Proxy 1 heading, you should see the registration status of the endpoint. Figure 9-9 illustrates the SIP Configuration menus on a DX80 endpoint.



SIP

ANAT	Off	
DefaultTransport	Tls	
DisplayName	Jason's DX80	(0 to 550 characters)
Line	Private	
ListenPort	On	
Mailbox		(0 to 255 characters)
PreferredIPMedia	IPv4	
PreferredIPSignaling	IPv4	
Proxy 1 Address	exp-c.caret&stic.com	(0 to 255 characters)
Proxy 2 Address		(0 to 255 characters)
Proxy 3 Address		(0 to 255 characters)
Proxy 4 Address		(0 to 255 characters)
TlsVerify	Off	
Type	Standard	
URI	Jason@caret&stic.com	(0 to 255 characters)

Figure 9-9 *SIP Configuration Menus on DX80 Endpoint*

Another method that you can use to manually configure a CE software-based endpoint to register with an Expressway Core is to use the CLI. The preceding section discussed different terminal emulators that can be used for CLI access and explained the process to log in to the endpoint using the PuTTY and Terminal emulators. The following CLI commands can be used to configure all of the settings previously mentioned using the web interface:

- **xConfiguration NetworkServices SIP Mode***: On*
- **xConfiguration Provisioning Mode***: VCS*
- **xConfiguration SIP DefaultTransport***: tls*
- **xConfiguration SIP DisplayName***: Andy_Dwyer_DX80*
- **xConfiguration SIP Proxy 1 Address***: exp-c.caret&stic.com*
- **xConfiguration SIP URI***: andy.dwyer@caret&stic.com*
- **xStatus SIP**

All of the settings in italic in the preceding list are examples of the values that you can add. Obviously, you would want to configure your own unique values in each of these fields. The last command, **xStatus SIP**, is how you can check the registration status for SIP on the endpoint. This will display all the settings configured for SIP with their values, the Registration 1 Status, and the Registration 1 URI address.

H.323 Registration to the Expressway Core

In addition to supporting SIP registration, the Cisco Expressway can also support H.323 registration. As discussed in Chapter 5, H.323 is an ITU-T standard for packet-switched communication over IP. H.323 and SIP cannot communicate with one another unless there is a gateway to bridge the differences between the two communication protocols. Therefore, the Expressway has a built-in SIP to the H.323 gateway that is enabled by default. This gateway can also bridge communications between IPv4 and IPv6. When communicating between SIP and H.323, it is important to pay attention to the aliases being used because the different alias mechanisms between the two protocols can cause further complications in bridging the communication chasm. Other tools within the Expressway can aid in bridging this gap, but they will not be discussed in this book.

H.323 Aliases

An alias can be generally defined as any identification method that is not an IP address. When video endpoints in a network are known to the rest of the environment only by their IP addresses, many limitations can occur. These limitations can be summarized by saying that having some flexibility and customization available to the administrator serves everyone well in terms of overall system administration, security, dial plan effectiveness, and so on. The two primary conferencing protocols, SIP and H.323, use very different alias methodologies and when not implemented properly can create unnecessary workload or configuration challenges.

Key Topic

H.323 aliases can take three forms. First, H.323ID is an alphanumeric string of characters that includes special characters but no spaces, such as *room231* or *helpdesk*. The H.323ID can also be configured in the form of a URI, such as *andy.dwyer@caret&stic.com*. Make no mistake: this is an H.323 ID and not a URI. Remember that the FQDN in the URI for SIP must be qualified against a domain configured in the Expressway. However, with an H.323

ID, the supposed "domain" part of the alias is not qualified against anything. The second alias supported with H.323 is an E.164 alias. This type of alias can only be configured with numeric values consisting of 1–15 digits. Incidentally, the E.164 protocol is a holdover from PSTN protocols and serves to unify legacy ISDN endpoints with newer IP-based endpoints. The third type of alias is a routing prefix. These prefixes are registered aliases that have been configured on gateways and bridges. They serve to route all calls that were dialed with that prefix number to the server that registered the routing prefix. For example, if an ISDN gateway were to register with a routing prefix of 9, and a user dialed 919195551001, the Expressway would identify the first digit as a routing prefix, ignore all the numbers that followed, and route the call to the ISDN gateway. The call connection would then depend on the routing rules configured in the ISDN gateway to match the call attempt and connect it across the PSTN to the number dialed. Another example could be an MCU of some type that registered a routing prefix of 814. When a user dialed 8144001, the Expressway would match the 814 prefix and route the call to the MCU regardless of remaining digits dialed. This second example serves to illustrate that a prefix does not have to be a single digit. It could contain multiple digits, but it should be kept simple so that dialing among employees does not become a cumbersome task. Endpoints do not use prefixes, so this alias type would not apply to them.

The previous information that a single endpoint can have as many as two different aliases is significant because the Expressway identifies endpoints by their alias. The Expressway will, therefore, make all its security, access, and bandwidth management decisions based on the alias of an endpoint, and will only be concerned with IP addresses when regarding routing the signaling and media. When an administrator is planning and configuring the dial plan for Cisco Expressway call routing, how the Expressway will treat each alias must be given careful consideration.

Manual Configuration of H.323 Settings

Just as with SIP registration configurations on CE software-based endpoints, H.323 registration configurations can be made using the web interface or the CLI. The following steps outline how to configure H.323 settings on CE software-based endpoints for registration to the Gatekeeper function on the Cisco Expressway Core. H.323 and SIP cannot be used simultaneously on CE software-based endpoints. Therefore, SIP will need to be disabled when H.323 is enabled on the endpoint.

Key Topic

Step 1. Log in to the web interface for the CE endpoint you want to configure.

Step 2. Choose **Setup > Configuration**.

Step 3. Choose **NetworkServices** from the menu column on the left side of the screen.

Step 4. Change the SIP Mode setting to **Off**, and then change the H.323 Mode to **On**. This setting is Off by default. Click **Save** when finished.

Step 5. Choose **Provisioning** from the menu on the left and change the Mode to **VCS**. This is an optional step because registration to the Expressway Core will occur whether this setting is changed or not. The mode could also be set to TMS or Auto and still register to the Expressway Core. Click **Save** after changing the setting.

Step 6. Choose **H323** from the menu on the left. Several settings under this menu can be configured. Some of those settings are as follows:

- **a.** **CallSetup Mode:** This setting can be set to Gatekeeper, which is the default, or Direct. If Gatekeeper is chosen, the endpoint must register to an H.323 Gatekeeper before it can place and receive calls. If the endpoint is set to Direct, it will never try to register but can place calls based on IP address dialing.
- **b.** **Gatekeeper Address:** This is where the IP address or URL of the Cisco Expressway Core needs to be entered for the endpoint to register.
- **c.** **Authentication:** Three settings pertain to authentication for H.323 registration:
  - i. **LoginName:** This is the login name used when Authentication services are enabled on the Expressway Core. If Authentication services are not enabled on the Expressway Core, this field can be left blank.
  - ii. **Mode:** This setting can be set to On or Off (default is Off). Authentication mode does not need to be turned on unless Authentication services are enabled on the Expressway Core. If this mode is turned on and Authentication services are not enabled on the Expressway Core, it will not impact registration. This setting will just be ignored by the Expressway Core.
  - iii. **Password:** This setting coincides with the Authentication username when the Authentication services are enabled on the Expressway Core.
- **d.** **H323Aliases:** Two aliases can be configured on CE software-based endpoints.
  - i. **E164:** This is the numeric alias assigned to H.323 endpoints. Digits can range between 0 and 9, and aliases can be composed of up to 15 digits in length.
  - ii. **ID:** This alias can contain alphanumeric and special characters up to 32 characters in length.

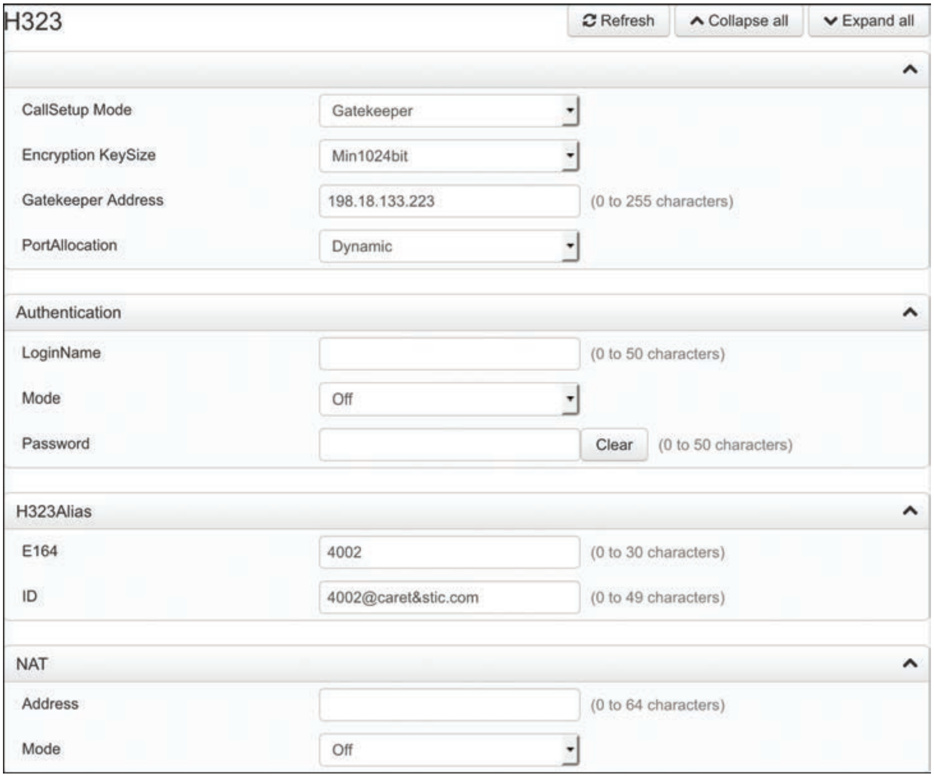
There are several more settings than what has been listed here, but the remainder of the settings are seldom used and therefore do not warrant any discussion. Figure 9-10 illustrates the previously described settings for H.323 configuration under the H.323 menu on a Cisco DX80 endpoint.

Another method that you can use to manually configure a CE software-based endpoint to register with an Expressway Core is to use the CLI. The CLI commands that can be used to configure all of the H.323 settings previously mentioned using the web interface are as follows:

- **xConfiguration NetworkServices SIP Mode***: Off*
- **xConfiguration NetworkServices H323 Mode***: On*
- **xConfiguration Provisioning Mode***: VCS*

9

- **xConfiguration H323 CallSetup Mode***: Gatekeepr*
- **xConfiguration H323 Gatekeeper Address***: exp-c.caret&stic.com*
- **xConfiguration H323 Authentication LoginName***:* ""
- **xConfiguration H323 Authentication Mode***: Off*
- **xConfiguration H323 Authentication Password***:* ""
- **xConfiguration H323 H323Alias E164***: 4002*
- **xConfiguration H323 H323Alias ID***: 4002@caret&stic.com*
- **xStatus H323**



H323

CallSetup Mode: Gatekeeper
Encryption KeySize: Min1024bit
Gatekeeper Address: 198.18.133.223 (0 to 255 characters)
PortAllocation: Dynamic

Authentication
LoginName: (0 to 50 characters)
Mode: Off
Password: (0 to 50 characters)

H323Alias
E164: 4002 (0 to 30 characters)
ID: 4002@caret&stic.com (0 to 49 characters)

NAT
Address: (0 to 64 characters)
Mode: Off

Figure 9-10 *H.323 Registration Menus on Cisco DX80*

All of the settings in italic in the preceding list are examples of the values that you can add. Obviously, you would want to configure your own unique values in each of these fields. Because the Authentication Username and Password are not needed in this example, quotation marks are used to show there is no value in that field. Quotation marks can be used to remove a setting as well. The last command, **xStatus H323**, is how you can check the registration status for H.323 on the endpoint. This will display the H.323 Gatekeeper Address, Port, Mode as Enabled, and Status as Registered. Aliases will not be displayed with the

xStatus H323 command. To see the alias configured on this system, type **xConfiguration H323** and press Enter. All H.323 settings will be displayed as they have been configured.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics 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
Table 9-2	Meraki Switch PoE Classifications	199
Table 9-3	Three PoE Types Supported on Cisco Switches	200
Commands	Enabling PoE on a Cisco Switch Port	200
Commands	Enabling CoS on Cisco Switches	203
Paragraph	Dual VLAN Tagging on a Switchport	204
List	Configure VLANs on Cisco 8800 Series Phones	205
List	Configure VLANs on Cisco CE Software-Based Endpoints	206
Commands	Configure DHCP with Option 150 on Cisco Router	207
List	DHCP Settings on Cisco 8800 Series Phones	209
List	DHCP Settings on Cisco CE Software-Based Endpoints	210
List	TFTP System File Types	211
Paragraph	TFTP GET Process Between Phone and CUCM	212
List	Components of a SIP REGISTER Request	213
Paragraph	TVS Explained	217
Paragraph	CAPF Explained	218
Paragraph	Static IP versus DHCP on Telepresence Endpoints	219
List	CLI Commands on CE Endpoints to Configure Network Settings	222
List	Steps to Configure SIP Registration to an Expressway via Web Interface	223
Paragraph	Three Forms of H.323 Aliases	225
List	Steps to Configure H.323 Registration to an Expressway via Web Interface	226

Define Key Terms

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

802.1p, 802.1Q, 802.3af, 802.3at, Asymmetric Cryptography, CA, CAPF, CDP, Classification Pulse, CLI, CoS, CTL, Data VLAN, DHCP, Diffie-Hellman Key Exchange, DN, DNS, E.164 alias, FQDN, H.323 ID, HTTP, HTTPS, IEEE, ITL, LLDP-MED, Mutual TLS, Option 150, Option 66, PD, PoE, PoE Power Budget, Prestandard PoE, PSE, QoS, Routing Prefix, RSA, SIPS, SSL, Symmetric Cryptography, TFTP, TLS, TLS Verify, TVS, URI, URL, VLAN, Voice VLAN, VVID, WAN

Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. It might not be necessary to memorize the complete syntax of every command, but you should be able to remember the basic keywords that are needed.

To test your memory of the commands, cover the right side of Table 9-5 with a piece of paper, read the description on the left side, and then see how much of the command you can remember.

The CLCOR (350-801) exam focuses on practical, hands-on skills that are used by a networking professional. Therefore, you should be able to identify the commands needed to configure and test switch commands for PoE and QoS, and router commands for DHCP and Option150.

Table 9-5 Cisco Meeting Server MMP Commands

Task	Command Syntax
This command enters configuration mode.	Switch# **Configure Terminal**
This command selects the interface to configure.	Switch(config)# **interface {fastethernet|gigabitethernet} (slot/port)**
The **auto** keyword sets the interface to automatically detect and supply power to the powered device. This is the default configuration. The **static** keyword sets the interface to higher priority than auto. If necessary, you can use the **max** keyword to specify the maximum wattage allowed on the interface (4000 to 15,400 milliwatts). You can use the **never** keyword to disable detection and power for the PoE-capable interface.	Switch(config-if)# **power inline {auto[max milli-watts] | never | static [max milli-watts]}**
This command exits configuration mode.	Switch(config-if)# **end**
This command displays the PoE state for the switch.	Switch# **show power inline {fastethernet|gigabitethernet} slot/port**
This command configures the port to delay shutting down.	Switch(config-if)# **power inline delay shutdown 20 initial 300**
This command creates a VLAN and associated number value.	Switch(config)# **vlan** *number*

Task	Command Syntax
This command provides a description of the VLAN.	Switch(config-vlan)# **name** *name*
This command enables the switchport to trust the CoS-to-QoS mapping embedded in the switch.	Switch(config-if)# **mls qos trust cos**
The **detect** command configures the interface to detect and recognize a Cisco IP phone. The **cisco-phone** option is the only one allowed when you initially implement the **switchport voice detect** command. The default is **no switchport voice detect cisco-phone [full-duplex]**. The optional **full-duplex** command configures the switch to accept only a full-duplex Cisco IP phone. The **vlan-id** command configures the phone to forward all voice traffic through the specified VLAN. By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5. Valid VLAN IDs are 1 to 4094. The **dot1p** command configures the phone to use IEEE 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. The **none** command allows the phone to use its own configuration to send untagged voice traffic. The **untagged** command configures the phone to send untagged voice traffic.	Switch(config-if)# **switchport voice {detect cisco-phone [full-duplex] | vlan {vlan-id | dot1p | none | untagged}}**
This command is used to hard-code the port into access mode.	SW1(config-if)# **switchport mode access**
This command is used for access VLAN tagging all data originating from the computer.	SW1(config-if)# **switchport access vlan number**
This command is used for voice VLAN tagging all voice and video traffic originating from the phone.	SW1(config-if)# **switchport voice vlan** *number*
This command creates a pool from which IP addresses can be issued to devices that send a DHCP request. The *name* field can be any name you want to give to the pool.	Router(config)# **ip dhcp pool** *name*
This command establishes all the available addresses within a pool that can be used for DHCP assignment.	Router(dhcp-config)# **network** *starting IP address subnet mask*
This command establishes the default gateway address that will be assigned to devices.	Router(dhcp-config)# **default-router** *default gateway address*

Task	Command Syntax
This command assigns the TFTP server address to the endpoint. You could also use the **option 66 ip** *address* command here, but Cisco recommends using **Option 150** to add additional redundancy.	Router(dhcp-config)# **option 150** *TFTP server address*
This command allows you to list up to four DNS server addresses. You must separate DNS addresses with a space.	Router(dhcp-config)# **dns-server** *DNS address*
This command enables you to assign the domain to devices through DHCP.	Router(dhcp-config)# **domain-name** *name*
This command determines how long a leased address can be used by a device before a new lease has to be requested. By default, the duration of a lease is one day. When you enter the **lease** *n* command, this duration will be extended to that number *n* of days. You can enter three values here to extend the duration to days, hours, and minutes.	Router(dhcp-config)# **lease** *n*
This command issues an exclusion range of addresses that will not be used in DHCP assignments.	Router(config)# **ip dhcp excluded-address** *starting IP address ending IP address*

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the three PoE protocols supported on Cisco switches and the maximum watts each can support.
2. Assuming the data VLAN ID is 100 and the VVID is 200, list the commands required to apply both the voice and data VLANs to a switchport.
3. What are the two options that can be configured in a DHCP server so that the TFTP server address can be discovered by an endpoint?
4. List the nine different file types that the TFTP file system can hold.
5. List the six different fields found in a SIP REGISTER header.

This page intentionally left blank

CHAPTER 10

Call Settings on Cisco CE Software-Based Endpoints

This chapter covers the following topics:

Calling Options: This topic will discuss the various ways calls can be placed from CE software-based endpoints.

Content Sharing Options: This topic will discuss the various options available for sharing content through a CE software-based endpoint both locally and during a call.

Other Options: Various other options can be leveraged from CE software-based endpoints. This topic will introduce the function of these other options and how they can be configured.

The previous chapter mentioned settings that can be configured on CE software-based endpoints that cannot be configured on Cisco Unified IP phones. H.323 and SIP registration settings are only some of the features that set these intelligent systems apart. This chapter will delve into some of the other features that uniquely identify the superiority of CE software-based endpoints. Topics discussed in this chapter include the following:

- **Calling Options:**
- Call by Alias
  - Call by Directory
  - Multipoint Calling
  - One Button to Push (OBTP) and Scheduled Conferences
- Content Sharing Options:
- Direct Sharing Content
  - Using Intelligent Proximity for Content Sharing
- Other Options:
- Audio Settings
  - Encryption Mode
  - AutoAnswer
  - Far-End Camera Control (FECC)
  - Phonebook
  - Video Settings

“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
Calling Options	1–4
Content Sharing Options	5–6
Other Options	7–11

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 user interface control devices can be used on the Cisco DX80 endpoint?
   - **a.** TRC5 Remote Control
   - **b.** Touchscreen
   - **c.** Touch 10 control pad
   - **d.** Web interface
2. How many directory entries can a Cisco CE software-based endpoint hold locally within the endpoint database?
   - **a.** 35
   - **b.** 350
   - **c.** 3500
   - **d.** 35,000
3. Which of the following terms is defined by any call involving three or more participants?
   - **a.** Multipoint
   - **b.** Multisite
   - **c.** Multiway
   - **d.** Ad hoc

4. Which of the following devices can be used to schedule OBTP meetings?

- **a.** CUCM
- **b.** VCS
- **c.** TMS
- **d.** CMS

5. Which of the following is the ITU standard for content sharing?

- **a.** DuoVideo
- **b.** People+Content
- **c.** H.224
- **d.** H.239
- **e.** BFCP

6. Which of the following devices can initiate content being shared via the Proximity application?

- **a.** Windows computer
- **b.** Smartphone
- **c.** Tablet
- **d.** Cisco Unified IP phone

7. Which of the following statements is true?

- **a.** The Microphone Mute Enabled setting will mute the microphone when a call is set up.
- **b.** The Microphone Mute Enabled setting will not mute the microphone when a call is set up.
- **c.** The Input Microphone Mode setting will mute the microphone when a call is set up.
- **d.** The Input Microphone Mode setting determines which microphone is set as the primary.

8. Which of the following is the default Encryption Mode setting on a CE software-based endpoint?

- **a.** AES 128
- **b.** AES 256
- **c.** On
- **d.** Best Effort

9. Which of the following is the standard for FECC?

- **a.** H.224
- **b.** H.239
- **c.** T.150
- **d.** BFCP

10. Which of the following directories requires the endpoint to send a subscribe message before phonebook entries can be retrieved?

- **a.** Local directory
- **b.** Global directory
- **c.** Corporate directory
- **d.** Both global and corporate directories
- **e.** No directory requires a subscribe message before phonebooks can be received.

11. The RGB Quantization Range setting overrides devices that do not follow the CEA-861 standard in order to provide the perfect image with any display. Which of the following settings is used to set the RGB quantization range based on the RGB Quantization Range bits (Q0, Q1) in the AVI infoframe?

- **a.** Auto
- **b.** Full
- **c.** Limited
- **d.** Manual
- **e.** None of these answers are correct.

Foundation Topics

Calling Options

Because the primary purpose of having an endpoint is to be able to place and answer calls, it is important to understand how to use these systems once they have registered to the call control system of your choosing. A call can be placed or answered from CE software-based systems in essentially three ways:

Key Topic

1. Call out or answer an incoming call from the user interface. This could be the Touch 10 controller, a remote control, or a touchscreen on the endpoint, depending on which device is being used. This could also be a personal device, such as a smartphone or tablet, through the Proximity application.
2. Use the web interface.
3. Use the command-line interface (CLI).

An administrator typically uses the web interface and CLI. Because end users will be sitting in front of the system, they would interact with the user interface.

Calls from a CE software-based endpoint can be made by dialing the destination alias or by selecting a participant from the directory, or phone book. Multipoint conference meetings can be arranged by dialing into a bridge that will host the meeting or by utilizing the Multisite option on the CE endpoint itself. The Multisite option is a licensed feature that must be added to the CE software-based endpoint before this feature can be used. Scheduled meetings can be accessed in a variety of ways as well, such as using a feature called *One Button to Push* (OBTP). The following sections will delve into each of these dialing behaviors to provide a more thorough understanding of call behavior and how to configure settings related to each of these calling components.

Call by Alias

Since the invention of automatic telephony switches, the most common means of initiating communication with another party, whether through a PSTN telephone, IP phone, or video phone, has been by dialing the alias of the destination. Traditional PSTN phones and most IP phones use E.164 aliases to dial, which is more commonly known as the *telephone number*. In the case of the Cisco Unified Communications Manager, these aliases are known as *directory numbers (DNs)*. However, as explained already in previous chapters, other alias types can be used, and they are growing in popularity. The most common type of alias used outside of E.164 aliases is the SIP URI. Regardless of the alias type, the endpoint used to place calls must possess the ability to dial the destination alias. All Cisco CE software-based endpoints share a common interface so that no matter what Cisco Telepresence endpoint is being used, the experience will be the same for every user. The following figures and descriptions are based on the Cisco DX80 endpoint, but they can be applied to any DX, MX, SX, IX, or Webex Telepresence endpoint.

Key Topic

Users can use three different control mechanisms available on Cisco CE software-based endpoints to interact with the different systems. The Cisco SX10 endpoint comes with a TRC5 remote control. The DX80 endpoint has a touch control screen, and all other Cisco endpoints come with a Touch 10 control pad. Regardless of which control device is being used on the Cisco endpoints, the screen layouts and menu options are the same. Figure 10-1 illustrates the menu layout options on a Cisco DX80 touchscreen.

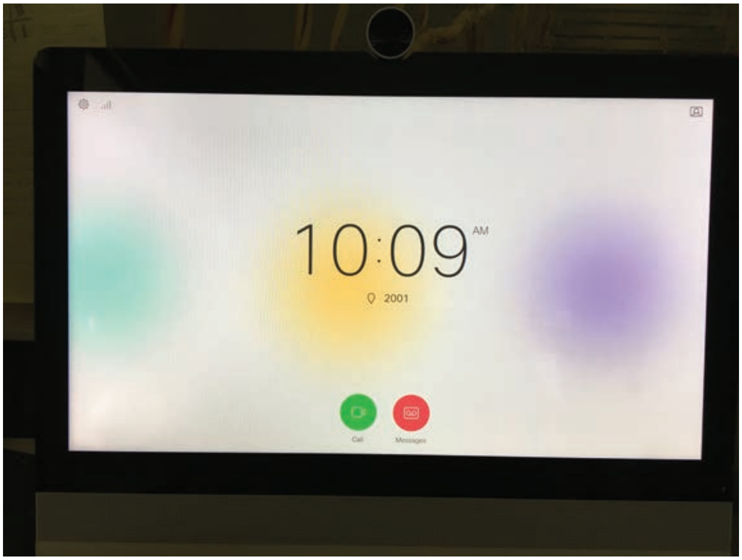


Figure 10-1 *Cisco DX80 Touchscreen Menu Layout*

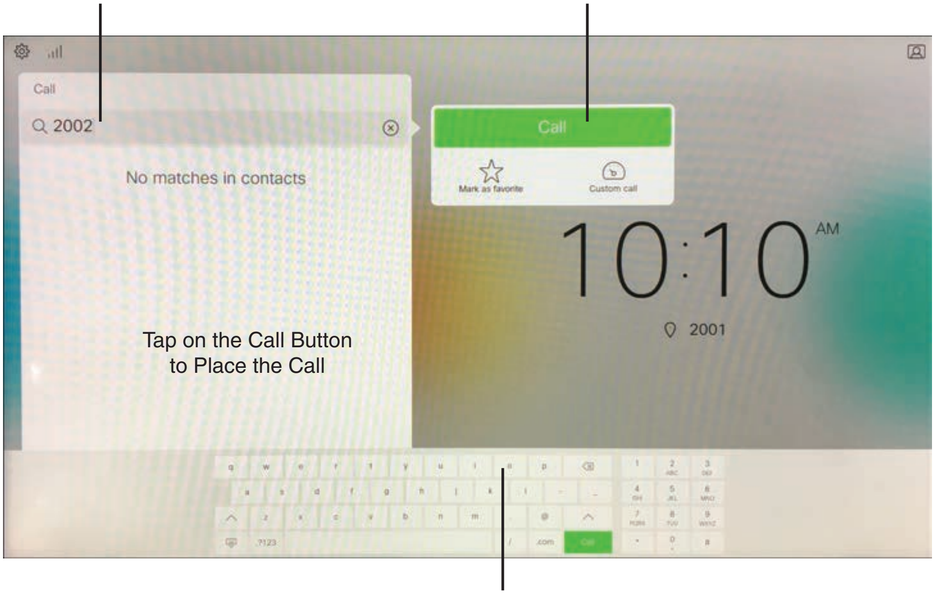
On the user interface, the time of day will always be displayed on the center of the screen. There is an option to set this to a 12-hour or 24-hour clock when the system is set up for the first time. In the top-right corner of the screen is an icon with a person displayed on a screen. If you select this option, a self-view window will appear. Once displayed, the self-view window can be moved to six different points around the screen: the top-left corner, top-right corner, middle-left edge, middle-right edge, bottom-left corner, or bottom-right corner. The gear icon in the top-left corner will bring up some selective menu options. The menus available from the top down are Do Not Disturb, Light Adjustment Bar, Forward All Calls To…, Forward All Calls to Voicemail, System Information, and Standby. The System Information menu will provide the endpoints' video address, IP address, MAC address, SIP Proxy, software version, and device type. The Settings button along the bottom of the screen will allow you to view and change some extended settings on the endpoint. However, advanced settings need to be configured from the web interface or the CLI.

Key Topic

At the bottom of the main screen, located under the clock, are two circles. The red circle is a direct access to a voicemail box, and the green circle is used for calling. If you select the green Call button, a dial box will display. When you select the dial box, a QWERTY keyboard with a numeric dialpad will display at the bottom of the screen. This allows for easier dialing of both SIP URIs and E.164 aliases. You can enter the alias of the destination and click the green Call button that appears to the right. This Call button will not appear until you start typing a destination alias. Once the Call button is pressed, the destination alias will ring, and the call will connect when the far-end participant answers the call. Figure 10-2 illustrates the call settings for dialing by alias from the user interface.

Tap in dial box for the keyboard to appear below.

Tap on the call button to place the call.



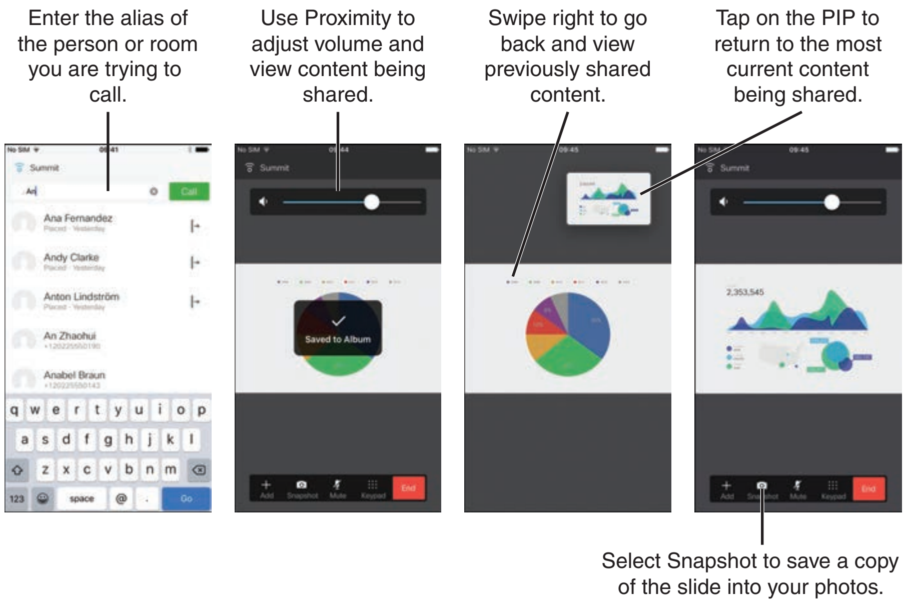
Tap on the Call Button to Place the Call

Use the QWERTY keyboard or numeric key pad to dial the destination alias.

Figure 10-2 *Cisco DX80 Dial by Alias Settings from User Interface*

Another way to dial from an endpoint is to use the Intelligent Proximity for Content Sharing application from a Windows or Mac computer, smartphone, or tablet. Once the Proximity application pairs with the endpoint, a dial box will appear in the middle of the screen. When you tap inside this box, a keyboard will display at the bottom of the screen. You can dial the alias of the destination endpoint and tap the green Call button. The endpoint, not the

Proximity app, will dial out to the destination. Once the call has connected, you can use the Proximity app to adjust the volume on the endpoint, receive content being shared, scroll through previously shared content, and save content to the Photos library on your device. There is also an End button on the Proximity app to hang up a call, and when the endpoint is being called, an Answer button will appear. Figure 10-3 illustrates some of the functionality that exists with Intelligent Proximity.



Enter the alias of the person or room you are trying to call.

Use Proximity to adjust volume and view content being shared.

Swipe right to go back and view previously shared content.

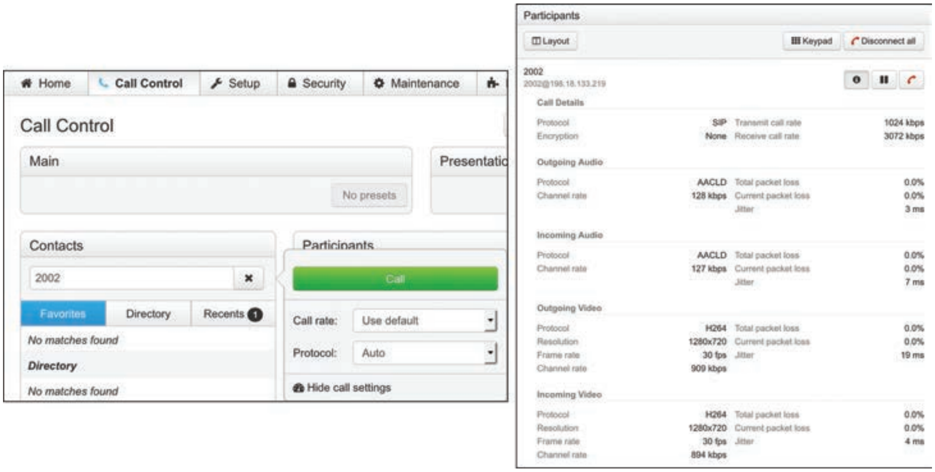
Tap on the PIP to return to the most current content being shared.

Select Snapshot to save a copy of the slide into your photos.

Figure 10-3 *Dialing from an Endpoint Using Proximity*

Key Topic

The next two options for dialing out from a Cisco CE software-based endpoint using the alias of a destination are only used typically by an administrator. The web interface or CLI allows an administrator to dial out from an endpoint without being physically present with the endpoint. This serves a great purpose when troubleshooting call setup issues from remote locations. This capability could also prove useful when an administrator needs to dial out on behalf of a user at the endpoint's location. Although this second point of reasoning may not make sense to everyone, many companies and organizations do not want users dialing out from conference endpoints. Therefore, a conference administrator will dial out on behalf of participants at the time a meeting is set to begin. From the web interface of a CE software-based endpoint, you click the Call Control menu from across the top of the screen. Under the Contacts section, click in the dial box and enter the alias of the destination. Once an alias has been entered, a green Call button will display. Below the Call button there is an option called Show Call Settings. This allows the person dialing to change the Call Rate, which is the requested bandwidth for this call attempt, and the Protocol, which could be SIP, H.323, or H.320. Only the protocol enabled and used on the endpoint will display under the Protocol section. Once the call connects, you can display call details on the web interface by selecting the i button. Beside this button there is also a Hold and Disconnect button. Figure 10-4 illustrates how to dial out from the web interface of a Cisco DX80 endpoint.



Contacts: 2002

Call rate: Use default

Protocol: Auto

2002
2002@198.18.133.219

Call Details

Protocol	SIP	Transmit call rate	1024 kbps
Encryption	None	Receive call rate	3072 kbps

Outgoing Audio

Protocol	AACLD	Total packet loss	0.0%
Channel rate	128 kbps	Current packet loss	0.0%
		Jitter	3 ms

Incoming Audio

Protocol	AACLD	Total packet loss	0.0%
Channel rate	127 kbps	Current packet loss	0.0%
		Jitter	7 ms

Outgoing Video

Protocol	H264	Total packet loss	0.0%
Resolution	1280x720	Current packet loss	0.0%
Frame rate	30 fps	Jitter	19 ms
Channel rate	909 kbps		

Incoming Video

Protocol	H264	Total packet loss	0.0%
Resolution	1280x720	Current packet loss	0.0%
Frame rate	30 fps	Jitter	4 ms
Channel rate	894 kbps		

Figure 10-4 *Dialing by Alias from the Web Interface of a DX80*

Dialing out from the CLI requires a simple command. You open an SSH connection to the endpoint and then enter the following command:

```
xCommand dial number: alias
```

The *alias* should be the alias of the destination endpoint, such as 2002. Once the call connects, you can enter the following commands to view call connection status and to disconnect the call:

```
xStatus call
```

```
xCommand call disconnect
```

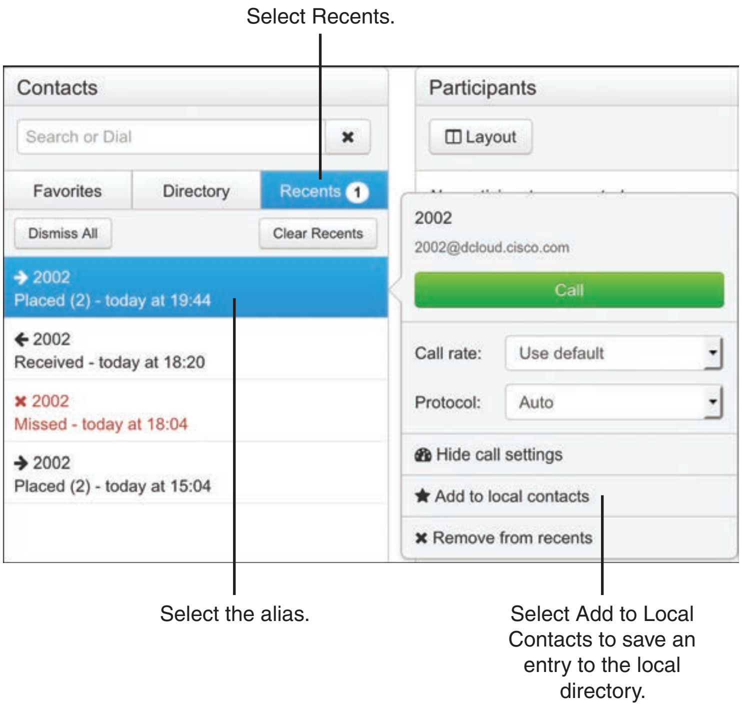
For more information about API commands on Cisco CE software-based Telepresence endpoints, use the following API reference guide: https://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/ce97/collaboration-endpoint-software-api-reference-guide-ce97.pdf.

Call by Directory

Key Topic

Another means of dialing out from an endpoint is to use the *directory*. A directory is a phonebook that the endpoint has access to but does not necessarily reside on the endpoint itself. Three different types of directories are available to endpoints: a local directory, a corporate directory, and a global directory.

The local directory is a collection of aliases that have been saved directly on the endpoint itself. The endpoint is the sole source of these directory entries; therefore, the endpoint will always contain these entries unless an administrator intentionally deleted them from the system. To add an entry into the local directory, a call attempt must be placed first. After a call has been attempted, whether the call successfully connected or not, locate the dialed alias in the Recents section of the call settings. When you select the entry, a list of options will appear. Select the Add to Local Contact option, and the entry will be added to the Favorites section, which is the local directory. Figure 10-5 illustrates how to add an alias to the local directory.



→ 2002
Placed (2) - today at 19:44

← 2002
Received - today at 18:20

✖ 2002
Missed - today at 18:04

→ 2002
Placed (2) - today at 15:04

2002
2002@dcloud.cisco.com

Call rate: Use default

Protocol: Auto

Select Recents.

Select the alias.

Select Add to Local Contacts to save an entry to the local directory.

Figure 10-5 *Adding an Alias to the Local Directory*

Key Topic

The corporate directory is the most common directory used in Cisco collaboration. The corporate directory is a phonebook that an endpoint subscribes to when an entry needs to be looked up. These directories do not live on the endpoint itself; rather, they exist solely on the system designed to deliver the aliases when requested. Two systems in a Cisco collaboration solution are capable of delivering a corporate directory to Cisco endpoints. They are the Cisco Unified Communications Manager and the Cisco Telepresence Management Suite, or TMS. Because the focus of this book is on the Cisco Unified Communications Manager, we will not discuss TMS at this time. Endpoints have a finite amount of storage. In fact, a Cisco Collaboration Telepresence endpoint could hold only about 350 directory entries locally. Therefore, the idea of a corporate directory is to create a much larger depository of directory entries on a server built to sustain the greater load and make these entries available to the endpoint as users need the information. The endpoint must have the corporate directory location configured so that it knows where to send the subscription request when inquiring about an entry. When an endpoint registers to the Cisco Unified Communications Manager, the corporate directory address is included in the TFTP Get information sent to the endpoint. You can verify this setting is configured on the endpoint by navigating in the web interface to **Setup > Configuration > Phonebook**. The Type should be set to CUCM, and there may or may not be a URL configured.

The global directory is similar to a corporate directory, in that it originates on a server outside the endpoint itself. However, a global directory is pushed out to the endpoint, so the directory entries live on the endpoint just as the local directory entries live on the endpoint. Obviously, the limitation to this type of directory is the same limitation to the number of directory entries that can exist on a Cisco Telepresence endpoint. However, global directories can be used with a corporate directory. A limitation to the corporate directory is that if the endpoint loses the connection to the corporate directory, then the endpoint also loses those phonebook entries. However, important aliases can be pushed to an endpoint using a global directory, so that those phonebook entries will never be lost to the endpoint. Unfortunately, the Cisco Unified Communications Manager does not support a global directory. This is a function that only the Cisco TMS can provide.

Regardless of the directory choice, users can be dialed by the directory on the endpoint. You initiate the dialing behaviors the same way as described in the previous section. As you type letters in a name or numbers in a DN, entries will populate the screen. This is the nature of a corporate directory on the endpoint. When you see the name of the person or room you wish to call, select that entry and press the green Call button. Alternatively, you could select the Directory tab and see an alphabetized list of contacts from the combined directories that exist on your endpoint. Figure 10-6 illustrates the use of the directory feature for dialing from a Cisco DX80.

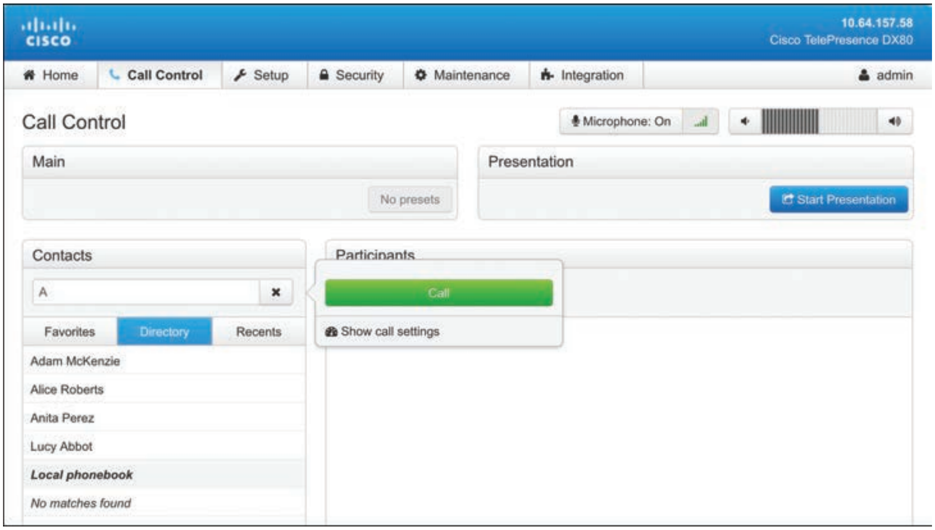


Figure 10-6 *Dialing by Directory on a Cisco DX80*

Multipoint Calling

Up to this point all the calling options discussed involve a point-to-point call. When you are connecting with a multipoint call, the options can be slightly different because different multipoint calling options exist. In a Cisco collaboration solution, three terms related to multipoint calling must be defined. They are *multipoint*, *multisite*, and *multiway*.

Key Topic

Multipoint is an industrywide term used to describe any call that involves three or more participants. Many conferencing products are available to host a multipoint call. Some of these products will be discussed momentarily. *Multisite* is a Cisco-specific term that came from the Tandberg acquisition. Multisite is the option key available on CE software-based endpoints that enables the endpoint to host a multipoint call. When multisite is used, no external conferencing resource is required. However, there are a lot of limitations to using the multisite option over an external conferencing resource. Depending on the endpoint being used for the multisite call, the number of participants allowed to join the call is limited. All participants in a multisite call must connect at a common bit rate, which is usually the lowest common bit rate among all the participants. Also, a lot more call options are available on a conferencing resource that are not available on the endpoint using multisite to host a call. The third term related to multipoint calling that needs to be defined is *multiway*. Like multisite, *multiway* is a Cisco-specific term that was adopted with the Tandberg merger. Multiway is simply call escalation from a point-to-point call to a multipoint call hosted on a Multipoint Conferencing Unit (MCU). Multiway is a function used by the Cisco VCS through a setting called the Conference Factory. It can be used only with a Cisco Telepresence MCU, which are end-of-life products.

A call escalation function is available through a Cisco Unified Communications Manager as well, although it is called *ad hoc conferencing*, not multiway. Ad hoc conferencing operates in the same capacity as multiway, allowing a point-to-point call to escalate to a multipoint call using an external conferencing resource to host the call. Any current Cisco conferencing resource can be used to support ad hoc calling on the Cisco Unified Communications Manager. Another conferencing option through the Cisco Unified Communications Manager is called rendezvous conferencing. Think of this conferencing type as an always-on conference space that can be joined at any time. Different settings must be configured on the Cisco Unified Communications Manager for ad hoc or rendezvous conferences, but both can exist at the same time. A third conferencing option is scheduled conferences, but these types of meetings cannot be configured from the Cisco Unified Communications Manager. Scheduled conferences must be configured through Cisco TMS.

Key Topic

Basically, three different Multipoint Conferencing Resources are available in a Cisco solution external to the multisite option on Cisco endpoints. Each of these conferencing options can be divided into an on-premises solution, a cloud-based solution, or a hybrid solution between the two. The on-premises solution Cisco offers is called the Cisco Meeting Server, or CMS. Licenses can be added to CMS for Personal Multiparty (PMP) or Shared Multiparty (SMP). PMP licenses are assigned to individual users, and no other party can join their personal space on CMS until the owner of the space has joined. SMP licenses are used to create a shared space into which any user can initiate a call. Therefore, it is recommended to protect SMP licensed meeting spaces on CMS with PINs in order to restrict who can utilize those resources. SMP licenses are also needed for scheduled meetings through TMS. When scheduled meetings are created, no participant can join the meeting until TMS initiates the conference. TMS can also create a private PIN, which participants must enter before joining the call.

Key Topic

Cloud-based meetings are hosted through the Cisco Webex Meeting Center. This is the same powerful tool that has been used for years to allow multipoint conferencing in the cloud. Participants can join via a Webex Meeting client, through a browser, using Webex Teams, or using a unified IP phone or Telepresence endpoint. Physical devices located on-premises, such as the Unified IP phones or Telepresence endpoints, require Expressway Core and Expressway Edge to be configured for firewall traversal to the Webex cloud before meetings can be joined from these devices. All the same tools that have traditionally been used with Webex Meetings are still available, such as high-quality voice and HD video communication, content sharing, polling, and annotation. Additionally, Cisco has added a few more enhancements to Webex Meeting Center, such as cognitive collaboration features.

Key Topic

Bandwidth limitations and network constrictions may negatively impact cloud-hosted meetings through the Webex Meetings solution. Therefore, Cisco has developed a new method to allow a hybrid service using both Webex Meetings and an on-premises conferencing service called the Video Mesh Node (VMN). The VMN is a virtual server that must be installed on-premises but operates in conjunction with Webex Meeting Center in the cloud. When Webex Meetings are scheduled, on-premises endpoints call into the VMN instead of calling into Webex directly. Then the VMN will send a single stream out to Webex with a composite of all the audio and video of the participants connected. Webex will send a composite of any participants connected directly to the cloud back to the VMN. In this manner, all participants are able to see and hear one another as if they were all connected to the same conferencing unit. The single stream sent between the VMN and Webex limits the bandwidth consumed across the edge network, and reduces the network constraints, creating a better user experience all around. Much more can be said for the hybrid conferencing solution, but that topic will have to be saved for another book.

One Button to Push (OBTP) and Scheduling Conferences

You should now have a basic understanding of the terms *multipoint*, *multisite*, and *multiway*, as well as *ad hoc*, *rendezvous*, and *scheduled conferences*. Furthermore, you should comprehend the differences between an on-premises conferencing solution compared to a cloud-based conferencing solution and a hybrid conferencing solution and be able to identify the different products used for each of these solutions. Bringing the subject back to the topic of dialing behaviors, each of these circumstances around multipoint communication can impact how participants are connected to meetings.

Similar to how participants call one another in a point-to-point call, participants can dial into a multipoint meeting if they know the associated alias. If multisite is used, this will be the alias of the endpoint hosting the call. If CMS or Webex are hosting the call, then the alias of the meeting space must be provided to the attendees before they will be able to dial in.

Multiway and ad hoc calls do not require the meeting ID to be known at all. One of the participants in a point-to-point call will place the second endpoint on hold while calling a third endpoint. With ad hoc, the Conference button must be selected to escalate the call. With multiway, the Join or Connect button must be selected to escalate the call. At that point the call control system, whether it is the Cisco Unified Communications Manager or the Expressway Core, is responsible for transferring the endpoints to the conferencing solution.

Key Topic

Scheduled multipoint calls can utilize any of the conferencing resources: multisite, CMS, or Webex with or without VMN. Many different circumstances influence how dialing behaviors will be impacted, but the following is simply a list of the possible ways through which calls can be connected. TMS can initiate calls from endpoints to the conferencing solution at a scheduled time. The user will not have to dial anything; the endpoint will just connect. TMS can also initiate calls from the conferencing solution out to the endpoint. In this case, the user will need to answer the incoming call. A combination of these two options can also be configured, where TMS will automatically dial from some of the endpoints into the meetings and dial from the meeting out to other endpoints. TMS can start the meeting but not connect any participants to the meeting. The participants will need to know the alias to call into the meeting and dial in manually. A final, and more commonly used, option for connecting participants to meetings is the use of a tool call One Button to Push (OBTP).

One Button to Push is a communication option Cisco created prior to the Tandberg acquisition. After the merger was completed, Cisco quickly incorporated this feature into all the Tandberg products acquired. As new products have been developed, Cisco has ensured this highly sought-after feature is continually updated and supported across all of Cisco's communications product portfolio. OBTP is a call connection option that functions only when meetings are scheduled. Although technology systems are very punctual, people are not always as prompt. If a scheduled meeting begins before the participants are ready to communicate, late participants entering the meeting room could be disruptive to others already connected to the meeting. The idea behind OBTP is that a Join button will appear on the endpoint scheduled for a meeting at the time the meeting is scheduled to begin. When the participants in the room of the endpoint are settled and ready to join the meeting, they select that Join button and are connected to the meeting at that time. There is no need know the meeting alias to join, and the endpoint will not be joined to the meeting before the participants are ready. It is no wonder this seamless solution is so widely adopted.

Content Sharing Options

Content sharing is a feature that allows media from a device external to the video endpoint to be displayed on or through the video endpoint. The content sharing feature has changed drastically over the last 30 years. Since video communication is a relatively new technology, the concept of sharing content over great distances had to be conceived and developed over time. The first standard that resembled content sharing was an old ITU standard that was part of the circuit-switched umbrella standard H.320. This standard was called T.150, and it was the *Terminal Equipment and Protocols for Telematic Services*, otherwise known as the *Telewriting Terminal Equipment*. This standard was originally drafted in 1983 and was later revised in 1993.

No other protocol was introduced for content sharing until 1999, when the Olivetti and Oracle Research Lab in Cambridge, UK, released an open-source protocol called virtual network computing, or VNC. VNC is a graphical desktop-sharing system that uses the Remote Frame Buffer (RFB) protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical-screen updates back in the other direction, over a network. Although VNC can be used for remote desktop control, it was commonly used for content sharing over an IP call, since there was not a viable standard for content sharing yet.

This situation led to two proprietary protocols that were developed and released in 2000, specifically designed for content sharing. Tandberg released the DuoVideo protocol first, and later that year PictureTel released the People+Content protocol. Polycom acquired PictureTel in 2001 and assumed the continued development of People+Content. By 2002 Polycom was offering People+Content for any vendor to use royalty free.

In 2003, the ITU used both the Tandberg and Polycom content sharing protocols to develop a standard that could be used across all H.323 IP calls known as H.239. As SIP was growing in popularity for voice and video calls, a standard had to be drafted for content sharing over SIP as well. In 2006, the IETF drafted RFC 4582 for the Binary Floor Control Protocol (BFCP), which is used for content sharing over SIP. Today, H.239 and BFCP are the two predominant content sharing protocols used industrywide. However, Cisco has been working on other means of sharing content for audio-only participants while in a call. Who knows what other crazy idea might shape the future of content sharing standardizations!

Sharing Content

Content sources could be any devices capable of connecting to the video endpoint. Common content sources could be a dedicated desktop computer; personal laptop computer; smartphone; tablet; VHS, DVD, or Blu-ray player; or even a digital media player (DMP), such as an Apple TV or TV tuner. Content can be shared locally, meaning only in the same room as the video endpoint when not in a call, or content can be shared remotely through the video endpoint to the remote destination at the other end of the call. Most Cisco CE software-based endpoints will display the local content on the screen as soon as the content source is connected. Typically, this is through an HDMI, VGA, or DVI cable, but other connection systems are available although they will not be discussed in this book.

Key Topic

Sharing content while in a call is a manual process that must be executed with intention. This is not a difficult task to impose, but there is no possible way content can be shared by accident. If you were sharing content locally and someone were to call the endpoint you were sharing content through, the content sharing would cease the moment the call was answered. To share content while in a call, you must first select the Show PC button. This will only share the content locally. This feature gives the presenter a chance to see the content that will be presented prior to actually sharing the content. When you are ready to share the content, select the Share button, and the content will be sent in a video stream to the participants at the far end of the call. Tap the Stop Sharing button to end the content sharing session. If you disconnect the call before stopping the content sharing, you will still cease to share content as the call is terminated. If the other party in a call tries to share content while you are currently sharing content, your content sharing session will end, and that person's content will be displayed as a replacement. The same behavior would occur if you were to try sharing content again while the far end was still sharing content.

Using Intelligent Proximity for Content Sharing

Earlier in the chapter, we discussed receiving content using the Proximity application. Any device running the Proximity application can receive content being shared; however, there is also a way to share content using the Proximity application. Content can be shared only if the Proximity application has been installed on a computer running Microsoft Windows or Apple Mac OS. Linux-based operating systems do not support the Proximity application, and smartphones and tablets do not support sharing content, only receiving content.

To install Proximity on your computer, navigate to www.proximity.cisco.com. Choose the appropriate operating system and download the executable file. When the download is complete, launch the installer, agree to the EULA, and begin using Proximity. Assuming the computer being used to share content through Intelligent Proximity meets the previous criteria, there are two ways to initiate the content sharing. Each way is slightly different depending on whether you are sharing content from a Windows PC or a Mac.

Key Topic

When you open the Proximity application on your Mac computer, a Proximity window will appear on the screen. In the app window is a Share Screen button. Tap this button to start sharing your screen. If you have two screens connected to your computer, select the Video System menu from the top left of the screen and choose **Select Screen > <choose screen>**. To stop sharing, bring the app back to the front of the screen and click the Stop Sharing button. When Proximity is installed, a Proximity icon also appears in the top bar on the screen. If you click this bar, you will see all the different menu options available. Go to the Select Screen menu to choose the appropriate display to present from. Then choose the Share

Screen menu option to start sharing content. Choose Stop Sharing when you are finished sharing.

There are two ways to share content from a Microsoft Windows computer as well. Sharing content using the Proximity app on a Windows computer is basically the same as sharing content through the app on a Mac computer. Alternatively, you could press Alt+F12 to start sharing content. Proximity must be running and connected to the endpoint before content can be shared through the application. If another user is sharing content and you start sharing from the Proximity app on your computer, your shared content will override that user's content, and they will stop sharing. The same would be true if someone else started sharing content while you were sharing. Figure 10-7 illustrates the two ways to share content through the Proximity application from a Mac.

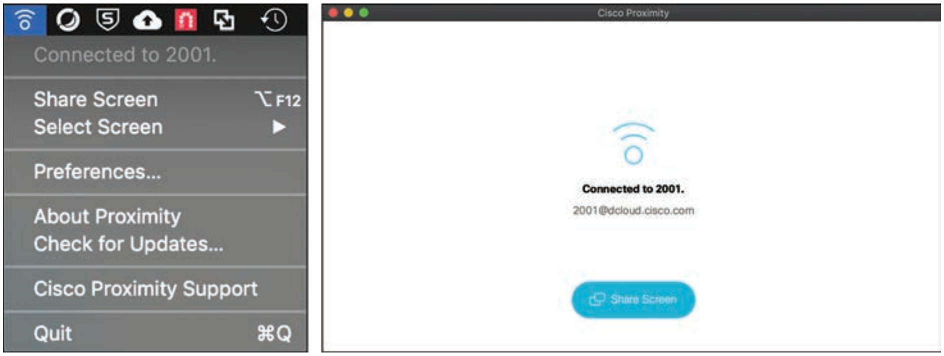


Figure 10-7 *Content Sharing from a Mac Using Proximity*

Other Features

Many calling features available through CE software-based endpoints provide administrators with granular control over the video Telepresence environment. There are more features than what is covered in the sections that follow; however, the following examples are some of the more commonly used settings on these endpoints. None of these settings can be configured from the user interface. They must all be configured from the web interface or the CLI. When an administrator accesses the **Setup > Configuration** menus of a CE software-based endpoint through the web interface, all of the following settings can be configured by selecting the appropriate menu in the left column. The sections that follow cover those menu options in order from the top down. Encryption Mode, AutoAnswer, and Far-End Camera Control are all features listed under **Setup > Configuration > Conference.**

Audio Settings

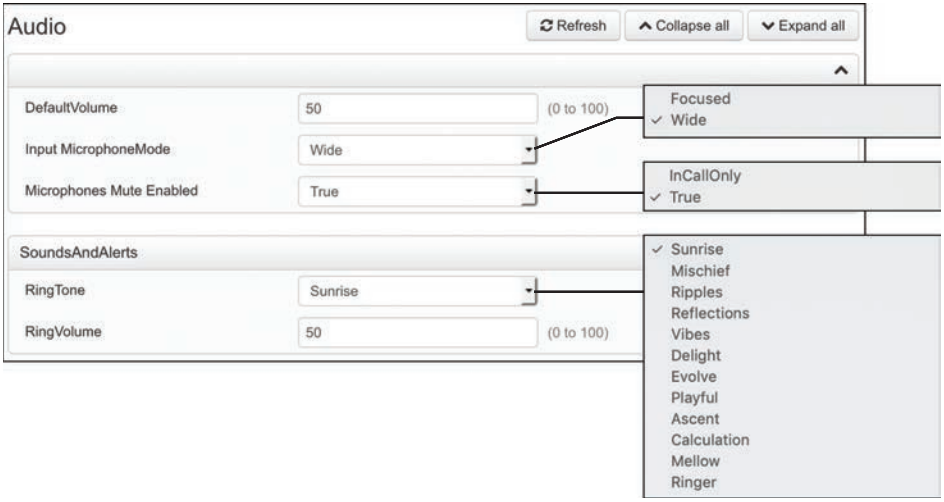
Some of the audio settings on certain CE software-based endpoints are more extensive than the audio settings on other endpoints. For example, the Cisco Telepresence DX80 endpoint does not have as many audio inputs and outputs as the Cisco Webex Room Kit Pro endpoint, which was built for custom integrator solutions. Therefore, the audio menu options on a Cisco Webex Room Kit Pro are much more extensive than the audio menu options on the Cisco Telepresence DX80. Depending on what endpoints you are planning to deploy and support, you should spend some time in the deployment guides to familiarize yourself with the different audio options available. However, all CE software-based endpoints share a few common audio settings.

Basic audio settings include audio output settings, such as DefaultVolume, and input settings, such as Input MicrophoneMode, which sets the microphone pickup area, or Microphone Mute Enabled. The DefaultVolume setting comes preset to 50 and can be changed to any value between 0 and 100. The Input MicrophoneMode is preset to Wide so that more participants can be accommodated around a single microphone, but it can be changed to Focused if the room is designed for fewer participants. The Microphone Mute Enabled setting can be set to True or InCallOnly. This setting does not mute the microphone; rather it enables the user to mute the microphone. Therefore, this setting can be configured to always allow the microphone to be muted, or it can prevent the microphone from being muted unless there is an active call in session. Some people like to mute the microphone prior to placing a call; therefore, the default value of True should be left unchanged.

Another section of audio settings that are consistent among all CE software-based endpoints is the SoundAndAlerts settings. The two settings that can be configured in this section are RingTone and RingVolume. RingTone is the audio tone a user will hear when an incoming call is being attempted. The following 12 different ringtones are available on Cisco Telepresence endpoints:

- Sunrise (default value)
- Mischief
- Ripples
- Reflections
- Vibes
- Delight
- Evolve
- Playful
- Ascent
- Calculation
- Mellow
- Ringer

RingVolume is different from DefaultVolume, in that it only impacts how loud the ringing signal will alert. DefaultVolume impacts the actual audio of the far-end participants as their dulcet tones are projected from the system speakers. Much like DefaultVolume, RingVolume defaults at 50 and can be modified between 0 and 100. Figure 10-8 illustrates these audio settings from a Cisco Telepresence DX80 endpoint.



Audio

DefaultVolume 50 (0 to 100)

Input MicrophoneMode Wide

Microphones Mute Enabled True

SoundsAndAlerts

RingTone Sunrise

RingVolume 50 (0 to 100)

Figure 10-8 *Audio Settings on a Cisco Telepresence DX80*

Key Topic

Encryption Mode

Encryption Mode, which is a setting located under the Conference menu, has to do with call encryption during call setup. Call encryption can occur for both H.323 and SIP calls, but the encryption they use is slightly different. Both use TLS for TCP and UDP packet encryption. However, H.323 supports 56-bit DES encryption or 128-bit AES encryption. SIP supports AES 128- or 256-bit encryption. Also, the means by which H.323 and SIP perform the handshake for secure transmission is different. Because so many different encryption options exist for the two call control protocols, only three settings on CE software-based endpoints revolve around Encryption Mode: BestEffort, On, and Off.

BestEffort is the default setting. The idea behind BestEffort is that the endpoint will try to encrypt when the call is first set up. If the far-end endpoint does not support the same encryption algorithms, or if the far-end endpoint has encryption disabled, then the call will continue as an unencrypted call. When the EncryptionMode is set to on, the call can proceed only if the destination endpoint is also configured to support call encryption and the two algorithms match. Otherwise, the call will fail. The same is true when the Encryption Mode is set to Off. The endpoint will never try to encrypt, so if the far-end endpoint requires encryption, then the call attempt will fail.

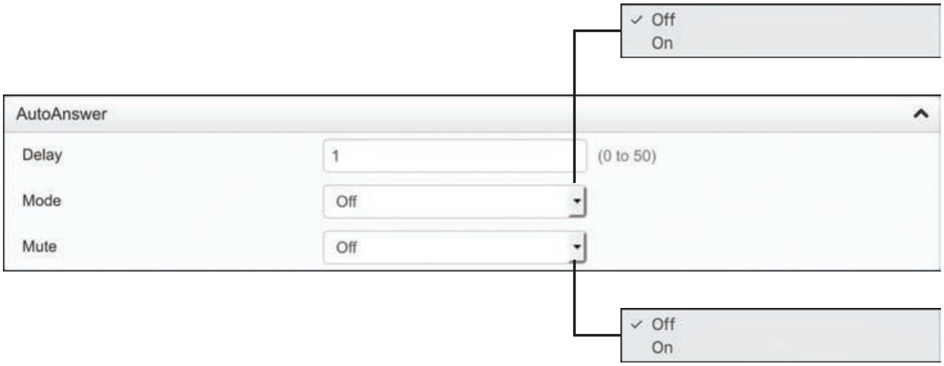
AutoAnswer

The second section located under the Conference menu is called AutoAnswer. This feature performs exactly as the name implies. When an endpoint is called and the AutoAnswer feature is enabled, the endpoint will answer the call on its own volition without any human interaction. This capability might seem scary to some people because with AutoAnswer enabled, a user may be caught unaware during a call. You should understand that this feature is disabled by default, so you would have to intentionally enable it before calls could be answered automatically. However, there was a time when AutoAnswer was the norm, and a lot of people had home video systems. People have been caught sleeping, coming out of the shower, and entrenched in many other precarious situations.

Key Topic

The idea behind why this feature exists came out of a time when the conference meeting bridge would dial out to all the scheduled endpoints at the time the meeting was supposed to start. Whether the participants were in attendance at their assigned location or not, the endpoint needed to answer the call to ensure the call connected at the scheduled time. Then Cisco released the OBTP feature discussed previously in this chapter, and just like that, the AutoAnswer feature became much less commonly used. If the AutoAnswer feature is going to be used, some best practice tips need to be taken into consideration. First, you should enable this feature only on meeting room endpoints. Do not enable the feature on personal video endpoints, and definitely do not enable this feature on home video devices. Second, if AutoAnswer is enabled, it is a good idea to enable the Mute on Answer feature. This way, the call will connect as it should, but while people are still settling in the meeting room, the noise will not be disturbing to other participants in the call at remote locations.

The AutoAnswer section consists of three settings: Delay, Mode, and Mute. Delay is measured in seconds and determines the time duration the incoming call should ring before the endpoint will answer the call automatically. The default value is 1, and this setting can be set to any number between 0 and 50. Mode is the setting used to enable the AutoAnswer feature. The default value is Off, and this setting can be changed to On. Mute can be set to Off, which is the default value, or On. When this feature is enabled along with Mode, the endpoint will mute the microphone(s) at the time the call is answered. It is strongly recommended to enable the Mute feature if AutoAnswer is enabled. Figure 10-9 illustrates the AutoAnswer settings in a DX80 endpoint.


AutoAnswer

Delay 1 (0 to 50)

Mode Off

Mute Off

Figure 10-9 *AutoAnswer Feature Settings on a DX80*

Far-End Camera Control (FECC)

Key Topic

A third setting located under the Conference menu that is commonly used is the Far-End Camera Control (FECC) settings. FECC is a setting that allows the camera on your video endpoint to be controlled remotely by another endpoint while in a call. Obviously, camera control can occur only if the camera on the endpoint is an auto PTZ camera, such as the Cisco Precision 60 camera. The camera built into the DX80 endpoint is a manual tilt and zoom camera, with no panning capability. Therefore, enabling FECC on this endpoint would be pointless. The same would be true for the Webex Room Kit series endpoints because the cameras integrated into those endpoints operate differently than the traditional auto PTZ cameras. The capability to control a camera on the far end of a call does not require any setting to be enabled. This capability is built into all Cisco Telepresence endpoints automatically and is always available.

To configure FECC on a Cisco CE software-based endpoint from **Setup > Configuration > Conference**, scroll down to the bottom of the page and look for the FarEndControl section. The Mode setting should be set to On by default. This means that FECC is automatically enabled on the endpoint. To disable FECC, change the Mode to Off. Another setting under the FarEndControl section, called SignalCapability, can be set to On (default) or Off. The standard for FECC is H.224, so this setting enables or disables the use of H.224 for FECC. Because the SignalCapability setting performs the same essential function as Mode, it should be configured using the same setting as Mode for the desired service of FECC. In other words, if Mode is set to On, then SignalCapability should be set to On. If Mode is set to Off, then SignalCapability should be set to Off.

Phonebooks

Key Topic

The earlier "Call by Directory" section discussed the differences between the local directory, corporate directory, and global directory. Local directories are created on the endpoint itself, and global directories are initiated from the Phonebook service; therefore, no settings need to be configured on the endpoint to receive global directories. However, corporate directories require the endpoint to initiate a Subscription message to the phonebook service for each individual phonebook lookup in order to receive entries in reply. This allows the phonebook service to supply only listings based on the characters or numbers that have been entered. You can configure subscription information on the Phonebook menu on Cisco Telepresence endpoints so that the endpoints know where to send the Subscription message. When an endpoint registers to the Cisco Unified Communications Manager, the Phonebook information is automatically provisioned on the endpoint, so no settings need to be configured. However, when the Cisco TMS services are used for Phonebook management, these settings may need to be changed.

There are three settings under the Phonebook > Server 1 section. The ID setting allows a name to be assigned to the phonebook. By default, no name is associated with the phonebook, and the phonebook will continue to function as normal if no name is assigned.

The Type setting allows an administrator to determine from where the phonebook source will come. The default value for this setting is Off, but it can be configured as any of the following:

- **CUCM:** Use this setting if the Cisco Unified Communications Manager is the source of the corporate directory. When the endpoint registers to the Cisco Unified Communications Manager, this setting will change automatically, and no other settings have to be configured on the endpoint.
- **Spark:** Use this setting if the Webex Control Hub is the source of the corporate directory. When the endpoint registers to the Webex Control Hub, this setting will change automatically, and no other settings have to be configured on the endpoint.
- **TMS:** Use this setting if Cisco TMS is the source of the corporate directory.
- **VCS:** Neither the Cisco VCS nor the Expressway can be the source of the corporate directory. However, if the endpoint is registered to one of these products, TMS can be the source for the phonebook. Therefore, Type can be set to VCS or TMS.

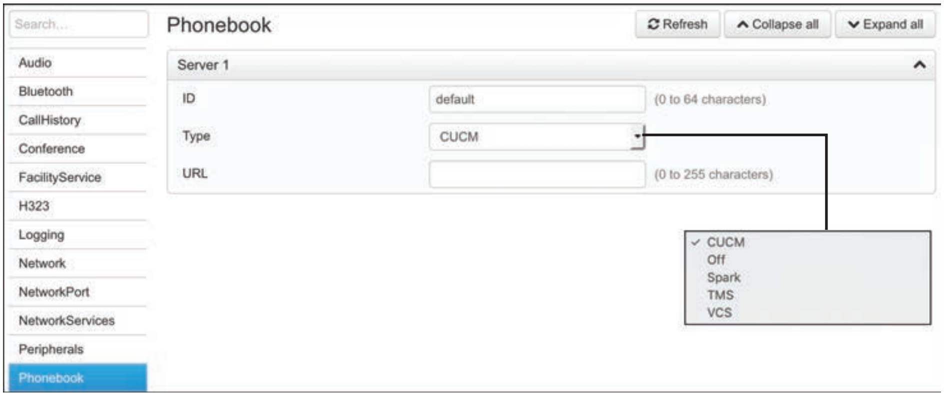
The third setting under Phonebook > Server 1 is the URL setting. In some instances, a URL address to the server providing phonebook services is required. This setting will never be required when **Type > Spark** is selected, will only occasionally be required when Type > CUCM is selected, and will always be required when Type > TMS or Type > VCS is selected. An example of the URL that may be used when the Type is set to CUCM could be as follows:

https://<*cucm-host-name*>:8443/cucm-uds/users

An example of the URL that may be used when the Type is set to TMS or VCS could be as follows:

https://<*tms-host-name*>/tms/public/external/phonebook/phonebookservice.asmx

In both examples, the portion of the URL that is in bold could be the IP address or DNS A-record of the server the name references, TMS or CUCM. Notice that within both URLs specific directories are referenced. You could use these URLs in any production environment by simply replacing the bold portion with your specific server address information. Figure 10-10 illustrates the Phonebook settings on a Cisco Telepresence endpoint.



Phonebook

Server 1

ID default (0 to 64 characters)

Type CUCM

URL (0 to 255 characters)

Figure 10-10 *Phonebook Settings on a Cisco Telepresence Endpoint*

Video Settings

The last group of settings that will be discussed in this chapter is the video settings. Under the **Setup > Configuration** section, Video is at the bottom of the menus in the left column. Much the same as audio settings, video settings may vary based on the endpoint's capabilities. Different endpoints have more or fewer video inputs and video outputs. Therefore, there may be more or fewer menu options based on the number of inputs and outputs. However, many common settings are consistent among all Cisco Telepresence endpoints regardless of the endpoint being used. The Video menu is divided into the following six sections:

- Top Main Video section
- DefaultLayoutFamily
- Input
- Output

- Presentation
- Selfview

The top main video section does not have a section title. The settings listed in this section are the main functional settings related to the endpoint. Some of the settings listed here include Active Speaker DefaultPIPPosition. PIP stands for Picture-in-Picture and refers to a video screen layout where a smaller video pane can exist within a larger video pane. The configuration options for this setting pertain to the positioning of the PIP, and they affect the layout only when a call is in session that uses a layout with a PIP overlay. The options for this setting can be any of the following:

Key Topic

- CenterLeft
- CenterRight
- Current
- LowerLeft
- LowerRight
- UpperCenter
- UpperLeft
- UpperRight

The next setting in the first section is the DefaultMainSource. This setting determines which display will be the main video display when a call is in session. Some of the Cisco CE software-based endpoints support two or more displays. In these environments the default main source displays the incoming video of the far-end participants, while the second display is used for content presentation only. When the endpoint is used for local meetings, both displays can support content sharing. The next setting in this section is called Monitors. Similar to the DefaultMainSource setting, the Monitors setting determines how many monitors are currently being supported from this endpoint.

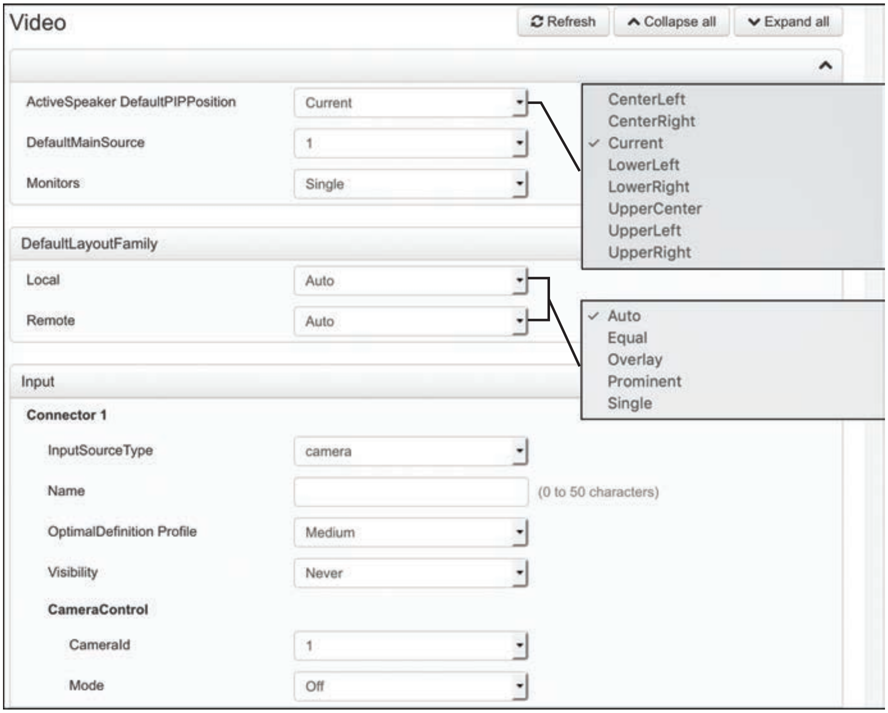
The next section under the Video menu is the DefaultLayoutFamily. These settings pertain only to multipoint calls that use the multisite feature on the endpoint. Five different layouts are supported with the multisite feature, and they can be configured differently for Local and Remote. Local is the layout that participants at this endpoint will view during a call, and Remote is the layout that will be presented to other participants connected to the call. The five layouts supported using the multisite feature are as follows:

Key Topic

- **Auto:** The default layout family, as given by the local layout database, will be used as the remote layout.
- **Equal:** All video participants will have equal-sized panes as long as there is enough space on the screen.
- **Overlay:** The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small PIPs. Transitions between active speakers are voice switched.

- **Prominent:** The active speaker, or the presentation if present, will be a larger picture, while the other participants will be smaller pictures. Transitions between active speakers are voice switched.
- **Single:** The active speaker, or the presentation if present, will be shown in full screen. The other participants will not be shown at all. Transitions between active speakers are voice switched.

The third Video section is the Input section. These settings are the controls for all of the video input ports on the endpoint itself, and therefore, there could be more or fewer settings listed based on the type of endpoint. Video input settings control devices such as cameras or content devices. Some endpoints support daisychaining multiple cameras together in a single room environment, so an administrator may want to assign a camera ID to each camera in the room and provide a name for the cameras, such as Rear Camera or Whiteboard Camera. Content sources could be an in-room computer, table-connected laptop, DVD or Blu-ray player, document camera, Apple TV, or any other device through which content can be shared. Because more than one content source can be connected to the endpoint at a time, the administrator may be inclined to name the content sources as well. Figure 10-11 illustrates the first three video sections that have been mentioned up to this point.



ActiveSpeaker DefaultPIPPosition: Current
DefaultMainSource: 1
Monitors: Single

DefaultLayoutFamily
Local: Auto
Remote: Auto

Input
Connector 1
InputSourceType: camera
Name: (0 to 50 characters)
OptimalDefinition Profile: Medium
Visibility: Never
CameraControl
CameraId: 1
Mode: Off

Figure 10-11 *Main, Layout, and Input Video Menu Sections*

Just as with the **Video > Input** section, the **Video > Output** section will have an equal number of Connector settings for configuration as the number of physical video output ports on the endpoint itself. So, the number of settings in this section could be more or fewer depending on the endpoint being used. Additionally, the setting options under each connector may differ based on the type of connection supported. Video outputs are the connector ports that the displays connect to on the endpoint. Some of the different settings you may encounter in the Output section on the endpoint include the following:

- **Brightness:** This setting defines the brightness level.
- **Resolution:** This setting defines the resolution and refresh rate for the connected screen. When Auto resolution is selected, the endpoint will automatically try to set the optimal resolution based on negotiation with the connected monitor.
- **Whitebalance Level:** This setting defines the camera's white balance level.
- **CEC Mode:** This video output (HDMI) supports Consumer Electronics Control (CEC). When this setting is On, the system will use CEC to set the screen in standby mode when the endpoint itself enters standby. Likewise, the system will wake up the screen when the system itself wakes up from standby mode. Note that different manufacturers use different marketing names for CEC, such as Anynet+ (Samsung); Aquos Link (Sharp); BRAVIA Sync (Sony); HDMI-CEC (Hitachi); Kuro Link (Pioneer); CE-Link and Regza Link (Toshiba); RIHD (Onkyo); HDAVI Control, EZ-Sync, VIERA Link (Panasonic); EasyLink (Philips); and NetCommand for HDMI (Mitsubishi).
- **OverscanLevel:** Some monitors may not present the entire image that they receive. This means that the outer parts of the image that is sent from the video system may be cut off when displayed on the monitor. You can use this setting to instruct the video system not to use the outer part of the available frame. This part might be cut off by the monitor. Both the video and messages onscreen will be scaled in this case.
- **RGBQuantizationRange:** Devices connected to an HDMI output should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately, some devices do not follow the standard, and this configuration may be used to override the settings to get a perfect image with any display. Most HDMI displays expect the full quantization range.
    - **Auto:** The RGB quantization range is automatically selected based on the RGB Quantization Range bits (Q0, Q1) in the AVI infoframe. If no AVI infoframe is available, the RGB quantization range is selected based on the video format according to CEA-861-E.
    - **Full:** Full quantization range. The RGB quantization range includes all code values (0–255). This is defined in CEA-861-E.
    - **Limited:** Limited quantization range. This RGB quantization range excludes some code values at the extremes (16–235). This is defined in CEA-861-E.
- **Location > HorizontalOffset/VerticalOffset:** These two settings are associated with each video output, and they are used to signal the relative position of the displays that are connected to these outputs. HorizontalOffset = 0 and VerticalOffset = 0 indicates that the display is positioned in the center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

The next section is the Presentation section, and two settings here can be configured. The DefaultPIPPosition is the same setting as the ActiveSpeaker DefaultPIPPosition setting discussed earlier. All of the configuration options are the same, except that this setting pertains specifically and exclusively to content being shared. Again, if the layout choice does not use PIP, this setting will not apply. The DefaultSource setting allows an administrator to specify the video input that will act as the primary source for content sharing. This setting will always be a number value and will be based on the video inputs the endpoint supports. For example, the DX80 has only one video input dedicated to content sharing, and that port is hard-coded as video input 2. Therefore, the DefaultSource setting for presentation will always be 2, and this setting cannot be changed. However, a Cisco Webex Room Kit Pro has several video input ports, so this setting would be configurable from the web interface.

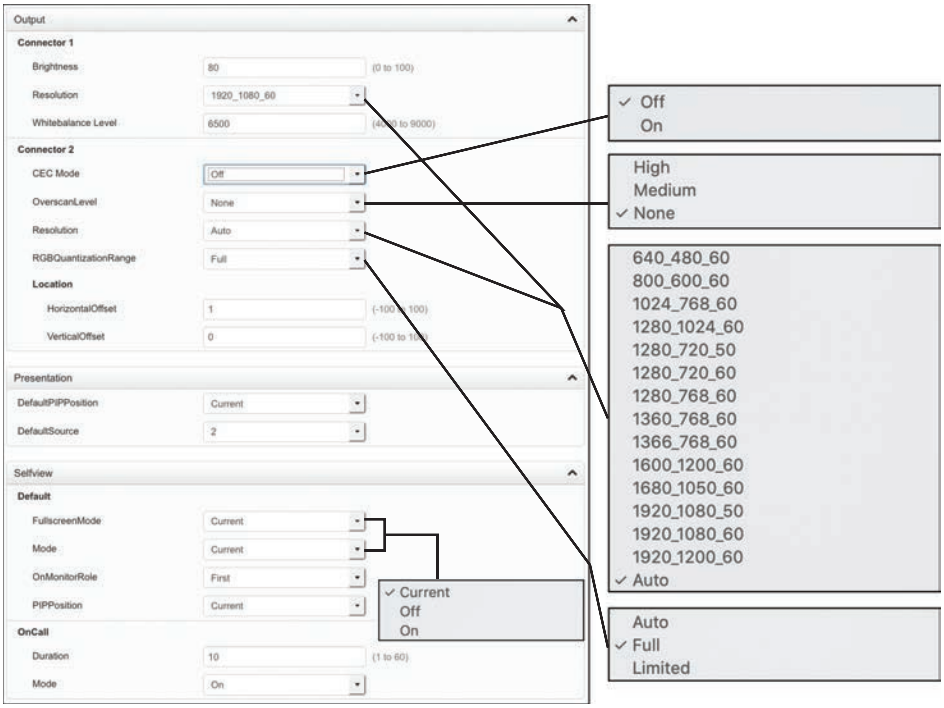
The Selfview section pertains to how the self-view window will appear when this feature is enabled. Self-view can be enabled, disabled, and positioned from the user interface, but the more advanced settings must be configured from the web interface or the CLI. The two subsections in the Selfview section are called Default and OnCall. The Default subsection contains the following parameters:

- **FullScreenMode:** This setting defines whether self-view should be shown in full-screen or as a small PIP after a call. The setting takes effect only when self-view is switched on.
- **Off:** Self-view will be shown as a PiP.
    - **Current:** The size of the self-view picture will be kept unchanged when leaving a call; that is, if it was a PiP during the call, it will remain a PiP after the call; if it was full-screen during the call, it will remain full-screen after the call.
    - **On:** The self-view picture will be shown in full-screen.
- **Mode:** This setting defines whether self-view should be displayed onscreen after a call. The position and size of the self-view window are determined by the **Video > Selfview > Default > PIPPosition** and the **Video > Selfview > Default > FullscreenMode** settings, respectively.
- **Off:** Self-view is switched off when leaving a call.
    - **Current:** Self-view is left as is; that is, if it was on during the call, it will remain on after the call; if it was off during the call, it will remain off after the call.
    - **On:** Self-view is switched on when leaving a call.
- **OnMonitorRole:** This setting defines which screen output to display the main video source for self-view after a call. The value reflects the monitor roles set for the different outputs in the **Video > Output > Connector > [n] > MonitorRole** setting. The setting applies both when self-view is displayed in full-screen, and when it is displayed as a PIP.
- **Current:** When leaving a call, the self-view picture will be retained on the same output as it was during the call.
    - **First:** The self-view picture will be shown on outputs with the **Video > Output > Connector > [n] > MonitorRole** set to First.

- **Second:** The self-view picture will be shown on outputs with the **Video > Output > Connector > [n] > MonitorRole** set to Second.
- **Third:** The self-view picture will be shown on outputs with the **Video > Output > Connector > [n] > MonitorRole** set to Third.

- **PIPPosition:** This setting defines the position onscreen of the small self-view PIP after a call. The setting takes effect only when self-view is switched on and full-screen view is switched off. All of the configuration options are the same as the ActiveSpeaker DefaultPIPPosition options, except that this setting pertains specifically and exclusively to self-view.

The OnCall subsection contains two parameters: Duration and Mode. **OnCall > Mode** is used to switch on self-view for a short while when setting up a call. The **Video > Selfview > OnCall > Duration** setting determines how long self-view will remain on at the beginning of a call. This setting applies when self-view in general is switched off. Duration defaults to 10 and can be set to any value between 1 and 60. Each numeric value represents one second. If Mode is set to On, then self-view will show momentarily at the beginning of a call. If Mode is set to Off, then self-view will not show at all during any point of the call. Figure 10-12 illustrates the video output settings, presentation settings, and selfview settings on a Cisco Telepresence endpoint.



Output

Connector 1

Brightness 80 (0 to 100)

Resolution 1920_1080_60

Whitebalance Level 6500 (4000 to 9000)

Connector 2

CEC Mode Off

OverscanLevel None

Resolution Auto

RGBQuantizationRange Full

Location

HorizontalOffset 1 (-100 to 100)

VerticalOffset 0 (-100 to 100)

Presentation

DefaultPIPPosition Current

DefaultSource 2

Selfview

Default

FullscreenMode Current

Mode Current

OnMonitorRole First

PIPPosition Current

OnCall

Duration 10 (1 to 60)

Mode On

Figure 10-12 *Output, Presentation, and Selfview Video Menu Sections*

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 10-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 10-2 Key Topics for Chapter 10

Key Topic Element	Description	Page Number
List	Three Ways to Place or Answer a Call on CE Endpoint	237
Paragraph	Three Control Mechanisms for CE Endpoints	238
Paragraph	Calling from CE Endpoint Using the On-Screen Display (OSD)	239
Paragraph	Reasons for Dialing from Web Interface or CLI	240
Paragraph	Three Types of Directories	241
Paragraph	Two Systems That Deliver Corporate Directories	242
Paragraph	Define Multipoint, Multisite, and Multiway	243
Paragraph	Explain CMS as the On-Premises Conferencing Solution	244
Paragraph	Explain Webex Meeting Center as the Cloud-Based Conferencing Solution	244
Paragraph	Explain VMN as the Hybrid Conferencing Solution	245
Paragraph	Call Connections Through Scheduled Multipoint Meetings	245
Paragraph	OBTP	246
Paragraph	Define VNC	246
Paragraph	How to Share Content while in a Call	247
Paragraph	How to Share Content Using Proximity App	247
Section	Encryption Mode	250
Paragraph	AutoAnswer Best Practices	251
Paragraph	Explain FECC	251
Paragraph	Corporate Directory Settings Explained	252
List	Active Speaker DefaultPIPPosition Settings	254
List	Five Layouts Supported by Multisite	254

Define Key Terms

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

Ad Hoc, BFCP, CEC, CLI, CMS, Corporate Directory, DN, DuoVideo, E.164 Alias, FECC, Global Directory, H.224, H.239, Local Directory, Multipoint, Multisite, Multiway, People+Content, PIP, PMP, Precision Camera, PTZ, Rendezvous Conferencing, RGBQuantizationRange, SMP, T.150, TMS, URI, VNC

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the five control mechanisms that allow users and administrators to interact with Cisco CE software-based endpoints.
2. List five devices that can be used as a content resource on Cisco CE software-based endpoints.
3. What are the four Type options for a phonebook source on the Cisco Telepresence endpoint?
4. List and describe the five multisite layouts supported on the Cisco Telepresence endpoint.

This page intentionally left blank

CHAPTER 11

Maintaining Cisco Endpoints

This chapter covers the following topics:

Upgrading Endpoints: This topic will discuss how to upgrade endpoints through the endpoint web interface, the Cisco Unified Communications Manager, and the Cisco TMS.

Backup and Restore CE Software-Based Endpoints: This topic will discuss how to perform a backup and restore on the Cisco Telepresence endpoints manually from the endpoint itself or through the Cisco TMS.

Throughout Part II of this book, with regard to Cisco Telepresence endpoints, we have covered everything from product portfolios to registering endpoints and configuring other feature settings unique to Cisco's premium endpoint products. This final chapter on Cisco endpoints will discuss the various maintenance tasks that need to be performed on all endpoints at some point in their lifecycle. Topics discussed in this chapter include the following:

- **Upgrading Endpoints:**
  - Upgrading Through the Cisco Unified Communications Manager
  - Upgrading CE Software-Based Endpoints Manually
  - Upgrading CE Software-Based Endpoints Through TMS
- **Backup and Restore CE Software-Based Endpoints:**
  - Manual Backup and Restore
  - Backup and Restore Through Cisco 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 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
Upgrading Endpoints	1–5
Backup and Restore CE Software-Based Endpoints	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. Which of the following format styles should upgrade software be in for CUCM endpoint upgrades?
   - **a.** .pkg
   - **b.** .iso
   - **c.** cop.sgn
   - **d.** .ova
2. What service on the CUCM must be restarted after software is uploaded, before endpoints can be upgraded?
   - **a.** TFTP
   - **b.** Call Manager
   - **c.** AXL
   - **d.** Phone Load
3. Which of the following format styles should upgrade software be in for manual endpoint upgrades?
   - **a.** .pkg
   - **b.** .iso
   - **c.** cop.sgn
   - **d.** .ova
4. When you are upgrading a Cisco SX80 endpoint, how many times will the endpoint reboot?
   - **a.** None
   - **b.** Once
   - **c.** Twice
   - **d.** Thrice
5. Which of the following is an advantage using TMS to upgrade endpoints over the CUCM?
   - **a.** TMS can upgrade all devices at once, but CUCM can upgrade only one endpoint at a time.
   - **b.** TMS can upgrade Unified IP phones and Telepresence endpoints, but the CUCM can only upgrade Telepresence endpoints.
   - **c.** There are no advantages to using TMS over CUCM for endpoint upgrades.
   - **d.** TMS can schedule when upgrades should occur, but the CUCM cannot schedule upgrades.

6. Which of the following options can be backed up on a CE software-based endpoint from the web interface backup tool?
   - a. Branding
   - b. Favorites
   - c. In-Room Controls
   - d. All of these answers are correct.
   - e. None of these answers are correct.
7. Which of the following statements is true?
   - a. TMS can be used to schedule endpoint Backup and Restore.
   - b. TMS can be used to schedule endpoint Backup only.
   - c. TMS can be used to schedule endpoint Restore only.
   - d. Neither Backup nor Restore can be scheduled through TMS.

Foundation Topics

Upgrading Endpoints

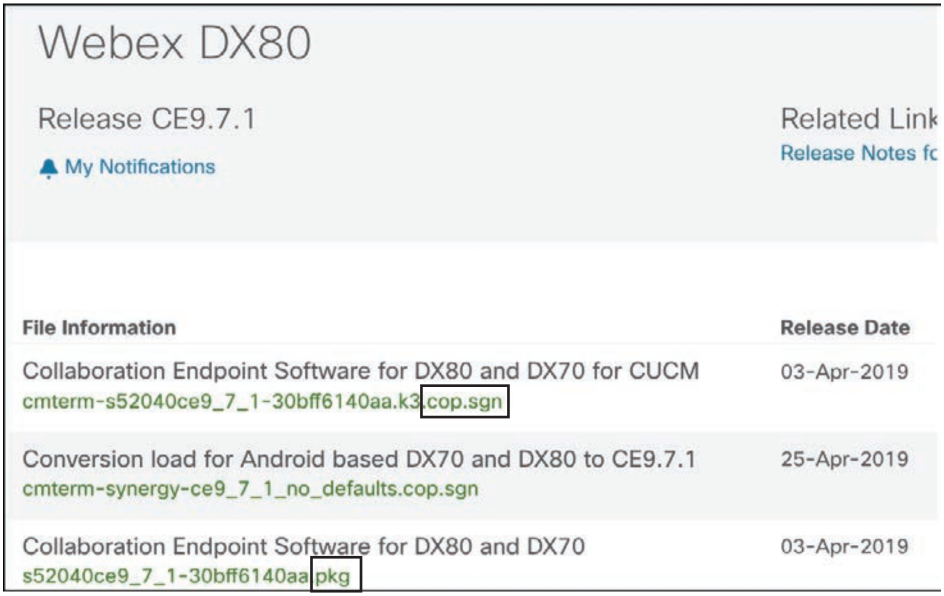
Cisco is continuously improving the quality of the user experience by creating new features and enhancing the capabilities of existing products. Therefore, it is essential for businesses to maintain service contracts on their investments so that equipment can be upgraded as newer versions come out. Newer software versions lead to new features and capabilities, which lead to better user experiences. There are three means through which endpoints can be upgraded within a Cisco environment. You can upgrade Cisco Unified IP phones and Cisco Telepresence endpoints through the Cisco Unified Communications Manager. Cisco Telepresence endpoints can also be manually upgraded on the endpoint itself, or upgrades can be pushed through Cisco Telepresence Management Suite (TMS).

Upgrading Through the Cisco Unified Communications Manager

Upgrading endpoints though the Cisco Unified Communications Manager is not a difficult process, but an administrator must perform many steps before upgrades can occur. Also, some network considerations must be taken into account as well before undertaking an enterprise-wide endpoint upgrade.

Key Topic

When a new upgrade load is released by Cisco, an administrator will need to download an appropriate copy of the firmware from the software.cisco.com website. With Cisco Telepresence endpoints, two image files will be released at the same time. The file ending in cop.sgn is the software load needed for Cisco Unified Communications Manager upgrades. The file ending in pkg is the software load needed for a manual upgrade or TMS upgrade. If a DX endpoint is still running the Android firmware, and an administrator wants to upgrade the endpoint to CE9.10, a conversion file is required, which can be downloaded from the Cisco website. There is also a SIP-only version of the firmware now available for download. Figure 11-1 illustrates the two software loads that can be downloaded from software.cisco.com.



Webex DX80

Release CE9.7.1

My Notifications

Related Link

Release Notes fc

File Information	Release Date
Collaboration Endpoint Software for DX80 and DX70 for CUCM cmterm-s52040ce9_7_1-30bff6140aa.k3.cop.sgn	03-Apr-2019
Conversion load for Android based DX70 and DX80 to CE9.7.1 cmterm-synergy-ce9_7_1_no_defaults.cop.sgn	25-Apr-2019
Collaboration Endpoint Software for DX80 and DX70 s52040ce9_7_1-30bff6140aa.pkg	03-Apr-2019

Figure 11-1 *Software Loads for Upgrading a Cisco DX80*

Once the cop.sgn file has been downloaded, it will need to be uploaded to the Cisco Unified Communications Manager. If the cop.sgn file has been burned to a disc, and the Cisco Unified Communications Manager is running on a server with an optical drive, the administrator can very easily upload the firmware load into the database store on the Cisco Unified Communications Manager. However, if the hosting server does not have an optical dive, or the administrator is remote from the server, an FTP server will need to be used to upload the cop.sgn file into the Cisco Unified Communications Manager. For either method, the administrator will need to complete the following steps to upload the file into the Cisco Unified Communications Manager:

Key Topic

Step 1. Navigate to the Cisco Unified OS Administration interface and log in with the appropriate username and password.

Step 2. Once logged in, navigate to the Software Upgrades > Install/Upgrade menu.

Step 3. If the cop.sgn file has been burned to a disc, leave the Source setting as **DVD/CD** and click **Next**. If an FTP server is needed, change the Source setting to **Remote Filesystem** and enter the following information:

- **a.** **Directory:** For remote file systems, enter the path to the patch file on the remote system.
- **b.** **Server:** For remote file systems, enter the FTP or SFTP server name.
- **c.** **User Name:** Enter the username for the remote node.
- **d.** **User Password:** Enter the password for the remote node.
- **e.** **Transfer Protocol:** Enter the transfer protocol (FTP or SFTP).

f. **SMTP Server:** Enter the IP address of your SMTP server. You will receive an email notification upon successful completion of the upgrade.

g. **Email Destination:** Enter your email address along with the SMTP server above. You will receive an email notification upon successful completion of the upgrade.

The last two fields, SMTP Server and Email Destination, are not required. When many cop.sgn files are being uploaded at the same time, this process could take a long time. These email notification settings exist only for the convenience of the administrator, to eliminate the need for watching and waiting for the process to complete.

Step 4. After all the appropriate fields have been completed, click **Next** and the Cisco Unified Communications Manager will begin communicating with the FTP server to upload the files.

Once the upload is complete, the TFTP service must be restarted. Phones will not be able to register while this service is being restarted; however, the entire restart process should not take more than two minutes to complete. If the TFTP service is running on more than one server, it will have to be started on both servers, but the administrator can stagger the restart intervals so that loss of service is not experienced. Follow these steps to restart the TFTP service on the Cisco Unified Communications Manager:

Step 1. In the Navigation window located in the top-right corner of the Cisco Unified Communications Manager Web interface screen, change the selection to **Cisco Unified Serviceability** and then click **Go**.

Step 2. Enter the appropriate username and password, and then click **Login**.

Step 3. Navigate to **Tools > Control Center – Feature Services**, and from the drop-down list, select the Cisco Unified Communications Manager that the TFTP Service is running on. Click **Go** when finished.

Step 4. Locate the Cisco TFTP service at the bottom of the CM Services section and select the radio button beside it.

Step 5. At the top or bottom of the screen, select the **Restart** button, and wait for the service to show a Status of Started and an Activation Status of Activated. You may need to refresh the page a few times while waiting for the service to restart.

When you reach this point, the software loads are uploaded into the Cisco Unified Communications Manager database, and the TFTP service is restarted so that the software loads are available for use. However, the upgrade does not occur automatically. The administrator will need to change the firmware load requirements for the endpoints. There are two ways an administrator can upgrade an endpoint. The following steps outline how to perform a bulk upgrade of all the endpoints within a specific product line:

Step 1. In the Navigation window located in the top-right corner of the Cisco Unified Communications Manager Web interface screen, change the selection to **Cisco**

Unified CM Administration, and then click **Go**. The same login credentials are used for Cisco Unified Serviceability and Unified CM Administration.

Step 2. Navigate to **Device > Device Settings > Device Defaults**.

Step 3. Scroll down to the Device Type that needs to be upgraded, and in the Load Information column, which is the third column from the right, enter the software load name. For example, if the cop.sgn file name was cterm-s52040ce9_7_1-30bff6140aa.k3.cop.sgn, then the software load name would be s52040ce9_7_1-30bff6140aa.k3.

Step 4. Click **Save** when finished.

There is a fundamental issue that could occur if a bulk upgrade were implemented, as previously mentioned. Depending on how many endpoints are actually being upgraded, this type of bulk upgrade could cause some network congestion issues because these upgrade files being forwarded are very large, and they are being sent out to a lot of devices across the network. A bulk upgrade can also overwhelm the TFTP server because it can handle only so many connections simultaneously. Performing these upgrades after regular office hours will help limit some of these issues. There is also an alternative way of upgrading endpoints that can overcome these obstacles by performing a staged upgrade of endpoints at different intervals in time. The steps an administrator would need to perform if one endpoint were being upgraded at a time are as follows:

Key Topic

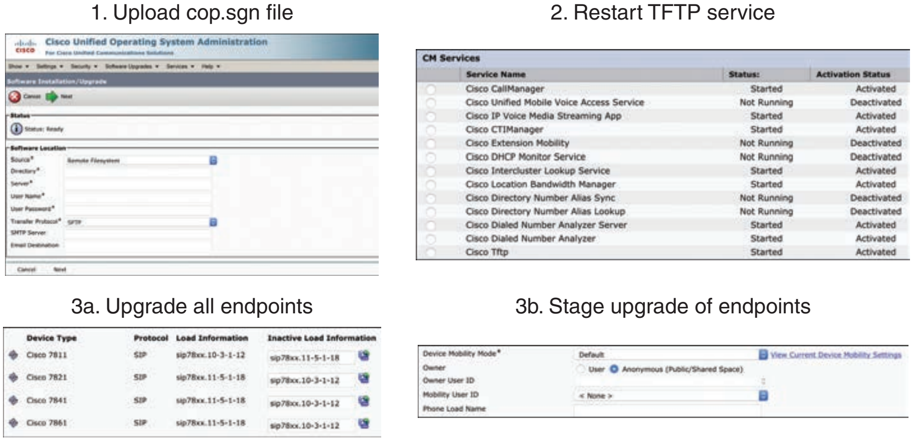
Step 1. While still logged in under Cisco Unified CM Administration, navigate to **Device > Phone**.

Step 2. Click **Find**, and then click a phone that will need to be upgraded.

Step 3. In the Device Information section, locate the Phone Load Name field.

Step 4. Enter the phone load name, and then click **Save**, followed by **Apply Config**. After about a minute, you will see the phone reboot, and the upgrade will occur.

Once the phone finishes rebooting, the upgrade is complete, and the user can begin using the new features on the phone. Obviously, an administrator would not want to upgrade a lot of phones one at a time. The purpose of illustrating these steps is to demonstrate the field that exists to upgrade an individual phone. This field can be populated in a CSV file and used through the Bulk Administration Tool (BAT) to deploy this setting on multiple phones. In this manner, the administrator can exercise much more control over what phones or endpoints upgrade at specific times. Chapter 17, "Registering SIP Endpoints to the Cisco Unified Communications Manager," will further discuss how to use BAT in a Cisco environment.
As you can see from the preceding steps, upgrading endpoints through the Cisco Unified Communications Manager is not a difficult process, but many steps are involved with setting up the environment before the upgrades can be performed. Figure 11-2 illustrates the upgrade process through the Cisco Unified Communications Manager.



1. Upload cop.sgn file

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾
Software Installation/Upgrade
Cancel
Next

Status

Status: Ready

Software Location

Source*	Remote Filesystem
Directory*	
Server*	
User Name*	
User Password*	
Transfer Protocol*	SFTP
SMTP Server	
Email Destination	

2. Restart TFTP service

CM Services

	Service Name	Status:	Activation Status
○	Cisco CallManager	Started	Activated
○	Cisco Unified Mobile Voice Access Service	Not Running	Deactivated
○	Cisco IP Voice Media Streaming App	Started	Activated
○	Cisco CTIManager	Started	Activated
○	Cisco Extension Mobility	Not Running	Deactivated
○	Cisco DHCP Monitor Service	Not Running	Deactivated
○	Cisco Intercluster Lookup Service	Started	Activated
○	Cisco Location Bandwidth Manager	Started	Activated
○	Cisco Directory Number Alias Sync	Not Running	Deactivated
○	Cisco Directory Number Alias Lookup	Not Running	Deactivated
○	Cisco Dialed Number Analyzer Server	Started	Activated
○	Cisco Dialed Number Analyzer	Started	Activated
○	Cisco Tftp	Started	Activated

3a. Upgrade all endpoints

Device Type	Protocol	Load Information	Inactive Load Information
Cisco 7811	SIP	sip78xx.10-3-1-12	sip78xx.11-5-1-18
Cisco 7821	SIP	sip78xx.11-5-1-18	sip78xx.10-3-1-12
Cisco 7841	SIP	sip78xx.11-5-1-18	sip78xx.10-3-1-12
Cisco 7861	SIP	sip78xx.11-5-1-18	sip78xx.10-3-1-12

3b. Stage upgrade of endpoints

Device Mobility Mode*	Default
Owner	○ User ● Anonymous (Public/Shared Space)
Owner User ID	
Mobility User ID	< None >
Phone Load Name	

Figure 11-2 *CUCM Upgrade Process*

Upgrading CE Software-Based Endpoints Manually

Cisco Unified IP phones cannot be upgraded manually, and they cannot be upgraded through TMS, so from this point forward the focus will be on Cisco Telepresence endpoints. As mentioned in the previous section, when the administrator downloads the software loads from the software.cisco.com website, two image files for each version will be released at the same time. The file ending in cop.sgn is the software load needed for Cisco Unified Communications Manager upgrades. The file ending in pkg is the software load needed for manual upgrade or TMS upgrade. If you are planning to manually upgrade your Cisco CE software-based endpoint, or if you're planning to use TMS to upgrade the endpoint, be sure to download the software file ending in pkg, and then follow these steps:

Key Topic

Step 1. Using a web browser, navigate to the web interface of the endpoint, and log in with the appropriate username and password.

Step 2. Navigate to **Maintenance > Software Upgrade**.

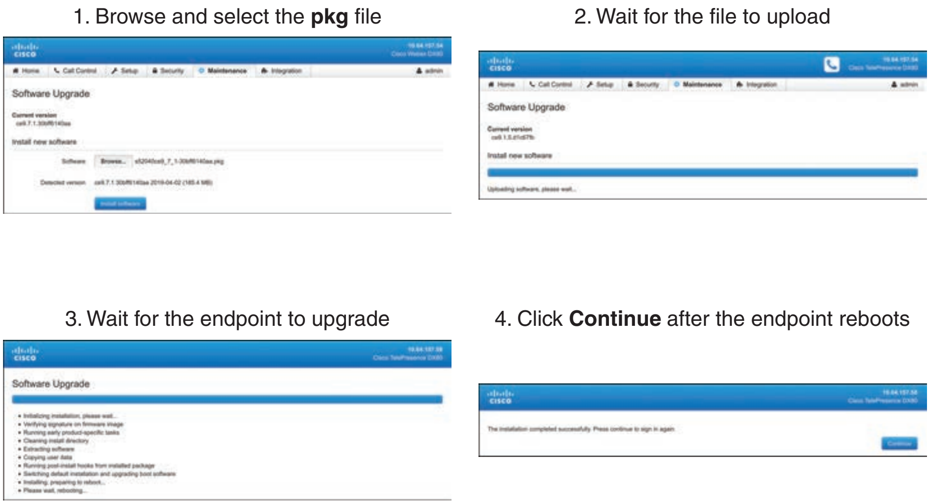
Step 3. Click the **Browse** button and select the pkg file that was previously downloaded, and then click **Open**.

Step 4. The detected version of the software load should appear on the screen. After confirming the version is correct, click the blue **Install Software** button.

Step 5. The software will upload to the endpoint. This part of the process could take a several minutes. Once the upload process is complete, the upgrade will automatically initialize.

Step 6. This process will take several more minutes to complete. Once the upgrade has completed, the endpoint will reboot.

Some of the endpoints use cameras that need a software upgrade as well. The camera software is included with the endpoint upgrade file. In these instances, the endpoint will reboot twice—once after the endpoint upgrades and a second time after the camera upgrades. Figure 11-3 illustrates the manual endpoint upgrade process on a Cisco DX80 endpoint.



1. Browse and select the **pkg** file

Software Upgrade

Current version
ce9.7.1.30bff6140aa

Install new software

Software: Browse... s52040ce9_7_1-30bff6140aa.pkg

Detected version: ce9.7.1.30bff6140aa 2019-04-02 (185.4 MB)

2. Wait for the file to upload

Software Upgrade

Current version
ce9.1.5.d1c67b

Install new software

Uploading software, please wait...

3. Wait for the endpoint to upgrade

Software Upgrade

- Initializing installation, please wait...
- Verifying signature on firmware image
- Running early product-specific tasks
- Cleaning install directory
- Extracting software
- Copying user data
- Running post-install hooks from installed package
- Switching default installation and upgrading boot software
- Installing, preparing to reboot...
- Please wait, rebooting...

4. Click **Continue** after the endpoint reboots

The installation completed successfully. Press continue to sign in again.

Figure 11-3 *Manual Upgrade Process on Cisco DX80*

Upgrading CE Software-Based Endpoints Through Cisco TMS

Although the manual process of upgrading a Cisco CE software-based endpoint is fairly easy, it could still prove to be very time consuming when an administrator has to upgrade a large number of endpoints. This is why bulk provisioning tools exist, such as the Cisco Unified Communications Manager and Cisco TMS. Before TMS can be used to upgrade endpoints, some administrative tasks must be performed first to prepare the system for the tasks it will perform, similarly to the Cisco Unified Communications Manager. Assuming the pkg file has already been downloaded, the following steps explain how to go into the back end of TMS on the Windows Server and load the software that will be used to upgrade the endpoint. There are two ways to upload the pkg file into TMS. You can use the TMS web interface, but it often does not work well because the file is so big. A faster and more proficient method is to access the folder on the back end where TMS would store the information anyway:

Key Topic

Step 1. Open a Remote Desktop session using the IP address of TMS. This will take you to the Windows Server where TMS is hosted. You will need the Windows Server login credentials to log in to the server.

Step 2. Open a folder and browse to **C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware.**

Step 3. Drag and drop the pkg file into this folder.

Step 4. Close all the windows and log out of the Windows Server.

Now that the upgrade software has been loaded into TMS, this system can be used to upgrade all of the endpoints being managed by TMS. Use the following steps to upgrade endpoints using TMS:

Key Topic

Step 1. Open a browser and log in to TMS.

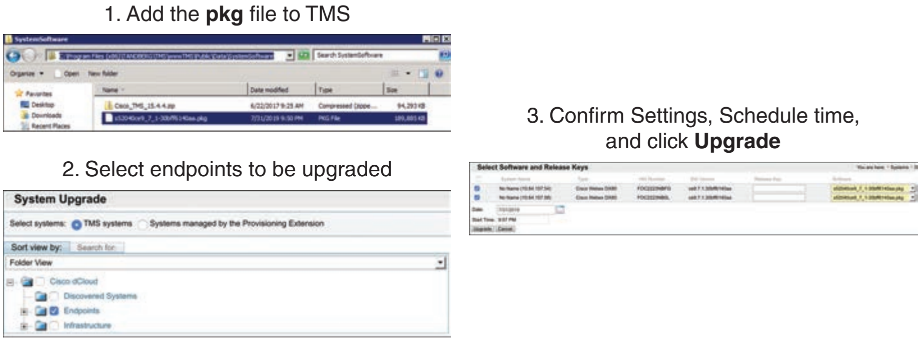
Step 2. Navigate to **System > System Upgrade > System Upgrade.**

Step 3. Select the box beside the folder where the endpoints are located or select the box beside the endpoint itself. In this manner, you can granularly choose what endpoints will be upgraded. At the bottom of the page, click the **Next** button.

Step 4. On the next page that appears, you will see a full list of the endpoints selected. They will be listed with the System Name, Type, HW Number (serial number), and SW Version (current version on the endpoint), and the last Software box identifies the version that will be pushed to the endpoint. Below all the systems listed are Date and Start Time fields. These fields allow you to schedule the upgrade at some point in the future, such as over a weekend or the middle of the night when no one is in the office.

Step 5. After all settings have been configured or verified, click the **Upgrade** button. TMS will ensure all endpoints listed will be upgraded. There is even a way for TMS to send an email confirmation after each system has been upgraded successfully.

TMS is a simpler system for upgrading than the Cisco Unified Communications Manager, but it is more complex than the manual upgrade process. However, both TMS and the Cisco Unified Communications Manager can push upgrades to multiple systems simultaneously. TMS can schedule upgrades while the Cisco Unified Communications Manager cannot. But the Cisco Unified Communications Manager can upgrade Cisco Unified IP phones and Cisco Telepresence endpoints, whereas TMS can only upgrade Telepresence endpoints. So, each method has its merits and drawbacks. It is up to each administrator to decide what method to use for upgrades, and when each will be used. Figure 11-4 illustrates the upgrade process through Cisco TMS.



1. Add the **pkg** file to TMS

SystemSoftware

Name	Date modified	Type	Size
Cisco_TMS_15.4.4.zip	6/22/2017 9:25 AM	Compressed (zippe...	94,293 KB
s52040ce9_7_1-30bff6140aa.pkg	7/31/2019 9:50 PM	PKG File	[illegible]

2. Select endpoints to be upgraded

System Upgrade

Select systems: ● TMS systems ○ Systems managed by the Provisioning Extension

Sort view by: Search for

Folder View

- □ Cisco dCloud
  - □ Discovered Systems
  - ☑ Endpoints
  - □ Infrastructure

3. Confirm Settings, Schedule time, and click **Upgrade**

Select Software and Release Keys

	System Name	Type	HW Number	SW Version	Release Key	Software
☑	No Name ([illegible])	Cisco Webex DX80	[illegible]	ce9.7.1.30bff6140aa		s52040ce9_7_1-30bff6140aa.pkg
☑	No Name ([illegible])	Cisco Webex DX80	[illegible]	ce9.7.1.30bff6140aa		s52040ce9_7_1-30bff6140aa.pkg

Date: 7/31/2019

Start Time: 9:57 PM

Figure 11-4 *Cisco Endpoint Upgrade Process through TMS*

Backing Up and Restoring CE Software-Based Endpoints

Endpoints are used and abused on a daily basis. Sometimes settings get changed, whether by accident or on purpose, causing the endpoint to stop working. Sometimes, parts just wear out and the endpoint needs to be replaced. In either scenario, a backup of the configuration settings will enable the support engineer to resolve the issues and bring the endpoints back online quickly and efficiently.

A backup of the system configurations should be performed on two occasions:

- When a new endpoint is deployed and a working configuration has been configured and tested on the endpoint
- Before an endpoint is upgraded

In this second scenario, the administrator should verify that no settings have been changed and the endpoint is working properly before performing the backup; otherwise, all of the issues misconfigured on the endpoint will be backed up, and that could be very counterproductive.

Once an administrator is prepared to perform a backup on a Cisco CE software-based endpoint, two methods can be executed:

- The administrator can manually perform a backup on the endpoint itself from the web interface or from the CLI.
- The administrator can perform the backup though Cisco TMS.

The advantage to performing a backup through TMS is that all the endpoints TMS is managing can be backed up simultaneously, and the backup data is stored in the TMS SQL database. A backup can be restored in the same manner as previously listed, except a restore through TMS can be scheduled and reoccurring.

Manual Backup and Restore

The administrator does not have to be in the same physical location as a Cisco CE software-based endpoint to be able to perform a manual backup of the endpoint. The administrator only needs to have network connectivity to the endpoint so that the web interface or CLI can be accessed. When these endpoints were first released, the only way to back up the endpoint manually was to use the CLI. When version TC7.x came out, a backup option was added to the web interface. Whichever method you choose to employ to back up the endpoint, both are equally effective and cross compatible.

Because the CLI was the original method of backing up an endpoint, the following instructions will detail how to use the CLI to this end. Different emulators could be used to access the CLI of the endpoint, and how information generated through the CLI is captured would differ. The following instructions are based on the use of PuTTY, which has been discussed previously.

Key Topic

Step 1. Open a PuTTY session and enter the IP address of the endpoint you are trying to access. Then select the radio button beside SSH, but do not select the Open button yet.

Step 2. In the left column, select the **Logging** menu option.

Step 3. From the menu options that appear on the right side of the screen, select the radio button beside **All Session Output**.

Step 4. In the Log File Name field, enter a name for the file you are creating. The name must end in .log and should be descriptive of its purpose, such as ConfA_Backup_3Aug2019.log. Click the **Browse** button to choose the location the file will be saved to.

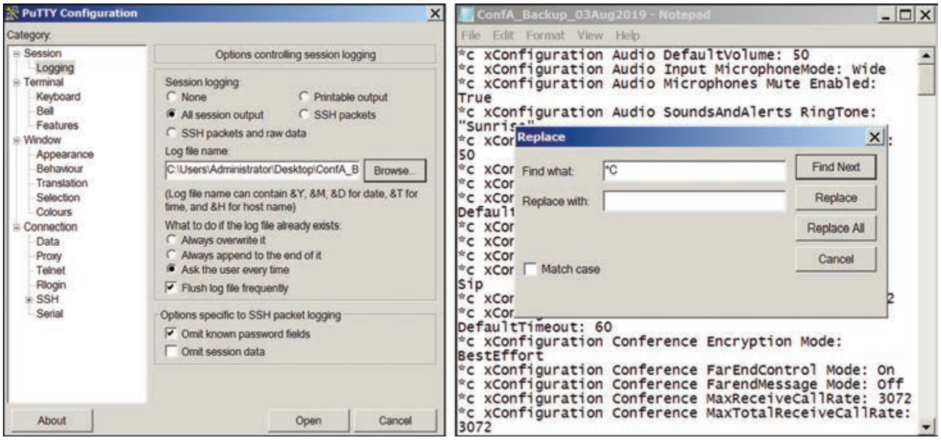
Step 5. Click **Open** to start the CLI session. Log in with the username and password when prompted. Once logged in, enter the command **xConfiguration** and press Enter. The output will be a copy of every configuration setting on this endpoint. Close the PuTTY session when finished.

Step 6. Open the text file you just created. You need to perform some cleanup before the backup will be usable.

- **a.** All of the login information at the top of the document needs to be deleted, down to and including the **xConfiguration** command.
- **b.** Each line will begin with *C followed by a space. This signifies that the line is a copy of the configuration. To remove this, simply perform a Find/Replace and search for ***C<space>**. Leave the Replace With field blank, and then click on **Replace All**.
- **c.** Some trailing information at the bottom of the document also will need to be deleted. Remove all lines that do not begin with **xConfiguration**.

Step 7. After all the cleanup has been completed, save the changes to the document, and the backup is complete.

This process for backing up an endpoint is not difficult, as you can see, but several steps must be completed to perform the backup, which makes this method a bit cumbersome. However, once the backup is made, performing a restore is quite simple. Open a new CLI session to the endpoint and log in. Copy the data from the backup document and paste it in the CLI session. To paste in PuTTY, you only need to right-click in the window. Now the restore is complete. A nice advantage to using the CLI to perform a restore is that you can choose what information will be configured on the endpoint. Copy and paste only the commands you want to use. You can even manipulate the data before pasting it into the CLI session. Figure 11-5 illustrates the manual backup method using the CLI.



Options controlling session logging

Session logging:
○ None ○ Printable output
● All session output ○ SSH packets
○ SSH packets and raw data

Log file name: C:\Users\Administrator\Desktop\ConfA_B

(Log file name can contain &Y, &M, &D for date, &T for time, and &H for host name)

What to do if the log file already exists:
○ Always overwrite it
○ Always append to the end of it
● Ask the user every time
☑ Flush log file frequently

Options specific to SSH packet logging
☑ Omit known password fields
□ Omit session data

```
*c xConfiguration Audio DefaultVolume: 50
*c xConfiguration Audio Input MicrophoneMode: Wide
*c xConfiguration Audio Microphones Mute Enabled:
True
*c xConfiguration Audio SoundsAndAlerts RingTone:
"Sunris
*c xCor
50
*c xCor
*c xCor
*c xCor
Defaul
*c xCor
*c xCor
*c xCor
*c xCor
Sip
*c xCor
*c xCor
DefaultTimeout: 60
*c xConfiguration Conference Encryption Mode:
BestEffort
*c xConfiguration Conference FarEndControl Mode: On
*c xConfiguration Conference FarendMessage Mode: Off
*c xConfiguration Conference MaxReceiveCallRate: 3072
*c xConfiguration Conference MaxTotalReceiveCallRate:
3072
```

Find what: *C
Replace with:
□ Match case

Figure 11-5 *Manual Backup Method Using the CLI*

A much easier method of backing up an endpoint manually is to use the web interface. Backup files taken through the web interface are in a similar plaintext format as the CLI-based backup. These files can be opened, and the data can be manipulated in a similar fashion as previously described. The following steps explain how to make a backup of a CE software-based endpoint using the web interface:

Key Topic

Step 1. Open a web browser and navigate to the web interface of the endpoint. Log in with the appropriate username and password.

Step 2. Once logged in, navigate to **Maintenance > Backup and Restore**.

Step 3. Under the Create Backup tab, you can choose what elements of the endpoint need to be backed up. If any of these elements are not installed or configured on the endpoint, they will not be selectable from this menu. Options that can be backed up include the following:

   a. Branding

   b. Favorites

   c. In-Room Control

   d. Macros

   e. Sign In Banner

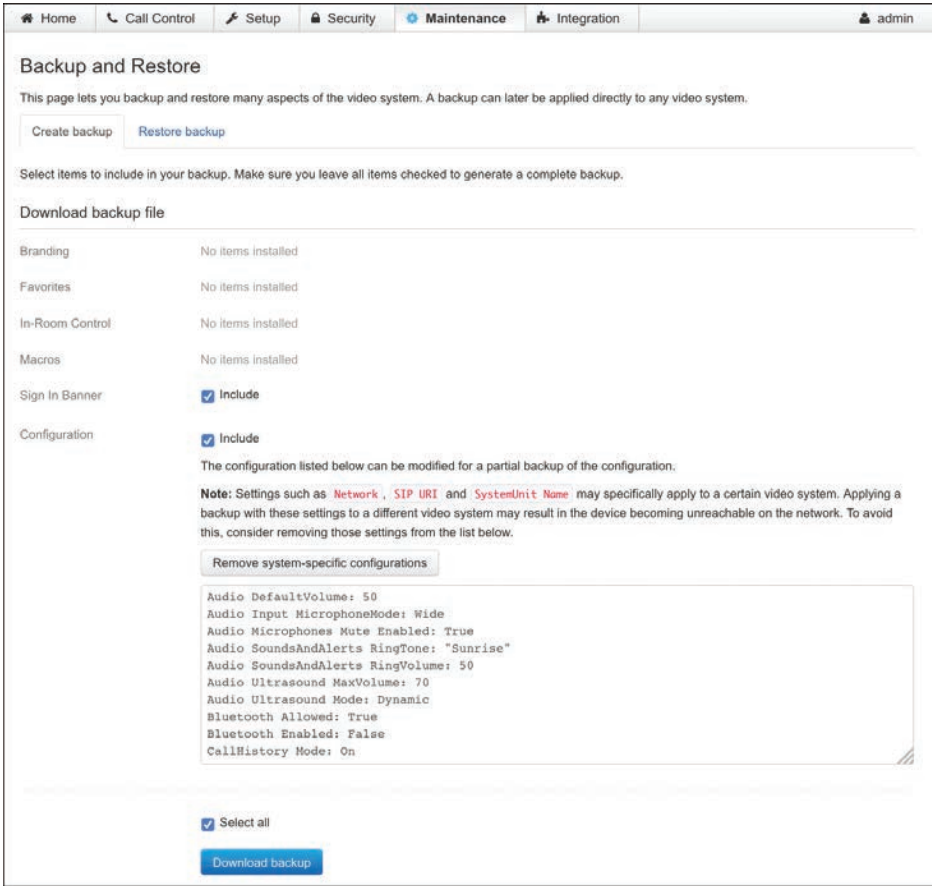
   f. Configuration

Step 4. Scroll down toward the bottom of the screen and find the configuration window. This list allows you to modify the information that will be backed up so that a partial backup can be taken from the system.

Step 5. Once all fields have been configured, click the **Download Backup** button at the bottom of the page.

Step 6. A popup window will appear asking if you want to open or save the backup. Choose **Save File** and click **OK**. Once the file finishes downloading on your computer, the backup is complete.

If you were to unzip the file and observe the data that was saved, it would look just like the CLI backup file, except that the **xConfiguration** command is missing. To perform a restore using the web interface is also quite simple. From the Backup and Restore page, click the **Restore Backup** tab. Click the **Browse** button and select the file you wish to restore. You can use either the zip file saved from the backup using the web interface or the .log file from the CLI backup. After you select the file, click **Open** and then click the **Upload File** button. Now the restore is complete. Figure 11-6 illustrates how to make a manual backup of the endpoint using the web interface.



Backup and Restore

This page lets you backup and restore many aspects of the video system. A backup can later be applied directly to any video system.

Select items to include in your backup. Make sure you leave all items checked to generate a complete backup.

Download backup file

Branding	No items installed
Favorites	No items installed
In-Room Control	No items installed
Macros	No items installed
Sign In Banner	☑ Include
Configuration	☑ Include

The configuration listed below can be modified for a partial backup of the configuration.

Note: Settings such as `Network`, `SIP URI` and `SystemUnit Name` may specifically apply to a certain video system. Applying a backup with these settings to a different video system may result in the device becoming unreachable on the network. To avoid this, consider removing those settings from the list below.

```
Audio DefaultVolume: 50
Audio Input MicrophoneMode: Wide
Audio Microphones Mute Enabled: True
Audio SoundsAndAlerts RingTone: "Sunrise"
Audio SoundsAndAlerts RingVolume: 50
Audio Ultrasound MaxVolume: 70
Audio Ultrasound Mode: Dynamic
Bluetooth Allowed: True
Bluetooth Enabled: False
CallHistory Mode: On
```

☑ Select all

Figure 11-6 *Manual Backup Method Using the Web Interface*

Backup and Restore Through Cisco TMS

There are some nice advantages to manually backing up and restoring Cisco Telepresence endpoints. Administrators can control the data being backed up and restored much more granularly. The backed-up data can be manipulated before it is pushed back out to the endpoint. The disadvantages could include the fact that backup files may not be saved at the same location. If a backup is needed for a restore and the file cannot be found, it is as bad as not having a backup at all. Also, data has to be manually backed up and restored on each individual endpoint. This is a huge time waster for the administrator, time that can be better used elsewhere. For these reasons, an administrator may opt to use Cisco TMS as the backup agent for the enterprise collaboration environment. The following steps explain how to configure a backup of Cisco Telepresence endpoints using Cisco TMS:

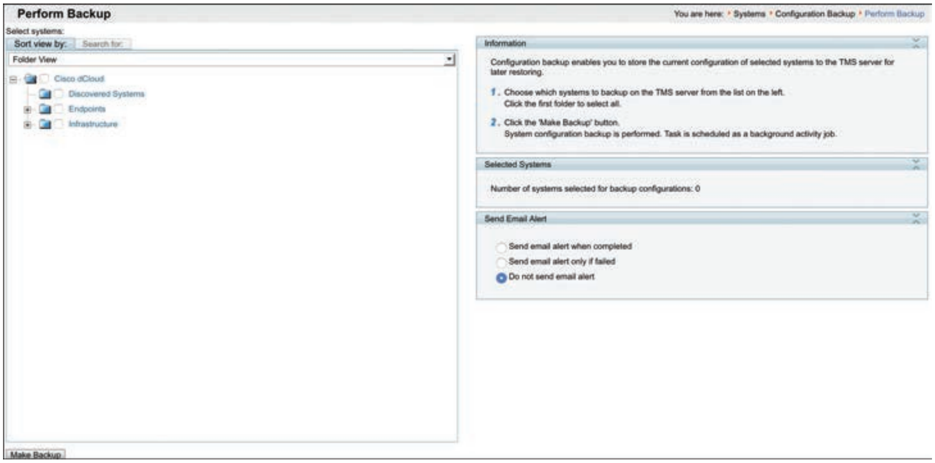
Key Topic

Step 1. Open a web browser and navigate to TMS. Sign in with the appropriate username and password.

Step 2. Once logged in, navigate to **Systems > Configuration Backup > Perform Backup.**

Step 3. Select the box beside the folders or endpoints that you want to back up, and then click the **Make Backup** button at the bottom of the screen.

That is all there is to making a backup of your endpoints through TMS. Three steps and all of your Cisco Telepresence endpoints are backed up. The backup data is saved and organized all in one place on the back-end SQL database for TMS. When a restore is initiated through TMS, TMS will collect that data and push it out to the endpoint. A lot of people have inquired in the past if TMS allows backups to be scheduled. The answer to that question is no, and why would you want to schedule a backup? If someone changes the settings on an endpoint and the endpoint stops working as a result, if a backup were scheduled, the misconfiguration would be backed up. This would defeat the purpose of performing a backup in the first place. For this reason, the administrator should always make sure the endpoint is configured correctly and is running properly before backing up the data. Figure 11-7 illustrates how to perform a backup from Cisco TMS.



Configuration backup enables you to store the current configuration of selected systems to the TMS server for later restoring.

1. Choose which systems to backup on the TMS server from the list on the left.
   Click the first folder to select all.
2. Click the 'Make Backup' button.
   System configuration backup is performed. Task is scheduled as a background activity job.

Number of systems selected for backup configurations: 0

○ Send email alert when completed
○ Send email alert only if failed
● Do not send email alert

Figure 11-7 *Backup from Cisco TMS*

By contrast, the administrator can schedule a restore of the configuration backup, and this makes a lot more sense. Because the endpoints are always prone to misconfiguration, when regular restorations of the configuration are scheduled, the endpoint will be continuously returned to a state of good working condition. The following steps explain how to use TMS to restore a backup to a Cisco Telepresence endpoint:

Key Topic

Step 1. From the web interface of Cisco TMS, navigate to **Systems > Configuration Backup > Perform Restore.**

Step 2. Select the box beside the folders or endpoints that you want to restore.

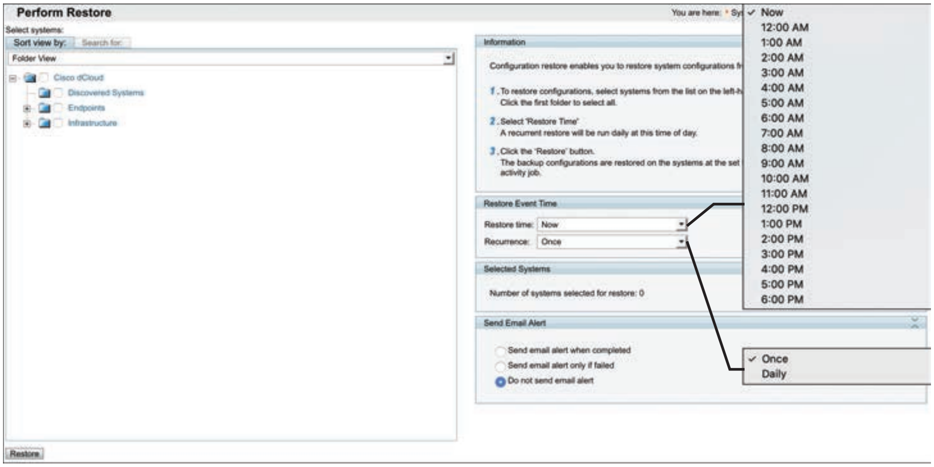
Step 3. If you want to restore the backup settings only this one time, click the **Restore** button at the bottom of the screen.

Step 4. If you want to restore the backup settings at a reoccurring schedule, use the Restore Event Time section on the right side of the screen to set up a schedule before selecting the **Restore** button.

a. The **Restore Time** drop-down menu allows you to set the time of day the restoration will occur. The default value is Now.

b. The **Recurrence** drop-down menu allows you to set the recurrence of the restore to Once or Daily. The default value is Once.

TMS also can send an email notification when a Restore event is successfully completed or if the restore event fails. Figure 11-8 illustrates how to perform a restore from TMS.



Configuration restore enables you to restore system configurations fr

1. To restore configurations, select systems from the list on the left-h
Click the first folder to select all.

2. Select 'Restore Time'
A recurrent restore will be run daily at this time of day.

3. Click the 'Restore' button.
The backup configurations are restored on the systems at the set
activity job.

Restore time: Now

Recurrence: Once

Number of systems selected for restore: 0

○ Send email alert when completed
○ Send email alert only if failed
● Do not send email alert

Figure 11-8 *Restore from 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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 11-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 11-2 Key Topics for Chapter 11

Key Topic Element	Description	Page Number
Paragraph	Two Image Files for Upgrading Endpoints	264
Steps	Uploading Image Files into the CUCM	265
Steps	Restarting TFTP Service on CUCM	266
Steps	Bulk Upgrade of Endpoints from CUCM	266
Steps	Controlled Upgrade of Endpoints from CUCM	267
Steps	Manual Upgrade of Endpoints	268
Steps	Upload Image Files into TMS	269

Key Topic Element	Description	Page Number
Steps	Upgrading Endpoints Using TMS	269
Steps	Manual Backup Using CLI	271
Steps	Manual Backup Using Web Interface	273
Steps	Backup Using TMS	274
Steps	Restore Using TMS	275

Define Key Terms

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

CSV, FTP, TFTP

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What are the three main steps to upgrading endpoints through the CUCM?
2. List the steps for manually upgrading a Cisco CE software-based endpoint.
3. What are the two ways a software file can be uploaded to TMS?
4. List three ways an endpoint can be backed up.

This part covers the following topics:

- **Chapter 12, Cisco Core Network Components:** This chapter will introduce the LAN, WAN, and wireless LAN network components and IOS gateways as they pertain to collaboration.
- **Chapter 13, Layer 2 and Layer 3 QoS Parameters:** This chapter will discuss QoS-related issues, QoS requirements, class models for provisioning QoS, DiffServ values, QoS Trust boundaries, and how to configure and verify LLQ.
- **Chapter 14, DNS, NTP, and SNMP:** This chapter will examine DNS settings, NTP settings, and SNMP settings within a network as they pertain to collaboration.

Part III

Network Requirements for Collaboration Deployments

CHAPTER 12

Cisco Core Network Components

This chapter covers the following topics:

LAN, WAN, and Wireless LAN: This topic will discuss the various layers of an enterprise network to cover the LAN, WAN, and wireless LAN as they relate to collaboration.

Gateways: This topic will introduce various types of gateways, both old and new, with special emphasis on IOS gateway services through the Cisco ISR routers and the features they support that impact the Cisco collaboration solution.

The network is the most important aspect to any business today because that is what connects people together across the world. In an episode of a funny British sitcom called *The IT Crowd*, the IT department's nontechnical boss was convinced that the "Internet" was a single black box. She was planning to use it as a prop in a presentation she was to present in hopes of wowing the audience. As I hope you are aware, the Internet, or any network for that matter, is not a single device. It is a combination of devices, software, and protocols that are the culmination of years of development by multiple vendors to become what it is today. It is a living entity in that it continues to grow and change as time passes, and it will continue to grow as long as people have a need for it. The vast embodiment of the Cisco core network components is too colossal to cover in one chapter. However, this chapter will introduce many concepts concerning the Cisco core network components as they pertain to collaboration. Topics discussed in this chapter include the following:

- LAN, WAN, and Wireless LAN
  - LAN (Access Layer, Distribution Layer, Core Layer)
  - WAN Aggregation Design
  - Wireless LAN (Basic Configuration and Design, High Availability, Capacity Planning, Design Considerations)
- Gateways
  - ISR, ASR, and IOS Software Comparisons
  - ISR Products Explained

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

1.3 Configure these network components to support Cisco Collaboration solutions

“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 Section	Questions
LAN, WAN, and Wireless LAN	1–6
IOS Gateways	7–10

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 is an element configured on a Layer 2 switch?
   - **a.** VLAN
   - **b.** QoS Policing
   - **c.** EIGRP
   - **d.** OSPF
2. Which of the following does the IEEE 802.1d standard define?
   - **a.** Layer 2 QoS
   - **b.** Spanning Tree Protocol
   - **c.** Rapid Spanning Tree Protocol
   - **d.** Multiple Instance Spanning Tree Protocol
3. Which of the following protocols protects data traffic from a failed router or circuit, while also allowing packet load sharing between a group of redundant routers?
   - **a.** HSRP
   - **b.** ARP
   - **c.** VRRP
   - **d.** GLBP

4. Which of the following is a "best effort" bandwidth option for network connections?
   a. DSL
   b. ATM
   c. Leased Lines
   d. Frame Relay
5. Which of the following is the wireless router to which a device would connect for network access?
   a. WLC
   b. LAN
   c. LWAP
   d. LWAPP
6. What is the recommended cell boundary overlap to provide high availability in a wireless network?
   a. There should not be any cell boundary overlap.
   b. 20 percent
   c. 50 percent
   d. 100 percent
7. Which of the following is an analog station gateway?
   a. E&M
   b. FXO
   c. PRI
   d. FXS
8. Which of the following routers supports the IOS XE software?
   a. ISRv
   b. ISR 800 Series
   c. ISR 2900 Series
   d. ASR 9000 Series
9. Which of the following Cisco routers should an engineer choose for a customer who needs to support 1000 users at a specific location?
   a. ISR 800 Series
   b. ISR 1000 Series
   c. ISR 2900 Series
   d. ISR 4000 Series
10. Which Cisco router should be used for machine-to-machine and device-to-device deployments such as ATMs, point-of-sale kiosks, and vending machines (fixed platform)?
    a. ISR 800M
    b. ISR 810
    c. ISR 860
    d. ISR 890

Foundation Topics

LAN, WAN, and Wireless LAN

The most foundational components of any corporate communication solution are the network infrastructure components. One of the reasons Cisco is the leader in the collaboration market is that only Cisco can offer an end-to-end solution to its customers. Of course, providing superior collaboration products with extensive capabilities and beautiful designs helps contribute to the company's ability to hold that leading position. The purpose of this chapter is not to provide an extensive education on these network components and how to configure them. However, there is such a close dependency on Cisco collaboration products and the network that it is essential to have an understanding of the network to a certain level. To provide a deeper understanding of basic networking components, Cisco offers the CCNP Enterprise certification courses, which can also be studied using the Cisco Press material. These courses and the material will provide a more thorough understanding of what each network component is and how to configure it. For the purposes of this book, we will examine the foundational network infrastructure components because they relate directly to the Cisco preferred architecture for enterprise collaboration.

A network can be defined as a group or system of interconnected things. A local-area network (LAN) is a network of devices within a limited area. This could be a business office, school, or campus. A home network is a LAN that might interconnect computers, smartphones, tablets, smart TVs, printers, and other media devices. A wide-area network (WAN) is a network of devices within a wider area than the LAN. Imagine two LAN offices, one located in New York City and the other in Washington DC, but devices within each of these locations can communicate with one another as if they were within the same LAN. This is a WAN. Then there is the wireless local-area network (WLAN) or wireless LAN. Because different technologies exist within wireless technology as compared to a physical LAN, this type of network must be categorized independently. Most home networks use some sort of consumer wireless router, but the technology behind a commercial wireless LAN goes far beyond what is available to the everyday consumer.

Key Topic

Now that we've defined the different types of networks, let's examine some of the physical network components and how they might be used. The only network component needed to set up a LAN is a switch. A basic switch is a device with multiple physical ports to which multiple devices can be connected using an Ethernet cable so that communication between these devices can be established. Switches operate on Layer 2 of the OSI model. Cisco switches have a higher level of intelligence than a basic switch, so a network administrator can configure parameters that control how traffic flows through these switches. In fact, some of the switch models that Cisco offers can be configured with Layer 2 and Layer 3 capabilities. As switches pertain to collaboration, several configuration elements can be configured, including virtual LANs (VLANs), Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED), and quality of service (QoS), to name a few. As essential as a switch is within a network, you cannot access the public Internet or establish a WAN without the next network component—the router.

Key Topic

Routers are Layer 3 components of the OSI model and provide communication into and out of the LAN. Many services can be provided through a router. Routers are often configured to offer Dynamic Host Configuration Protocol (DHCP) services to devices on the network. DHCP provides devices with an IP address, subnet mask, and default gateway (also known as the default router) address at a minimum. It can also provide Domain Name System (DNS) address(es) and Trivial File Transfer Protocol (TFTP) server address(es). Devices connected to a switch know how to route traffic to a router using the Default Gateway Address, which is the internal IP address of the router. TFTP addresses can be provided using Option 66 or the Cisco proprietary Option 150.

Because a LAN operates using private IP addresses, which are not publicly routable, the router can masquerade these private IP addresses with a public IP address so that traffic can be routed out to the public Internet. The service used to masquerade these addresses is known as Network Address Translation (NAT) or Port Address Translation (PAT). Many devices on the network require the timing to be synchronized for services to operate properly, such as endpoints joining a scheduled meeting. Therefore, these networked devices rely on Network Time Protocol (NTP) to provide timestamp information. When the edge router is configured as the NTP authority, it can provide a Stratum 2+ NTP reference to these devices.

Firewall software is typically also available on routers. Some companies opt for a firewall server in lieu of, or in addition to, the firewall software available on the router. Firewalls protect nodes within your network from malicious attacks coming from outside your network. Think of firewalls as a first line of defense. Other defensive control mechanisms available on the router are access control lists (ACLs). ACLs are lists of protocols and port numbers that are allowed or not allowed to flow through a router. ACLs can be applied on an inbound or outbound (physical) port on the router. For example, an ACL could be configured on a router that allows TLS traffic on port 5061 but rejects TCP traffic on port 5060. The idea here is to allow encrypted SIP signaling and reject nonencrypted SIP signaling. ACLs can also be used as a stateless inspection of the traffic, which differentiates ACLs from firewalls.

Routers offer many more features, but one last feature worth mentioning is QoS. As mentioned previously with Layer 2 switches, QoS can be applied at Layer 3 on the router. In fact, Layer 3 QoS is even more critical than Layer 2 QoS because this is typically where you will find congestion in a network. Ideally, you want to mark packets as close to the source as possible; therefore, Layer 2 QoS is designed to mark packets early in the routing process. Layer 3 QoS prioritizes how traffic will flow during these high-congestion times. On the router, you need to convert Layer 2 QoS marking to Layer 3 QoS marking. Other Layer 3 tools for QoS include shaping, policing, queuing, and QoS type. Cisco has a lot of information available on QoS, and it is essential to research and understand QoS to work effectively in collaboration as a technician or engineer. QoS will be covered in a little more depth in the next chapter, although QoS is a very deep topic that could fill volumes of books all on its own.

Among Cisco routers, one stands out above the rest: the Cisco Integrated Services Router (ISR). The ISR has all the same services that other routers have, as mentioned previously. However, additional services and modules can be added to the ISR. Some of the collaboration services available on an ISR include Cisco Unified Communications Manager Express (CUCME), Survivability Remote Site Telephony (SRST), Cisco Unified Border Element

(CUBE), and Cisco Unity Express (CUE). Modules that are supported in select models of ISRs include PRI cards (E1 and T1), FXS and FXO cards, and PVDM cards.

Key Topic

Collectively, Cisco is known as "The Network People" for a reason. It offers the best proven network products available on the market. Over 80 percent of the public Internet space consists of Cisco networking products. And the company is continually releasing software advancements on its network products that push the edge of what is possible. One such software advancement that provides added intelligence to your network is known as Medianet. Cisco Medianet can be defined as an end-to-end architecture for a network comprising advanced, intelligent technologies and devices in a platform optimized for the delivery of rich-media experiences. Medianet allows network devices to be media-aware so that they can detect and optimize different media and application types to deliver the best experience to the user, such as Telepresence, video surveillance, desktop collaboration, and streaming media, to name a few. Medianet also makes networking devices endpoint-aware to automatically detect and configure media endpoints. Finally, Medianet makes networking equipment network-aware so that it can detect and respond to changes in device, connection, and service availability. With the increasing adoption of new video and rich-media applications, Medianet technologies become critically important to address challenges associated with the transmission of video, voice, and data over the network, including ensuring predictability, performance, quality, and security. By accelerating deployment of applications, minimizing complexity and ongoing operational costs, increasing visibility into the network, and helping to scale the infrastructure for the best quality of experience, Medianet technologies help address these challenges. Check out the Cisco Medianet Data Sheet at Cisco.com for more information on Medianet.

Depending on the environment being configured, there might be a need for Layer 2 switches, Layer 3 switches, and Layer 3 routers. A large enterprise network can be divided into four layers at the central office and two layers at a branch office. The central office can be divided into the Access layer, Distribution layer, Core layer, and the WAN Aggregation layer. The Access layer is typically made up of Layer 2 switches. The Distribution layer is typically made up of Layer 3 switches. The Core layer can be made up of Layer 3 switches or Layer 3 routers. The WAN Aggregation layer is always a Layer 3 router. The branch office typically utilizes a branch router and a branch switch to form the two layers needed for communication. Figure 12-1 illustrates how a typical enterprise network infrastructure is designed.

LAN

A properly designed LAN will take into consideration the needs for high availability and quality of service. This will account for the Access layer, Distribution layer, and Core layer of the typical enterprise network infrastructure. The Access layer offers in-line power to the phones, multiple queue support, 802.1p and 802.1q, and fast link convergence. The Distribution and Core switches offer multiple queue support as well as 802.1p and 802.1q, the same as the Access layer, along with traffic classification and reclassification. An IEEE protocol, 802.1p refers to the support of QoS on Layer 2 switches. Also an IEEE protocol, 802.1Q refers to the support of virtual LANs on Layer 2 switches.

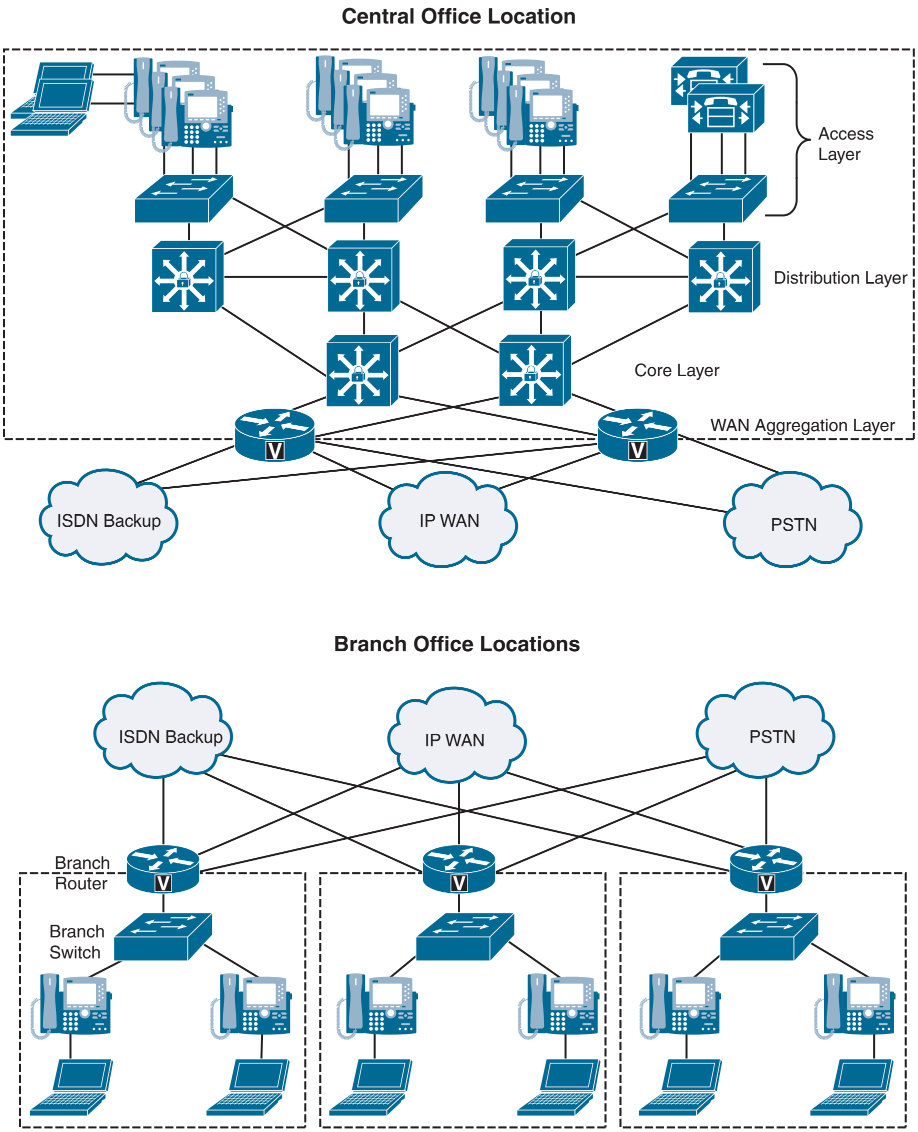


Figure 12-1 *Typical Enterprise Network Infrastructure*

Access Layer

Key Topic

High availability can be configured on the Access layer by using the Spanning Tree Protocol (STP). STP is a Layer 2 protocol that runs on switches and is specified by the IEEE standard 802.1d. The purpose of STP is to prevent loops when configuring redundant paths within the network. In Figure 12-1, observe that each switch is connected to two or more other switches, so that if one path fails, there is a redundant path to the destination. On the switch ports, STP can be configured to block traffic on one port and forward traffic on the other port. In the event that the forwarding port can no longer send and receive communications, the state of the blocking port will change to allow the data to flow along the alternate path.

This ensures that there is an alternate path for routing traffic but eliminates the chance of a loop occurring with two open ports. Different flavors of STP can be used, and each one requires different timing for convergence. Therefore, it is recommended that the same version of STP be used within a single environment. Some of the other Spanning Tree Protocols that exist include IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Instance Spanning Tree Protocol (MISTP). These two can converge at much higher rates than the traditional STP.

Key Topic

A virtual local-area network, or VLAN, is another essential part of the Access layer switch, and it should be configured prior to setting up STP. A VLAN is a logical grouping of devices connected to the switch that allows data traffic in the network to be decoupled for access control and prioritization. VLANs can be used to group devices in several ways, such as device type or department. For example, there may be a server where accounting software resides. The accounting team needs access to this software, but the sales team does not need access. The accounting team also needs to be able to communicate with the sales team for handling expense reports. In this scenario, three VLANs can be used to control who can access the accounting software. The server where the software resides can be placed in VLAN110, the accounting team computers can be placed in VLAN120, and the sales team computers can be placed in VLAN130. Then the network administrator can create connections from VLAN120 to VLAN110, and from VLAN120 to VLAN130. This will allow the accounting team to access the accounting software and communicate with the sales team. However, the sales team will be restricted from accessing the accounting software.

In a Cisco collaboration environment, VLANs are essential to implementing proper QoS. At least two VLANs should be created in this environment: a data VLAN and a voice and video VLAN, which is typically signified as VVID (Voice VLAN ID). Voice and video data can traverse the same VLAN, even though they typically experience different QoS markings. The reason these two VLANs need to be created is that Cisco phones have a NIC connecting the phone to a switch and a computer NIC connecting a computer to the phone. The phone and the computer require different QoS treatment and therefore should belong in different VLANs. This is where the configuration gets really interesting. If the phone is connected to the switch and the computer is connected to the phone, how can they possibly be decoupled into different VLANs? On the port at the switch where the phone is connected, both the Data VLAN and the VVID can be assigned. When the phone boots up, CDP or LLDP-MED can be used to discover both of these VLANs. There is a third virtual NIC in the phone that exists to monitor egress traffic and determine which VLAN should be used. Data traffic sourced from the computer will use the Data VLAN. Voice and video data from the phone will use the VVID. If content is being shared from the computer during a video call, then the VVID will be used for that particular data sourced from the computer.

One final offering that can be utilized at the Access layer needs to be mentioned here: inline power. Inline power, or Power over Ethernet (PoE), has already been discussed at great length. For a review of the information coving PoE, refer to Chapter 9, “Endpoint Registration.” Table 12-2 outlines the different types of PoE and the maximum power available. Some examples of Cisco switches that support the different types of PoE can also be found in Table 12-2.

Table 12-2 PoE Types and Supported Power

PoE Type	PoE Power Capabilities	Example Switches
Pre-Standard Inline Power	6.3 Watts power	3550-24 or 48 ports
802.3af PoE	15.4 Watts power (Type 1)	3560-24 ports or 3670-48 ports
802.3at PoE	30 Watts power (Type 2)	2960-24 is Type 1 or Type 2
	60 Watts power (Type 3)	4500 supports all types of PoE
	100 Watts power (Type 4)	9000 supports all types of PoE

Distribution Layer

The Distribution layer switches can offer the same multiple queue support, 802.1p, 802.1q, and fast link convergence as the Access layer. However, the focus of the Distribution layer should be to offer Layer 3 routing, load balancing, and fault tolerance. These Distribution layer switches are the bridge between Layer 2 and Layer 3 of the enterprise network.

The Distribution layer switch can often serve as the Layer 3 default gateway for the Layer 2 devices. Should the Distribution layer switch fail, then many devices could lose communication across the network. Cisco initially released the Hot Standby Router Protocol (HSRP) to provide a fault-tolerant default gateway. The IETF developed a similar protocol called the Virtual Router Redundancy Protocol (VRRP) with RFC 5798. Although these two protocols are similar in nature and resolve the gateway redundancy issue, they are not compatible protocols and they each have some limitations. Cisco overcame these limitations when it released another protocol called the Gateway Load Balancing Protocol (GLBP). This protocol protects data traffic from a failed router or circuit, while also allowing packet load sharing between a group of redundant routers.

Endpoints use the Address Resolution Protocol (ARP) to learn the physical MAC address of their default gateway. With HSRP, a single virtual MAC address is provided to these endpoints. With GLBP, two virtual MAC addresses can be provided to the endpoints—one from the primary gateway and one from a peer gateway—which are distributed using round-robin technique.

Another way to ensure fast convergence, load balancing, and fault tolerance on the Distribution layer is to use Layer 3 routing protocols such as OSPF or EIGRP. You can use parameters such as routing protocol timers, path or link costs, and address summaries to optimize and control convergence times as well as to distribute traffic across multiple paths and devices. Cisco also recommends using the **passive-interface** command to prevent routing neighbor adjacencies via the access layer. These adjacencies are typically unnecessary, and they create extra CPU overhead and increased memory utilization because the routing protocol keeps track of them. By using the **passive-interface** command on all interfaces facing the access layer, you prevent routing updates from being sent out on these interfaces, and therefore, neighbor adjacencies are not formed.

Core Layer

The Core layer operates entirely in Layer 3 of the enterprise network. This layer can consist of Layer 3 switches or routers. The purpose of the Core layer is to provide redundancy between different Distribution switches. In the event of network outages, the Core layer can redirect traffic along a more stable path. The types of redundancy that need to be provided at the Core layer include Layer 1 link paths, redundant devices, and redundant device subsystems, such as power supplies and module cards. The Cisco Catalyst switches with

Virtual Switching System (VSS) provide a method to ensure redundancy in all of these areas by pooling together two Catalyst supervisor engines to act as one. This is why Cisco recommends using a Layer 3 switch at the Core layer. Routing protocols at the Core layer should again be configured and optimized for path redundancy and fast convergence. There should be no STP in the core because network connectivity should be routed at Layer 3. Finally, each link between the core and distribution devices should belong to its own VLAN or subnet and be configured using a 30-bit subnet mask.

In the campus LAN, bandwidth provisioning recommendations can be summarized by the motto "overprovision and undersubscribe." This motto implies careful planning of the LAN infrastructure so that the available bandwidth is always considerably higher than the load and there is no steady-state congestion over the LAN links. The addition of voice traffic onto a converged network does not represent a significant increase in overall network traffic load; the bandwidth provisioning is still driven by the demands of the data traffic requirements. The design goal is to avoid extensive data traffic congestion on any link that will be traversed by telephony signaling or media flows. Contrasting the bandwidth requirements of a single G.711 voice call (approximately 86 kbps) to the raw bandwidth of a Fast Ethernet link (100 Mbps) indicates that voice is not a source of traffic that causes network congestion in the LAN, but rather it is a traffic flow to be protected from LAN congestion.

WAN

The next layer in the enterprise network solution is the WAN Aggregation layer. These are the edge routers that allow different locations to communicate over the public Internet. There are general design considerations for deploying a WAN, as well as specific bandwidth considerations. There are also QoS tools at the WAN that will need careful design because the WAN presents the greatest potential for congestion. QoS topics will be discussed in the next chapter.

Key Topic

The Cisco recommendation when designing the WAN Aggregation layer is to establish multiple links for redundancy in case one of the links should fail. WAN designs include hub and spoke, full mesh, and partial mesh. The hub-and-spoke design contains one central "hub" router connected to multiple "spoke" routers. Each spoke is one hop away from the hub and two hops away from other spokes. Alternatively, a full mesh or partial mesh design could be implemented. In this type of design, multiple WAN links are established between locations so that each location has at least two WAN links, each link to a different router. Redundancy should be built into the WAN Aggregation layer using multiple links. This will ensure connectivity in the event one link fails, and additional bandwidth can be provisioned for load-balancing network traffic. Another design consideration for WAN Aggregation is noncentralized resources so that these services are available to all locations in the event of a WAN failure. These resources include media resources, DHCP servers, voice gateways, and call-processing applications. Earlier in this chapter, we discussed some of the call-processing applications such as SRST or Cisco Unified Communications Manager Express. If you are unfamiliar with these call-processing applications, you may want to research them on your own because they are outside the scope of this book.

The two types of bandwidth options to choose from when designing the WAN Aggregation layer are best-effort bandwidth and guaranteed bandwidth. Examples of best-effort bandwidth include the public Internet, DSL, cable, satellite, and wireless. With best effort there is no QoS, and bandwidth availability is on a first-come basis. Although these types of links are suitable for home offices or commuters, voice and video traffic will suffer. Therefore, Cisco recommends that you do not use best effort for voice-enabled networks that require enterprise-class voice services and quality.

Alternatively, you can choose from available guaranteed bandwidth link options. Leased Lines, Frame Relay, Asynchronous Transfer Mode (ATM), and ATM/Frame-Relay Service Interworking are older technologies that use dedicated circuits through a telephony service provider. These were the best options available to corporations prior to the introduction of broadband and high-speed Internet. Today, these technologies are very expensive and offer lower bandwidth rates compared to other packet-switched solutions available.

Key Topic

Some other guaranteed bandwidth link options available include Multiprotocol Label Switching (MPLS), Cisco Voice and Video Enabled IP Security Virtual Private Network (IPSec V3PN), and Dynamic Multipoint Virtual Private Network (DMVPN). MPLS is a transport protocol that uses "labels" to route traffic rather than network addresses. Packets are forwarded based on the content of the label, so deciphering between voice, video, and data is simple. It is protocol agnostic, so it will function in circuit-switched or packet-switched networks. IPSec V3PN integrates three core Cisco technologies: IP Telephony, QoS, and IPSec VPN. This results in an end-to-end VPN service that can guarantee the delivery of latency-sensitive voice and video communications. DMVPN is a solution that provides an alternative to the complicated administrative setup and maintenance that comes with establishing a mesh network. Initially, the DMVPN is set up as a hub-and-spoke network. Once communication is established between the spokes and the hub, each spoke will dynamically discover each of the other spokes and establish a tunnel between one another. This will reduce the amount of traffic at the hub, preserving bandwidth and processing capacity limits. For information on the deployment of multisite DMVPN WANs with centralized call processing, refer to "Cisco Unified Communications Voice over Spoke-to-Spoke DMVPN Test Results and Recommendations," available at https://www.cisco.com/go/designzone. Figure 12-2 illustrates how a DMVPN network operates.

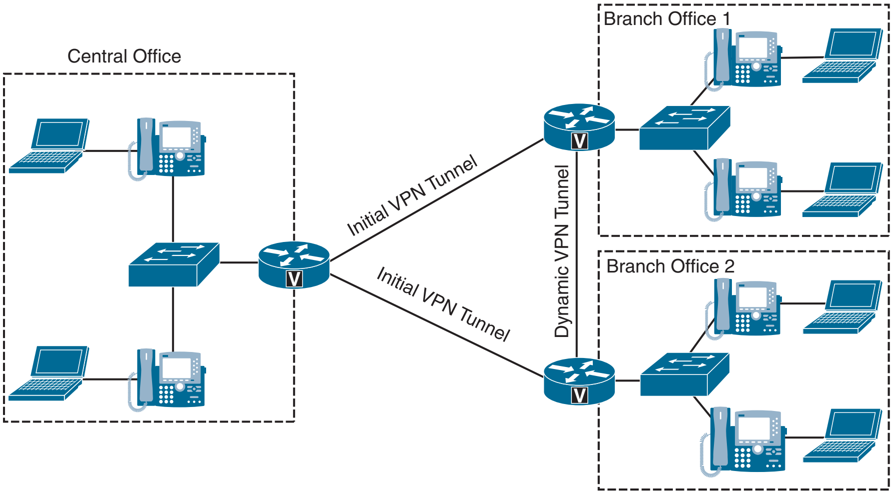


Figure 12-2 *DMVPN Network Operations*

WLAN

The wireless local-area network (WLAN) is a whole infrastructure deployment that hangs off the LAN but requires a unique set of configurations. WLAN infrastructure design becomes important when collaboration endpoints are added to the WLAN portions of a converged network. With the introduction of Cisco Unified Wireless endpoints, voice and video traffic has moved onto the WLAN and is now converged with the existing data traffic there. Just as with wired LAN and wired WAN infrastructure, the addition of voice and video in the WLAN requires following basic configuration and design best practices for deploying a highly available network. In addition, proper WLAN infrastructure design requires understanding and deploying QoS on the wireless network to ensure end-to-end voice and video quality on the entire network.

Basic Configuration and Design

Wireless IP network architectures enable IP telephony to deliver enterprise mobility by providing on-premises roaming communications to the users with wireless IP telephony devices. Wireless IP telephony and wireless IP video telephony are extensions of their wired counterparts, which leverage the same call elements. Additionally, wireless IP telephony and IP video telephony take advantage of wireless 802.11-enabled media, thus providing a cordless IP voice and video experience. The cordless experience is achieved by leveraging the wireless network infrastructure elements for the transmission and reception of the control and media packets. The architecture for voice and video over wireless LAN includes the following basic elements:

Key Topic

- Wireless access points
- Wireless LAN controllers
- Authentication database
- Supporting wired network
- Wireless collaboration endpoints
- Wired call elements

The wireless access points enable wireless devices to communicate with wired network elements. In the case of a Cisco Collaboration environment, these wireless devices include all the UC voice and video endpoints that support wireless communications. Access points function as adapters between the wired and wireless world, creating an entryway between these two media components. Cisco access points can be managed by a wireless LAN controller (WLC), or they can function in autonomous mode. When the access points are managed by a WLC, they are referred to as lightweight access points (LWAPs), and in this mode, they use the Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points (CAPWAP) protocol, depending on the controller version, when communicating with the WLC.

Many corporate environments require deployment of wireless networks on a large scale. The wireless LAN controller (WLC) is a device that assumes a central role in the wireless network and helps make it easier to manage such large-scale deployments. Traditional roles of access points, such as association or authentication of wireless clients, are handled by the WLC. Access points, called lightweight access points in the Unified Communications environment, register themselves with a WLC and tunnel all the management and data packets to the WLCs, which then switch the packets between wireless clients and the wired portion of the network. All the configurations are done on the WLC. LWAPs download the entire configuration from WLCs and act as a wireless interface to the clients. Figure 12-3 illustrates the relationship between the WLC and the LWAP.

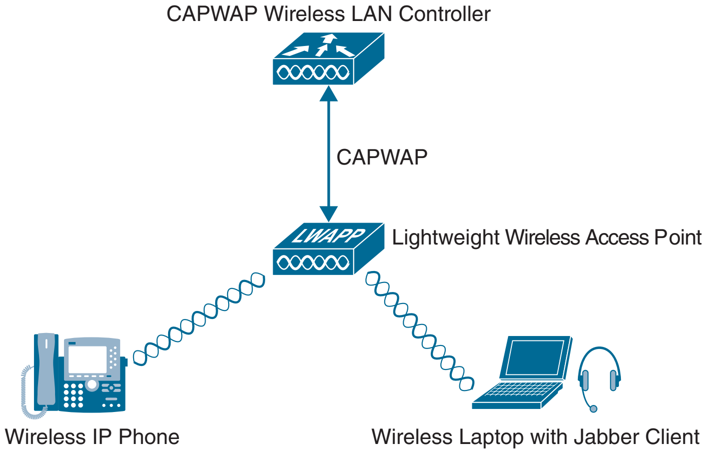

CAPWAP Wireless LAN Controller
CAPWAP
LWAPP
Lightweight Wireless Access Point
Wireless IP Phone
Wireless Laptop with Jabber Client

Figure 12-3 *WLC Deployment with LWAP*

The authentication database is a core component of the wireless networks, and it holds the credentials of the users to be authenticated while the wireless association is in progress. The authentication database provides network administrators with a centralized repository to validate the credentials. Network administrators simply add the wireless network users to the authentication database instead of having to add the users to all the wireless access points with which the wireless devices might associate. In a typical wireless authentication scenario, the WLC couples with the authentication database to allow the wireless association to proceed or fail. Authentication databases commonly used are LDAP and RADIUS, although under some scenarios the WLC can also store a small user database locally that can be used for authentication purposes.

The supporting wired network is the portion of the system that serves as a path between WLCs, WAPs, and wired call elements. Because the WAPs need to communicate to the wired world, part of the wired network has to enable those communications. The supporting wired network consists of the LAN switches, routers, and WAN links that work together to communicate with the various components that form the architecture for voice and video over WLAN.

Key Topic

The wireless collaboration endpoints are the user-facing voice and video nodes that operate over the WLAN, which are used for communication. These endpoints can be voice only or enabled for both voice and video. When end users employ the wireless communication endpoints to call a desired destination, the endpoints in turn forward the request to their associated call-processing server. If the call is allowed, the endpoints process the voice or video, encode it, and send it to the receiving device or the next hop of processing. Typical Cisco wireless endpoints are wireless IP phones, voice and video software clients running on desktop computers, mobile smartphones connected through wireless media, and mobile collaboration enterprise tablets. Specifically, the Cisco Unified IP Phones 7861, 8861, and 8865 support wireless communication. Any Windows or Mac computer running the Cisco Jabber application, or any smartphone or tablet running Jabber, could be connected wirelessly to the network. Also, the Cisco DX series endpoints support wireless connections to the network.

Whether the wireless collaboration endpoints initiate a session between each other or with wired endpoints, wired call elements are involved in some way. Wired call elements, such as gateways and call-processing entities, are the supporting infrastructure for voice and video endpoints coupled to that infrastructure. Figure 12-4 illustrates all of the components needed in a WLAN deployment.

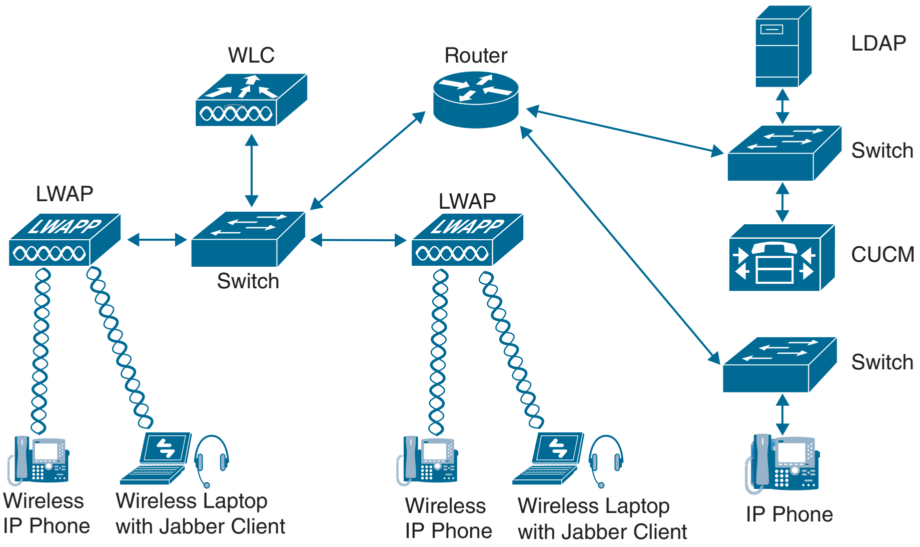


Figure 12-4 *Components of a Full WLAN Deployment*

High Availability

Providing high availability in collaboration solutions is a critical requirement for meeting the modern demands of continuous connectivity. Collaboration deployments designed for high availability increase reliability and uptime. Using real-time applications such as voice or video over WLAN without high availability could have very adverse effects on the end-user experience, including an inability to make voice or video calls.

A unique aspect of high availability for voice and video over WLAN is high availability of radio frequency (RF) coverage to provide Wi-Fi channel coverage that does not depend on a single WLAN radio. The Wi-Fi channel coverage is provided by the AP radios in the 2.4 GHz and 5 GHz frequency bands.

Key Topic

The primary mechanism for providing RF high availability is cell boundary overlap. In general, a cell boundary overlap of 20 to 30 percent on nonadjacent channels is recommended to provide high availability in the wireless network. For mission-critical environments, at least two APs should be visible at the required signal level (67 dBm or better). An overlap of 20 percent means that the RF cells of APs using nonadjacent channels overlap each other on 20 percent of their coverage area, while the remaining 80 percent of the coverage area is handled by a single AP. Furthermore, when determining the locations for installing the APs, you should avoid mounting them on reflective surfaces, such as metal, glass, and so forth, which could cause multipath effects that result in signal distortion. Figure 12-5 illustrates a high availability deployment of WLANs using overlapping channel cells.

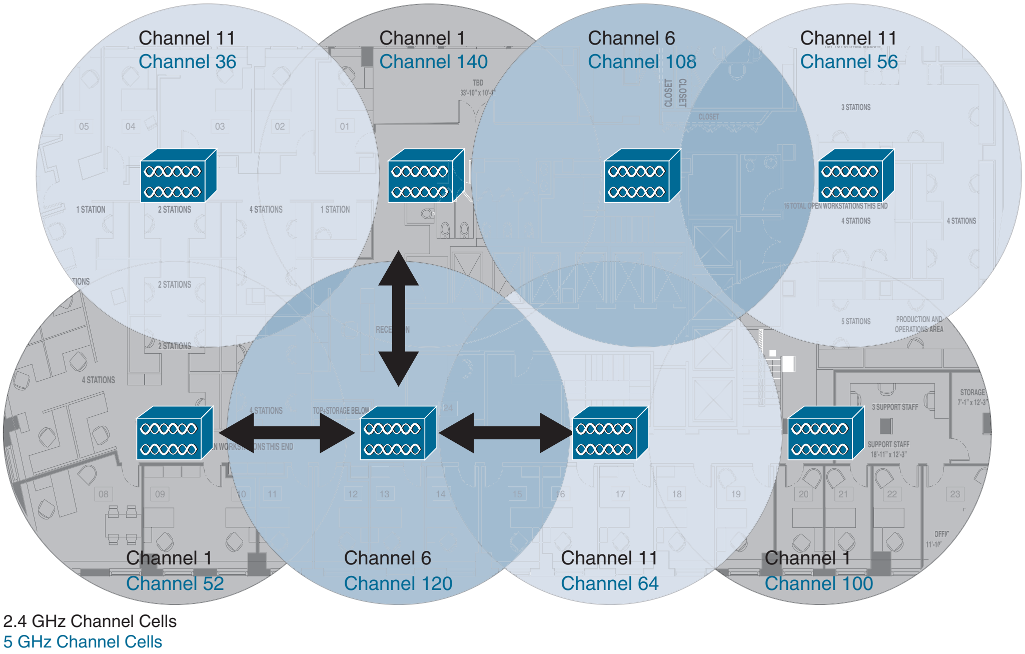


Figure 12-5 *High Availability Deployment of WLANs Using Overlapping Channel Cells*

Careful deployment of APs and channel configuration within the wireless infrastructure are imperative for proper wireless network operation. For this reason, Cisco requires customers to conduct a complete and thorough site survey before deploying wireless networks in a production environment. The survey should include verifying nonoverlapping channel configurations, Wi-Fi channel coverage, and required data and traffic rates; eliminating rogue APs; and identifying and mitigating the impact of potential interference sources. Additionally, you should evaluate utilizing a 5 GHz frequency band, which is generally less crowded and thus usually less prone to interference. If Bluetooth is used, it is highly recommended to use a 5 GHz WLAN band (802.11a/n/ac) whenever possible for endpoint connectivity. Similarly, the use of Cisco CleanAir technology will increase the WLAN reliability by detecting radio frequency interference in real time and providing a self-healing and self-optimizing wireless network.

Capacity Planning

A crucial piece in planning for voice and video over WLAN is adequately sizing the solution for the desired call capacity. Capacity is defined as the number of simultaneous voice and video sessions over WLAN that can be supported in a given area. Capacity can vary depending on the RF environment, the collaboration endpoint features, and the WLAN system features. For instance, a solution using Cisco Unified Wireless IP Phones 8861 on a WLAN that provides optimized WLAN services would have a maximum call capacity of 27 simultaneous sessions per channel at a data rate of 24 Mbps or higher for both 802.11a and 802.11g. On the other hand, a similar solution with a wireless device such as a tablet running the Jabber client making video calls at 720p and a video rate of 2500 kbps on a WLAN, where access points are configured as 802.11a/n with a data rate index of Modulation and Coding Scheme 7 in 40 MHz channels, would have a maximum capacity of seven video calls and two bidirectional voice and video streams per channel. To achieve these capacities, there must be minimal wireless LAN background traffic and RF utilization, and Bluetooth must be disabled in the devices. It is also important to understand that call capacities are established per nonoverlapping channel because the limiting factor is the channel capacity and not the number of access points (APs). The call capacity specified by the actual wireless endpoint should be used for deployment purposes because it is the supported capacity of that endpoint.

Design Considerations

It is easy to understand that the design and implementation of a WLAN environment in the workplace is very complex and requires many considerations to be factored into the overall network design. Additionally, WLAN configuration specifics can vary depending on the voice or video WLAN devices being used and the WLAN design. Other design considerations for a proper WLAN deployment include the following:

- VLANs
- Roaming
- Wireless channels
- Wireless interference and multipath distortion
- Multicast on the WLAN
- Wireless AP configuration and design
- Wireless LAN controller design considerations
- WLAN quality of service

An entire series of books could be written just to cover the WLAN components and considerations that must be accounted for in a network design that supports voice and video communications. Cisco has a CCNP and CCIE certification track that deals with the many facets of a WLAN environment, and many resources are available to extend an engineer's understanding of these solutions. To keep the contents of this section relevant to the scope of this book, we will not cover the preceding topics. However, the next chapter will delve into some of the WLAN QoS settings that need to be configured to support voice and video over a WLAN environment.

Gateways

Gateways provide a number of methods for connecting a network of collaboration endpoints to the public switched telephone network (PSTN), a legacy PBX, or external systems. Voice and video gateways range from entry-level and standalone platforms to high-end, feature-rich integrated routers, chassis-based systems, and virtualized applications.

During the 1990s and early 2000s, the only way for an enterprise to connect its internal voice and video network to services outside the enterprise was by means of time-division multiplexing (TDM) or serial gateways through the traditional PSTN. Cisco still offers a full range of TDM and serial gateways with analog and digital connections to the PSTN as well as to PBXs and external systems. TDM connectivity covers a wide variety of low-density analog (FXS and FXO), low-density digital (BRI), and high-density digital (T1, E1, and T3) interface choices. Starting around 2006, new voice and video service options to an enterprise became available from service providers, often as SIP trunk services. Using a SIP trunk for connecting to the PSTN and other destinations outside the enterprise involves an IP-to-IP connection at the edge of the enterprise's network. The same functions traditionally fulfilled by a TDM or serial gateway are still needed at this interconnect point, including demarcation, call admission control, quality of service, troubleshooting boundary, security checks, and so forth. For voice and video SIP trunk connections, the Cisco Unified Border Element and the Cisco Expressway Series fulfill these functions as an interconnection point between the enterprise and the service provider network.

Key Topic

There are two types of Cisco TDM gateways: analog and digital. Both types support voice calls, but only digital gateways support video. The two categories of Cisco analog gateways are station gateways and trunk gateways. Analog station gateways connect the Cisco Unified Communications Manager to plain old telephone service (POTS) analog telephones, interactive voice response (IVR) systems, fax machines, and voicemail systems. Station gateways provide foreign exchange station (FXS) ports. Analog trunk gateways connect the Cisco Unified Communications Manager to PSTN central office (CO) or PBX trunks. Analog trunk gateways provide foreign exchange office (FXO) ports for access to the PSTN, PBXs, or key systems, and E&M (recEive and transMit, or ear and mouth) ports for analog trunk connection to a legacy PBX. Analog Direct Inward Dialing (DID) and Centralized Automatic Message Accounting (CAMA) are also available for PSTN connectivity. Cisco analog gateways are available on the following products and series:

- Cisco Analog Voice Gateways VG204XM and VG300 Series (VG310, VG320, VG350) all support SCCP.
- Cisco Integrated Services Routers Generation 2 (ISR G2) 2900, 3900, 3900E, and 4000 Series (4300 and 4400) with appropriate PVDMs and service modules or cards. PVDM4s utilized by ISR 4000 Series do not support video today.
- Cisco Analog Telephone Adapter (ATA) 190 (SIP only) provides a replacement for the ATA188.

A Cisco digital trunk gateway connects the Cisco Unified Communications Manager to the PSTN or to a PBX via digital trunks such as Primary Rate Interface (PRI), Basic Rate Interface (BRI), serial interfaces (V.35, RS-449, and EIA-530), or through T1 Channel Associated Signaling (CAS). Digital T1 PRI and BRI trunks can be used for both video and audio-only calls. Cisco digital trunk gateways are available on the following products and series:

- Cisco Integrated Services Routers Generation 2 (ISR G2) 1900, 2900, 3900, 3900E, 4300, and 4400 Series with appropriate PVDMs and service modules or cards (The PVDM2 cards were end of life as of June 30, 2019. Cisco recommends using the PVDM3 or PVDM4 cards on appropriate routers.)
- Cisco Telepresence ISDN GW 3241 and MSE 8321 (These products were end of sale as of May 2, 2017.)
- Cisco Telepresence Serial GW 3340 and MSE 8330 (These products were end of sale as of May 2, 2017.)

The Cisco Telepresence ISDN link is a compact appliance that provides Cisco Telepresence endpoints direct ISDN and external IP network connectivity. This unit is supported on all Cisco Telepresence endpoints running TC or CE software. While traditional voice and video gateways are shared resources that provide connectivity between the IP network and the PSTN for many endpoints, each Cisco ISDN link is paired with a single Cisco endpoint.

ISR, ASR, and IOS Software Comparisons

Cisco has a line of routers that offer advanced services beyond what traditional routers can offer. These routers are ideal for use in voice and video environments as well as support of smaller branch office locations or hybrid communication to the cloud. They are the Integrated Services Routers (ISRs), Aggregation Services Routers (ASRs), and Cloud Services Routers (CSRs). The biggest difference between Cisco ASR and ISR routers is that ASR routers are for enterprises and service providers, whereas ISRs are for customers with small- or medium-sized networks. CSRs go beyond the scope of this book, so the focus will be on the ISR and ASR options.

Two factors that should be considered will influence which of these router product lines should be used within a particular customer environment. Sizing is the most important factor, followed by the software running on the router. Different software will provide different features and capabilities. The classic IOS software was used on all Cisco routers prior to 2007 and may still be found running on some routers in production today. However, most current products in the Cisco ISR and ASR routers use either the IOS XE or IOS XR software version.

Cisco IOS XE software is an open and flexible operating system optimized for a new era of enterprise networks. Its standards-based programmable interfaces automate network operations and give you deep visibility into user, application, and device behaviors. As the single OS for enterprise wired and wireless access, aggregation, core, and WAN, Cisco IOS XE reduces business and network complexity. Cisco IOS XE software is open because it includes the following open standards-based capabilities: NETCONF (RFC 6241) programmable interfaces, IETF YANG push telemetry, OpenConfig and IETF YANG data models, and Guest Shell Linux Containers (LXC). Yet the user interface is the same familiar CLI that engineers have been using throughout the lifecycle of the older classic IOS software. This highly scalable software has been developed with resiliency in mind; Cisco IOS XE reduces planned and unplanned downtime. Service and software upgrades are more efficient, and Graceful Insertion and Removal lets you update or debug a switch without disrupting network traffic. Cisco IOS XE software also has built-in security and trust, which helps protect against modern cyberattacks. It assures that Cisco hardware and software are genuine and unmodified. And its enhanced platform integrity, security, and resilience mean you can be confident that data is trustworthy. Additionally, all IOS XE software-based routers support hybrid cloud services.

IOS XR is Cisco IOS software used on the high-end Network Converging System (NCS), carrier-grade routers such as the CRS Series, 12000 Series, and ASR9000 Series. In fact, the ASR9000 Series are the only ASR or ISR routers that support the IOS XR software. Cisco's IOS XR software shares very little infrastructure or feature support with the other IOS software options and is instead built on a preemptive, memory-protected, multitasking, microkernel-based operating system. The microkernel was formerly provided by QNX; versions 6.0 and up use the Wind River Linux distribution. IOS XR is an on-premises-only software solution with no hybrid cloud support, and it aims to provide the following advantages over the earlier IOS versions:

- Improved high availability (largely through support for hardware redundancy and fault containment methods such as protected memory spaces for individual processes and process restart-ability)
- Better scalability for large hardware configurations (through a distributed software infrastructure and a two-stage forwarding architecture)
- A package-based software distribution model (allowing optional features such as multicast routing and MPLS to be installed and removed while the router is in service)
- The ability to install package upgrades and patches (potentially while the router remains in service)
- A web-based GUI for system management (making use of a generic, XML management interface)

As mentioned previously, the number of users the router needs to support for sizing and the software version will determine the specific product needed for a given customer site. Table 12-3 identifies all the different series of ISR and ASR routers available with their sizing limitations and software availability.

Key Topic

Table 12-3 ISR and ASR Routers and Software Options

Router Model	Software Version	Sizing Limitations (SRTP/RTP Sessions)
ASR 900	IOS XE	Unknown
ASR 1000 Series	IOS XE	Unknown
ASR 9000 Series	IOS XR	Unknown
ISRv	IOS XE	Up to 1000
ISR 1000	IOS XE	75 to 100
ISR 4000 Series	IOS XE	40 to 1500
CSR 1000v	IOS XE	225 to 800 (1 or 4 vCPU)
ISR 800 Series	Classic IOS	20
ISR 900 Series	Classic IOS	50
ISR 2900 Series	Classic IOS	Up to 200

ISR Products Explained

As Table 12-3 shows, you have many product lines to choose from when deploying the Cisco ISR. This section will delve into four specific ISRs: the ISRv (which is a virtual router), 800 Series ISR, 1000 Series ISR, and the 4000 Series ISR. The 800 Series ISR is the only router discussed in this section that runs the classic IOS software instead of the IOS XE software. However, this is a great router to use for remote office locations, and it supports DMVPN.

There are many benefits to using the ISRv. First, it supports rapid deployment and service automation. The virtual form factor accelerates deployment and eliminates hardware costs such as complete equipment upgrades and return materials authorization (RMA). It also supports single-tenant use. This feature allows a cloud service provider to provision a routing instance per tenant, simplifying service delivery and tenant management. It also helps the provider overcome VLAN scale limits, increasing tenant scale. The enterprise network extension to the cloud feature provides enterprises highly secure direct connections from their distributed sites to their cloud-hosted applications, improving application response time and user experience. The network consistency feature uses familiar enterprise-class Cisco IOS software features for consistent network operation across premises and the cloud, allowing the enterprise to view the cloud as just another node in its network. Network scalability allows scale beyond the limitations of 802.1q VLAN tagging by building a VXLAN network or extending Layer 3 routing deeper into the cloud environment. Finally, consolidation of network functions eliminates the facility requirements and complexity of physical network devices by consolidating multiple network functions onto a single piece of server hardware.

The following features are supported on the Cisco ISRv:

Key Topic

- **Routing:** Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Policy-Based Routing, IPv6, Virtual Route Forwarding Lite (VRF-Lite), Multicast, LISP, and Generic Routing Encapsulation (GRE)
- **Addressing:** Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Network Address Translation (NAT), 802.1Q VLAN, Ethernet Virtual Connection (EVC), and VXLAN
- **VPN:** IPsec VPN, DMVPN, Easy VPN, SSL VPN, and FlexVPN
- **MPLS:** MPLS VPN, VRF, and Bidirectional Forwarding Detection (BFD)
- **Security:** Cisco IOS Zone-Based Firewall (ZBFW); access control list (ACL); authentication, authorization, and accounting (AAA); RADIUS; and TACACS+
- **High availability:** HSRP, Virtual Router Redundancy Protocol (VRRP), Gateway Load Balancing Protocol (GLBP), and box-to-box high availability for ZBFW and NAT
- **Traffic redirection:** AppNav (to Cisco Wide Area Application Services [WAAS]) and Web Cache Communication Protocol (WCCP) application visibility, performance monitoring, and control: quality of service (QoS), AVC, and IP service-level agreement (SLA)
- **Hybrid cloud connectivity:** OTV, Virtual Private LAN Service (VPLS), and Ethernet over MPLS (EoMPLS)
- **Management:** Command-line interface (CLI), Secure Shell (SSH) Protocol, NetFlow, Simple Network Management Protocol (SNMP), Embedded Event Manager (EEM), and RESTful application programming interfaces (APIs)
- **NFV:** Virtual route reflector (vRR), virtual broadband network gateway (vBNG), and virtual intelligent services gateway (vISG)

An affordable router series that supports important network services such as security is the Cisco 800 Series Integrated Services Routers. These ISRs deliver secure, reliable WAN connectivity that small offices and remote workers need. Additionally, they support built-in voice features, wireless, WAN optimization, and machine-to-machine communications. Different models in the series support different connection types to serve the specific needs of a small office. That could be xDSL, Wi-Fi, 4G LTE, Ethernet, fiber, or something else. Routing, switching, wireless, and intelligent IP network services are all bundled into one compact form factor that's quick to install using the Cisco Configuration Professional Express tool. They can all be managed centrally from a data center with Cisco Prime Infrastructure and LiveAction applications. The 800 ISRs provide comprehensive security—encryption, VPN, firewall, and cloud-based URL filtering—to help safeguard customers and data. Table 12-4 outlines the models in the 800 Series ISRs and includes deployment recommendations and top WAN speeds.

Key Topic

Table 12-4 800 Series ISRs

Model	Deployment Recommendation	Top WAN Speed with Services On
860	Home or small offices with up to 10 users	10 Mbps
880	Remote workers, small offices, and branch locations with up to 20 users	15 Mbps
810	Machine-to-machine and device-to-device deployments such as ATMs, point-of-sale, kiosks, vending machines (fixed platform)	15 Mbps
890	Enterprise remote offices with up to 50 users	>20 Mbps
800M	Microbranches, industrial, Internet of Things/IoT (modular platform)	Various Cellular Data Rates

The Cisco 1000 Series ISR platform with its small form factor is best suited for small and midsize businesses, enterprise branches, and as customer premises equipment in managed services environments. The routers come with four or eight LAN ports in various model options. They have high performance with Gigabit Ethernet packet-forwarding capabilities. The multicore architecture has separate cores for the data plane and control plane. The 1000 Series ISRs support Power over Ethernet (PoE) and PoE+ to power branch devices such as IP phones and cameras. They are easy to deploy with zero-touch provisioning using Plug-and-Play capability. There are multiple combinations to choose from, including LAN, WLAN, WAN, DSL, LTE, and pluggable, depending on your branch needs. The 1000 Series can be used in ATMs, retail stores, and kiosks, as well as for various other purposes. The 1000 Series ISRs address the demands of increased mobility with LTE Advanced and 802.11ac (Wave 2) Wi-Fi. It has a comprehensive set of WAN connectivity options such as Ethernet, Fiber, LTE, and the latest DSL technologies, like G.fast. The routers provide a great return on investment, allowing you to save on operating expenses by reducing WAN link costs with software-defined WAN capability and transport independence using Cisco SD-WAN. You can also reduce capital expenses using pay-as-you-grow licensing for IPsec performance. The 1000 Series ISRs answer the latest security threats to networking devices with advanced features such as zone-based firewall, Trustworthy Systems, Cisco Umbrella security, and Encrypted Traffic Analytics.

The Cisco 1000 Series ISRs include the following models:

Key Topic

- Cisco 1100-8P ISR with LTE Advanced
- Cisco 1100-4P ISR with DSL
- Cisco 1101-4P
- Cisco 1101-4PLTEP

As you build out the digital capabilities in your enterprise branch offices, you should consider the full-service sophistication of the Cisco 4000 Series Integrated Services Routers. The 4000 Series ISRs consolidate many must-have IT functions, including network, security, compute, storage, and unified communications. So, you get everything you need in a single platform. That means significant savings in capital, operational, and management expenses for lower total cost of ownership. The platform is modular and upgradable, so you can add new services without changing equipment. It supports multiple application-aware services concurrently while maintaining WAN performance of up to 2 Gbps, even during heavy traffic loads. The backplane architecture supports high-bandwidth, module-to-module communication at speeds up to 10 Gbps. The 4000 Series includes Cisco Trust Anchor Technologies that help mitigate modern cyberattacks by verifying platform integrity and providing protection from counterfeit and unauthorized modification of hardware and software.

The 4000 Series runs Cisco Intelligent WAN (IWAN), a comprehensive set of traffic control and security features. IWAN includes all the business-grade capabilities of a Multiprotocol Label Switching (MPLS) VPN using other types of less-expensive links, such as per-application traffic management, WAN optimization, and VPN tunneling, which can be put to work across Internet, cellular, and other lower-cost services as connections are added. Additionally, new router services can be activated on demand through a simple licensing change. Local IT staff are not needed in the branch to deliver a fully comprehensive computing and networking experience with remote application installation and management capabilities.

Cisco IWAN features can now be configured in next to no time, thanks to Cisco's enterprise software-defined networking (SDN) controller, the Application Policy Infrastructure Controller Enterprise Module (APIC EM). APIC EM allows automation of lots of tasks across the network. You can implement an SDN on the Cisco WAN infrastructure without having to upgrade any equipment; just install the no-charge APIC EM software-based controller between applications and network infrastructure. The controller translates business policy directly into network device-level policy for automatic compliance with any corporate and industry-mandated polices. For additional WAN management simplicity, you can also use the IWAN app for APIC EM. The app automates the configuration of Cisco Intelligent WAN features, such as quality of service, WAN optimization, and security, in Cisco branch and edge WAN routers. The app slashes what used to require 1000 CLI steps to just 10 mouse clicks per site. With the IWAN app's template functionality, the ability to configure, deploy, and manage large numbers of branch offices has never been easier. The 4000 Series ISR contains these platforms: the 4451, 4431, 4351, 4331, 4321, and 4221 ISRs.

APIC EM is now wrapped into DNA Center, which falls under SD-Access. It could also be described as "Cisco's Software-Defined Access (SD-Access) solution" because it's the blanket term of the software-defined LAN side. Also, to add to the confusion, APIC EM and IWAN are still being used, but more attention is focused on the Cisco SD-WAN solution that's based on the Viptela acquisition. Lastly, both SD-Access and SD-WAN fall under Cisco Digital Network Architecture (Cisco DNA), similar to how everything in collaboration now falls under Webex.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

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

Key Topic

Table 12-5 Key Topics for Chapter 12

Key Topic Element	Description	Page Number
Paragraph	LAN Communication and Layer 2 Switches Overview	283
Paragraph	Layer 3 Routers and Basic Services They Provide	283
Paragraph	Medianet Explained	285
Paragraph	Spanning Tree Protocol Explained	286
Paragraph	VLANs Explained	287
Table 12-2	PoE Types and Supported Power	288
Paragraph	Comparison of HSRP, VRRP, and GLBP	288
Paragraph	WAN Aggregation Design Models	289
Paragraph	DMVPN Explained	290
List	Basic Elements of a WLAN	291
Paragraph	Examples of Wireless Voice and Video Endpoints	292
Paragraph	Cell Boundary Overlap	293
List	WLAN Design Considerations	295
Paragraph	Gateway Categorization	296
Table 12-3	ISR and ASR Routers and Software Options	298
List	ISRv Features Supported	299
Table 12-4	800 Series ISRs	300
List	Cisco 1000 Series ISR Models	301

Define Key Terms

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

802.1d, 802.1p, 802.1Q, 802.1s, 802.1w, ACL, ADDTS, Advanced Networking, Annunciator, ARP, BRI, CAMA, CAPWAP, CAS, CDP, Cell Boundary Overlap, CleanAir, DHCP, DID, DMVPN, DNS, EIGRP, FXO, FXS, GLBP, HSRP, IPSec V3PN, ISR, IVR, LAN, LLDP-MED, LWAP, LWAPP, MPLS, NAT, NTP, Option 66, Option 150, OSPF, PAT, PBX, POTS, PRI, PSTN, QoS, RF, STP, TDM, TFTP, VLAN, VRRP, VSS, VVID, WAN, WAP, WLAN, WLC

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What are the three types of Spanning Tree that can be configured on Cisco switches?
2. What are three fault-tolerant default gateway protocols?
3. List three guaranteed bandwidth options for Internet connection that are currently being used.
4. List the four Cisco ISR 1100 Series routers.

CHAPTER 13

Layer 2 and Layer 3 QoS Parameters

This chapter covers the following topics:

QoS-Related Issues: This topic will discuss latency, jitter delay, and bandwidth issues that can be overcome with a good QoS solution.

Class Models for Provisioning QoS: This topic will discuss three different models for classifying network traffic using QoS: the 4/5 class model, 8 class model, and the 11 class model. All three are based on the QoS Baseline model.

QoS Requirements: This topic will begin to explain the layered components that make up a complete QoS solution, such as Layer 2 trust boundaries; congestion management tools; congestion avoidance tools; and policing, shaping, and link efficiency methods.

Traffic Classifications: This topic will break down different traffic classifications within the LAN, across the WAN, and over the wireless LAN.

Configure and Verify LLQ: This topic will explain how to configure and verify an LLQ QoS deployment through configuring a class map, policy map, and service policy.

Quality of service (QoS) refers to the capability of a network to provide improved service to selected network traffic over various underlying technologies. This chapter will explain what QoS is, review different components that make up a QoS solution, and provide a basic understanding of how to configure a QoS solution on an IOS router. Topics discussed in this chapter include the following:

- QoS-Related Issues:
  - Latency, Jitter, and Packet Loss
  - Bandwidth
- Class Models for Provisioning QoS:
  - 4/5 Class Model
  - 8 Class Model
  - QoS Baseline Model (11 Class)
- QoS Requirements:
  - QoS Trust Boundaries
  - Congestion Management

    - Congestion Avoidance
    - Policing
    - Shaping
    - Link Efficiency Methods
- Traffic Classifications:
    - LAN and WAN Traffic Classifications
    - WLAN Traffic Classifications
- Configure and Verify LLQ:
    - Class Map
    - Policy Map
    - Service Policy

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 1.1.h QoS
- 5.1 Describe problems that can lead to poor voice and video quality
    - 5.1.a Latency
    - 5.1.b Jitter
    - 5.1.c Packet loss
    - 5.1.d Bandwidth
- 5.2 Describe the QoS requirements for voice and video
- 5.3 Describe the class models for providing QoS on a network
    - 5.3.a 4/5 Class model
    - 5.3.b 8 Class model
    - 5.3.c QoS Baseline model (11 Class)
- 5.4 Describe the purpose and function of these DiffServ values as it pertains to collaboration
    - 5.4.a EF
    - 5.4.b AF41
    - 5.4.c AF42
    - 5.4.d CS3
    - 5.4.e CS4

- 5.5 Describe QoS trust boundaries and their significance in LAN-based classification and marking
- 5.6 Describe and determine location-based CAC bandwidth requirements
- 5.7 Configure LLQ (class map, policy map, service policy)

"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
QoS-Related Issues	1–3
Class Models for Provisioning QoS	4–6
QoS Requirements	7–9
Traffic Classifications	10–11
Configure and Verify LLQ	12–14

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 is an example of drop-insensitive data?
   - **a.** FTP data packets
   - **b.** Call setup messages
   - **c.** Email
   - **d.** Voice media during a call
2. Which of the following is described as a variable of the delay over a period of time?
   - **a.** Latency
   - **b.** Jitter
   - **c.** Packet loss
   - **d.** Slow bandwidth

3. An engineer is trying to calculate how much bandwidth is being consumed across the network for video calls. All video calls are required to consume no more than 512 kbps bandwidth per call. How much bandwidth is actually being consumed per call?
   - **a.** (512k + 40 + 32) × 50 pps × 8 bits/bytes = 524,800 bps or 524 kbps
   - **b.** 512 kbps
   - **c.** 512 × 1.2 = 614.4 or 614 kbps
   - **d.** 512 × 2 (send and receive) = 1024 kbps
4. Which of the following classifications is part of the 4/5 class model?
   - **a.** Real Time
   - **b.** Audio
   - **c.** Video
   - **d.** Bulk Data
5. Cisco recommends that call signaling be marked with CS3 for proper QoS handling. However, older model phones do not use CS3 for call signaling. What is the other QoS marking for call signaling that may need to be accounted for?
   - **a.** EF
   - **b.** DF
   - **c.** AF31
   - **d.** AF41
6. When establishing the QoS Baseline 11 class model, how much bandwidth should be allocated for interactive video?
   - **a.** 13%
   - **b.** 23%
   - **c.** 25%
   - **d.** 33%
7. What command can be entered into a switch to enable QoS at the Layer 2 level?
   - **a.** **mls qos**
   - **b.** **mls qos interface fastethernet 0/1**
   - **c.** **mls qos trust cos**
   - **d.** No command is needed because QoS is enabled by default.
8. Which of the following congestion management mechanisms allows delay-sensitive data, such as voice and video, to be given preferential treatment over other traffic by letting this data be dequeued and sent first?
   - **a.** FIFO
   - **b.** PQ
   - **c.** CQ
   - **d.** WFQ
   - **e.** CBWFQ
   - **f.** LLQ

9. Which of the following is an early detection congestion avoidance mechanism that ensures high-precedence traffic has lower loss rates than other traffic during times of congestion?
   - a. CBWFQ
   - b. WRED
   - c. CAR
   - d. GTS
   - e. FRTS

10. The PHB QoS marking for voice-only packets is EF. What is the DSCP equivalent to this marking?
    - a. 32
    - b. 34
    - c. 46
    - d. 48

11. How many QoS queues do Cisco APs provide for downstream traffic being sent to wireless clients?
    - a. 2
    - b. 4
    - c. 8
    - d. 11

12. When it comes to Class-Based Weighted Fair Queuing, what advantage does LLQ offer over CBWFQ without LLQ?
    - a. LLQ provides WFQ based on defined classes for CBWFQ.
    - b. LLQ provides strict priority queueing for CBWFQ.
    - c. The weight for a packet belonging to a specific class is derived from the bandwidth assigned to the class when LLQ is used.
    - d. All packets are serviced fairly based on weight with LLQ.

13. Which of the following statements is true regarding traffic classification and traffic marking?
    - a. Traffic marking can be viewed as an additional action, specified in a policy map, to be taken on a traffic class.
    - b. Traffic classification can be viewed as an additional action, specified in a policy map, to be taken on a traffic class.
    - c. Traffic marking allows you to organize packets into traffic classes on the basis of whether the traffic matches specific criteria.
    - d. After the traffic is organized into traffic classes, traffic classification allows you to mark an attribute for the traffic belonging to that specific class.

14. You can configure class policies for as many classes as are defined on the router, up to what maximum value?

a. 11

b. 16

c. 64

d. 128

Foundation Topics

QoS-Related Issues

Quality of service (QoS) was developed out of necessity. Early networks suffered from bursty data flows due to the rate at which data came into the network. As data packets arrived on the network, they would try to consume as much bandwidth as possible. Access was on a first-come, first-served basis. The data rates available to any one user depended on the number of users accessing the network at that given time. The networking protocols that were developed prior to QoS were intentionally designed to adapt to the bursty nature of the network so that packets being sent could survive bursty traffic and brief outages within the network. The nature of how TCP packets are sent is a great example of the ingenuity behind these earlier protocols. TCP packets require an acknowledgment for each packet sent. If the acknowledgment doesn't come within a given period of time, the TCP transmission will be resent. Email uses TCP. For this reason, an email may come into an inbox seconds after it is sent or several minutes later. The contents of the email are whole and intact, so the delivery time is irrelevant, though the arrival time of the email might be annoying. This type of traffic is referred to as *drop-insensitive data* because lost packets will not prevent the data from eventually transmitting.

Drop-sensitive data is negatively impacted when data packets are lost because the nature of the transmission does not allow for the packets to be resent. Drop-sensitive data is typically in real time, and the nature of UDP packets uses a one-way, one-time send delivery mechanism. It's like a shipping company that delivers a package to your front door when you are not home to receive it. The delivery person's job is to get the package to the door. If it is stolen before you get home, that is not the delivery company's issue. As companies began using the packet-switched network for drop-sensitive data, such as voice and video communications, a more permanent solution had to be developed to contend with the bursty and sporadic nature of the network. Early network engineers faced with these issues would develop and support nonintegrated networks, each designed to carry a specific type of traffic. However, these network setups were very complex, not scalable, and very difficult to support.

Key Topic

The concept of QoS allows for various data traffic types to be carried over a single converged network, and yet each type of traffic can be treated differently. Four factors in a network design can lead to poor audio and video quality. They are bandwidth capacity, latency (delay), jitter, and packet loss. The end goal of QoS is to provide better and more predictable network services by providing dedicated bandwidth, controlled jitter and latency, and improved loss characteristics as required by the business applications. QoS achieves these goals by providing tools for managing network congestion, shaping network traffic, using expensive wide-area links more efficiently, and setting traffic policies across the network.

Latency, Jitter, and Packet Loss

Latency is the delay packets experience when traversing across many different network devices. Jitter is similar to latency in that it is also a delay, but jitter is a variable of the latency that occurs over a period of time. If every packet sent between phone A and phone B took the exact same amount of time to traverse the network, there would be no jitter, but there could still be a delay. When the time between when packets are delivered is different, that time variance is referred to as *jitter*. Jitter can be overcome with buffers, but that will add to the overall latency that occurs. *Packet loss* refers to packets being dropped by the router due to congestion on a link. As mentioned before, TCP packets are drop insensitive because they will be retransmitted if an acknowledgment is not received by the initiating application. By contrast, UDP packets, such as voice and video, will not be retransmitted and are therefore drop sensitive.

Bandwidth

Bandwidth capacity limitations come into play when multiple flows through the router compete for limited bandwidth. QoS is not a substitute for bandwidth, and increasing the available bandwidth will not solve all these problems either. Before bandwidth issues can be resolved, an engineer needs to calculate the bandwidth being consumed across the network. Based on the information covered earlier in this book, calculating bandwidth consumption for voice and video is relatively easy.

To calculate bandwidth requirements for voice-only traffic, an engineer must first identify the codecs being used. Other codecs may be chosen to control or limit bandwidth consumption. Although the actual codec being used is the most important parameter in this assessment, it is still very important to know about packetization and the technologies that will be used. The payload size is comparable to the header size. The more packets being sent and the shorter the packetization time, the more overhead is being consumed. If the G.711 codec, which consumes 64 kbps bandwidth, is being used with a packetization period of 20 ms, and the voice payload is 160 bytes at 50 packets per second, the bandwidth for the call is 87.2 kbps. However, this calculation does not factor in the Layer 2 or Layer 3 overhead. If we take the overhead into account, the total bandwidth being consumed will be even higher. Some QoS tools also affect overhead bandwidth, such as Compressed Real-time Transport Protocol (cRTP) and link fragmentation and interleaving (LFI), but they will be discussed later in this chapter. All packets being equal, there are definitive bit counts to the Layer 2 and Layer 3 headers. Figure 13-1 illustrates the total bandwidth calculations for a G.711 call with Layer 2 and Layer 3 overhead included.

Calculating the bandwidth for a video call is similar to an audio call, except the math required for calculating the overhead is much simpler. First, an engineer must specify the codec being used along with the resolution of the call. These two factors together determine the bandwidth and compression of the video call. The codec alone cannot determine the bandwidth used for a video call, nor can the resolution alone. A user can place a video call at 720p30 using H.263 and will consume 1152 kbps bandwidth. The same call can be placed using the 720p30 resolution and the H.264 codec and consume only 768 kbps bandwidth. However, if the H.264 codec is used for a 480p30 call, the bandwidth required could range anywhere between 256 kbps and 512 kbps.

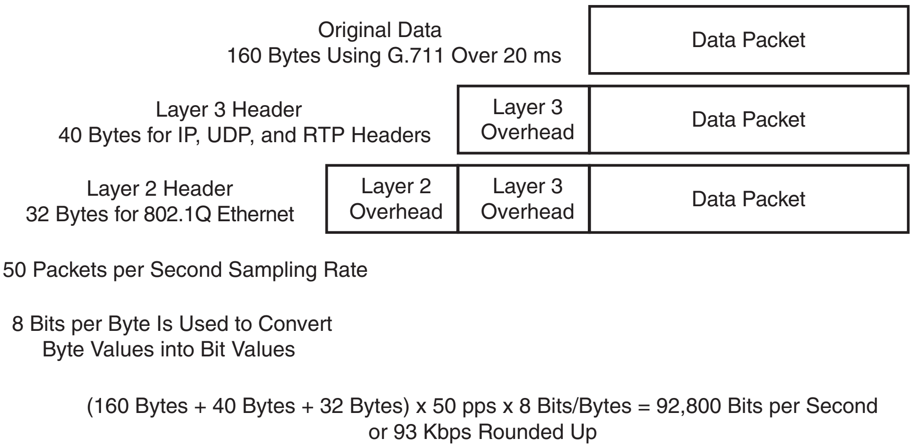

Original Data
160 Bytes Using G.711 Over 20 ms
Data Packet
Layer 3 Header
40 Bytes for IP, UDP, and RTP Headers
Layer 3 Overhead
Data Packet
Layer 2 Header
32 Bytes for 802.1Q Ethernet
Layer 2 Overhead
Layer 3 Overhead
Data Packet
50 Packets per Second Sampling Rate
8 Bits per Byte Is Used to Convert Byte Values into Bit Values
(160 Bytes + 40 Bytes + 32 Bytes) x 50 pps x 8 Bits/Bytes = 92,800 Bits per Second or 93 Kbps Rounded Up

Figure 13-1 *Total Bandwidth Calculations for a Call with Overhead*

Another consideration when calculating bandwidth for a video call is that the total bandwidth allocated for the call is for both audio and video. If you were to place a 384 kbps call using the G.711 codec for audio and H.264 codec for video, 64 kbps would be allocated to audio, leaving 320 kbps for video. In that same call, if G.722 were used at 48 kbps, 336 kbps bandwidth would be available for video.

Once you know the total bandwidth available for the call and the codecs being used for audio and video, you can break down the Layer 2 and Layer 3 headers for audio and video separately and then add the total bandwidth back together. There is an easier way to calculate total bandwidth consumption for video calls. Simply add in 20 percent to the payload bandwidth for overhead. So, a 768 kbps call will consume approximately 922 kbps bandwidth with overhead. A 384 kbps call will consume 460 kbps bandwidth with overhead. You can do the math the long way, but you will find the actual numbers are very close to 20 percent overhead.

Once the bandwidth consumption has been calculated per call, some simple math based on actual call volume will determine the overall bandwidth consumed via voice and video communications. Determining the other limitations within a network will require other assessments of the network itself. A proper QoS design begins with a network audit and a business audit to determine the type of traffic that is running on the network and then determine the QoS requirements for the different types of traffic. Once that has been accomplished, the next step is to group the traffic into classes with similar QoS requirements. The third step occurs at the WAN Aggregation layer: to define QoS policies that will meet the QoS requirements for each traffic class.

Class Models for Provisioning QoS

Businesses should define the strategy and goals for different applications running in their network before deciding on a QoS plan or applying any QoS tools. The number of different traffic classes identified within the company's network should directly correlate to the end-to-end QoS objectives of the business. Three different QoS strategy models can be deployed, depending on the granularity of applications running within a company's network:

- 4/5 Class Model
- 8 Class Model
- QoS Baseline Model (11 Class)

Although the more classes you define, the more specific and granular traffic treatment will be per application, the selection of a certain strategy model must be based on application requirements coupled with the WAN provider QoS model. The following sections provide a detailed view of each of these QoS strategy models.

4/5 Class Model

The 4/5 class model is the simplest of the three models in terms of QoS polices and typically accounts for real-time communications, call signaling, critical data, best-effort data, and scavenger data. The call signaling and critical data are often grouped together as a "mission-critical" category, thus this model is called the 4/5 class model. There could be four or five classes depending on how services are grouped together. The mission-critical class can also be used for multimedia conferencing, multimedia streaming, and bulk data applications. The 4/5 class model is commonly used within small and medium-sized businesses (SMB) that have deployed VoIP telephony. The five traffic classes of QoS markings and guarantees are as follows:

- **Real Time:** Typically voice-only communications. Marked with EF and provisioned to leverage up to 33 percent of link bandwidth.
- **Call Signaling:** Marked with CS3 and provisioned to leverage a minimum of 7 percent of link bandwidth.
- **Critical Data:** Marked with AF31 and provisioned to leverage 35 percent of link bandwidth. When Signaling and Critical Data are combined, CS3 is used across the board.
- **Best Effort Data:** Marked with DF and provisioned to take advantage of 25 percent of link bandwidth.
- **Scavenger:** Marked with CS1 and provisioned to utilize any unused available link bandwidth. The Scavenger class does not have bandwidth directly provisioned, so packets marked CS1 will be sent only if bandwidth is available and will be the first packets to drop during high congestion times.

Voice and signaling guarantees must be selected based on the volume of voice calls and the VoIP codec that is used through the given link. Mission-critical data is selected based on the decision of the director of each company department who has given info about critical business application needs to the networking team. Platform-specific constraints or service-provider constraints may affect the number of classes of service. Businesses should consider a migration strategy to allow the number of classes to be smoothly expanded as future needs arise.

8 Class Model

As needs arise, businesses might need to expand their service groups to the 8 class model, which builds on the 4/5 class model by dividing three of the classes into two more granular classes each. The additions to this model include splitting the Real Time class into two distinct classes: Voice and Video. The Critical Data class is divided into Network Control and Critical Data. The explicitly defined Network Control traffic class is used for applications such as network routing protocol updates or network infrastructure control traffic such as operations, administration, and maintenance (OAM). Finally, the Best Effort class is divided into Bulk Data and Best Effort classes. The recommendations for each traffic class in this model are as follows:

- **Voice:** Marked with EF and limited to 10 percent of link bandwidth in a strict-priority queue.
- **Video:** Marked with AF41 or sometimes as EF and limited to 23 percent of link bandwidth in a strict-priority queue.
- **Call Signaling:** Marked CS3 and provisioned with a minimum of 2 percent of link bandwidth.
- **Network Control:** Marked with CS2 and provisioned with a minimum of 5 percent of link bandwidth.
- **Critical Data:** Marked with AF31 and provisioned with 25 percent of link bandwidth.
- **Bulk Data:** Marked with AF11 and provisioned with 10 percent of link bandwidth with WRED enabled.
- **Best Effort:** Marked with DF and provisioned with 25 percent of link bandwidth.
- **Scavenger:** Marked with CS1 and provisioned to utilize any unused available link bandwidth. The Scavenger class does not have bandwidth directly provisioned, so packets marked CS1 will be sent only if bandwidth is available and will be the first packets to drop during high congestion times.

Although Cisco does recommend configuring call signaling with CS3, some legacy Cisco Unified IP phone products still mark call signaling to AF31. Cisco has been working on a marking migration from AF31 to CS3 with its newer Cisco Unified IP phone models, but some businesses that use older phone models may still want to reserve both AF31 and CS3 for call signaling. In these cases, the critical data applications should be marked to a temporary placeholder nonstandard DSCP, such as 25. After companies migrate their phones to the newer IP phone models, the QoS Baseline marking recommendations of CS3 for call signaling and AF31 for critical data applications should be used.

QoS Baseline Model (11 Class)

Cisco has adopted a new initiative called the *QoS Baseline*. The QoS Baseline is a strategic document designed to unify QoS within Cisco, from enterprise to service provider and from engineering to marketing. The QoS Baseline was written by Cisco's most qualified QoS experts, who have developed or contributed to the related IETF RFC standards and as such are supremely qualified to interpret these standards. The QoS Baseline also provides uniform, standards-based recommendations to help ensure that QoS designs and deployments are unified and consistent. You can see the "QoS Baseline at a Glance" document at the following link: https://www.cisco.com/en/US/technologies/tk543/tk759/technologies_white_paper0900aecd80295a9b.pdf. Several books that go into more detailed information about this model also are available.

The QoS Baseline defines up to 11 classes of traffic that might be viewed as critical to a given enterprise. The 11 class QoS Baseline model builds on the 8 class model, and represents Cisco's interpretation of the RFC 4594 recommendation, which outlines 12 different classes of traffic. The recommendations for each traffic class in this model are as follows:

Key Topic

- **Voice:** Refers to voice only, and it is marked with EF and limited to 10 percent of link bandwidth in a strict-priority queue.
- **Interactive Video:** Refers to voice and video, and it is marked with AF41 or sometimes as EF and limited to 13 percent of link bandwidth.
- **Streaming Video:** Marked with CS4 or sometimes as EF and limited to 10 percent of link bandwidth.
- **Call Signaling:** Marked with CS3 and provisioned with a minimum of 2 percent of link bandwidth.
- **IP Routing:** Marked with CS6 and limited to 3 percent of link bandwidth.
- **Network Management:** Marked with CS2 and provisioned as guaranteed 2 percent of link bandwidth.
- **Mission Critical Data:** Marked with AF31 and provisioned with 15 percent of link bandwidth.
- **Transactional Data:** Marked with AF21 and provisioned with 10 percent of link bandwidth with Weighted Random Early Detection (WRED) enabled.
- **Bulk Data:** Marked with AF11 and provisioned with 10 percent of link bandwidth with WRED enabled.
- **Best Effort Data:** Marked with 0 and provisioned with 25 percent of link bandwidth.
- **Scavenger:** Marked with CS1 and provisioned to utilize any unused available link bandwidth. The Scavenger class does not have bandwidth directly provisioned, so packets marked CS1 will be sent only if bandwidth is available and they will be the first packets to drop during high congestion times.

Enterprises do not need to deploy all 11 classes of the QoS Baseline model. This model is intended to be a forward-looking guide that considers as many classes of traffic with unique QoS requirements as possible. Familiarity with this model can assist in the smooth expansion of QoS policies to support additional applications as future requirements arise. However, at the time of QoS deployment, the enterprise needs to clearly define its organizational objectives, which will correspondingly determine how many traffic classes will be required.

This consideration should be tempered with the determination of how many application classes the networking administration team feels comfortable with deploying and supporting. Platform-specific constraints or service-provider constraints may also affect the number of classes of service. At this point, you should also consider a migration strategy to allow the number of classes to be smoothly expanded as future needs arise. Figure 13-2 illustrates the strategy Cisco recommends for expanding the number of classes of service over time.

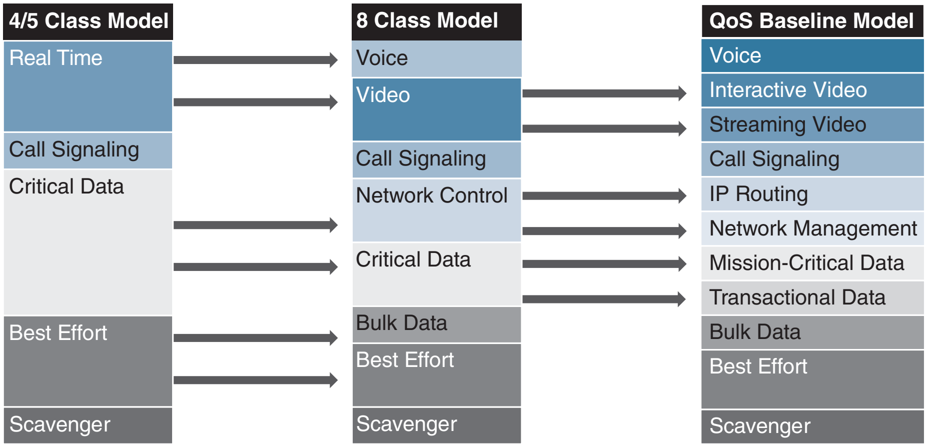


Figure 13-2 *Strategy for Expanding the Number of Classes of Service over Time*

QoS Requirements

Key Topic

After a network has been assessed and a class model for provisioning QoS has been chosen, many layers to a proper QoS solution must still be deployed. As mentioned earlier in this chapter, the end goal of QoS is to provide better and more predictable network services by providing dedicated bandwidth, controlled jitter and latency, and improved loss characteristics as required by the business applications. Therefore, understanding what the voice and video QoS requirements are will help in deploying the other aspects of the QoS solution. The end goal of a properly designed voice and video network solution should be to maintain a delay of less than 150 ms, jitter less than 30 ms, and a packet loss of less than 1 percent.

The first step in designing a QoS solution is to identify and establish the QoS trust boundaries. Then you will need to set up the congestion management and the congestion avoidance. Additional tools that will need to be configured include policing and shaping. Optionally, you might want to also deploy some link efficiency methods. All of these topics will be discussed in depth in this section of the chapter. It is also important to bear in mind that QoS parameters will not be enforced until there is congestion over the network.

QoS Trust Boundaries

Key Topic

When it comes to QoS, it is best practice to mark packets as close to the source as possible. Most devices, such as computers and servers, cannot mark their own packets and should not be trusted even if they can. Cisco phones, however, can mark their own packets and can be trusted with the QoS markings they provide. Therefore, QoS trust boundaries should be set up so that the switch will trust the QoS markings that phones place on their own packets. Layer 2 QoS uses a mechanism called class of service (CoS), which operates on the 802.1Q

VLAN. Unlike Layer 3 QoS mechanisms, CoS does not ensure network performance or guarantee priority in packets being delivered. Therefore, after packets are marked with CoS, they will need to be converted to DSCP using the cos-to-dscp map, which is built into all Cisco switches. By default, QoS on a Cisco access switch is disabled. Once enabled, the switch does not trust QoS settings from a phone. Two simple commands can be entered under the global menu on a switch to enable QoS and change the trust boundary. Once it is enabled, you can use a **show** command to verify these settings. Example 13-1 illustrates the QoS enable and trust boundary commands and the **show** verification command.

Example 13-1 *QoS Enable and Trust Boundary Commands*

```
Switch(config)# mls qos
Switch(config)# interface fastethernet 0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# end
Switch# show mls qos interface fastethernet 0/1
FastEthernet0/1
trust state: trust cos
trust mode: trust cos
cos override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
```

Obviously, this is the simplest design, and there are many other concerns to consider, along with many other settings that can be configured. This example is intended to provide a basic understanding of QoS at the Layer 2 level. For more information on QoS, refer to the “Enterprise QoS Solution Reference Network Design Guide” available at https://community.cisco.com/legacyfs/online/legacy/3/2/6/64623-qossrnd.pdf.

Congestion Management

The WAN presents the greatest potential to be a bottleneck point within an enterprise network. WAN Internet speeds are usually much slower than LAN speeds; however, the network switches use hardware-based buffers, which compared to the interface speed are much smaller than those found on WAN interfaces in routers. This merely increases the potential for even short-lived traffic bursts on the LAN to cause buffer overflow and dropped packets. For these reasons, different QoS tools are available at the WAN than what exist within the LAN; however, all of these tools work together to provide an overall QoS implementation that has been carefully designed. The content that follows examines some of the key concepts to a proper QoS implementation.

Three models of QoS can be implemented in a Cisco network design:

- **Best Effort model:** This model uses no QoS and does not guarantee that packets will be delivered. Obviously, this is not the model most companies would choose to implement.

- **IntServ model:** This model uses RSVP to guarantee predictable behavior on the network for applications that have specific bandwidth and delay requirements.
- **DiffServ model:** This model operates on classes that require special QoS treatment. It is the model that has been discussed up to this point and will continue to be the focus of this dialogue. QoS components used in the DiffServ model include classification, marking, congestion management, congestion avoidance, policing and shaping, and link efficiency.

Classification was discussed previously in the examination of class models. Markings were discussed briefly with class models and Layer 2 CoS marking and Layer 2 to Layer 3 conversion mapping. A detailed explanation of these markings is available later in the section titled "Traffic Classifications."

Congestion management mechanisms use the marking on each packet to determine in which queue to place packets. Different queues are given different treatment by the queueing algorithm that is based on the class of packets in the queue. Generally, queues with high-priority packets receive preferential treatment. The Cisco IOS software for congestion management, or queuing, includes the following queuing methods:

- **First-In First-Out (FIFO):** Performs no prioritization of data packets on user data traffic. It entails no concept of priority or classes of traffic. When FIFO is used, ill-behaved sources can consume available bandwidth, bursty sources can cause delays in time-sensitive or important traffic, and important traffic may be dropped because less important traffic fills the queue.
- **Priority Queue (PQ):** Guarantees strict priority in that it ensures that one type of traffic will be sent, possibly at the expense of all others. For PQ, a low-priority queue can be detrimentally affected, and, in the worst case, never allowed to send its packets if a limited amount of bandwidth is available or if the transmission rate of critical traffic is high.
- **Custom Queuing (CQ):** Guarantees some level of service to all traffic because bandwidth can be allocated to all classes of traffic. You can define the size of the queue by determining its configured packet-count capacity, thereby controlling bandwidth access.
- **Weighted Fair Queuing (WFQ):** Does not require configuration of access lists to determine the preferred traffic on a serial interface. Rather, the fair queue algorithm dynamically sorts traffic into messages that are part of a conversation.
- **Class-Based Weighted Fair Queuing (CBWFQ):** Provides class bandwidth guarantee for user-defined traffic classes. It provides flow-based WFQ support for nonuser-defined traffic classes.
- **Low-Latency Queuing (LLQ):** A congestion management mechanism developed by Cisco to bring strict priority queuing (PQ) to Class-Based Weighted Fair Queuing (CBWFQ). LLQ allows delay-sensitive data, such as voice and video, to be given preferential treatment over other traffic by letting this data be dequeued and sent first.

Congestion Avoidance

Congestion avoidance mechanisms monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Congestion avoidance mechanisms are typically implemented on output interfaces where a high-speed link feeds into a lower-speed link, such as a LAN feeding into a WAN. Weighted Random Early Detection (WRED) is an early detection congestion avoidance mechanism that ensures high-precedence traffic has lower loss rates than other traffic during times of congestion. WRED is not recommended for voice and video queues, and the network should not be designed to drop voice and video packets.

Policing

Policing is used to condition traffic before transmitting or receiving through the network. Policing controls traffic bursts by marking or dropping packets when predefined limits are reached. Policing mechanisms can drop traffic classes that have lower QoS priority markings. Policing tools include class-based policing and committed access rate (CAR). CAR services limit the input or output transmission rate on an interface or subinterface based on a flexible set of criteria.

Shaping

Shaping mechanisms are used on output interfaces to help smooth out mismatches in the network and limit transmission rates. Although these mechanisms are typically used to limit the flow from a high-speed link to a low-speed link, shaping could also be used to manage the flow of traffic at a point in the network where multiple flows are aggregated. Cisco IOS software uses two traffic-shaping tools called Generic Traffic Shaping (GTS) and Frame Relay Traffic Shaping (FRTS) to manage traffic and congestion on the network.

Link Efficiency Methods

Link efficiency methods reduce the overhead that is associated with voice and video transportation. These bandwidth-saving mechanisms, such as compression and link fragmentation and interleaving (LFI), help support large amounts of traffic over a slower link. Compression is one of the link efficiency mechanisms that work in conjunction with queuing and traffic shaping to manage existing bandwidth more efficiently and predictably. Two types of compression are available. Compression of the payload of Layer 2 frames can be implemented using the Stacker or Predictor algorithm. The other compression available is cRTP, which can compress the IP, UDP, and RTP headers down from 40 bytes to 2–4 bytes. Compression should be used only on slow WAN links because the drawback is the consumption of computational resources on a hop-by-hop basis. Another link efficiency method is link fragmentation and interleaving. Interactive traffic, such as voice and video, is susceptible to increased latency and jitter when the network processes large packets. This susceptibility increases as the traffic is queued on slower links. LFI can reduce delay and jitter on slower-speed links by breaking up large data packets and interleaving low-delay traffic packets with the resulting smaller packets. LFI is typically used on slow WAN links to ensure minimal delay for voice and video traffic. Figure 13-3 summarizes all of the QoS components needed for an efficient network deployment.

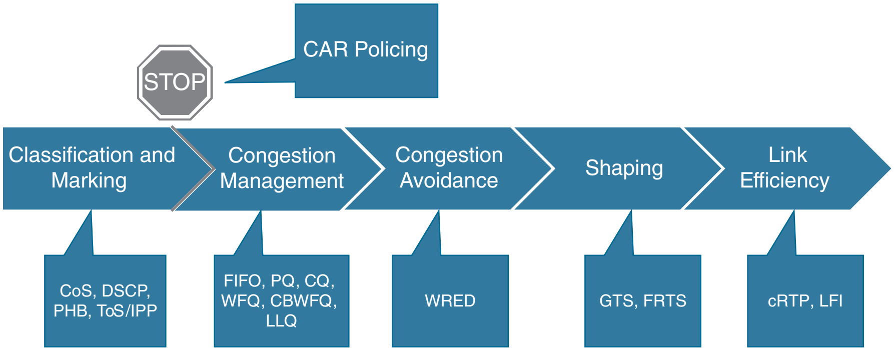


Figure 13-3 *QoS Components*

Traffic Classifications

QoS classification initially takes place in the Access layer; however, other QoS tools are needed to ensure voice and video quality is maintained throughout the network. In addition to traffic classification, queuing and bandwidth provisioning also ensure voice and video quality.

LAN and WAN Traffic Classifications

As mentioned previously, Layer 2 classification uses CoS markings for packets at the Access layer. The Distribution and Core layers use the existing CoS markings to map QoS to Layer 3 classifications. These Layer 3 classifications include differentiated services code point (DSCP), per hop behavior (PHB), and type of service (ToS) or IP Precedence (IPP). Table 13-2 summarizes each of these classifications and how they map to one another for different applications.

Key Topic

Table 13-2 Traffic Classification Map

Application	Layer 3 Classification			Layer 2 Classification
	ToS/IPP	PHB	DSCP	CoS
Routing	6	CS6	48	6
Voice Only	5	EF	46	5
Voice/Video	4	AF41	34	4
Telepresence Video	4	CS4	32	4
Streaming Video	3	CS4	32	3
Call Signaling	3	CS3	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Scavenger	1	CS1	8	1
Best Effort	0	0	0	0

In Table 13-2, voice only and voice with video traffic are separated into two different categories. The reason for this is so that when a video call is placed, both voice and video packets reach the destination at roughly the same time. There is no support for lip synchronization in SIP, so this will help preserve lip-syncing during the call. Also, when a video call is placed, the expectation is that both the voice and video media will share the same quality during the call. These reasons are why Cisco recommends deploying QoS in this manner. Notice, however, that this table is slightly different from the QoS Baseline model, although there are 11 classes in both design models. Table 13-2 provides a classification for Voice/Video and another for Telepresence Video. Cisco offers different endpoints that will utilize different QoS classifications based on type. Based on Cisco's current endpoint portfolio, the Voice/Video applications include the 8845, 8865, and Jabber client endpoints. If you have a DX endpoint running the legacy Android software, it would fall under this category too. The Telepresence Video applications include all endpoints running CE or CTS software, including the DX, MX, SX, IX, and Webex endpoints.

After packets have been classified for Layer 2 and Layer 3, the next step is to queue traffic based on the classification. Transmit interface buffers within a campus tend to congest in small, finite intervals as a result of the bursty nature of network traffic. When this congestion occurs, any packets destined for that transmit interface are dropped. The only way to prevent dropped voice traffic is to configure multiple queues on campus switches. By enabling multiple queues on campus switches, you can configure all voice traffic to use separate queues, thus virtually eliminating the possibility of dropped voice packets when an interface buffer fills instantaneously. For this reason, Cisco recommends always using a switch that has at least two output queues on each port and the ability to send packets to these queues based on QoS Layer 2 or Layer 3 classification. The majority of Cisco Catalyst switches support two or more output queues per port.

WLAN Traffic Classifications

Just as QoS is necessary for the LAN and WAN wired network infrastructure in order to ensure high voice and video quality, QoS is also required for the wireless LAN infrastructure. Because of the bursty nature of data traffic and the fact that real-time traffic such as voice and video are sensitive to packet loss and delay, QoS tools are required to manage wireless LAN buffers; limit radio contention; and minimize packet loss, delay, and delay variation. Unlike most wired networks, however, wireless networks are a shared medium, and wireless endpoints do not have dedicated bandwidth for sending and receiving traffic. While wireless endpoints can mark traffic with 802.1p CoS, ToS, DSCP, and PHB, the shared nature of the wireless network means limited admission control and access to the network for these endpoints.

As with the wired network infrastructure, it is important to classify or mark pertinent wireless traffic as close to the edge of the network as possible. Because traffic marking is an entrance criterion for queuing schemes throughout the wired and wireless network, marking should be done at the wireless endpoint device whenever possible. Marking or classification by wireless network devices should be identical to that for wired network devices. In accordance with traffic classification guidelines for wired networks, the Cisco wireless endpoints mark voice media traffic or voice RTP traffic with DSCP 46 (or PHB EF), video media traffic or video RTP traffic with DSCP 34 (or PHB AF41), and call control signaling traffic (SCCP or SIP) with DSCP 24 (or PHB CS3). Once this traffic is marked, it can be given priority of better than best-effort treatment and queuing throughout the network. All wireless voice and video devices that are capable of marking traffic should do so in this manner. All other traffic on the wireless network should be marked as best-effort or with some intermediary classification as outlined in wired network marking guidelines. If the wireless voice or video devices are unable to do packet marking, alternate methods such as port-based marking should be implemented to provide priority to video and voice traffic.

While 802.1p and differentiated services code point (DSCP) are the standards to set priorities on wired networks, 802.11e is the standard used for wireless networks. This is commonly referred as user priority (UP), and it is important to map the UP to its appropriate DSCP value. Table 13-3 compares the 802.11e QoS values compared to wired QoS values.

Table 13-3 QoS Value Comparison with 802.11e

Traffic Type	DSCP (PHB)	802.1p UP	802.11e UP
Voice	46 (EF)	5	6
Video	34 (AF41)	4	5
Voice and Video Signaling	24 (CS3)	3	4

After traffic marking has occurred, it is necessary to enable the wired network access points (APs) and devices to provide QoS queuing so that voice and video traffic types are given separate queues to reduce the chances of this traffic being dropped or delayed as it traverses the wireless LAN. Queuing on the wireless network occurs in two directions: upstream and downstream. Upstream queuing concerns traffic traveling from the wireless endpoint up to the AP, and from the AP up to the wired network. Downstream queuing concerns traffic traveling from the wired network to the AP and down to the wireless endpoint.

For upstream queuing, devices that support Wi-Fi Multimedia (WMM) are able to take advantage of queueing mechanisms, including priority queueing. As for downstream QoS, Cisco APs currently provide up to eight queues for downstream traffic being sent to wireless clients. The entrance criterion for these queues can be based on a number of factors, including DSCP, access control lists (ACLs), and VLAN. Although eight queues are available, Cisco recommends using only two queues when deploying wireless voice. All voice media and signaling traffic should be placed in the highest-priority queue, and all other traffic should be placed in the best-effort queue. This ensures the best possible queuing treatment for voice traffic.

To set up this two-queue configuration for autonomous APs, you can create two QoS policies on the AP. Name one policy Voice and configure it with the class of service *Voice < 10 ms Latency (6)* as the Default Classification for all packets on the VLAN. Name the other policy Data and configure it with the class of service *Best Effort (0)* as the Default Classification for all packets on the VLAN. Then assign the Data policy to the incoming and outgoing radio interface for the data VLAN(s) and assign the Voice policy to the incoming and outgoing radio interfaces for the voice VLAN(s). With the QoS policies applied at the VLAN level, the AP is not forced to examine every packet coming in or going out to determine the type of queuing the packet should receive.

For lightweight APs, the WLAN controller has built-in QoS profiles that can provide the same queuing policy. Voice VLAN or voice traffic is configured to use the Platinum policy, which sets priority queueing for the voice queue. Data VLAN or data traffic is configured to use the Silver policy, which sets best-effort queuing for the Data queue. These policies are then assigned to the incoming and outgoing radio interfaces based on the VLAN. The preceding configurations ensure that all voice and video media and signaling are given priority queuing treatment in a downstream direction.

To avoid exceeding the capacity limit of a given AP channel, some form of call admission control is required. Cisco APs and wireless Unified Communications clients now use Traffic Specification (TSPEC) instead of QoS Basic Service Set (QBSS) for call admission control. Wi-Fi Multimedia Traffic Specification (WMM TSPEC) is the QoS mechanism that enables WLAN clients to provide an indication of their bandwidth and QoS requirements so that APs can react to those requirements. When a client is preparing to make a call, it sends an Add Traffic Stream (ADDTS) message to the AP with which it is associated, indicating the TSPEC. The AP can then accept or reject the ADDTS request based on whether bandwidth and priority treatment are available. If the call is rejected, the client receives a Network Busy message. If the client is roaming, the TSPEC request is embedded in the reassociation request message to the new AP as part of the association process, and the TSPEC response is embedded in the reassociation response. Alternatively, endpoints without WMM TSPEC support, but using SIP as call signaling, can be managed by the AP. Media snooping must be enabled for the Service Set Identifier (SSID). The client's implementation of SIP must match that of the wireless LAN controller, including encryption and port numbers.

Configure and Verify LLQ

Without LLQ, CBWFQ provides WFQ based on defined classes with no strict priority queue available for real-time traffic. CBWFQ allows you to define traffic classes and then assign characteristics to that class, such as designating the minimum bandwidth delivered to the class during congestion. For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth you assigned to the class when you configured it. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight; no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.

LLQ provides strict priority queueing for CBWFQ, reducing jitter in voice conversations. Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued. Configured by the **priority** command, LLQ enables use of a single, strict priority queue within CBWFQ at the class level, allowing you to direct traffic belonging to a class to the CBWFQ strict priority queue. To enqueue class traffic to the strict priority queue, you specify the named class within a policy map and then configure the **priority** command for the class. (Classes to which the **priority** command is applied are considered priority classes.) Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is enqueued to the same, single, strict priority queue.

One of the ways in which the strict PQ used within CBWFQ differs from its use outside CBWFQ is in the parameters it takes. Outside CBWFQ, you can use the **ip rtp priority** command to specify the range of UDP ports whose voice traffic flows are to be given priority service. Using the **priority** command, you are no longer limited to a UDP port number to stipulate priority flows because you can configure the priority status for a class within

CBWFQ. Instead, all of the valid match criteria used to specify traffic for a class now apply to priority traffic. These methods of specifying traffic for a class include matching on access lists, protocols, and input interfaces. Moreover, within an access list, you can specify that traffic matches are allowed based on the IP differentiated services code point (DSCP) value that is set using the first six bits of the ToS byte in the IP header.

Although it is possible to enqueue various types of real-time traffic to the strict priority queue, Cisco strongly recommends that you direct only voice traffic to it because voice traffic is well behaved, whereas other types of real-time traffic are not. Moreover, voice traffic requires that delay be nonvariable in order to avoid jitter. Real-time traffic such as video could introduce variation in delay, thereby thwarting the steadiness of delay required for successful voice traffic transmission.

To configure network traffic marking, you use the modular quality of service (QoS) command-line interface (CLI), also referred to as MQC. The MQC is a CLI structure that allows you to complete the following tasks:

1. Specify the matching criteria used to define a traffic class.
2. Create a traffic policy (policy map). The traffic policy defines the QoS policy actions to be taken for each traffic class.
3. Apply the policy actions specified in the policy map to an interface, subinterface, or ATM PVC by using the **service-policy** command.

Figure 13-4 illustrates the process used to configure QoS within a Cisco environment.

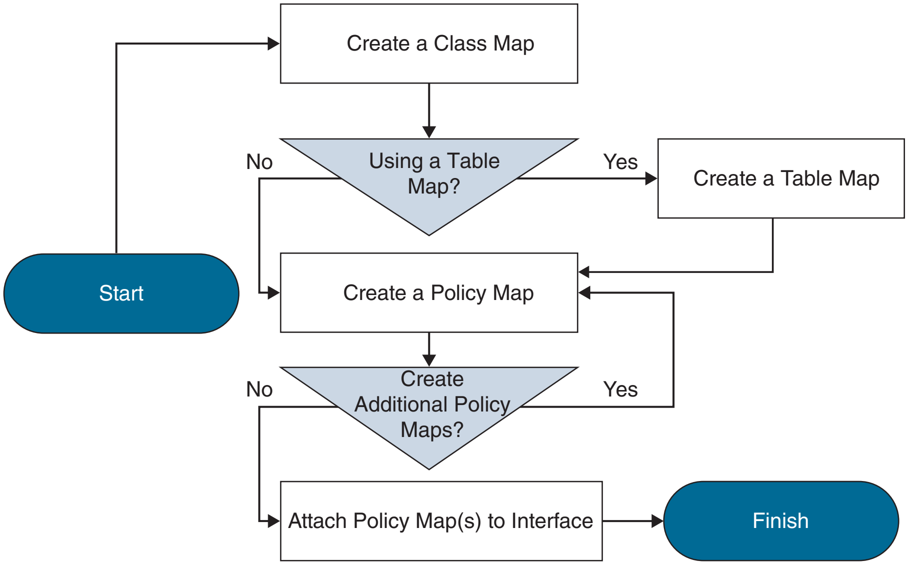


Figure 13-4 *QoS Configuration Process*

Class Map

Traffic classification and traffic marking are closely related and can be used together. Traffic marking can be viewed as an additional action, specified in a policy map, to be taken on a traffic class. Traffic classification allows you to organize packets into traffic classes on the basis of whether the traffic matches specific criteria. For example, all traffic with a CoS value of 2 is grouped into one class, and traffic with DSCP value of 3 is grouped into another class. The match criterion is user defined.

After the traffic is organized into traffic classes, traffic marking allows you to mark an attribute for the traffic belonging to that specific class. For instance, you may want to change the CoS value from 2 to 1, or you may want to change the DSCP value from 3 to 2. The match criteria used by traffic classification are specified by configuring a match command in a class map. The marking action taken by traffic marking is specified by configuring a set command in a policy map. These class maps and policy maps are configured using the MQC.

The following commands explain how to create a class map to define traffic classes. Within the class map, the appropriate match command is used to specify the matching criteria for the traffic classes. To create the class map and specify the matching criteria, complete the following steps:

```
Router> enable

Router# configure terminal

Router(Config)# class-map class-map-name
```

From this point, you can use a few options available within the class map to establish the search criterion against which packets are checked to determine if they belong to the class. Table 13-4 identifies four of these criteria.

Table 13-4 Four Criterion Matches for Packet Classification

MQC Command	Description
Router(config-cmap)# **match access-group** *access-group-name*	Specifies the name of the access control list (ACL) against whose contents packets are checked to determine if they belong to the class.
Router(config-cmap)# **match input-interface** *interface-name*	Specifies the name of the input interface used as a match criterion against which packets are checked to determine if they belong to the class.
Router(config-cmap)# **match protocol** *protocol*	Specifies the name of the protocol used as a match criterion against which packets are checked to determine if they belong to the class.
Router(config-cmap)# **match fr-dlci** *dlci-number*	Specifies the Frame Relay DLCI number as a match criterion against which packets are checked to determine if they belong to the class.

Policy Map

As previously mentioned, creating a table map is not required unless the desired outcome is to change some of the CoS or DSCP values. The table map contains the mapping scheme used for establishing the to-from relationship and equivalency between one traffic-marking value and another. The table map can be configured for use with multiple policy maps. The policy maps can then be configured to convert and propagate the traffic-marking values defined in the table map. Then the policy maps can be attached to the input or output interface of either the ingress or egress router, as appropriate, to serve the QoS requirements of your network. To create and configure the table map, enter the following MQC commands:

```
Router> enable

Router# configure terminal

Router# table-map name map from from-value to to-value
[default default-action-or-value]
```

To configure a policy map and create class policies that make up the service policy, begin with the **policy-map** command to specify the policy map name. Then use one or more of the following commands to configure the policy for a standard class or the default class:

- **priority**
- **bandwidth**
- **queue-limit** or **random-detect**
- **fair-queue** (for class-default class only)

For each class that you define, you can use one or more of the commands listed to configure the class policy. For example, you might specify bandwidth for one class and both bandwidth and queue limit for another class. The default class of the policy map, commonly known as the class-default class, is the class to which traffic is directed if that traffic does not satisfy the match criteria of the other classes defined in the policy map.

You can configure class policies for as many classes as are defined on the router, up to the maximum of 64. However, the total amount of bandwidth allocated for all classes in a policy map must not exceed the minimum committed information rate (CIR) configured for the virtual circuit (VC) minus any bandwidth reserved by the **frame-relay voice bandwidth** and **frame-relay ip rtp priority** commands. If the minimum CIR is not configured, the bandwidth defaults to one-half of the CIR. If all of the bandwidth is not allocated, the remaining bandwidth is allocated proportionally among the classes on the basis of their configured bandwidth.

Key Topic

The following commands describe how to create and configure a policy map to use the class map and the table map. The policy map applies the appropriate QoS feature to the network traffic based on the traffic classification. To configure class policies in a policy map, use the MQC commands described in the following sections.

```
Router> enable

Router# configure terminal

Router(Config)# policy-map name

Router(Config-pmap)# class {class-name | class-default}

Router(Config-pmap-c)# set cos cos-value
```

or

```
Router(Config-pmap-c)# set cos dscp table name
```

The **policy-map** *name* command creates a policy map by the name provided and enters the policy-map configuration mode. The **class** command specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier. You can either enter the name of the class created earlier or enter the **class-default** keyword. The **class-default** class is used to classify traffic that does not fall into one of the defined classes. Even though the class-default class is predefined when you create the policy map, you still have to configure it. If a default class is not configured, then traffic that does not match any of the configured classes is given best-effort treatment, which means that the network will deliver the traffic if it can, without any assurance of reliability, delay prevention, or throughput. The **set cos** command and **set cos dscp table** *name* commands are examples of the **set** commands that can be used when marking traffic. Other **set** commands can be used as well. For a list of other **set** commands, refer to the "Cisco IOS Quality of Service Solutions Configuration Guide" at Cisco.com.

Other class policies can be configured here as well. To configure a class policy for a priority queue, enter the following command:

```
Router (config-pmap-c)# priority bandwidth in kbps
```

This command creates a strict priority class and specifies the amount of bandwidth in kbps to be assigned to the class.

To configure a class policy using a specified bandwidth, enter the following command:

```
Router (config-pmap-c)# bandwidth bandwidth in kbps
```

This command specifies the amount of bandwidth to be assigned to the class in kbps, or as a percentage of the available bandwidth. Bandwidth must be specified in kbps or as a percentage consistently across classes. Bandwidth of the priority queue must be specified in kbps.

To configure a class policy that specifies a number of queues, enter the following command:

```
Router (config-pmap-c)# fair-queue number-of-dynamic-queues
```

This command specifies the number of dynamic queues to be reserved for use by flow-based WFQ running on the default class. The number of dynamic queues is derived from the bandwidth of the interface.

You can create and configure as many policy maps as you need for your network. To create and configure additional policy maps, repeat the preceding commands per your network deployment plan. After all the policy maps have been created, they will need to be attached to the appropriate interface. The next section on service policy will explain how to attach the policy maps to the interfaces.

Service Policy

Key Topic

After you create the policy map, you must attach it to an interface. Policy maps can be attached to either the input or output direction of the interface. Depending on the needs of your network, you can attach policy maps to an interface, a subinterface, or an ATM permanent virtual circuit (PVC). To attach the policy map, enter the following commands in the MQC:

```
Router> enable

Router# configure terminal
```

```
Router(Config)# interface type number [name-tag]

Router(Config-if)# service-policy {input | output} policy-map-
name
```

This last command is the key. It attaches the specified service policy map to the output interface and enables LLQ, assuming LLQ has been configured throughout this process. Next, all these QoS settings will need to be verified.

Verify and Monitor LLQ Settings

After the QoS designs have been finalized and the proof of concept tested, it is vital to ensure that the networking team thoroughly understand the QoS features and syntax before enabling features on production networks. Such knowledge is critical for both rollout and subsequent troubleshooting of QoS-related issues. Furthermore, it is recommended to schedule network downtime in order to roll out QoS features. While QoS is required end-to-end, it does not have to be deployed end-to-end at a single instance. A pilot network-segment can be selected for an initial deployment, and pending observation, the rollout can be expanded in stages to encompass the entire enterprise. A rollback strategy is always recommended, to address unexpected issues arising from the QoS deployment.

From the Privileged Exec Mode on the router, you can use several **show** commands to verify that all the QoS settings have been configured correctly. Table 13-5 illustrates these **show** commands with a description of what information each command displays.

Key Topic

Table 13-5 IOS Router Show Commands for QoS

Command	Description
Router# **show policy-map**	Displays all configured policy maps.
Router# **show policy-map** *policy-map* **class** *class-name*	Displays the configuration for the specified class of the specified policy map. Enter the policy map name and the class name.
Router# **show frame-relay pvc dlci**	Displays statistics about the PVC and the configuration of classes for the policy map on the specified data-link connection identifier (DLCI).
Router# **show policy-map interface** *interface-name*	When LLQ is configured, displays the configuration of classes for all policy maps.
Router# **show policy-map interface** *interface-name* **dlci**	When LLQ is configured, displays the configuration of classes for the policy map on the specified DLCI.
Router# **show policy-map interface** *interface-name*	Displays traffic statistics of all classes configured for all service policies on the specified interface, subinterface, or PVC on the interface. When a policy map has multiple instances of the same class, and this policy map is attached to an interface, the following command returns only the first instance: **show policy-map interface** *interface_name* **output class** *class-name*

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 13-6 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 13-6 Key Topics for Chapter 13

Key Topic Element	Description	Page Number
Paragraph	Four Factors Requiring QoS	309
Section	Latency, Jitter, and Packet Loss	310
Paragraph	Calculating Bandwidth for Voice Packets	310
Paragraph	Calculating Bandwidth for Video Calls	311
List	Three QoS Strategy Models	312
List	Five Traffic Classes of QoS Markings	312
List	Eight Traffic Classes of QoS Markings	313
List	Eleven Traffic Classes of QoS Markings	314
Paragraph	End goal of a properly designed QoS deployment for voice and video	315
Paragraph	COS and Trust Boundaries	315
List	Three models of QoS	316
Table 13-2	Traffic Classification Map	319
Paragraph	802.11e Explained	321
Table 13-3	QoS Value Comparison with 802.11e	321
Paragraph	Upstream and Downstream Queueing for Wireless Networks	321
Commands	Commands to Create a Class Map	324
Table 13-4	Four Criterion for Packet Classification	324
Commands	Commands to Create a Table Map	324
Commands	Commands to Configure Class Policies in a Policy Map	325
Commands	Commands to Attach a Policy Map to an Interface	326
Table 13-5	IOS Router Show Commands for QoS	327

Define Key Terms

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

802.11e, ADDTS, CAR, CBWFQ, Compression, Congestion Avoidance, Congestion Management, CoS, CQ, cRTP, DiffServ, DSCP, FIFO, FRTS, GTS, IntServ, IPP, Jitter, Latency, LFI, Link Efficiency, LLQ, OAM, Packet Loss, PHB, Policing, PQ, PVC, Shaping, SSID, Stacker, ToS, TSPEC, WFQ, WMM TSPEC, WRED

Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. It might not be necessary to memorize the complete syntax of every command, but you should be able to remember the basic keywords that are needed.

To test your memory of the commands, cover the left side of Tables 13-7 through 13-8 with a piece of paper, read the description on the right side, and then see how much of the command you can remember.

The 350-801 exam focuses on practical, hands-on skills that are used by a networking professional. Therefore, you should be able to identify the commands needed to configure and test QoS.

Table 13-7 Layer 2 QoS Commands

Command Syntax	Task
Switch(config)# **mls qos**	Enables QoS on the Layer 2 switch and CoS to DSCP mapping.
Switch(config-if)# **mls qos trust cos**	Establishes a trust boundary between a phone and the switch for QoS. Must be enabled on the actual switchport.
Switch# **show mls qos interface fastethernet 0/1**	Reveals that QoS has been enabled and a QoS trust boundary has been set up.

Table 13-8 Layer 3 QoS Commands

Command Syntax	Task
Router(Config)# **class-map** *class-map-name*	Creates a class map to be used for matching traffic to a specified class and enters class-map configuration mode. The class map name must be specified after the **class-map** command.
Router(config-cmap)# **match access-group** *access-group-name*	Specifies the name of the access control list (ACL) against whose contents packets are checked to determine if they belong to the class.
Router(config-cmap)# **match input-interface** *interface-name*	Specifies the name of the input interface used as a match criterion against which packets are checked to determine if they belong to the class.
Router(config-cmap)# **match protocol** *protocol*	Specifies the name of the protocol used as a match criterion against which packets are checked to determine if they belong to the class.
Router(config-cmap)# **match fr-dlci** *dlci number*	Specifies the Frame Relay DLCI number as a match criterion against which packets are checked to determine if they belong to the class.

Command Syntax	Task
Router(Config)# **table-map** *name* **map from** *from-value* **to** *to-value* [**default** *default-action-or-value*]	Creates a table map using the specified name and enters table-map configuration mode. Enter the name of the table map you want to create. Enter each value mapping on a separate line. Enter as many separate lines as needed for the values you want to map. The **default** keyword and *default-action-or-value* argument set the default value (or action) to be used if a value is not explicitly designated.
Router(config)# **policy-map** *name*	Specifies the name of the policy map created earlier and enters policy-map configuration mode. The policy map name must be entered with this command.
Router(config-pmap)# **class** *name*	Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier. Enter the name of the class or enter the **class-default** keyword.
Router(config-pmap)# **class class-default** *name*	Specifies the default class so that you can configure or modify its policy.
Router(config-pmap-c)# **set cos** *cos-value*	(Optional) Sets the CoS value in the type of service (ToS) byte.
Router(config-pmap-c)# **set cos dscp table** *name*	(Optional) If a table map was created earlier, sets the CoS value based on the DSCP value (or action) defined in the table map.
Router(config-pmap-c)# **priority** *bandwidth in kbps*	Creates a strict priority class and specifies the amount of bandwidth, in kbps, to be assigned to the class.
Router (config-pmap-c)# **bandwidth** *bandwidth in kbps*	Specifies the amount of bandwidth to be assigned to the class, in kbps, or as a percentage of the available bandwidth. Bandwidth must be specified in kbps or as a percentage consistently across classes. Bandwidth of the priority queue must be specified in kbps.
Router (config-pmap-c)# **fair-queue** *number-of-dynamic-queues*	This command specifies the number of dynamic queues to be reserved for use by flow-based WFQ running on the default class. The number of dynamic queues is derived from the bandwidth of the interface.
Router(Config-if)# **service-policy** {**input** | **output**} *policy-map-name*	Attaches the specified service policy map to the output interface and enables LLQ.

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Name the four factors in a network design that can lead to poor audio and video quality.
2. List the 11 classes in the QoS Baseline model.
3. The end goal of a properly designed voice and video network solution should be to maintain what parameters for delay, jitter, and packet loss?
4. Outline the QoS mapping for 802.11e User Priority to Layer 2 802.1p and Layer 3 DSCP for Voice, Video, and Signaling.
5. List all of the commands, from the switch to the router, required for a QoS deployment. Do not include optional commands.

CHAPTER 14

DNS, NTP, and SNMP

This chapter covers the following topics:

DNS Settings: This topic will explain various DNS settings that need to be configured to support a Cisco collaboration solution, including A-records, SRV records, and PTRs.

NTP Settings: This topic will explain the dependency between Cisco Unified Communications Manager and NTP.

SNMP Settings: This topic will discuss other unified communications components that use SNMP for collecting and organizing information from various devices within the UC environment.

This chapter will look at some of the network-related components that can impact the Cisco Unified Communications environment. Although the Cisco Unified Communications Manager can operate without a Domain Name System (DNS), many services cannot function without DNS in place. The Cisco Unified Communications Manager cannot function at all without Network Time Protocol (NTP), but the level of strata can influence the effectiveness of the Cisco Unified Communications Manager. Other services that can enhance the user experience in a Cisco Unified Communications Manager environment have a dependency on the Simple Network Management Protocol. These topics are all addressed in this chapter in the following sections:

- DNS Settings
  - A/AAAA Records
  - SRV Records
  - Reverse Pointer Record (PTR)
- NTP Settings
- SNMP Settings

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 1.5 Explain these components to support Cisco Collaboration solutions
  - 1.5.a SNMP
  - 1.5.b DNS

“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
DNS Settings	1–4
NTP Settings	5
SNMP Settings	6

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 is a disadvantage to not using DNS in a Cisco Unified Communications Manager environment?
   - a. If you lose the connection with DNS, you lose the connection to the server.
   - b. Domain verification certificates cannot be used.
   - c. Management of the network is simplified.
   - d. NAT services do not work without DNS.
2. Which of the following statements best describes an AAAA-record?
   - a. AAAA-records allow four different IP addresses to resolve to the same domain.
   - b. AAAA-records allow a single IP address to resolve to four domains.
   - c. AAAA-records allow 32-bit IP addresses to resolve to a domain.
   - d. AAAA-records allow 128-bit IP addresses to resolve to a domain.
3. Which of the following SRV records is used for the Cisco Unified Communications Manager?
   - a. _sips._tcp.fqdn. 7200 10 10 5061 cucm.fqdn
   - b. _sip._tcp.fqdn. 7200 10 10 5060 cucm.fqdn
   - c. _cisco-uds._tcp.fqdn. 7200 10 10 8443 cucm.fqdn
   - d. _cucmlogin._tcp.fqdn. 7200 10 10 8443 cucm.fqdn

4. When manually configuring an RPT, what should you do first as an administrator after logging in to the DNS server and pulling up the menu?
   a. Click the New Pointer (PTR) menu option.
   b. Right-click the domain you want to create the PTR under and select New Pointer (PTR).
   c. Right-click the reverse lookup zone you want to create the PTR under and select New Pointer (PTR).
   d. Right-click the domain you want to create the PTR under and select Other New Record.
5. What stratum level does Cisco recommend using when installing a Cisco Unified Communications Manager Publisher?
   a. Stratum 1
   b. Stratum 3
   c. Stratum 4
   d. Stratum 9
6. Which of the following devices does not use SNMP to collect information from other devices?
   a. Cisco Unified Communications Manager
   b. Cisco Emergency Responder
   c. Cisco Paging Server
   d. Cisco Unified CVP

Foundation Topics

DNS Settings

There is much to be said about the Domain Name System (DNS), the different record types that can be used, and the different settings for each record type. Entire books have been dedicated to the extent of capabilities within DNS, which can be referenced for more information. I recommend *DNS Bind* as a reference resource that should exist in every IT engineer's library. This chapter will not go into the same detail as *DNS Bind* concerning DNS settings, but a basic explanation of A-records, SRV records, and reverse proxy settings is warranted.

Cisco collaboration products, such as the Cisco Unified Communications Manager, can use IP addresses or names to refer to other IP devices in application settings. When names are used, DNS needs to resolve them to IP addresses. Both methods have some advantages and disadvantages.

When using IP addresses, the systems do not depend on a DNS server, which can prevent loss of service when the DNS server cannot be reached. When a device initiates a connection to a server for the first time, the time that is required to establish the connection is shorter because a DNS query—a DNS lookup sent to the DNS server followed by a DNS reply sent back from the server—is not required. When the need for DNS is eliminated, there is no danger of errors that are caused by DNS misconfiguration. Troubleshooting is simplified because there is no need to verify proper name resolution. A big disadvantage is related to certificate security. Many certificates used in the Cisco collaboration solution require domain verification, which in turn requires DNS. This codependency between the certificate server and DNS might require using DNS in your environment.

When DNS is used in the Cisco collaboration solution, management is simplified because logical names are simpler to manage than 32-bit addresses. If IP addresses change, there is no need to modify the application settings because they can still use the same names; only the DNS server configuration has to be modified in this case. IP addresses of Cisco Unified Communications Manager servers can be translated toward IP phones because the IP phone configuration files include server names, not the original server IP address, which should appear differently to the IP phone. As long as these names are resolved to the correct IP address when Cisco Unified IP phones send out DNS requests, the NAT is no problem. Also, most IP clients cache the IP address information that is received from the DNS servers to avoid subsequent name resolution requests for the same name. Although DNS provides an additional point of failure caused by configuration errors or unavailability of the service, Cisco recommends using DNS within the Cisco collaboration solution. This is due to the increased use of certificates for secure communication across networked devices.

By default, the Cisco Unified Communications Manager propagates the machine name and not the IP addresses of its active *Cisco CallManager Services*. These host names are part of TFTP configuration files for devices such as IP phones. DNS reliance refers to the requirement for IP phones to use DNS servers to resolve host names of Cisco CallManager Services. Some situations might require administrators to remove DNS reliance from the Cisco Unified Communications Manager. To remove DNS reliance, navigate to **System > Server** in Cisco Unified CM Administration, choose each available server from the list, and change the server name to the IP address. By default, host names are also used in phone URLs. When DNS reliance is removed, host names that are used in these phone URLs must also be replaced by IP addresses. Phone URLs are configured by using enterprise parameters. Enterprise parameters and their configuration will be explained in Chapter 15, “Cisco Unified Communications Manager Setup.”

A/AAAA-Records

Key Topic

An A-record in DNS is a type of lookup record that resolves 32-bit IPv4 addresses to URLs. A Uniform Resource Locator, or URL, is a string of numbers, characters, or letters that identifies a resource. URLs are more commonly known as website addresses. If a user were to put the URL www.cisco.com into a web browser, DNS would resolve this URL to an IPv4 address. The web browser could now forward the query on to the resource at that associated IP address. A-records in DNS contain a host, domain, URL, and an IP address. The URL is the host and domain together. DNS will create the URL field automatically. A sample A-record may look something like this:

Host	Domain	URL	IP Address
cucm_pub	*cisco.com*	*cucm_pub.cisco.com*	*10.1.1.40*

Similar to A-records, AAAA-records resolve 128-bit IPv6 addresses to URLs. This should be easy to remember because this record type has four *A*s. If each *A* represents 32 bits, then 32 times 4 equals 128, and IPv6 addresses are 128 bits in length. When DNS is used for B2B communications over IP, whether A-records, AAAA-records, or both are used, a public

DNS should be configured with a registered domain. The URL should resolve to a public IP address assigned to the Expressway-E or CUBE, so that incoming calls can be routed to that server.

Different companies offer different DNS software, and the menus to set up these services might be quite different; however, the DNS settings within each software offering are the same, as previously mentioned. The most common DNS used among businesses is the Microsoft Windows Server DNS services. To configure a DNS A-record using the Microsoft DNS, follow these steps:

Step 1. Log in to the Windows Server hosting the DNS services, and open the DNS application.

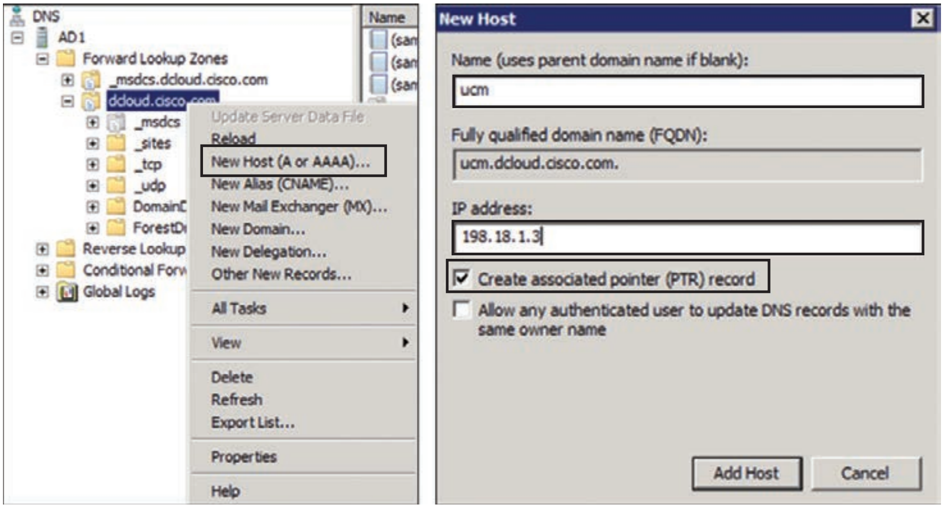
Step 2. Right-click the domain you wish to create the A-record under, and select **New Host (A or AAAA)...** from the menu that appears.

Step 3. When the New Host window pops up, enter the host name of the URL in the Name (Uses Parent Domain Name if Blank): field. The Fully Qualified Domain Name (FQDN): field will autopopulate as the host name is being typed.

Step 4. Enter the IP address of the server for which the record is being created. This will be the IPv4 address for A-records or the IPv6 address for AAAA-records.

Step 5. (optional) You can check the box beside the **Create Associated Pointer (PTR) Record** if you want DNS to automatically create a reverse DNS record for this server. This topic will be discussed after SRV records. It is recommended that all A-records have a reverse DNS record created as well.

Step 6. Once all fields above have been populated, click the **Add Host** button to create the A-record. The New Host popup will remain open so that other A-records can be created. When you are finished creating records, close the New Host window. Figure 14-1 illustrates the menus used to create DNS A-records as indicated in the preceding steps.



Name (uses parent domain name if blank): ucm

Fully qualified domain name (FQDN): ucm.dcloud.cisco.com.

IP address: 198.18.1.3

☑ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

Figure 14-1 *Menus for Creating DNS A-records*

SRV Records

Key Topic

The DNS Service record, or SRV record, is a location service within DNS that can be used to identify protocols, port numbers, and host names of servers for particular services. SRV records should be configured after A-records because the A-record is configured as the Target address in an SRV record. An SRV record will always use the following format:

_ service. _ protocol.<fqdn>.   TTL   Priority   Weight   Port   Target

SRV records must be created for B2B communication over the public Internet. An SRV record is primarily used for port association, so DNS knows how to handle incoming requests on these ports. However, SRV records can also be used for redundancy and load balancing. If both SIP and H.323 are being used, an SRV record must be created for every port that is associated with these two protocols. H.323 uses UDP port 1719 and TCP port 1720. SIP uses UDP port 5060, TCP port 5060, and TLS port 5061. Therefore, five SRV records will need to be created. The Cisco Unified Communications Manager and the IM and Presence servers use special protocols and ports for communication, which will require unique SRV records as well. Using the preceding A-record example, Table 14-2 outlines the different SRV fields that need to be configured for each of these seven SRV records. The TTL, Priority, and Weight are recommended basic setting values. Also, the service _sips. and protocol _tcp. can be replaced with the service _sip. and the protocol _tls. Pay close attention to the underscores and dots. These are essential characters when configuring SRV records.

Key Topic

Table 14-2 SRV Records Needed for SIP, H.323, CUCM, and IMP

_service.	_protocol.	FQDN.	TTL	Priority	Weight	Port	Target
_sips.	_tcp.	cisco.com.	7200	10	10	5061	exp1.cisco.com
_sip.	_tcp.	cisco.com.	7200	10	10	5060	exp1.cisco.com
_sip.	_udp.	cisco.com.	7200	10	10	5060	exp1.cisco.com
_h323ls.	_udp.	cisco.com.	7200	10	10	1719	exp1.cisco.com
_h323cs.	_tcp.	cisco.com.	7200	10	10	1720	exp1.cisco.com
_cisco-uds.	_tcp.	cisco.com.	7200	10	10	8443	ucm.cisco.com
_cuplogin.	_tcp.	cisco.com.	7200	10	10	8443	imp.cisco.com

To configure an SRV record using the Microsoft DNS, follow these steps:

Step 1. Log in to the Windows Server hosting the DNS services, and open the DNS application.

Step 2. Right-click the domain you wish to create the SRV record under, and select **Other New Records…** from the menu that appears.

Step 3. On the next popup window, scroll down to and select the **Service Location (SRV)** menu option.

Step 4. When the New Resource Record window pops up, enter the appropriate information for each field. The following information is an example based on the ucm.cisco.com SRV information from Table 14-2.

a. **Domain:** (auto-populated)

b. **Service:** _cisco-uds.

c. Protocol: _tcp.

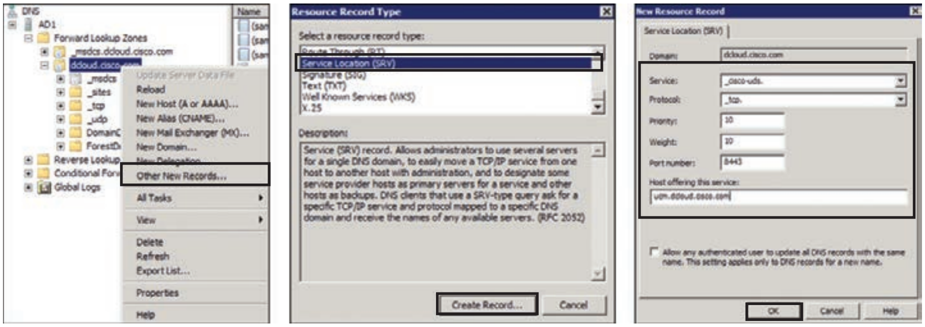
d. Priority: 10

e. Weight: 10

f. Port Number: 8443

g. Host Offering This Service: ucm.cisco.com

Step 5. After all of the fields in Step 4a–g have been populated, click the **OK** button to create the SRV record. The New Resource Record popup will remain open so that other SRV records can be created. Once finished creating records, close the New Resource Record window. Figure 14-2 illustrates the menus used to create DNS SRV records as indicated in the preceding steps.



Service (SRV) record. Allows administrators to use several servers for a single DNS domain, to easily move a TCP/IP service from one host to another host with administration, and to designate some service provider hosts as primary servers for a service and other hosts as backups. DNS clients that use a SRV-type query ask for a specific TCP/IP service and protocol mapped to a specific DNS domain and receive the names of any available servers. (RFC 2052)

Domain: dcloud.cisco.com

Service: _cisco-uds.

Protocol: _tcp.

Priority: 10

Weight: 10

Port number: 8443

Host offering this service: ucm.dcloud.cisco.com

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

Figure 14-2 *Menus for Creating DNS SRV Records*

Reverse Pointer Record (PTR)

In a DNS lookup, sometimes referred to as a forward lookup, the DNS server resolves a URL to the associated IP address. A-records and AAAA-records are used for forward lookups within DNS. However, sometimes the inverse is required, where the IP address is provided to DNS so that the associated URL can be provided in response. This is referred to as the reverse lookup, and the setting that needs to be configured within DNS to provide reverse lookup is the reverse pointer record, or PTR.

Although many iterations of reverse lookup have been ratified over the years, RFC 2317 outlines Classless IN-ADDR.ARPA, which describes a way to do IN-ADDR.ARPA delegation on nonoctet boundaries for address spaces covering fewer than 256 addresses. In other words, when different companies have leased public IP addresses within the same 256-bit IP range that resolve to different URLs for each company, respectively, classless PTRs can be used to identify domain boundaries so that each company can manage its own domain space without transecting into another company's domain space. This is one of many examples illustrating how PTRs can be used within DNS.

Key Topic

There are no standards that require PTRs to be created for A-records, and there are many A-records that function without PTRs ever being created. However, it is recommended that a PTR be created for each A-record that is created. Reverse pointer records can be configured automatically at the time A-records are configured by simply checking the box titled Create Associated Pointer (PTR) Record. Refer to Figure 14-1 to see this setting. However, the reverse lookup zones that divide the PTRs into their respective groups must be established before the auto setting will function. In other words, if an administrator selects the Create Associated Pointer (PTR) Record check box while creating an A-record, and no reverse lookup zones for PTRs have been established prior to the A-record creation, then the associated PTR will not be created. In some instances, PTRs can be created manually. To manually create a PTR, follow these steps:

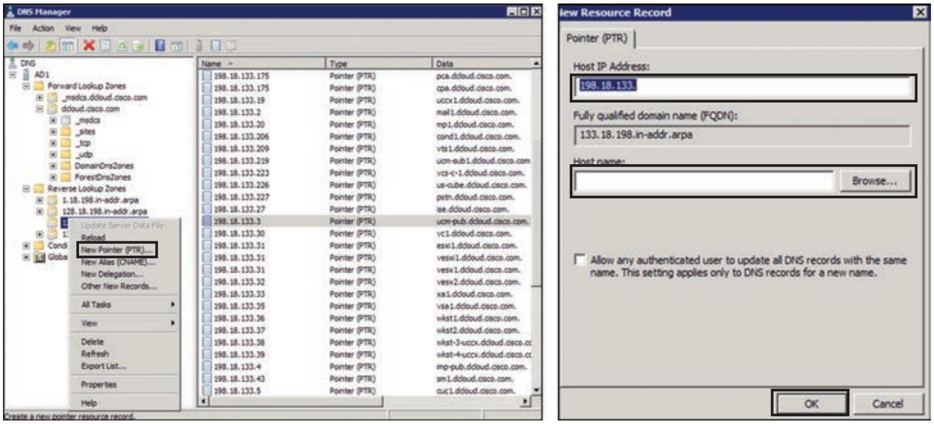
Step 1. Log in to the Windows Server hosting the DNS services, and open the DNS application.

Step 2. Right-click the reverse lookup zone you wish to create the PTR under, and select **New Pointer (PTR)…** from the menu that appears.

Step 3. When the New Resource Record window pops up, enter the Host IP Address in the first field. Note the address that appears in the Fully Qualified Domain Name (FQDN) field. The IP address is listed in reverse order from the way it was originally entered, followed by in-addr.arpa.

Step 4. In the Host Name field, you can enter the A-record URL this PTR is associated with, but it may be more prudent to click the **Browse** button and select the A-record from the list.

Step 5. Once all fields above have been populated, click the **OK** button to create the PTR. The New Resource Record popup will remain open so that other PTRs can be created. When you are finished creating records, close the New Resource Record window. Figure 14-3 illustrates the menus used to create pointer records as indicated in the preceding steps.



Name	Type	Data
198.18.133.175	Pointer (PTR)	pca.dcloud.cisco.com.
198.18.133.175	Pointer (PTR)	cpa.dcloud.cisco.com.
198.18.133.19	Pointer (PTR)	uccx1.dcloud.cisco.com.
198.18.133.2	Pointer (PTR)	mail1.dcloud.cisco.com.
198.18.133.20	Pointer (PTR)	mp1.dcloud.cisco.com.
198.18.133.206	Pointer (PTR)	cond1.dcloud.cisco.com.
198.18.133.209	Pointer (PTR)	vts1.dcloud.cisco.com.
198.18.133.219	Pointer (PTR)	ucm-sub1.dcloud.cisco.com
198.18.133.223	Pointer (PTR)	vcs-c-1.dcloud.cisco.com.
198.18.133.226	Pointer (PTR)	us-cube.dcloud.cisco.com.
198.18.133.227	Pointer (PTR)	pstn.dcloud.cisco.com.
198.18.133.27	Pointer (PTR)	ise.dcloud.cisco.com.
198.18.133.3	Pointer (PTR)	ucm-pub.dcloud.cisco.com.
198.18.133.30	Pointer (PTR)	vc1.dcloud.cisco.com.
198.18.133.31	Pointer (PTR)	esxi1.dcloud.cisco.com.
198.18.133.31	Pointer (PTR)	vesxi1.dcloud.cisco.com.
198.18.133.31	Pointer (PTR)	vesx1.dcloud.cisco.com.
198.18.133.32	Pointer (PTR)	vesx2.dcloud.cisco.com.
198.18.133.33	Pointer (PTR)	xa1.dcloud.cisco.com.
198.18.133.35	Pointer (PTR)	vsa1.dcloud.cisco.com.
198.18.133.36	Pointer (PTR)	wkst1.dcloud.cisco.com.
198.18.133.37	Pointer (PTR)	wkst2.dcloud.cisco.com.
198.18.133.38	Pointer (PTR)	wkst-3-uccx.dcloud.cisco.cc
198.18.133.39	Pointer (PTR)	wkst-4-uccx.dcloud.cisco.cc
198.18.133.4	Pointer (PTR)	imp-pub.dcloud.cisco.com.
198.18.133.43	Pointer (PTR)	sm1.dcloud.cisco.com.
198.18.133.5	Pointer (PTR)	cuc1.dcloud.cisco.com.

Host IP Address: 198.18.133.

Fully qualified domain name (FQDN): 133.18.198.in-addr.arpa

Host name:

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

Figure 14-3 *Menus for Creating Pointer Records*

NTP Settings

The Network Time Protocol (NTP) is used to provide common and consistent timestamp information to networked devices. The Cisco Unified Communications Manager uses NTP to obtain time information from a time server; however, only the publisher sends NTP requests to the external NTP server or servers. Subscribers synchronize their time with the publisher.

NTP is a protocol for synchronizing computer system clocks over IP networks. NTP has a hierarchical organization that is based on clock strata. Stratum 0 is an extremely precise clock source, such as an atomic clock or radio clock. A stratum 1 server is directly connected to a stratum 0 clock and can provide time information to other (stratum 2) devices, which in turn serve stratum 3 devices and so on. Cisco Unified Communications Manager typically uses stratum 1 but can be set to a stratum 3 without installation failing, which is the recommended maximum stratum for the Cisco Unified Communications Manager. Companies that try to install the Cisco Unified Communications Manager with a stratum 4 or higher might experience issues during installation. If installation doesn't fail entirely, then production performance will most certainly ensue.

NTP must be enabled and configured during the installation of Cisco Unified Communications Manager. At least one external NTP server must be reachable and functioning when installing the Cisco Unified Communications Manager publisher to complete the installation. Cisco recommends using a minimum of three external NTP servers in a production environment. It is extremely important that all network devices have accurate time information because the system time of Cisco Unified Communications Manager is relevant in the following situations:

Key Topic

- Cisco IP phones display date and time information. This information is obtained from Cisco Unified Communications Manager.
- CDR and CMR, which are used for call reporting, analysis, and billing, include date and time information.
- Alarms and events in log files, as well as trace information in trace files, include time information. Troubleshooting a problem requires correlation of information that is created by different system components, such as Cisco Unified Communications Manager, Cisco IOS gateway, and so on. This problem solving is possible only if all devices in the network have the same correct time information.
- Some Cisco Unified Communications Manager features are date-based or time-based and therefore rely on correct date and time. These features include time-of-day routing and certificate-based security features.
- Certificates include a validity period. If a system that receives a certificate has an invalid future date, it may consider the received certificate to be invalid or expired.
- Endpoints joining a scheduled meeting may also have issues pertaining to when and if they are able to join the scheduled meeting when NTP is out of sync.

To ensure that all network devices have the correct date and time, it is recommended that all network devices use NTP for time synchronization. The master reference clock should be a stratum 0 or stratum 1 NTP server.

SNMP Settings

Simple Network Management Protocol (SNMP) is an Internet standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more. Within a Cisco collaboration network, there are a lot of different devices that use SNMP.

The primary method for location identification in Cisco Emergency Responder is the detection of an endpoint via Layer 2 discovery at the switch port level. Discovering an endpoint though Layer 2 Cisco Discovery Protocol (CDP) enables Emergency Responder to determine the exact physical location of the calling device based on the physical termination of the network cable to a network jack in a cubicle or office. Although the discovery mechanism of the connected device is reliable, the accuracy of the physical location relies on two main assumptions:

- The wired infrastructure of the enterprise is well established and does not change sporadically, and any wiring closet changes trigger notification to the Emergency Responder administrator indicating what changed.
- The infrastructure is available for Cisco Emergency Responder to browse; that is, Cisco Emergency Responder can establish SNMP sessions to the underlying network infrastructure and can scan the network ports for the discovery of connected phones.

The Cisco Paging Server allows users to send audio-only messages to groups of up to 50 IP phones in an organization. The Cisco Paging Server communicates with the Cisco Unified Communications Manager using SIP, SNMP, AXL, and CTI. When the Cisco Paging Server starts, and at configurable intervals after that, it connects with the Cisco Unified Communications Manager using SNMP. The Cisco Paging Server uses SNMP to find the other Cisco Unified Communications Manager cluster member IP addresses as well as a list of phones registered to each cluster member. Once the SNMP communications are complete, the Cisco Paging Server uses AXL to determine additional information regarding each registered phone, such as device name, description, device pool, calling search space, directory number, and location. This information can be used to build logical groups of phones, called recipient groups. In the Cisco Paging Server, recipient groups can contain a maximum of 50 phones.

Cisco Unified Contact Center Enterprise (UCCE) is managed with SNMP. UCCE devices have a built-in SNMP agent infrastructure that supports SNMP v1, v2c, and v3, and it exposes instrumentation defined by the CISCO-CONTACT-CENTER-APPS-MIB. This MIB provides configuration, discovery, and health instrumentation that can be monitored by standard SNMP management stations. Moreover, UCCE provides a rich set of SNMP notifications that alert administrators of any faults in the system. UCCE also provides a standard syslog event feed for those administrators who want to take advantage of a more verbose set of events. For more information about configuring the UCCE SNMP agent infrastructure and the syslog feed, refer to the SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Unified CVP health can be monitored by using any SNMP standard monitoring tool to get a detailed visual and tabular representation of the health of the solution network. All Unified CVP product components and most Cisco Unified Customer Voice Portal (CVP) solution components also issue SNMP traps and statistics that can be delivered to any standard SNMP management station or monitoring tool. Cisco Unified Contact Center Express, or UCCX, can also be managed with SNMP and a syslog interface.

Prime Collaboration's automated device discovery is based on a Cisco Discovery Protocol (CDP) table. Ping Sweep may be used instead of CDP, but IP phones discovered using Ping Sweep are reported in "unmanaged" state. Another protocol that Prime Collaboration uses to monitor the Unified Communications elements is SNMP. SNMP is an application layer protocol using UDP as the transport layer protocol. There are three key elements in an SNMP managed network:

- **Managed devices:** Network devices that have an SNMP agent, such as Cisco Unified Communications Manager, routers, switches, and so on.
- **Agent:** A network management software module that resides in a managed device. This agent translates the local management information on the device into SNMP messages.
- **Manager:** Software running on a management station that contacts different agents in the network to get the management information, such as Prime Collaboration.

The SNMP implementation supports three versions: SNMP v1, SNMP v2c, and SNMP v3. SNMP v3 supports authentication, encryption, and message integrity. SNMP v3 may be used if security is desired for management traffic. Prime Collaboration supports all three versions of SNMP. SNMP v1 and v2c read/write community strings, or SNMP v3 credentials must be configured on each device for agent and manager to communicate properly. Prime Collaboration needs only SNMP read access to collect network device information. SNMP must also be enabled on network devices to allow Prime Collaboration to get information on network devices at configured polling intervals and to receive alerts and faults via trap notification sent by the managed devices. For more information on SNMP, refer to the Cisco Prime Collaboration documentation available at https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html.

Cisco TMS can manage endpoints registered to both Cisco Expressway (or VCS) and Cisco Unified Communications Manager. There are two types of device management: direct managed and provisioned. Direct-managed devices are manually added into the Cisco TMS system navigator. Cisco TMS supports 5,000 direct-managed devices. Cisco TMS communicates with the endpoints directly via HTTP or SNMP protocols. When a direct-managed endpoint is registered to the Cisco Unified Communications Manager, the Cisco Unified Communications Manager handles most management capabilities such as software upgrades. When a direct-managed endpoint is registered to Cisco Expressway, Cisco TMS handles management and provisioning of the endpoint, including capabilities such as software upgrades.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics 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	DNS A-record Example and Definition	335
Paragraph	DNS SRV Record Example and Definition	337
Table 14-2	SIP, H.323, CUCM, and IMP Services and Ports for SRV Records	337
Paragraph	Automatic Creation of PTRs	338
List	NTP Relevance in a CUCM Environment	340
List	Dependencies for Emergency Responder Accuracy	341

Define Key Terms

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

A-records, AAAA-records, AXL, CDP, CER, CTI, DNS, NTP, PTR, SNMP, SRV Record, Stratum, TMS, UCCE, UCCX, Unified CVP, URL, VCS

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What are the SRV records for the CUCM and IM and Presence servers?
2. List the five important reasons that NTP services must be synchronized correctly.
3. List seven devices that use SNMP in a Cisco UC environment.

This part covers the following topics:

- **Chapter 15, Cisco Unified Communications Manager Setup:** This chapter will introduce key settings on the Cisco Unified Communications Manager that should be configured before using this server in a production environment. These settings include enabling application services and configuring service parameters, enterprise parameters, and other such settings.
- **Chapter 16, LDAP Integration with Cisco Unified Communications Manager:** This chapter will examine the differences between application users and end users on the Cisco Unified Communications Manager, and how to use an LDAP service for user synchronization and authentication.
- **Chapter 17, Registering SIP Endpoints to the Cisco Unified Communications Manager:** This chapter will examine three different methods for registering endpoints to the Cisco Unified Communications Manager: registering manually, Self-Provisioning, and using the Bulk Administration Tool.
- **Chapter 18, Cisco Unified Communications Manager Call Admission Control (CAC):** This chapter will introduce the Cisco Unified Communications Manager endpoint addressing, digit analysis process, and toll fraud prevention components using Cost of Service (COS). Then this chapter will delve into location-based CAC deployment through the Cisco Unified Communications Manager.
- **Chapter 19, Configuring Globalized Call Routing in Cisco Unified Communications Manager:** This chapter will explain how to configure globalized call-routing components on the Cisco Unified Communications Manager, such as route patterns, translation patterns, SIP route patterns, and the standard local route group.

Part IV

Call Control Mechanisms

CHAPTER 15

Cisco Unified Communications Manager Setup

This chapter covers the following topics:

Services: This topic will introduce the two different types of services that exist on the Cisco Unified Communications Manager and explain how to enable services needed for basic Cisco Unified Communications Manager operation.

Enterprise Parameters: This topic will introduce the enterprise parameters that exist for all nodes within a Cisco Unified Communications Manager cluster.

Service Parameters: This topic will examine how to configure service parameters for feature services that have been enabled on the Cisco Unified Communications Manager.

Other Settings: This topic will overview other key settings that may need to be configured on the Cisco Unified Communications Manager for production use.

Codec Negotiations using Regions: This topic will bring the audio and video basics discussed in Part 1 to an applicable configuration within the Cisco Unified Communications Manager as regions are used to apply audio and video codecs to groups of endpoints.

The Cisco Unified Communications Manager has been described in the past as a very complex solution that is difficult to understand and configure. However, this highly complex solution also offers incredible granularity in how it can manage a collaboration solution. This chapter begins an intricate examination of how to set up and utilize the many tools available through the Cisco Unified Communications Manager. Before an organization can begin using this system, some foundational settings must be configured. This chapter will explain these foundational settings and how to configure them. Topics discussed in this chapter include the following:

- Services
- Enterprise Parameters
- Service Parameters
- Other Settings
  - Groups
  - Device Settings (Device Defaults, Phone Button Template, Soft Key Template)
  - Phone Services

    - SIP Profile
    - Device Pool Settings
- Codec Negotiations Using Regions

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 2.2 Identify the collaboration codecs for a given scenario
- 3.1 Configure voice gateway elements
    - 3.1.a DTMF
- 3.3 Identify the appropriate IOS XE media resources

"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
Services	1–2
Enterprise Parameters	3
Service Parameters	4
Other Settings	5–8
Codec Negotiations Using Regions	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 is only a network service category on the CUCM?

a. CDR Services

b. CM Services

c. Performance and Monitoring Services

d. SOAP Services

2. At a minimum, which two of the following feature services must be enabled? (Choose two.)

a. Cisco CallManager

b. Cisco CTIManager

c. Cisco TFTP

d. Cisco DirSync

e. Cisco Device Activation Service

f. Cisco AXL Web Service

3. Which of the following statements about enterprise parameters is true?

a. Enterprise parameters must be configured on each peer within a CUCM cluster.

b. Enterprise parameters are applied clusterwide across all CUCM peers within the cluster.

c. Dependency records are enabled by default and must be disabled in the enterprise parameters if an administrator does not want to use them.

d. URL parameters default using the CUCM's IP address and must be changed to use the URL if DNS reliance is desired.

4. What is the purpose of the T302 timer?

a. T302 timers are the bases for call reporting, accounting, and billing.

b. It lists various codecs of voice media-streaming applications.

c. It specifies the interdigit timer for variable-length numbers.

d. It sets the NTP reference and time zone for phones.

5. What is the maximum number of Server nodes in a CUCM cluster that can run the CallManager service?

a. 2

b. 4

c. 8

d. 12

6. Which of the following is a disadvantage to using a 1:1 redundancy group on the CUCM?

a. Upgrading servers may cause temporary outages.

b. If multiple primary servers fail, the backup servers may be overwhelmed.

c. 1:1 redundancy groups are more complex to deploy.

d. The cost of deploying 1:1 redundancy groups is higher than other options.

7. Where would an administrator customize the phone button templates for phones registering to the CUCM?

a. **Device > Phone**

b. **Device > Device Settings**

c. **System > Device Pool**

d. **User Management > End User**

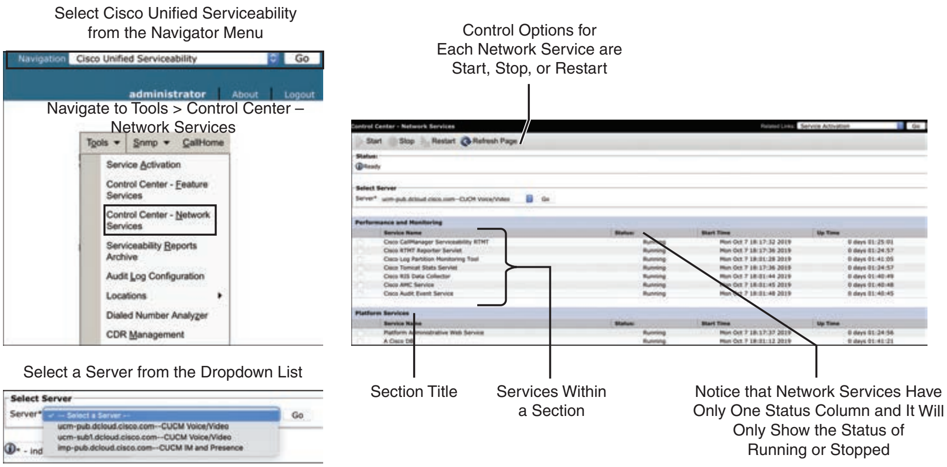
8. Where would an administrator configure a Media Resource Group List for all phones in a particular location to use?
   a. **Device > Phone**
   b. **Device > Device Settings**
   c. **System > Device Pool**
   d. **User Management > End User**
9. How much bandwidth is required for a video call using the H.263 codec at 1080p30 resolution?
   a. 768 kbps
   b. 1024 kbps
   c. 1536 kbps
   d. 2048 kbps
10. Which of the following is an important region setting for audio that should be selected along with the codec selection?
   a. Compression setting
   b. Bandwidth rate
   c. Video codec
   d. Video bandwidth rate

Foundation Topics

Services

A service on the Cisco Unified Communications Manager is a set of parameters that encapsulate a specific feature or function within the Cisco Unified Communications Manager. When a cluster is set up, each server in a Cisco Unified Communications Manager cluster can fulfill different tasks, such as running a TFTP or DHCP server, being the database publisher, processing calls, or providing media resources. Depending on the usage of a server, different services must be activated on the system. There are two types of services on Cisco Unified Communications Manager servers: network services and feature services.

Network services are automatically activated on each Cisco Unified Communications Manager node and are required for the operation of the server. Network services cannot be activated or deactivated by the administrator, but they can be stopped, started, or restarted. To perform these actions on network services, the administrator should select Cisco Unified Serviceability from the Navigator drop-down menu in the top-right corner of the screen and then choose **Tools > Control Center–Network Services**. Then you can select a server from the drop-down list to view the network services for that server. Figure 15-1 illustrates the Network Services menu and options on the Cisco Unified Communications Manager.


Navigation
Cisco Unified Serviceability
Go
administrator
About
Logout
Tools
Snmp
CallHome
Service Activation
Control Center - Feature Services
Control Center - Network Services
Serviceability Reports Archive
Audit Log Configuration
Locations
Dialed Number Analyzer
CDR Management
Control Center - Network Services
Related Links:
Service Activation
Go
Start
Stop
Restart
Refresh Page
Status:
Ready
Select Server
Server*
ucm-pub.dcloud.cisco.com--CUCM Voice/Video
Go
-- Select a Server --
ucm-pub.dcloud.cisco.com--CUCM Voice/Video
ucm-sub1.dcloud.cisco.com--CUCM Voice/Video
imp-pub.dcloud.cisco.com--CUCM IM and Presence
Go

Performance and Monitoring

Service Name	Status:	Start Time	Up Time
Cisco CallManager Serviceability RTMT	Running	Mon Oct 7 18:17:32 2019	0 days 01:25:01
Cisco RTMT Reporter Servlet	Running	Mon Oct 7 18:17:36 2019	0 days 01:24:57
Cisco Log Partition Monitoring Tool	Running	Mon Oct 7 18:01:28 2019	0 days 01:41:05
Cisco Tomcat Stats Servlet	Running	Mon Oct 7 18:17:36 2019	0 days 01:24:57
Cisco RIS Data Collector	Running	Mon Oct 7 18:01:44 2019	0 days 01:40:49
Cisco AMC Service	Running	Mon Oct 7 18:01:45 2019	0 days 01:40:48
Cisco Audit Event Service	Running	Mon Oct 7 18:01:48 2019	0 days 01:40:45

Platform Services

Service Name	Status:	Start Time	Up Time
Platform Administrative Web Service	Running	Mon Oct 7 18:17:37 2019	0 days 01:24:56
A Cisco DB	Running	Mon Oct 7 18:01:12 2019	0 days 01:41:21

Select Cisco Unified Serviceability from the Navigator Menu

Navigate to Tools > Control Center – Network Services

Select a Server from the Dropdown List

Control Options for Each Network Service are Start, Stop, or Restart

Section Title

Services Within a Section

Notice that Network Services Have Only One Status Column and It Will Only Show the Status of Running or Stopped

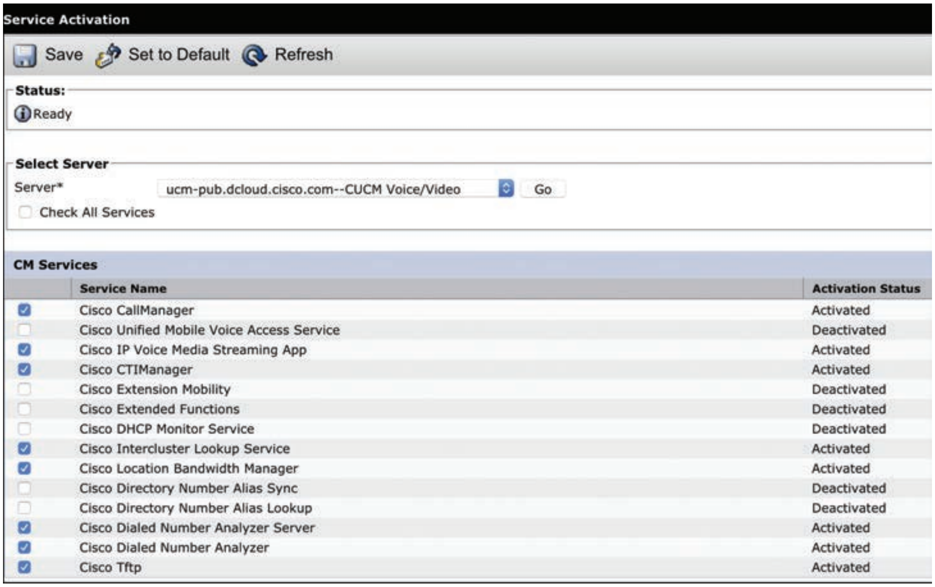
Figure 15-1 *Network Services on the CUCM*

The network services by category are as follows:

Key Topic

- **Performance and Monitoring:** Cisco CallManager Serviceability RTMT, Cisco RTMT Reporter Servlet, Cisco Log Partition Monitoring Tool, Cisco Tomcat Stats Servlet, Cisco RIS Data Collector, Cisco AMC Service, Cisco Audit Event Service
- **Platform Services:** Platform Administrative Web Service, A Cisco DB, A Cisco DB Replicator, SNMP Master Agent, MIB2 Agent, Host Resources Agent, Cisco CDP Agent, Cisco Syslog Agent, Cisco Certificate Expiry Monitor, Cisco Certificate Change Notification, Cisco Tomcat, Platform Communication Web Service, Cisco Smart License Manager
- **System Services:** Cisco CallManager Serviceability, Cisco CDP, Cisco Trace Collection Servlet, Cisco Trace Collection Service
- **DB Services:** Cisco Database Layer Monitor
- **Admin Services:** Cisco CallManager Admin
- **SOAP Services:** SOAP-Real-Time Service APIs, SOAP-Performance Monitoring APIs, SOAP-Log Collections APIs, SOAP-Diagnostic Portal Database Service
- **Backup and Restore Services:** Cisco DRF Local, Cisco DRF Master
- **CDR Services:** Cisco CDR Repository Manager, Cisco CDR Agent, Cisco CAR Scheduler, Cisco SOAP-CallRecord Service, Cisco CAR DB
- **CM Services:** Cisco Extension Mobility Application, Cisco User Data Services, Cisco Change Credential Application, Cisco E911, Cisco Push Notification Service
- **Security Services:** Cisco Trust Verification Service
- **Cloud-based Management Services:** Cisco Management Agent Service

Opposite the network services, all feature services are deactivated by default and must be activated before they can be used. Feature services can be selectively activated or deactivated per server to assign specific tasks or functions, such as call processing or TFTP, to a specific server. The two feature services required to be activated before phones will be able to register or call through the Cisco Unified Communications Manager include the Cisco CallManager service and the Cisco TFTP service. Feature services can be activated and deactivated by selecting Cisco Unified Serviceability from the Navigator drop-down menu in the top-right corner of the screen and then choosing the **Tools > Service Activation**. Remember to select the server where each service is being activated. This is critical with feature services because different services will run on different nodes within a Cisco Unified Communications Manager cluster. In a Cisco Unified Communications Manager cluster, one specific node is often designated as just the TFTP server or the Music On Hold (MOH) server because of the processing load requirements. Service Activation is the place where these designations are made. Figure 15-2 illustrates how to enable feature services on the Cisco Unified Communications Manager.



Status:
Ready

Select Server
Server* ucm-pub.dcloud.cisco.com--CUCM Voice/Video Go
□ Check All Services

CM Services

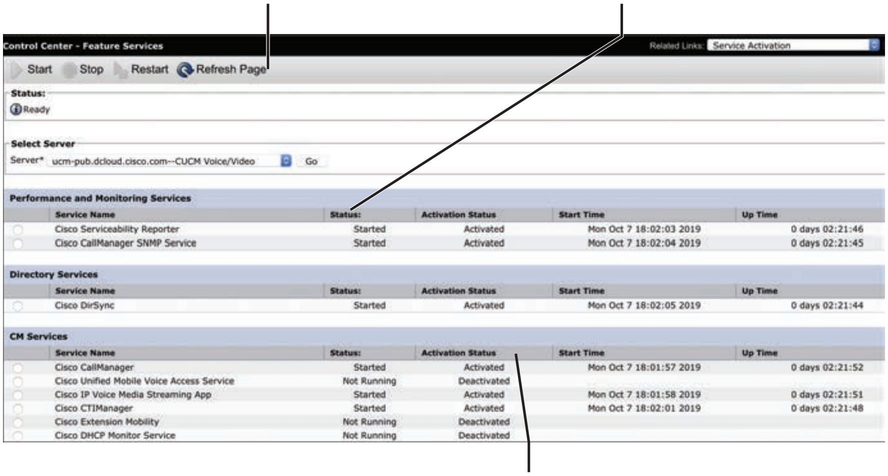
	Service Name	Activation Status
☑	Cisco CallManager	Activated
□	Cisco Unified Mobile Voice Access Service	Deactivated
☑	Cisco IP Voice Media Streaming App	Activated
☑	Cisco CTIManager	Activated
□	Cisco Extension Mobility	Deactivated
□	Cisco Extended Functions	Deactivated
□	Cisco DHCP Monitor Service	Deactivated
☑	Cisco Intercluster Lookup Service	Activated
☑	Cisco Location Bandwidth Manager	Activated
□	Cisco Directory Number Alias Sync	Deactivated
□	Cisco Directory Number Alias Lookup	Deactivated
☑	Cisco Dialed Number Analyzer Server	Activated
☑	Cisco Dialed Number Analyzer	Activated
☑	Cisco Tftp	Activated

Figure 15-2 *Enabling Feature Services on the CUCM*

When feature services are first activated, they should start automatically; however, best practice dictates that you verify that each service has started and that it has been activated. Therefore, to verify feature services are running, or to stop, start, or restart each of these feature services, select **Tools > Control Center-Feature Services** under Cisco Unified Serviceability. Remember to select the server where each service is being activated. This step is critical with feature services because different services will run on different nodes within a Cisco Unified Communications Manager cluster. This menu will identify that each feature service is either Started or Not Running, and that each service is Activated or Deactivated. Figure 15-3 illustrates how to check whether feature services are Activated or Started.

Notice the different control options from the Service Activation menu in Figure 15-2.

Notice the Status column that reflects Started or Not Running status messages.


Control Center - Feature Services
Related Links: Service Activation
Start
Stop
Restart
Refresh Page
Go

Status:
Ready

Select Server
Server* ucm-pub.dcloud.cisco.com--CUCM Voice/Video

Performance and Monitoring Services

	Service Name	Status:	Activation Status	Start Time	Up Time
○	Cisco Serviceability Reporter	Started	Activated	Mon Oct 7 18:02:03 2019	0 days 02:21:46
○	Cisco CallManager SNMP Service	Started	Activated	Mon Oct 7 18:02:04 2019	0 days 02:21:45

Directory Services

	Service Name	Status:	Activation Status	Start Time	Up Time
○	Cisco DirSync	Started	Activated	Mon Oct 7 18:02:05 2019	0 days 02:21:44

CM Services

	Service Name	Status:	Activation Status	Start Time	Up Time
○	Cisco CallManager	Started	Activated	Mon Oct 7 18:01:57 2019	0 days 02:21:52
○	Cisco Unified Mobile Voice Access Service	Not Running	Deactivated		
○	Cisco IP Voice Media Streaming App	Started	Activated	Mon Oct 7 18:01:58 2019	0 days 02:21:51
○	Cisco CTIManager	Started	Activated	Mon Oct 7 18:02:01 2019	0 days 02:21:48
○	Cisco Extension Mobility	Not Running	Deactivated		
○	Cisco DHCP Monitor Service	Not Running	Deactivated		

Notice the Activation Status column that reflects Activated or Deactivated status messages.

Figure 15-3 *Control Center Feature Services Status*

The following list identifies all the feature services by category:

Key Topic

- **Performance and Monitoring Services:** Cisco Serviceability Reporter, Cisco CallManager SNMP Service
- **Directory Services:** Cisco DirSync
- **CM Services:** Cisco CallManager, Cisco Unified Mobile Voice Access Service, Cisco IP Voice Media Streaming App, Cisco CTI Manager, Cisco Extension Mobility, Cisco DHCP Monitor Service, Cisco Intercluster Lookup Service, Cisco Location Bandwidth Manager, Cisco Directory Number Alias Sync, Cisco Directory Number Alias Lookup, Cisco Device Activation Service, Cisco Dialed Number Analyzer Server, Cisco Dialed Number Analyzer, Cisco TFTP
- **CTI Services:** Cisco IP Manager Assistant, Cisco WebDialer Web Service, Self Provisioning IVR
- **Voice Quality Reporter Services:** Cisco Extended Functions
- **Database and Admin Services:** Cisco Bulk Provisioning Service, Cisco AXL Web Service, Cisco UXL Web Service, Cisco TAPS Service
- **Location-based Tracking Services:** Cisco Wireless Controller Synchronization Service
- **Security Services:** Cisco Certificate Authority Proxy Function, Cisco Certificate Enrollment Service, Cisco CTL Provider
- **CDR Services:** Cisco SOAP-CDROnDemand Service, Cisco CAR Web Service

As you can see, some services exist as both network services and feature services. The administrator controls the availability of the feature by activating or deactivating the corresponding feature service. Cisco Unified Communications Manager automatically enables the required network services depending on the activated feature services.

Enterprise Parameters

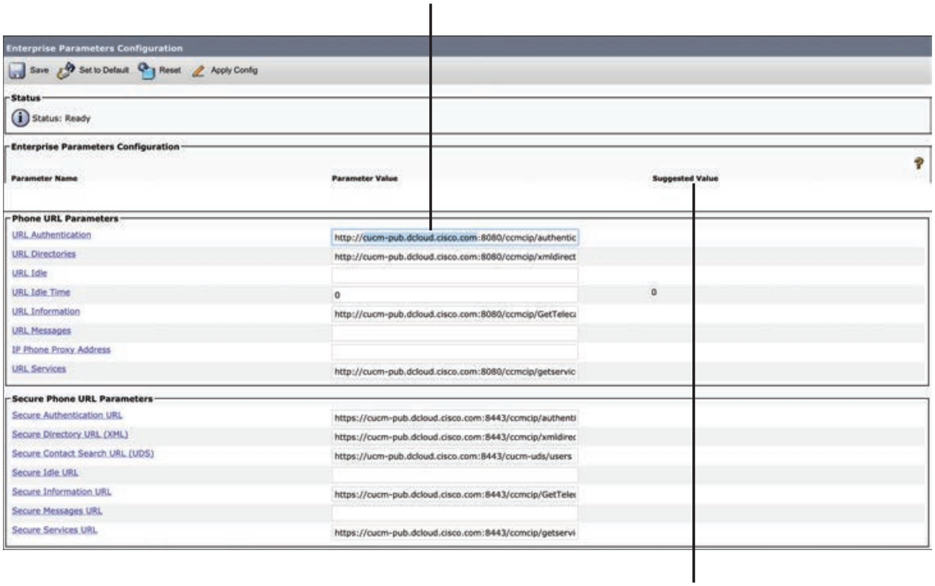
Key Topic

Enterprise parameters are used to define clusterwide system settings, and these parameters apply to all devices and services across all nodes within the entire cluster. After installation of all Cisco Unified Communications Manager nodes and activation of the feature services, enterprise parameter default values should be verified, and modified if required, before deploying endpoints. Keep in mind, however, that you should change enterprise parameters only if you are completely aware of the impact of your modifications or if instructed to do so by the Cisco Technical Assistance Center.

Enterprise parameters can be accessed under the main Cisco Unified Communications Manager menus by selecting Cisco Unified CM Administration from the Navigator drop-down menu in the top-right corner of the screen and then navigating to **System > Enterprise Parameter.** On the Enterprise Parameters Configuration page, you will find enterprise parameters that are grouped into categories with the current configuration and the default value shown per parameter. Some enterprise parameters specify initial values of device defaults.

When DNS reliance is removed, all host names within enterprise URL parameters must be changed to IP addresses. When DNS reliance is set up during the installation of the Cisco Unified Communications Manager, these addresses will appear within the Enterprise URL Parameters as the URL of the Cisco Unified Communications Manager. Figure 15-4 illustrates the different fields in the Enterprise Parameters Configuration, as well as the URL Parameters settings.

There are 33 different sections within the enterprise parameters of the Cisco Unified Communications Manager, and there could be between 1 and 21 different parameters within each section. Most parameters can be left as the default values, and any parameters that need to be changed will include instructions to do so in the corresponding deployment guides from Cisco. An example of one such deployment scenario could be enabling Dependency records, which are a feature of the Cisco Unified Communications Manager that allows an administrator to view configuration database records that reference the currently displayed record. Dependency records are useful when you want to delete a configuration entry, such as a device pool, but the deletion fails because the record is still referenced by a depending faculty within the Cisco Unified Communications Manager, such as an IP phone. Without dependency records, you would have to rifle through many different menus and settings to determine where the dependency exists for the device pool that you tried to delete. If the enterprise parameter called Enable Dependency Records is changed from False to True, a record of all setting dependencies is kept within the Cisco Unified Communications Manager and can be accessed by the administrator.


Enterprise Parameters Configuration
Save
Set to Default
Reset
Apply Config
Status
Status: Ready
Enterprise Parameters Configuration
?

Parameter Name	Parameter Value	Suggested Value
Phone URL Parameters		
URL Authentication	http://cucm-pub.dcloud.cisco.com:8080/ccmcip/authentic	
URL Directories	http://cucm-pub.dcloud.cisco.com:8080/ccmcip/xmldirect	
URL Idle		
URL Idle Time	0	0
URL Information	http://cucm-pub.dcloud.cisco.com:8080/ccmcip/GetTeleca	
URL Messages		
IP Phone Proxy Address		
URL Services	http://cucm-pub.dcloud.cisco.com:8080/ccmcip/getservic	
Secure Phone URL Parameters		
Secure Authentication URL	https://cucm-pub.dcloud.cisco.com:8443/ccmcip/authenti	
Secure Directory URL (XML)	https://cucm-pub.dcloud.cisco.com:8443/ccmcip/xmldirec	
Secure Contact Search URL (UDS)	https://ucm-pub.dcloud.cisco.com:8443/cucm-uds/users	
Secure Idle URL		
Secure Information URL	https://cucm-pub.dcloud.cisco.com:8443/ccmcip/GetTele	
Secure Messages URL		
Secure Services URL	https://cucm-pub.dcloud.cisco.com:8443/ccmcip/getservi	

The highlighted value will change between nodes and show whether DNS dependence is required.

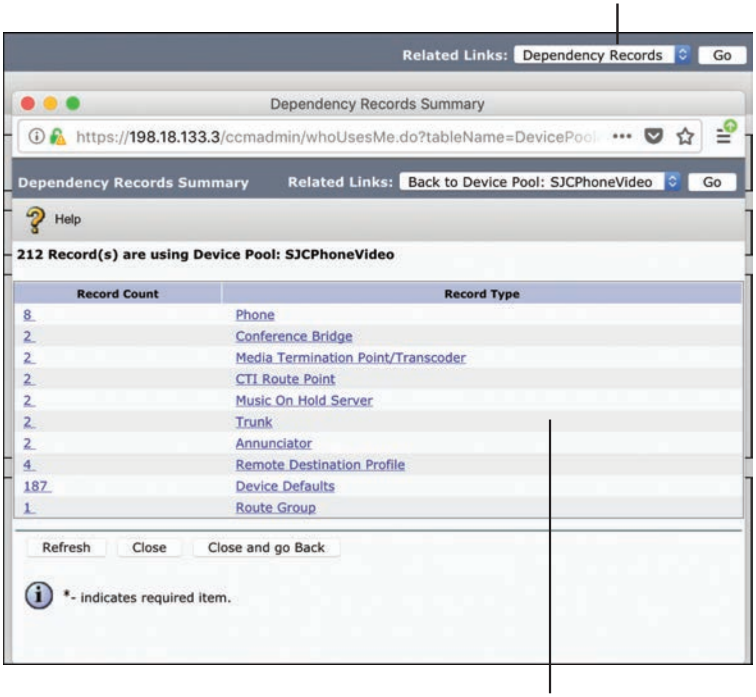
Anything listed in the Suggested Value column is a default value.

Figure 15-4 *Enterprise Parameter Settings Within the CUCM*

Once dependency records have been enabled, a specific faculty must be selected before the records can be accessed. For example, navigating to **System > Device Pool** will not allow the dependency records to be accessed, but selecting a specific device pool and entering into the configuration menus will allow access to these records. A Related Links drop-down menu will appear in the top-right corner of the screen, just under the Navigator drop-down menu. Use the drop-down menu to select the Dependency Records option and click the **Go** button. A Dependency Records Summary popup window will appear with all the dependent records related to that one setting—in this case, the device pool. This summary will include a Record Count and a Record Type with hyperlinks. The hyperlinks will allow the administrator to view specific information within each categorized group. Figure 15-5 illustrates the Dependency Records summary. In this summary, one of the Record Types is Phone, and the Record Count is 8. If the hyperlink were selected for Phone or 8, the resulting data displayed would be a list of the eight phones that have a dependency on this device pool.

Throughout this book I will continue to reference settings within the enterprise parameters settings as other topics are discussed. To obtain additional information about enterprise parameters, navigate to **System > Enterprise Parameters** and click the question mark symbol at the top-right corner of the Enterprise Parameters Configuration section on the screen. A complete list of all the enterprise parameters, along with a description, will be provided.

Related Links Dropdown Menu



Related Links: Dependency Records

Dependency Records Summary

https://198.18.133.3/ccmadmin/whoUsesMe.do?tableName=DevicePool

Dependency Records Summary Related Links: Back to Device Pool: SJCPhoneVideo

212 Record(s) are using Device Pool: SJCPhoneVideo

Record Count	Record Type
8	Phone
2	Conference Bridge
2	Media Termination Point/Transcoder
2	CTI Route Point
2	Music On Hold Server
2	Trunk
2	Annunciator
4	Remote Destination Profile
187	Device Defaults
1	Route Group

*- indicates required item.

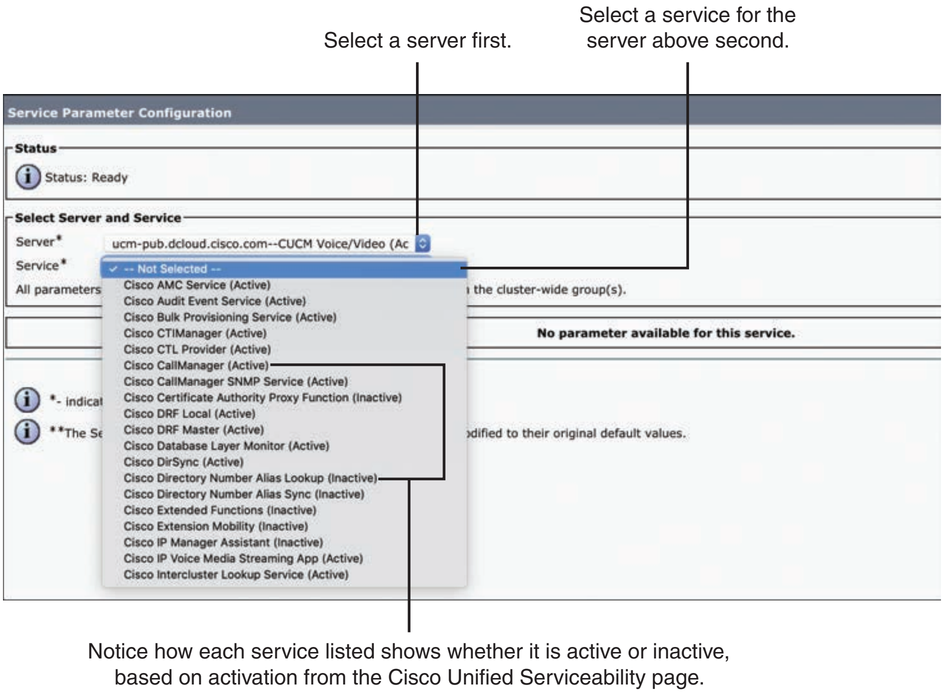
Dependency Records Summary Popup Window

Figure 15-5 *Dependency Records Summary Page*

Service Parameters

Service parameters are used to define settings for a specific feature service on an individual server. Unlike enterprise parameters, service parameters are defined separately for each server in the cluster and for each feature service enabled on each server, such as the call-processing Cisco CallManager service on the Publisher server. After activation of feature services, service parameter default values should be verified and possibly modified, if required, before deploying endpoints.

To access the service parameters on the Cisco Unified Communications Manager from the Cisco Unified CM Administration, navigate to **System > Service Parameters**. In the Select Server and Service section, use the drop-down tool beside the Server menu to select a server within the Cisco Unified Communications Manager cluster. Remember that service parameters are specific to each server within the cluster and to each service on that particular server. Once the server has been chosen, a new menu option called Service will appear. Use the drop-down tool next to this menu option to select a feature service on the previously selected server. This will display all the service settings for that specific service on that particular server. The service options in the drop-down list will also identify whether each service listed is Active or Inactive. Figure 15-6 illustrates the menu options for accessing service parameters.



Select a server first.

Select a service for the server above second.

Service Parameter Configuration

Status

Status: Ready

Select Server and Service

Server* ucm-pub.dcloud.cisco.com--CUCM Voice/Video (Ac

Service* ✓ -- Not Selected --

- Cisco AMC Service (Active)
- Cisco Audit Event Service (Active)
- Cisco Bulk Provisioning Service (Active)
- Cisco CTIManager (Active)
- Cisco CTL Provider (Active)
- Cisco CallManager (Active)
- Cisco CallManager SNMP Service (Active)
- Cisco Certificate Authority Proxy Function (Inactive)
- Cisco DRF Local (Active)
- Cisco DRF Master (Active)
- Cisco Database Layer Monitor (Active)
- Cisco DirSync (Active)
- Cisco Directory Number Alias Lookup (Inactive)
- Cisco Directory Number Alias Sync (Inactive)
- Cisco Extended Functions (Inactive)
- Cisco Extension Mobility (Inactive)
- Cisco IP Manager Assistant (Inactive)
- Cisco IP Voice Media Streaming App (Active)
- Cisco Intercluster Lookup Service (Active)

All parameters ı the cluster-wide group(s).

No parameter available for this service.

*- indicat

**The Se ɔdified to their original default values.

Notice how each service listed shows whether it is active or inactive, based on activation from the Cisco Unified Serviceability page.

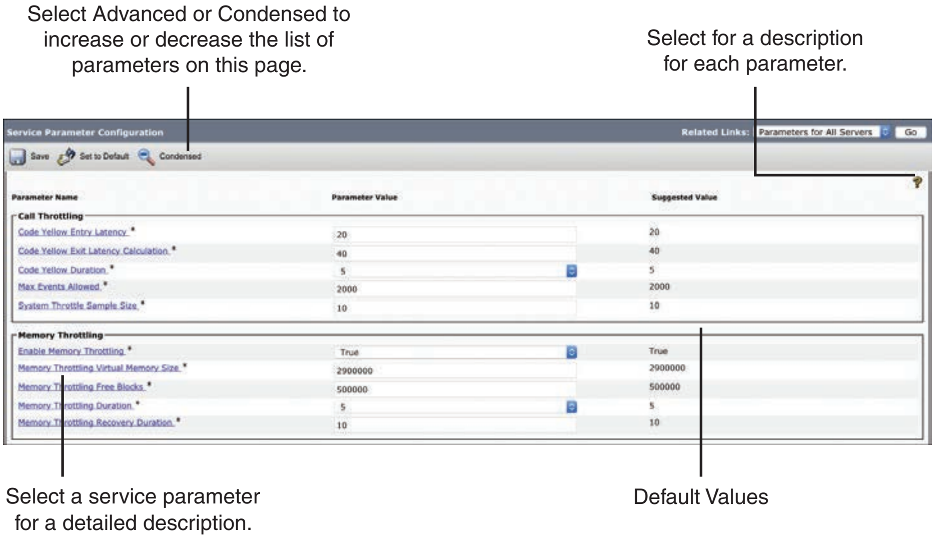
Figure 15-6 *Accessing Service Parameters on the CUCM*

For each of the feature services listed earlier in this chapter, there is an entire web page of settings within the Cisco Unified Communications Manager. Much like the enterprise parameters, the System Configuration Guide for Cisco Unified Communications Manager will identify which service parameters need to be modified based on special deployment scenarios. The link to access this guide is as follows: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_0_1/systemConfig/cucm_b_system-configuration-guide-1201/cucm_b_system-configuration-guide-1201_chapter_0101.html. Although not all of these settings are listed in this chapter, three commonly referenced service parameters for the Cisco CallManager service are the following:

Key Topic

- **T302 Timer:** This setting specifies the interdigit timer for variable-length numbers. Reducing the default value will speed up dialing (shorter post-dial delay).
- **CDR and CMR:** Call detail records and call management records are the bases for call reporting, accounting, and billing. The service parameters are used to enable CDRs and CMRs (both are disabled by default). While the CDR service parameter can be easily found by using the search function (the parameter is named CDR Enabled Flag), it is more challenging to find the CMR parameter (the parameter is named Call Diagnostics Enabled).
- **Clusterwide Parameters (System-Location and Region):** This section lists various codecs of voice media-streaming applications. These codecs can be modified or disabled if needed.

By default, not all service parameters are displayed. If you cannot find the service parameter that you want to change, click Advanced to see the complete list of available service parameters. The Change B-Channel Maintenance Status service parameter is an example of a Cisco CallManager service parameter that is not shown by default. Descriptions for all service parameters can be found by clicking the yellow question mark symbol in the upper-right corner, similar to the enterprise parameters. Figure 15-7 illustrates the Service Parameters Configuration page.



Select Advanced or Condensed to increase or decrease the list of parameters on this page.

Select for a description for each parameter.

Select a service parameter for a detailed description.

Default Values

Service Parameter Configuration
Related Links: Parameters for All Servers
Go
Save
Set to Default
Condensed
?

Parameter Name	Parameter Value	Suggested Value
Call Throttling		
Code Yellow Entry Latency *	20	20
Code Yellow Exit Latency Calculation *	40	40
Code Yellow Duration *	5	5
Max Events Allowed *	2000	2000
System Throttle Sample Size *	10	10
Memory Throttling		
Enable Memory Throttling *	True	True
Memory Throttling Virtual Memory Size *	2900000	2900000
Memory Throttling Free Blocks *	500000	500000
Memory Throttling Duration *	5	5
Memory Throttling Recovery Duration *	10	10

Figure 15-7 *Service Parameter Configuration Page*

Other Settings

All of the settings discussed in this chapter up to this point need to be configured by an administrator in a greenfield deployment prior to releasing the Cisco Unified Communications Manager into a production network. However, services or enterprise parameters and service parameters can also be enabled or configured in brownfield deployments of the Cisco Unified Communications Manager as the administrator adds functionality to an already-existing solution. Although all of the settings covered so far are foundational to using the Cisco Unified Communications Manager, you might need to configure other settings prior to a greenfield deployment or before expanding a brownfield deployment.

Groups

A Cisco Unified Communications Manager cluster is a collection of physical servers that work as a single IP PBX system. A Cisco Unified Communications Manager cluster may contain as many as 20 server nodes. Of these 20, a maximum of 8 servers may run the Cisco CallManager service to perform call processing in a cluster. Other services, such as dedicated database publisher, dedicated TFTP server, or MOH servers, may also be enabled on a separate server that registers with the cluster. The same holds true for media-streaming applications, such as the audio conference bridge or media termination point (MTP). Each cluster must provide a TFTP service. The TFTP service is responsible for delivering IP phone configuration files to telephones, along with streamed media files, such as MOH and ring files. Therefore, the server that is running the TFTP service can experience a considerable network and processor load. Depending on the number of devices that a server supports, you can run the TFTP service on a dedicated server, on the database publisher server, or on any other server in the cluster.

Cisco Unified Communications Manager *groups* are used to collect servers within a cluster that run the Cisco CallManager service to provide call-processing redundancy. A Cisco Unified Communications Manager group is a prioritized list of one or more call-processing servers. Architects and sales engineers designing Cisco Unified Communications Manager cluster solutions for customers should consider the following rules prior to building Cisco Unified Communications Manager groups:

Key Topic

- Multiple Cisco Unified Communications Manager groups can exist in the same cluster.
- Each call-processing server can be assigned to more than one Cisco Unified Communications Manager group.
- Each device must have a Cisco Unified Communications Manager group assigned, which will determine the primary and backup servers to which the device can register.

Cisco IP phones register with their primary server. When idle, the IP phones and the Cisco Unified Communications Manager exchange signaling application keepalives. In addition, Cisco IP phones establish a TCP session with their secondary server and exchange TCP keepalives. When the connection to the primary server is lost and no keepalive messages are received by the phone, the IP phone registers to the secondary server. The IP phone will continuously try to reestablish a connection with the primary server even after it has registered to the secondary server. Once a connection has been reestablished, the IP phone will register back to the primary server again.

Two models of redundancy can be configured on the Cisco Unified Communications Manager using groups. A 1:1 Cisco Unified Communications Manager redundancy deployment design guarantees that Cisco IP phone registrations will never overwhelm the backup servers, even if multiple primary servers fail concurrently. However, the 1:1 redundancy design has an increased server count compared with other redundancy designs and may not be cost effective. Figure 15-8 illustrates how a 1:1 redundancy design can be used with Cisco Unified Communications Manager groups.

In the first scenario of Figure 15-8, the two call-processing servers support a maximum of 10,000 Cisco IP phones. One of these two servers is the primary server; the other server is a dedicated backup server. The function of the database publisher and the TFTP server can be provided by the primary or secondary call-processing server in a smaller IP telephony deployment of fewer than 10,000 IP phones. In this case, only two servers are needed in total. When you increase the number of IP phones, you must increase the number of Cisco Unified Communications Manager servers to support those endpoints. Some network engineers may consider the 1:1 redundancy design excessive because a well-designed network is unlikely to lose more than one primary server at a time. With the low possibility of server loss and the increased server cost, many network engineers choose a 2:1 redundancy design.

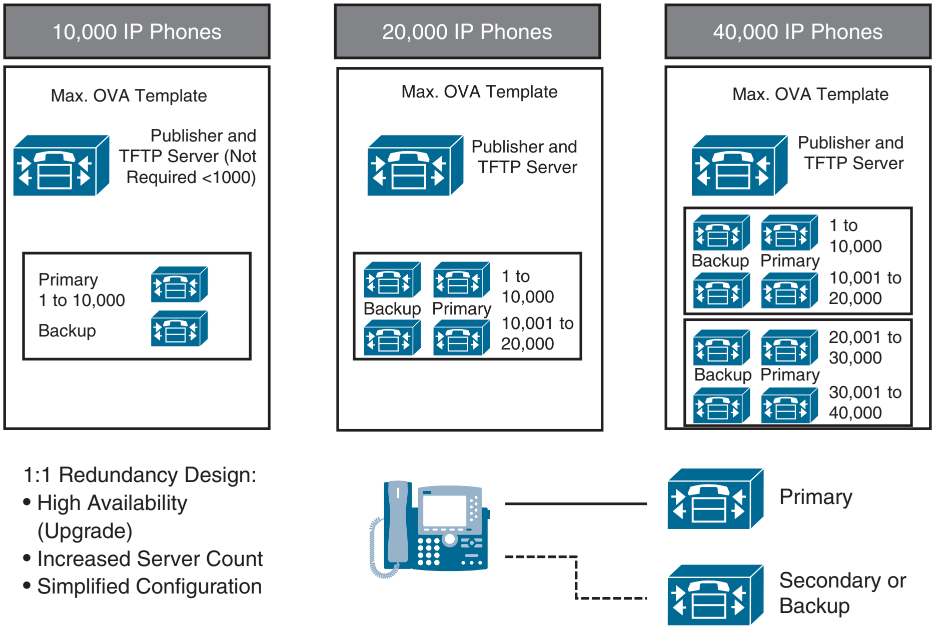


Figure 15-8 *Cisco Unified Communications Manager Groups Using 1:1 Redundancy*

Although the 2:1 redundancy design offers some redundancy, there is the risk of overwhelming the backup server if multiple primary servers fail. In addition, upgrading the Cisco Unified Communications Manager servers can cause a temporary loss of some services, such as TFTP or DHCP, because a reboot of the Cisco Unified Communications Manager servers is needed after the upgrade is complete. Even with the limitation presented, network engineers use this 2:1 redundancy model in most IP telephony deployments because of the reduced server costs. If a virtual machine with the largest OVA template is used, then the UCS server hosting that VM will be equipped with redundant, hot-swappable power supplies and hard drives. When these servers are properly connected and configured, it is unlikely that multiple primary servers will fail at the same time, which makes the 2:1 redundancy model a viable option for most businesses. Figure 15-9 illustrates how a 2:1 redundancy design can be used with Cisco Unified Communications Manager groups.

Notice that the first scenario is the same as shown in the 1:1 redundancy in Figure 15-8. When using no more than 10,000 IP phones, there are no savings in the 2:1 redundancy design compared with the 1:1 redundancy design simply because there is only a single primary server. In the scenario with up to 20,000 IP phones, there are two primary servers (each serving 10,000 IP phones) and one secondary server. As long as only one primary server fails, the backup server can provide complete support. If both primary servers failed, the backup server would be able to serve only half of the IP phones. The third scenario shows a deployment with 40,000 IP phones. Four primary servers are required to facilitate this number of IP phones. For each pair of primary servers, there is one backup server. As long as no more than two servers fail, the backup servers can provide complete support, and all IP phones will operate normally.

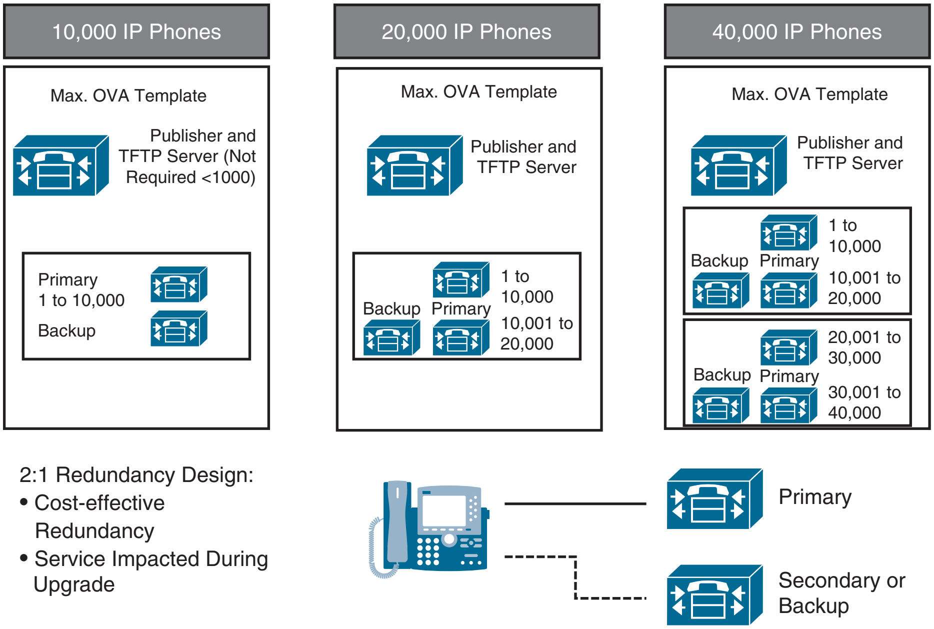


Figure 15-9 *Cisco Unified Communications Manager Groups Using 2:1 Redundancy*

Device Settings

While enterprise parameters deal with clusterwide settings and service parameters deal with server or service-related settings, device settings include parameters that are tied to individual devices or device pools. In several menus within the Cisco Unified Communications Manager, various device settings can be configured. An administrator can configure device settings under **Device > Device Settings** or under **Device > Phone**. In fact, many of the settings under the Phone menu depend on device settings being configured first.

When an administrator is configuring a phone in the Cisco Unified Communications Manager, some minimum settings must be configured before a phone can register. Those settings include Device Pool, Phone Button Template, Common Phone Profile, Owner User ID, Device Security Profile, and SIP Profile. The setting under the Device Pool menu warrants a deeper discussion, so that topic will be discussed more later. The Owner User ID setting is configured under **User Management > End User** and is required only if the Owner setting is set to User and not Anonymous (Public/Shared Space). The device security profile is configured under **System > Security > Phone Security Profile**. There are preconfigured nonsecure device security profiles in the Cisco Unified Communications Manager for all supported phone models. Additional phone security profiles need to be configured only if secure phone profiles are going to be used. The rest of the required settings for endpoint registration, which include Phone Button Template, Common Phone Profile, and SIP Profile, can be configured under **Device > Device Settings**.

The menu options under Device Settings include some preconfigured templates, but administrators can create custom templates for specific deployment scenarios. The sections that follow describe the most commonly used device settings.

Device Defaults

You can use device defaults to set the default characteristics of each type of device that registers with a Cisco Unified Communications Manager. The device defaults for a device type apply to all auto-registered devices of that type within a Cisco Unified Communications Manager cluster. You can set the following device defaults for each device type to which they apply:

- Device load
- Device pool
- Phone button template

When a device auto-registers with a Cisco Unified Communications Manager, it acquires the device default settings for its device type. After a device registers, you can update its configuration individually to change the device settings. Installing Cisco Unified Communications Manager automatically sets device defaults. You cannot create new device defaults or delete existing ones, but you can change the default settings.

Phone Button Template

Phone button templates are used to customize the line keys on a Cisco Unified IP phone. Cisco Unified Communications Manager includes default templates for each Cisco Unified IP phone model because the line keys are different on each phone model type. When you add phones, you can assign one of these templates to the phone or create a template of your own. You can make changes to the custom, nonstandard templates that you created, and you can change the label of the custom phone button template. You cannot change the function of the buttons in the default templates. You can update a custom, nonstandard phone button template to add or remove features; add or remove lines and speed dials; or assign features, lines, and speed dials to different buttons on the phone. You also can change the button labels in the default phone button templates, but you cannot change the function of the buttons in the default templates. If you update a phone template, be sure to inform affected users of the changes. The Programmable Line Key (PLK) feature expands the list of features that can be assigned to the line buttons to include features that are normally controlled by softkeys, such as New Call, Call Back, End Call, and Forward All. If you create a template for a Cisco Unified IP phone, you can change the default template for that phone during auto-registration.

Soft Key Template

Soft keys are the buttons on Cisco Unified IP phones that are located under the display and are usually associated with different menu options. Softkey templates can be used to manage softkeys that are associated with applications such as Cisco Unified Communications Manager Assistant, or features such as Call Back on Cisco Unified IP phones. Cisco Unified Communications Manager supports two types of softkey templates: standard and nonstandard. Standard softkey templates in the Cisco Unified Communications Manager database contain the recommended selection and positioning of the softkeys for an application. Cisco Unified Communications Manager provides the following standard softkey templates:

- Cisco Assistant with Feature Hardkeys
- Cisco Chaperone Phone with Feature Hardkeys

- Cisco Feature with Feature Hardkeys
- Cisco Manager with Feature Hardkeys
- Cisco Protected Phone with Feature Hardkeys
- Cisco Shared Mode Manager with Feature Hardkeys
- Cisco User with Feature Hardkeys
- Standard User
- Standard Chaperone Phone
- Standard Feature
- Standard Assistant
- Standard Protected Phone
- Standard Shared Mode Manager
- Standard Manager

To create a nonstandard softkey template, you can copy a standard softkey template and modify it. You can add and remove applications, and you can configure softkey sets for each call state. The Softkey Template Configuration window lists the standard and nonstandard softkey templates and uses different icons to differentiate between standard and nonstandard templates. After you have configured a softkey template, you can use any of the following configuration windows to assign the softkey template to devices:

- Common Device Configuration (Device > Device Settings > Common Device Configuration)
- Phone Configuration for SIP and SCCP phones (**Device > Phone > Phone Configuration**)
- UDP Template Configuration (**Bulk Administration > User Device Profiles > User Device Profile Template**)
- Default Device Profile Configuration (**Device > Device Settings > Default Device Profile**)

Phone Services

Using Cisco Unified Communications Manager Administration, you can define and maintain the list of IP phone services that can display on supported Cisco Unified IP phone models. IP phone services comprise XML applications or Cisco-signed Java MIDlets that enable the display of interactive content with text and graphics on some Cisco Unified IP phone models. Cisco Unified Communications Manager provides Cisco-provided default IP phone services, which install automatically with Cisco Unified Communications Manager. You can also create customized Cisco Unified IP phone applications for your site. After you configure the services, you can add services to the phones in the database, that is, if they are not classified as enterprise subscriptions, and you can assign the services to the Services, Directory, or Messages buttons/options, if the phone model supports these buttons/options. Users can log in to the Cisco Unified Communications Self Care Portal and subscribe to these services for their Cisco Unified IP phones, so long as these IP phone services are not classified as enterprise subscriptions.

SIP Profile

A Session Initiation Protocol (SIP) profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on. The profiles contain some standard entries that cannot be deleted or changed.

Device Pool Settings

Configuring device settings the way they are designed in the Cisco Unified Communications Manager is advantageous to administrators. When a phone is being configured in the Cisco Unified Communications Manager, the administrator needs to select only one device setting for a group of settings to apply to a single phone. However, many other settings under the **Device > Phone** menu still are not affected by the Device Settings menu options. Some of those settings include Media Resource Group List, Network MOH Audio Source, Location, AAR Group, and Network Locale. Although these settings can be configured individually for a phone, they can also be grouped together using a tool called a device pool in the Cisco Unified Communications Manager.

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 system, device, and location-related information. The Common Device Configuration window under **Device > Device Settings > Common Device Configuration** records all the user-oriented information such as type of softkey template that is used and locale information. You should ensure that each device is associated with a device pool and with a common device configuration for user-oriented information. After adding a new device pool to the database, you can use it to configure devices such as Cisco Unified IP phones, gateways, conference bridges, transcoders, media termination points, voicemail ports, CTI route points, and so on. Before you configure a device pool, you must configure the following items if you want to choose them for the device pool:

Key Topic

- **Cisco Unified Communications Manager Group:** This is a required field in the device pool. We already discussed the purpose and model options for Cisco Unified Communications Manager Groups earlier in this chapter. Device pools are used to apply this setting on endpoints.

- **Date/Time Group:** This is a required field. Network Time Protocol (NTP) was discussed in a previous chapter. Cisco Unified IP phones receive their NTP reference from the Cisco Unified Communications Manager. Date/Time groups are used to establish a common time zone, date format, and time format, along with the NTP reference.

- **Region:** This is also a required field. Regions are used to establish the codec selection and per-call bandwidth rate between phones registered to the Cisco Unified Communications Manager. This setting requires a deeper explanation, which is provided in the next section of this chapter.

- **SRST Reference:** This is an optional field. Survivable Remote Site Telephony is a redundancy feature available on Cisco IOS routers that allows Cisco Unified IP phones registered to the Cisco Unified Communications Manager from remote office locations to register to their local router during WAN network failure events. The SRST reference determines where those phones should register during these situations.

- **Media Resource Group List:** This is an optional field. MRGL is a prioritized list of media resource groups. These lists are used to determine which media resource should be used in various situations. Media resources could be Music on Hold (MOH), Conferencing, Annunciator, or other such resources.

Other fields within device pools can be configured beyond those mentioned here; however, the preceding list is a compilation of the most common settings configured in a device pool.

Codec Negotiations Using Regions

An enterprise network uses bandwidth for many different purposes, and all IP-based communication usually crosses the same network edge. You could have voice and video traffic crossing the WAN, while large files are being transferred to an FTP server at a remote location, and other devices are accessing email or other services in the cloud all at the same time. The result is that each of these devices competes for bandwidth across the company's network. Individual sites of a multisite deployment are usually interconnected by an IP WAN. Bandwidth on WAN links is limited and relatively expensive. Therefore, the goal is to use the available bandwidth as efficiently as possible. You should discourage unnecessary traffic, such as social media sites and personal use, and consider implementing methods for bandwidth optimization. Implementing QoS policies will certainly help during high congestion times across the network, but QoS will not prevent overutilization of bandwidth. Cisco has several Call Admission Control (CAC) mechanisms that can be implemented to control how bandwidth is used across your network.

Before we delve into how to implement CAC on the Cisco Unified Communications Manager, it is important to first understand what happens on the network when bandwidth is overutilized. Assume with this scenario that the WAN can handle up to 1 Mbps total bandwidth. If two endpoints place an audio call using G.711 codec for audio, then they will consume 87.2 kbps; 64 kb are for the payload, and 23.2 kb are for headers. That means that the WAN link can support up to roughly 11 calls, assuming no other network traffic is consuming bandwidth at the time of the calls. So, what happens when the twelfth call attempt is placed? The call isn't dropped. Rather, this call leg will begin barrowing bandwidth from the other existing calls, and everyone will suffer quality loss during their calls, even with proper QoS in place. This is where CAC comes into the picture. Using CAC in the Cisco Unified Communications Manager allows administrators to control the codec used on a per-call basis dependent on the sites between which calls are placed, as well as the overall bandwidth used when calls are placed across the WAN.

Regions are the first settings on the CUCM you should configure for Call Admission Control. Regions control the codecs used between endpoints when calls are set up. Careful planning should precede implementing regions to avoid call drops and quality issues related to codec mismatch between regions. A specific bandwidth allocation is associated with each audio codec, so you can easily plan and predict how much bandwidth is going to be consumed. G.711 is an uncompressed codec and consumes 87.2 kbps per call with average audio quality. G.729 is a compressed audio codec that consumes only 31.2 kbps but suffers from poorer quality. Other codecs can be compressed or uncompressed and will have varying levels of quality accordingly.

Compression involves utilizing encoding algorithms to reduce the size of digital data. Compressed data must be decompressed to be used. This extra processing imposes computational or other costs into the transmission hardware. *Lossless* and *lossy* are descriptive terms used to describe whether or not the data in question can be recovered exactly bit-for-bit, when the file is uncompressed or whether the data will be reduced by permanently altering or eliminating certain bits, especially redundant bits. Lossless compression searches content for statistically redundant information that can be represented in a compressed state without losing any original information. By contrast, lossy compression searches for nonessential content that can be deleted to conserve storage space. Figure 15-10 illustrates the differences between lossless and lossy compression.

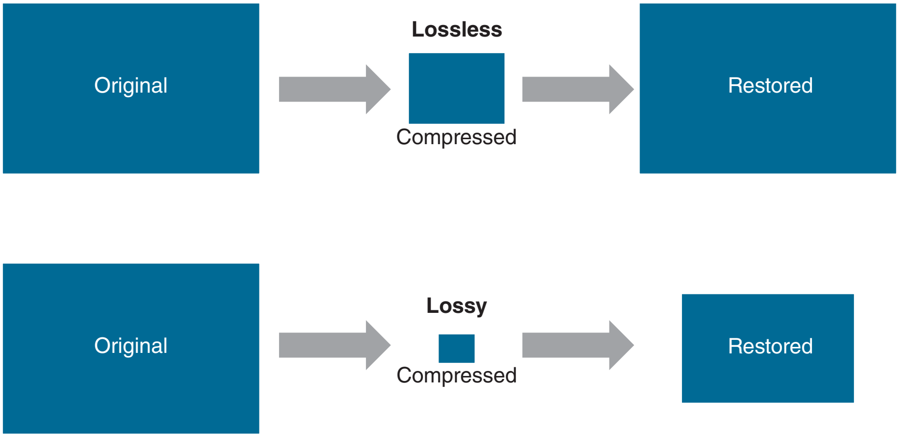


Figure 15-10 *Compression Types with Regions*

When configuring region settings for audio in the Cisco Unified Communications Manager, the administrator simply needs to select the compression type and audio codec preference. Audio media is so predictable that the bandwidth used is based directly on the codec selection. However, video is very greedy and bursty when it comes to bandwidth consumption. Video codecs do not have a specific set bandwidth rate to them like audio codecs. A video call can be placed using 480p30 resolution at 384 kbps or at 2 Mbps. However, using a higher codec can provide better efficiency and thus consume less bandwidth. Therefore, when configuring regions in the Cisco Unified Communications Manager, administrators do not select a codec specifically; instead, they set the per-call bandwidth rate that is allowed between each site. There are two fields to configure video bit rates in the Regions settings page:

- The Video Calls column has to do with UC endpoints that can place video calls, such as the 8845 and 8865 IP video phones and Jabber client.
- The Immersive Video Calls column has to do with any Cisco Telepresence video endpoint, such as the DX80, MX700, SX80, or Webex endpoints.

Table 15-2 identifies the average bandwidth consumption for various video resolutions per the four main video codecs. The bandwidth rates represented in the table do not reflect any overhead calculations.

Table 15-2 Average Bandwidth Consumption per Video Codec

Codec	H.261	H.263	H.264	H.265 HEVC
Bandwidth rate at 480p30	512 kbps	384 kbps	256 kbps	128 kbps
Bandwidth rate at 720p30	N/A	1024 kbps	768 kbps	384 kbps
Bandwidth rate at 1080p30	N/A	1536 kbps	1024 kbps	512 kbps
Bandwidth rate at 1080p60	N/A	N/A	2048 kbps	1024 kbps
Bandwidth rate at 4Kp60	N/A	N/A	N/A	2048 kbps

Follow these steps to configure region information on the Cisco Unified Communications Manager:

Step 1. In a web browser, navigate to the address of the Cisco Unified Communications Manager followed by /ccmadmin and log in. For example, if the address were cucm.company.com, you would navigate to https://cucm.company.com/ccmadmin.

Step 2. Navigate to **System > Region Information > Region** and click the **Find** button. One region, called Default, will exist.

Step 3. Click the **Add New** button to create a new region.

Step 4. Give it a name, such as **RTP_Region**, and click the **Save** button.

Step 5. Two other sections will open below: Region Relationships and Modify Relationship to Other Regions. Under the second section, select your region from the list in the Regions box and modify the codec selection as mentioned here:

a. **Audio Codec Preference List:** Use System Default (Factory Default low loss)

b. **Maximum Audio Bit Rate:** 64 kbps (G.722, G.711)

c. **Maximum Sessions Bit Rate for Video Calls:** 2048 kbps

d. **Maximum Sessions Bit Rate for Immersive Video Calls:** 2048 kbps

Step 6. Click the **Save** button when finished. This action establishes the codec selection between endpoints using the same RTP_Region.

Step 7. You can create additional regions and determine a codec selection when calling between these regions. For example, on the same page, select the **Default** region and change the codec selections as noted here:

a. **Audio Codec Preference List:** Factory Default Lossy

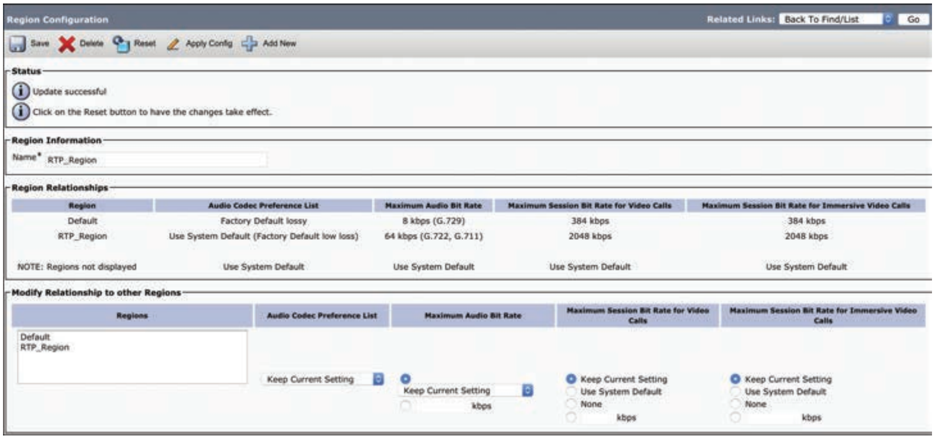
b. **Maximum Audio Bit Rate:** 8 kbps (G.729)

c. **Maximum Sessions Bit Rate for Video Calls:** 384 kbps

d. **Maximum Sessions Bit Rate for Immersive Video Calls:** 384 kbps

Step 8. Click the **Save** button again.

Both regions should be added to the Region Relationships section, but different codecs will be listed for each. When an endpoint assigned the RTP_Region calls an endpoint assigned the Default region, a different audio compression, codec, and video bandwidth rate will be used, as compared to two endpoints that are both assigned the RTP_Region. Region settings are bidirectional; therefore, any settings configured in one region will automatically be reflected in other regions. Locations play hand-in-hand with regions, but that discussion will be saved for a later chapter. Figure 15-11 illustrates the region settings as described in the preceding steps.



Status

Update successful

Click on the Reset button to have the changes take effect.

Region Information

Name* RTP_Region

Region Relationships

Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Default	Factory Default lossy	8 kbps (G.729)	384 kbps	384 kbps
RTP_Region	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	2048 kbps	2048 kbps
NOTE: Regions not displayed	Use System Default	Use System Default	Use System Default	Use System Default

Modify Relationship to other Regions

Regions	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Default RTP_Region	Keep Current Setting	● Keep Current Setting ○ kbps	● Keep Current Setting ○ Use System Default ○ None ○ kbps	● Keep Current Setting ○ Use System Default ○ None ○ kbps

Figure 15-11 *Region Settings*

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics 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.

Key Topic

Table 15-3 Key Topics for Chapter 15

Key Topic Element	Description	Page Number
List	CUCM Network Services	350
List	CUCM Feature Services	352
Paragraph	Enterprise Parameters Explained	353
List	Cisco CallManager Service Parameter Settings	356
List	Rules for Creating Cisco Unified Communications Manager Groups	358

Key Topic Element	Description	Page Number
List	Device Pool Menu Options	363
Table 15-2	Average Bandwidth Consumption per Video Codec	366
Steps	Configuring Regions in the CUCM	366

Define Key Terms

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

CDR, CMR, Codec, Compression, Enterprise Parameters, Groups, H.261, H.263, H.264, H.265 HEVC, Java MIDlets, Lossless, Lossy, MRGL, Network Services, Regions, Service Parameters, Services, SRST, T302 Timer, XML Applications

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the eight different feature service categories available on the Cisco Unified Communications Manager.
2. Define *enterprise parameters*.
3. What are the three most important CallManager service parameters mentioned in this book?
4. What are the two models of redundancy that can be configured on the Cisco Unified Communications Manager using groups?
5. List and define the two main compression types available through CUCM regions.

This page intentionally left blank

CHAPTER 16

LDAP Integration with Cisco Unified Communications Manager

This chapter covers the following topics:

Application Users and End Users: This topic will introduce the two types of user accounts available on the Cisco Unified Communications Manager and how they relate to a Lightweight Directory Access Protocol (LDAP) integration.

Cisco Unified Communications Directory Architecture: This topic will overview the local directory architecture as it exists within the Cisco Unified Communications Manager.

LDAP Synchronization: This topic will delve into the intricate components of an LDAP synchronization with the Cisco Unified Communications Manager.

LDAP Authentication: This topic will examine how LDAP authentication works in a Cisco Unified Communications Manager environment in conjunction with LDAP synchronization.

The preceding chapter examined different components that should be configured on the Cisco Unified Communications Manager before it can be used in a production environment. This chapter builds on that chapter by examining the differences between application users and end users within the Cisco Unified Communications Manager and what the purpose of each type of user entails. From there, this chapter continues down the journey to an LDAP integration with the Cisco Unified Communications Manager for both synchronization and authentication. Topics discussed in this chapter include the following:

- Application Users and End Users
- Cisco Unified Communications Directory Architecture
- LDAP Synchronization
  - Synchronization Mechanism
  - Automatic Line Creation
  - Enterprise Group Support
  - Security Considerations
  - Design Considerations for LDAP Synchronization
  - Additional Considerations for Microsoft AD

- LDAP Authentication
  - Design Considerations for LDAP Authentication
  - Additional Considerations for Microsoft AD

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 1.4.c LDAP integration on Cisco UCM

"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
Application Users and End Users	1
Cisco Unified Communications Directory Architecture	2
LDAP Synchronization	3–9
LDAP Authentication	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 end-user settings can be set only from a Cisco Unified Communications Manager and not imported from LDAP?
   a. User ID
   b. Last name
   c. Password
   d. PIN
2. What is defined as the management of individuals and the authentication and authorization of these individuals?
   a. SSO
   b. Identity Management
   c. LDAP
   d. UPN

3. Which of the following is the Microsoft AD attribute equivalent to the user ID on the CUCM?

a. sAMAccountName

b. uid

c. sn

d. objectGUID

4. When the CUCM is integrated with an LDAP directory, when does the garbage collection process remove inactive user accounts?

a. As soon as they go inactive.

b. Once every 24 hours at the configured time.

c. Once every 24 hours at 3:15 a.m.

d. Garbage collection is not part of the LDAP process.

5. If the number 14085551234 exists in the LDAP directory and the synchronization agreement includes the mask +XXXXXXXXXXXXXXXXX, what will the resulting match be when synchronization runs?

a. 14085551234

b. +14085551234

c. +14085551234140855

d. No resulting number will match because there are too many wildcard characters to match the phone number.

6. What is the maximum number of enterprise groups supported through an LDAP synchronization to the CUCM?

a. 150

b. 1500

c. 15,000

d. 150,000

7. Which of the following security measures can be included through LDAP synchronization on the CUCM?

a. PINs can be imported to the CUCM.

b. Passwords can be imported to the CUCM.

c. SLDAP can encrypt signaling only.

d. SLDAP can encrypt data using SSL.

8. Which of the following is a consideration for LDAP synchronization?

a. All synchronization agreements on a given cluster can integrate with any family of LDAP servers.

b. Synchronization agreements should be scheduled so that multiple agreements query the same LDAP servers simultaneously. You should choose synchronization times that occur during quiet off-peak hours.

  c. If security of user data is required, you should enable Secure LDAP by checking the Use SSL field on the LDAP directory configuration page in the Cisco Unified Communications Manager Administration.

  d. Ensure that the LDAP directory attribute chosen to map into the Cisco Unified Communications Manager User ID field is the same within all synchronization agreements for that cluster.

9. An organization has an AD tree structure that incorporates users under the root domain cisco.com as well as the two child domains emea.cisco.com and apac.cisco.com. How many synchronization agreements are required to import all the users?

  a. One

  b. Two

  c. Three

  d. It can be done with one or three agreements.

10. Which of the following statements is true?

  a. Application users are always authenticated against the local database on the CUCM.

  b. PINs are always authenticated against the local database on the CUCM.

  c. Synchronized end users are authenticated against the local database on the CUCM unless authentication has been configured.

  d. All these answers are correct.

Foundation Topics

Application Users and End Users

Although this chapter describes LDAP integration, it is essential to first understand users within the Cisco Unified Communications Manager. By default, all users are provisioned manually in the publisher database through the Cisco Unified Communications Manager Administration web interface. There are two types of user accounts in the Cisco Unified Communications Manager: end users and application users. All end users are associated with a physical person and an interactive login. This category includes all IP telephony users as well as Cisco Unified Communications Manager administrators when using the user groups and roles configurations. The attributes that are associated with end users are separated into three categories and include the following information:

Key Topic

- **Personal and organizational settings:**
  - User ID
  - Last Name
  - Middle Name
  - First Name
  - Phone Numbers

    - Mail ID
    - Manager User ID
    - Department
- **Password**
- **Cisco Unified Communications Manager Settings:**
    - PIN
    - [SIP] Digest Credentials
    - Associated PC/Site Code
    - Controlled Devices
    - Extension Mobility
    - Directory Numbers Associations
    - Mobility Information
    - Multilevel Precedence and Preemption Authorization (MLPP)
    - CAPF Information
    - Permissions Information (Groups and Roles)

All application users are associated with Cisco Unified Communications Manager features or applications, such as Cisco Unified Contact Center Express or Cisco Unified CM Assistant. These applications must authenticate with Cisco Unified Communications Manager, but these internal "users" do not have an interactive login and serve purely for internal communications between applications. Table 16-2 lists the application users created by default in the Unified CM database, together with the feature or application that uses them. Additional application users can be created manually when integrating other Cisco Unified Communications applications, such as the AC application user for Cisco Attendant Console or the JTAPI application user for Cisco Unified Contact Center Express.

Key Topic

Table 16-2 Default Application Users in the CUCM

Application User	Used by
CCMAdministrator	Unified CM Administration (default "super user")
CCMQRTSecureSysUser	Cisco Quality Reporting Tool
CCMQRTSysUser	Cisco Quality Reporting Tool
CCMSysUser	Cisco Extension Mobility
IPMASecureSysUser	Cisco Unified Communications Manager Assistant
IPMASysUser	Cisco Unified Communications Manager Assistant
WDSecureSysUser	Cisco WebDialer
WDSysUser	Cisco WebDialer

End users access the Cisco Unified Communications Manager User Options page via HTTPS and authenticate with a username and password. If they have been configured as administrators by means of user groups and roles, they can also access the Cisco Unified Communications Manager Administration pages with the same credentials. Similarly, other Cisco features and applications authenticate to the Cisco Unified Communications Manager via HTTPS with the username and password associated with their respective applications' user account. The authentication challenge carried by the HTTPS messages are relayed by the web service on the Cisco Unified Communications Manager to an internal library called the Identity Management System (IMS). In its default configuration, the IMS library authenticates both end users and application users against the embedded database. In this way, both "physical" users of the Unified Communications system and internal application accounts are authenticated using the credentials configured in the Cisco Unified Communications Manager. End users may also authenticate with their username and a numeric PIN when logging in to the Extension Mobility service from an IP phone. In this case, the authentication challenge is still relayed by the web service to the IMS library, which authenticates the credentials against the embedded database but is carried via HTTP to Cisco Unified Communications Manager instead of HTTPS. In addition, user lookups performed by UC endpoints via the Directories button communicate with the web service on the Cisco Unified Communications Manager via HTTP and access data on the embedded database.

The important distinction between end users and application users becomes apparent when integration with a corporate directory is required. This integration is accomplished by means of the following two separate processes:

- **LDAP synchronization:** This process uses an internal tool called Cisco Directory Synchronization, or DirSync, on the Cisco Unified Communications Manager to synchronize a number of user attributes from a corporate LDAP directory. When this feature is enabled, users are automatically provisioned from the corporate directory in addition to local user provisioning through the Cisco Unified Communications Manager Administration GUI. This means that the Cisco Unified Communications Manager can support both end users synchronized from an LDAP directory and locally generated users simultaneously. This feature applies only to end users, whereas application users are kept separate and are still provisioned via the Cisco Unified Communications Manager Administration interface. Also, synchronization allows access to only certain user information—specifically, the personal and organizational settings listed at the beginning of this section. Password and Cisco Unified Communications Manager settings must still be configured locally on the Cisco Unified Communications Manager. The frequency that information will synchronize from the LDAP server to the Cisco Unified Communications Manager can also be configured. The default setting is to allow only a single synchronization at the time LDAP is first set up.
- **LDAP authentication:** This process enables the IMS library to authenticate user credentials of LDAP synchronized end users against a corporate LDAP directory using the LDAP standard Simple_Bind operation. When this feature is enabled, end-user passwords of LDAP-synchronized end users are authenticated against the corporate directory, while application-user passwords and passwords of local end users are still authenticated locally against the Cisco Unified Communications Manager database.

Cisco Extension Mobility PINs are also still authenticated locally. In fact, all settings previously listed under the Cisco Unified Communications Manager Settings must always be configured locally on the Cisco Unified Communications Manager.

Key Topic

Maintaining and authenticating the application users internally to the Cisco Unified Communications Manager database provide resilience for all the applications and features that use these accounts to communicate with the Cisco Unified Communications Manager, independent of the availability of the corporate LDAP directory. Cisco Extension Mobility PINs are also kept within the Cisco Unified Communications Manager database because they are an integral part of a real-time application, which should not have dependencies on the responsiveness of the corporate directory. Later sections describe in more detail LDAP synchronization and LDAP authentication, and they provide design best practices for both functions. In summary, end users can be defined locally, or they can be defined in the corporate directory and synchronized into the Cisco Unified Communications Manager database, whereas application users are only stored locally in the Cisco Unified Communications Manager database and cannot be defined in the corporate directory.

Cisco Unified Communications Directory Architecture

Identity management is a fundamental concept required in any application. Identity management involves the management of individuals and the authentication and authorization of these individuals. Historically, each application handled identity management individually. This led to a situation where users had to authenticate against every individual application. Centralizing identity management, authentication, and authorization helps greatly to improve the user experience by providing services such as single sign-on (SSO).

The first step of centralizing identity management is to centralize storage of information about individuals in an enterprise. These centralized enterprisewide datastores are commonly known as directories. Directories are specialized databases that are optimized for a high number of reads and searches, and occasional writes and updates. Directories typically store data that does not change often, such as employee information, user privileges, and group membership on the corporate network. Directories are extensible, meaning that the type of information stored can be modified and extended. The term *directory schema* defines the type of information stored, its container (or attribute), and its relationship to users and resources.

The Lightweight Directory Access Protocol (LDAP) provides applications with a standard method for accessing and potentially modifying the information stored in the directory. This capability enables companies to centralize all user information into a single repository and then make that information available to several applications. This offers a remarkable reduction in maintenance costs through the ease of adds, moves, and changes.

The embedded database on the Cisco Unified Communications Manager stores all configuration information, including device-related data, call routing, feature provisioning, and user profiles. This database is present on all servers within a Cisco Unified Communications Manager cluster and is replicated automatically from the publisher server to all subscriber servers. Figure 16-1 shows the basic architecture of a Cisco Unified Communications Manager cluster.

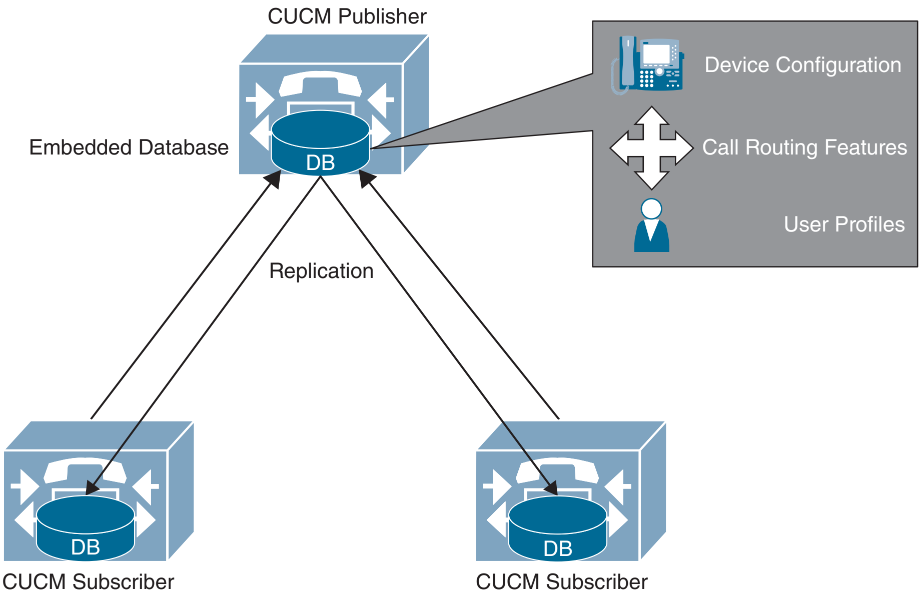
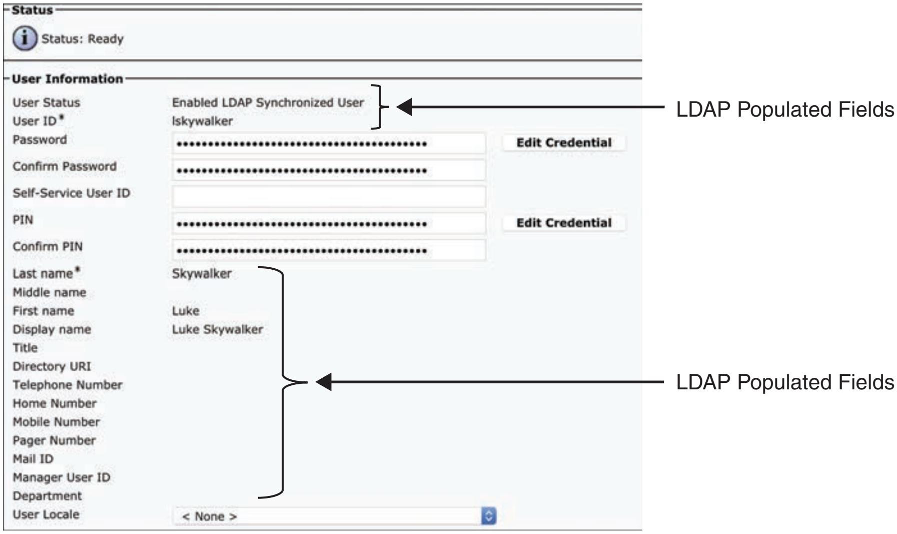


Figure 16-1 *Basic Architecture of a Cisco Unified Communications Manager Cluster*

LDAP Synchronization

Synchronization of the Cisco Unified Communications Manager with a corporate LDAP directory allows the administrator to provision users easily by mapping Cisco Unified Communications Manager data fields to directory attributes. Critical user data maintained in the LDAP store is copied into the appropriate corresponding fields in the Cisco Unified Communications Manager database on a scheduled or on-demand basis. The corporate LDAP directory retains its status as the central repository. The Cisco Unified Communications Manager has an integrated database for storing user data and a web interface within the Cisco Unified Communications Manager Administration for creating and managing user accounts and data. When LDAP synchronization is enabled, the local database is still used, and additional local end-user accounts can be created. Management of end-user accounts is then accomplished through the interface of the LDAP directory and the Cisco Unified Communications Manager Administration GUI collectively. Accounts for application users can be created and managed only through the Cisco Unified Communications Manager Administration web interface.

The end user account information is imported from the LDAP directory into the database located on the Cisco Unified Communications Manager publisher server. Information that has been imported from the LDAP directory cannot be changed locally on the Cisco Unified Communications Manager. User information synchronized from the LDAP directory can be converted to local user information so that the user information can then be edited locally on the Cisco Unified Communications Manager but will not change the information within the LDAP directory in any capacity. Additional user information specific to the Cisco Unified Communications Manager can be configured locally and is stored only within the local database. Device-to-user associations, speed dials, call forward settings, and user PINs are all examples of data that is managed by the Cisco Unified Communications Manager and does not exist in the corporate LDAP directory. The user data is then propagated from the Cisco Unified Communications Manager publisher server to the subscriber servers through the built-in database synchronization mechanism. Figure 16-2 illustrates the populated fields in an end-user account through an LDAP synchronization. Notice that the data that has populated fields through the LDAP synchronization cannot be changed or deleted in any way.



Status

Status: Ready

User Information

User Status	Enabled LDAP Synchronized User	
User ID*	lskywalker	
Password	••	Edit Credential
Confirm Password	••	
Self-Service User ID		
PIN	••	Edit Credential
Confirm PIN	••	
Last name*	Skywalker	
Middle name		
First name	Luke	
Display name	Luke Skywalker	
Title		
Directory URI		
Telephone Number		
Home Number		
Mobile Number		
Pager Number		
Mail ID		
Manager User ID		
Department		
User Locale	< None >	

LDAP Populated Fields

LDAP Populated Fields

Figure 16-2 *End-User Fields Populated Through LDAP Synchronization*

Local end users can be added manually using the Cisco Unified Communications Manager Administration GUI after an LDAP synchronization. During an LDAP sync, an existing locally created end user can be converted to an active LDAP user if a user with the same user ID is found in the LDAP directory. The locally configured data is then replaced with data from the directory and can no longer be changed locally on the Cisco Unified Communications Manager.

When LDAP synchronization is activated, only one type of LDAP directory may be chosen globally for the cluster at any one time. Several types of LDAP services are supported on the Cisco Unified Communications Manager, such as Microsoft Active Directory (AD), Oracle DSEE, SUN, and OpenLDAP. Even within the Microsoft AD option, there are many different choices, such as Microsoft Active Directory Application Mode (ADAM) or Active Directory Lightweight Directory Service (AD LDS). Also, one attribute of the LDAP directory user is chosen to map into the Cisco Unified Communications Manager User ID field. The steps to enable the LDAP system on the Cisco Unified Communications Manager are as follows:

Step 1. Change the Navigation drop-down to Cisco Unified Serviceability and click **Go**.

Step 2. Navigate to **Tools > Service Activation**, select the Publisher server from the list, and click **Go**.

Step 3. Check the box next to the **Cisco DirSync** service and click **Save**.

Step 4. After the service has been verified as Active, change the Navigation drop-down to **Cisco Unified CM Administration** and click **Go**.

Step 5. Navigate to **System > LDAP > LDAP System.**

Step 6. Check the box beside the **Enable Synchronizing from LDAP Server setting.**

Step 7. In the LDAP Server Type drop-down menu, select the type of LDAP server that will be used for this deployment, such as Microsoft Active Directory.

Step 8. In the LDAP Attribute for User ID drop-down menu, select the attribute that will be used to identify user accounts within the LDAP directory database (refer to Table 16-3 for the LDAP Directory Attribute Map).

The Cisco Unified Communications Manager uses standard LDAPv3 to access the data and imports data from standard attributes. Therefore, extending the directory schema is not required. The data of the directory attribute that is mapped to the Cisco Unified Communications Manager user ID must be unique within all entries for that cluster. The attribute mapped to the Cisco Unified Communications Manager UserID field must be populated in the directory, and the sn attribute must be populated with data; otherwise, those records are skipped during the import. If the primary attribute used during the import of end-user accounts matches any application user in the Cisco Unified Communications Manager database, that user is not imported from the LDAP directory. Table 16-3 lists the attributes that are imported from the LDAP directory into corresponding Cisco Unified Communications Manager user fields, and it describes the mapping between those fields. Some Cisco Unified Communications Manager user fields might be mapped from one of several LDAP attributes.

Key Topic

Table 16-3 LDAP Directory Attribute Map

CUCM User Field	Microsoft AD	ADAM or AD LDS	Oracle DSEE and SUN	OpenLDAP and Other LDAPv3 Types
User ID	One of:	One of:	One of:	One of:
	sAMAccountName	uid	uid	uid
	mail	mail	mail	mail
	employeeNumber	employeeNumber	employee-Number	employeeNumber
	telephoneNumber	telephoneNumber	telephone-Number	telephoneNumber
	userPrincipalName	userPrincipal-Name	userPrincipal-Name	userPrincipal-Name
First Name	givenName	givenName	givenName	givenName
Middle Name	One of:	One of:	initials	initials
	middleName	middleName		
	initials	initials		
Last Name	sn	sn	sn	sn
Manager ID	manager	manager	manager	manager
Mail ID	One of:	One of:	One of:	One of:
	mail	mail	mail	mail
	sAMAccountName	uid	uid	uid

CUCM User Field	Microsoft AD	ADAM or AD LDS	Oracle DSEE and SUN	OpenLDAP and Other LDAPv3 Types
objectGUID	objectGUID	objectGUID	N/A	N/A
Title	title	title	Title	title
Home Phone Number	homePhone	homePhone	Homephone	homeTelephone Number
Mobile Phone Number	mobile	mobile	Mobile	mobileTelephone Number
Directory URI	One of:	One of:	One of:	One of:
	msRTCSIP-PrimaryUserAddress	mail	mail	mail
	mail	none	none	none
	none			
Display Name	displayName	displayName	displayName	displayName

The synchronization is performed by a process called Cisco Directory Synchronization (or DirSync), which is enabled through the Serviceability web page. When enabled, it allows 1 to 20 synchronization agreements to be configured in the system. This number is reduced to 10 if more than 80,000 users are synchronized. An agreement specifies a search base that is a position in the LDAP tree where the Cisco Unified Communications Manager will begin its search for user accounts to import. The Cisco Unified Communications Manager can import only users that exist in the domain specified by the search base for a particular synchronization agreement. Figure 16-3 illustrates how two synchronization agreements can be represented to create a more granular LDAP search base.

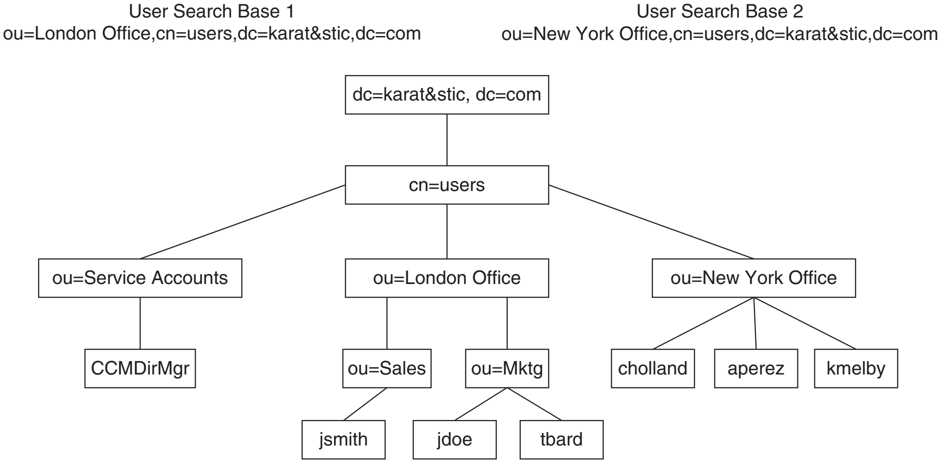


Figure 16-3 *Using Two Synchronization Agreements in an LDAP Search*

One synchronization agreement specifies User Search Base 1 and imports users jsmith, jdoe, and tbard. The other synchronization agreement specifies User Search Base 2 and imports users cholland, aperez, and kmelby. The CCMDirMgr is not imported because the Service Accounts organizational unit does not reside below the point specified by a user search base. When users are organized in a structure in the LDAP directory, that structure can be used to control which user groups are imported. In the tree structure represented in Figure 16-3, a single synchronization agreement could have been used to specify the root of the domain, such as cn=users,dc=karat&stic,dc=com. However, that search base would have also imported CCMDirMgr. The search base does not have to specify the domain root; it may specify any point in the tree.

To import the data into the Cisco Unified Communications Manager database, the system performs a bind to the LDAP directory using the account specified in the configuration as the LDAP Manager Distinguished Name, and the database is read with this account. The account must be available in the LDAP directory for the Cisco Unified Communications Manager to log in, and Cisco recommends that you create a specific account with permissions to allow it to read all user objects within the subtree that was specified by the user search base. The sync agreement specifies the full distinguished name of that account so that the account may reside anywhere within that domain. In Figure 16-3, CCMDirMgr is the account used for the synchronization. It is possible to control the import of accounts through use of permissions of the LDAP Manager Distinguished Name account. In this example, if that account is restricted to have read access to ou=Sales but not to ou=Mktg, then only the accounts located under Sales will be imported. You can use the following steps to configure the synchronization agreement on the Cisco Unified Communications Manager. Figure 16-4 illustrates the main fields that need to be configured when creating a synchronization agreement.

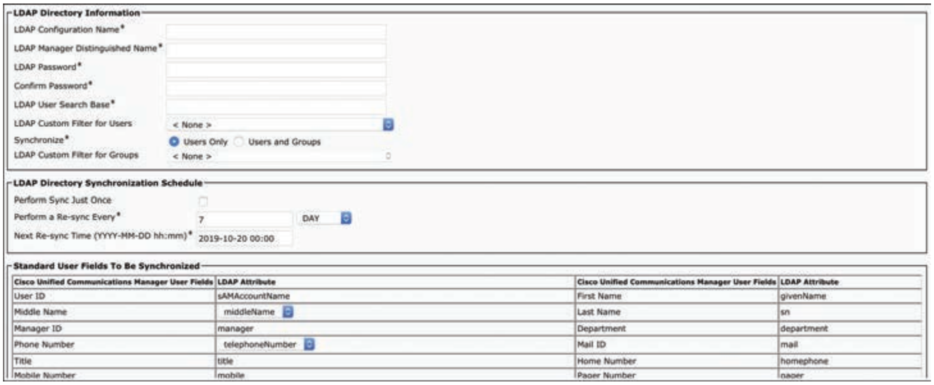
Step 1. Navigate to **System > LDAP > LDAP Directory** and click **Add New**.

Step 2. Enter appropriate information in the following fields. The following examples are intended only to provide a guideline as to how these settings can be configured.

- **a.** **LDAP Configuration Name**: Karat&STIC Users
- **b.** **LDAP Manager Distinguished Name:** cn=CCMDirMgr,ou=Service Accounts,cn=users,dc=karat&stic,dc=com
- **c.** **LDAP Password:** <enter a secure password>
- **d.** **Confirm Password:** <enter password again>
- **e.** **LDAP User Search Base:** ou=London Office,cn=users,dc=karat&stic,dc=com

Step 3. Add the LDAP server address at the bottom of the page and click **Save**.

In addition to the direct mapping of directory attributes to local user attributes, other characteristics of the synchronized users are determined by settings on the LDAP directory synchronization agreement. Access Control Group membership of users created through LDAP synchronization is directly configured in the LDAP directory configuration setting. Further user capabilities are determined by the feature group template selected. The selection of a feature group template on an LDAP directory synchronization agreement is optional. The feature group templates allow administrators to define user characteristics, including home cluster selection, IM and Presence capabilities, mobility features, services profiles, and user profiles. The user profiles allow administrators to define a universal line template that is considered for automatic creation of directory numbers for LDAP synchronized users by the Cisco Unified Communications Manager.



LDAP Directory Information

LDAP Configuration Name*

LDAP Manager Distinguished Name*

LDAP Password*

Confirm Password*

LDAP User Search Base*

LDAP Custom Filter for Users: < None >

Synchronize*: ● Users Only ○ Users and Groups

LDAP Custom Filter for Groups: < None >

LDAP Directory Synchronization Schedule

Perform Sync Just Once □

Perform a Re-sync Every*: 7 DAY

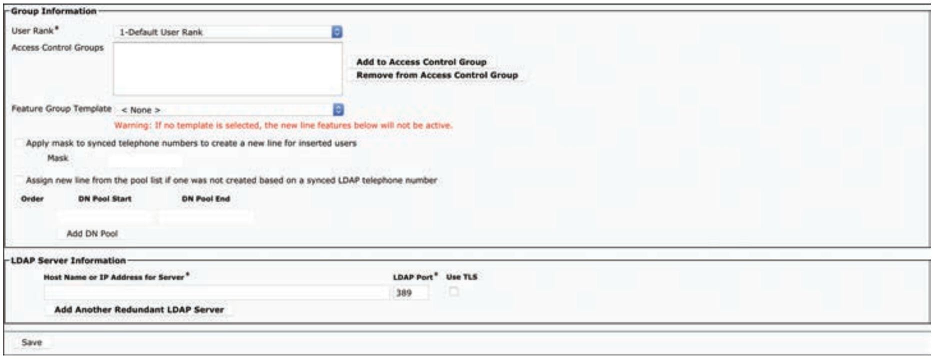
Next Re-sync Time (YYYY-MM-DD hh:mm)*: 2019-10-20 00:00

Standard User Fields To Be Synchronized

Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified Communications Manager User Fields	LDAP Attribute
User ID	sAMAccountName	First Name	givenName
Middle Name	middleName	Last Name	sn
Manager ID	manager	Department	department
Phone Number	telephoneNumber	Mail ID	mail
Title	title	Home Number	homephone
Mobile Number	mobile	Pager Number	pager

Figure 16-4 *Synchronization Agreement Configuration Fields*

Synchronization agreements also can specify multiple directory servers to provide redundancy. You can specify an ordered list of up to three directory servers in the configuration that will be used when attempting to synchronize. The servers are tried in order until the list is exhausted. If none of the directory servers respond, then the synchronization fails, but it will be attempted again according to the configured synchronization schedule. Figure 16-5 illustrates the synchronization agreement fields for Access Control Group memberships and the addition of redundant LDAP servers.



Group Information

User Rank*: 1-Default User Rank

Access Control Groups

Feature Group Template: < None >

Warning: If no template is selected, the new line features below will not be active.

□ Apply mask to synced telephone numbers to create a new line for inserted users

Mask

□ Assign new line from the pool list if one was not created based on a synced LDAP telephone number

Order DN Pool Start DN Pool End

LDAP Server Information

Host Name or IP Address for Server* LDAP Port* Use TLS

389 □

Figure 16-5 *Synchronization Agreement Fields for Access Control Groups and Redundant LDAP Servers*

Synchronization Mechanism

The synchronization agreement specifies a time for synchronizing to begin and a period for resynchronizing that can be specified in hours, days, weeks, or months (with a minimum value of six hours). A synchronization agreement can also be set up to run only once at a specific time.

When synchronization is enabled for the first time on a Cisco Unified Communications Manager publisher server, user accounts that exist in the corporate directory are imported into the Cisco Unified Communications Manager database. Then either existing end-user accounts are activated and data is updated, or a new end-user account is created according to the following process:

1. If end-user accounts already exist in the Cisco Unified Communications Manager database and a synchronization agreement is configured, all preexisting accounts that have been synchronized from LDAP previously are marked inactive in the Cisco Unified Communications Manager. The configuration of the synchronization agreement specifies a mapping of an LDAP database attribute to the Cisco Unified Communications Manager user ID. During the synchronization, accounts from the LDAP database that match an existing Cisco Unified Communications Manager account cause that account to be marked active again.
2. After the synchronization is completed, any LDAP synchronized accounts that were not set to active are permanently deleted from the Cisco Unified Communications Manager when the garbage collection process runs. Garbage collection is a process that runs automatically at the fixed time of 3:15 a.m., and it is not configurable. However, garbage collection will not delete any inactive accounts until they have been inactive for at least 24 hours.
3. Subsequently when changes are made in the corporate directory, the synchronization from Microsoft Active Directory occurs as a full resynchronization at the next scheduled synchronization period. On the other hand, the Sun ONE directory products perform an incremental synchronization triggered by a change in the directory.

After users are synchronized from LDAP into the Cisco Unified Communications Manager database, deletion of a synchronization configuration will cause users that were imported by that configuration to be marked inactive in the database. Garbage collection will subsequently remove those users at the predetermined time. Users deleted from the Cisco Unified Communications Manager will not be deleted from the LDAP server. The issue that may arise with an Active Directory integration is that the accounts in the Cisco Unified Communications Manager that were deleted in Active Directory will not be marked inactive until the scheduled resynchronization time occurs. User passwords will no longer work because they must be authenticated against the LDAP database itself; however, local PINs on the Cisco Unified Communications Manager will still work. If an account has been created in Active Directory, it will be imported into the Cisco Unified Communications Manager at the periodic resynchronization that occurs and will immediately be active on the Cisco Unified Communications Manager.

Sun ONE products support incremental synchronization agreements and use a different synchronization timeline from Microsoft Active Directory. The synchronization makes use of the Persistent Search mechanism supported by many LDAP implementations. Using the same scenario, if a user account is deleted from the Sun ONE database, an incremental synchronization will take place and that user account will immediately be marked as Inactive in the Cisco Unified Communications Manager. Accounts that are newly created in the directory are synchronized to the Cisco Unified Communications Manager via incremental updates as well, and they may be used as soon as the incremental update is received.

Automatic Line Creation

For users created during LDAP synchronization, the Cisco Unified Communications Manager can automatically create directory numbers. These autogenerated directory numbers are either based on information found in the directory and defined based on a mask to be applied to the phone number found in the directory, or the numbers are taken from directory number pools defined on the LDAP synchronization agreement. If a mask is defined on the synchronization agreement, then to allow for variable length +E.164 directory numbers to be generated, the following rules apply:

- If the mask is left empty, then the Cisco Unified Communications Manager takes all digits and also a leading + (plus sign) if present from the directory.
- X is used as a wildcard character in the mask.
- A wildcard matches on digits and + (plus sign).
- Wildcards in the mask are filled from the right.
- Unfilled wildcards in the mask are removed.

Table 16-4 provides some examples illustrating how a mask will impact the number in the LDAP directory when it is imported to the Cisco Unified Communications Manager for directory number creation.

Key Topic

Table 16-4 Directory Number Creation Using Masks with LDAP Integration

Number in LDAP	Mask	Result
14085551234		14085551234
14085551234	+XXXXXXXXXX	+14085551234
14085551234	+XXXXXXXXXXXXXXXXX	+14085551234
14085551234	XXXX	1234
+14085551234		+14085551234
+14085551234	+XXXXXXXXXXXXXXXXX	+14085551234
+490100123	+XXXXXXXXXXXXXXXXX	+490100123

As an alternative to creating directory numbers based on information from LDAP, directory numbers for new users can also be taken from predefined number pools. Each pool is defined by a start and an end number. Directory number pools support +E.164 numbers. Up to five pools can be defined. Numbers are assigned from the first pool until all numbers of that pool have been assigned. Number assignment then starts to take numbers from the next pool.

Automatic line creation is enabled only if both of the following conditions are met:

- A feature group template is assigned in the directory synchronization agreement.
- A universal line template is selected in the user profile selected in the feature group template.

Ultimately, the universal line template defines the characteristics for all directory numbers that are automatically created for users added through the corresponding LDAP synchronization definition. Figure 16-6 shows the hierarchy of configuration elements required to define line-level settings for automatic line creation.

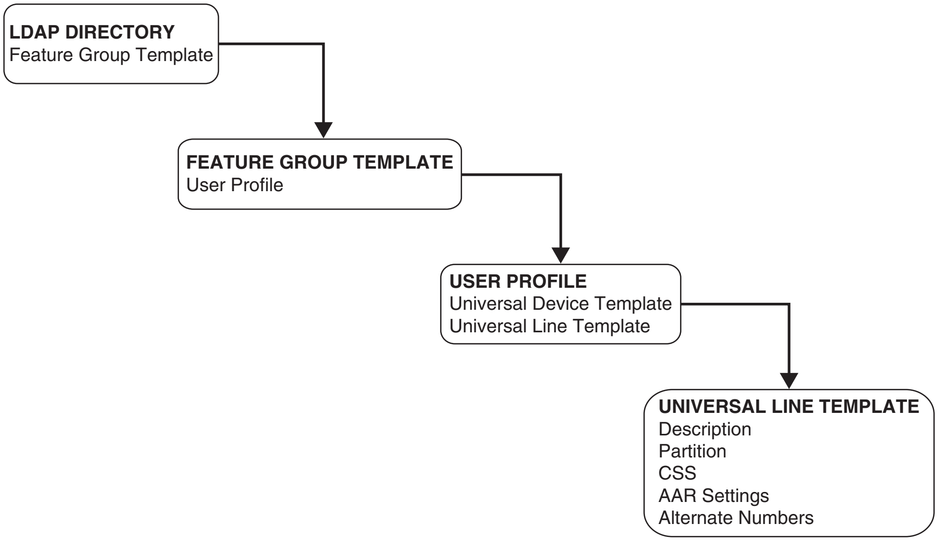


Figure 16-6 *Configuration Hierarchy for Line-Level Settings*

Configuration of the various elements outlined in Figure 16-6 must be performed in the reverse order of their execution. You can use the following steps to configure each of these components:

Step 1. Navigate to **User Management > User/Phone Add > Universal Line Template.** Click **Add New**, provide a name for the line template, and fill out all the appropriate fields. Click **Save** when finished.

NOTE Navigate to **User Management > User/Phone Add > Universal Device Template** and configure a device template before proceeding to the next step if a device template is also needed.

Step 2. Navigate to **User Management > User Settings > User Profile** and click **Add New**. Provide a name for the user profile and configure all the necessary settings, including selecting the universal line template and the universal device template that were configured previously.

Step 3. Navigate to **User Management > User/Phone Add > Feature Group Template** and click **Add New**. Provide a name for the feature group template, check all the feature boxes that apply, and select the user profile that was created previously from the drop-down list. Click **Save** when finished.

Step 4. Navigate to **System > LDAP > LDAP Directory**, click **Add New**, and fill out all the required fields as described earlier in this chapter. Scroll down to the Group Information section close to the bottom of the page and select the feature group template that was previously configured from the drop-down menu.

Step 5. Once the feature group template has been selected, a Mask and DN Pool can also be configured and applied in the Group Information section of the synchronization agreement.

You must account for some design considerations when deploying automatic line creation elements through an LDAP integration. The calling search space defined in the universal line template determines the class of service of devices using any of the autogenerated directory numbers. This implies that all directory numbers created through the same LDAP synchronization agreement share the same class of service, and thus if directory numbers for multiple sites and multiple classes of service need to be autogenerated, then multiple LDAP synchronization agreements (one per site and class of service) need to be configured. For each of these synchronization agreements, disjunct LDAP filters need to be defined, each exactly matching on only the users belonging to one of the site-specific and class-of-service-specific user groups. This mapping from LDAP attributes to site and class of service groups can be challenging unless the group membership based on site and class of service is explicitly encoded in few LDAP attributes, potentially even in a custom attribute. Also, the maximum number of supported LDAP agreements is limited, which limits the number of distinct user groups for which directory numbers can be created automatically.

Second, automatic creation of directory numbers applies only to users created during LDAP directory synchronization. Adding, changing, or updating the universal line template for a given LDAP synchronization agreement will not create directory numbers for already existing users and will not change the settings of already existing directory numbers.

Finally, the universal line template allows administrators to define call forward unregistered destinations and either select voicemail as the forward destination or define an explicit destination. To reach endpoints in remote sites from registered endpoints in case of WAN failure, the call forward unregistered destination for the remote site's phones must be set to the PSTN alias, meaning the +E.164 number of the remote phone. This cannot be achieved with universal line template settings because this would require defining the call forward unregistered destination to be set based on the assigned directory numbers, potentially with a mask applied.

Enterprise Group Support

To enable Jabber clients to search for groups in Microsoft Active Directory, you can configure the Cisco Unified Communications Manager to not only synchronize end users from Active Directory but also to include distribution groups defined in Active Directory. Synchronization of enterprise groups is supported only with Microsoft Active Directory as the data source. It is not supported with Active Directory Lightweight Directory Services (AD LDS) or other corporate directories. Synchronization of enterprise groups is enabled in the Cisco Unified Communications Manager LDAP directory configuration. The maximum number of enterprise groups is 15,000 and the maximum number of members per group is 100. While groups and members cannot be added or modified in the Cisco Unified Communications Manager Administration, the groups synchronized from Active Directory can be reviewed in the **User Management > User Settings > User Group** menu. For each group member, the following information is available on Jabber clients:

Key Topic

- Display name
- User ID
- Title
- Phone number
- Mail ID

Security Considerations

During the import of accounts, no passwords or PINs are copied from the LDAP directory to the Cisco Unified Communications Manager database. If LDAP authentication is not enabled in the Cisco Unified Communications Manager and single sign-on is not used, the password for the end user is managed by using the Cisco Unified Communications Manager Administration. The password and PIN are stored in an encrypted format in the Cisco Unified Communications Manager database. The PIN is always managed on the Cisco Unified Communications Manager. If you want to use the LDAP directory password to authenticate an end user, then LDAP authentication needs to be configured in the Cisco Unified Communications Manager. This topic will be discussed later in this chapter.

The connection between the Cisco Unified Communications Manager publisher server and the directory server can be secured by enabling Secure LDAP (SLDAP) on the Cisco Unified Communications Manager and the LDAP servers. Secure LDAP enables LDAP to be sent over a Secure Socket Layer (SSL) connection and can be enabled by adding the LDAP server into the Tomcat trust store within the Cisco Unified Communications Manager Platform Administration. For detailed procedure steps, refer to the Cisco Unified Communications Manager product documentation available at https://www.cisco.com. Refer to the documentation of the LDAP directory vendor to determine how to enable SLDAP.

Design Considerations for LDAP Synchronization

Up to this point, this section on LDAP synchronization has provided a foundation outlining all the different settings and components that are involved with establishing an LDAP synchronization to the Cisco Unified Communications Manager. There are still many design considerations that should be observed before an LDAP synchronization should be attempted. Observe the following design and implementation best practices when deploying LDAP synchronization with the Cisco Unified Communications Manager:

Key Topic

- Use a specific account within the corporate directory to allow the Cisco Unified Communications Manager synchronization agreement to connect and authenticate to it. Cisco recommends that you use an account dedicated to the Cisco Unified Communications Manager, with minimum permissions set to "read" all user objects within the desired search base and with a password set never to expire. The password for this account in the directory must be kept in synchronization with the password configuration of the account in the Cisco Unified Communications Manager. If the service account password changes in the directory, be sure to update the account configuration in the Cisco Unified Communications Manager.
- All synchronization agreements on a given cluster must integrate with the same family of LDAP servers.
- Stagger the scheduling of synchronization agreements so that multiple agreements are not querying the same LDAP servers simultaneously. Choose synchronization times that occur during quiet off-peak hours.
- If security of user data is required, enable Secure LDAP by checking the Use SSL field on the LDAP directory configuration page in the Cisco Unified Communications Manager Administration.

- Ensure that the LDAP directory attribute chosen to map into the Cisco Unified Communications Manager User ID field is unique within all synchronization agreements for that cluster.
- The attribute chosen as User ID must not be the same as that for any of the application users defined in the Cisco Unified Communications Manager.
- The LDAP attribute sn, which is the last name, is a mandatory attribute for LDAP synchronization of users.
- An LDAP-generated account in the Cisco Unified Communications Manager database that existed before synchronization occurred will be maintained only if an account imported from the LDAP directory has a matching attribute. The attribute that is matched to the Cisco Unified Communications Manager User ID is determined by the synchronization agreement.
- Administer end-user accounts through the LDAP directory's management tools and manage the Cisco-specific data for those accounts through the Cisco Unified Communications Manager Administration web page.
- For AD deployments, the ObjectGUID is used internally in the Cisco Unified Communications Manager as the key attribute of a user. Therefore, the attribute in AD that corresponds to the Cisco Unified Communications Manager User ID may be changed in AD. For example, if sAMAccountname is being used, a user may change his or her sAMAccountname in AD, and the corresponding user record in the Cisco Unified Communications Manager would be updated.

With all other LDAP platforms, the attribute that is mapped to User ID is the key for that account in the Cisco Unified Communications Manager. Changing that attribute in LDAP will result in a new user being created in the Cisco Unified Communications Manager, and the original user will be marked inactive.

Additional Considerations for Microsoft AD

Several other additional considerations are specific to a Microsoft AD synchronization with the Cisco Unified Communications Manager. A synchronization agreement for a domain will not synchronize users outside of that domain or within a child domain because the Cisco Unified Communications Manager does not follow AD referrals during the synchronization process. If an organization has an AD tree structure that incorporated users under the root domain karat&stic.com as well as the two child domains emea.karat&stic.com and apac.karat&stic.com, then this AD environment would require three synchronization agreements to import all of the users. In this example, each of the domains and subdomains contain at least one domain controller (DC) associated with them. Each DC will have information only on users within the domain where they reside; therefore, three synchronization agreements are required to import all of the users.

When synchronization is enabled with an AD forest containing multiple trees, multiple synchronization agreements are still needed for the same reasons listed above. The DC for each tree under the same AD will be completely different from one another, such as karat&stic.com and lab.local. Additionally, Active Directory guarantees the UserPrincipalName (UPN) attribute to be unique across the forest, and it must be chosen as the attribute that is mapped to the Cisco Unified Communications Manager User ID. For additional considerations on the use of the UPN attribute in a multitree AD scenario, refer to the Cisco Collaboration SRND Guide, which can be found at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html.

One final consideration worth mentioning is that the Cisco Unified Communications Manager sends a default LDAP search filter string to AD when performing the synchronization of accounts. One of the clauses is to not return accounts that have been marked as disabled in AD. An account marked disabled by AD, such as when failed login attempts are exceeded, will be marked inactive if synchronization runs while the account is disabled.

LDAP Authentication

Application users and locally configured end users are always authenticated against the local database. Also, PINs of all end users are always checked against the local database only. When users are imported to the Cisco Unified Communications Manager using LDAP synchronization, they are also authenticated against the local database unless LDAP authentication is configured. The LDAP authentication feature enables the Cisco Unified Communications Manager to authenticate LDAP synchronized users against the corporate LDAP directory. Although synchronization will import certain user data into the Cisco Unified Communications Manager, LDAP authentication will never import password information. This authentication is accomplished with an LDAPv3 connection established between the Identity Management System (IMS) module within the Cisco Unified Communications Manager and a corporate directory server. Figure 16-7 illustrates the process and mechanisms required for LDAP authentication.

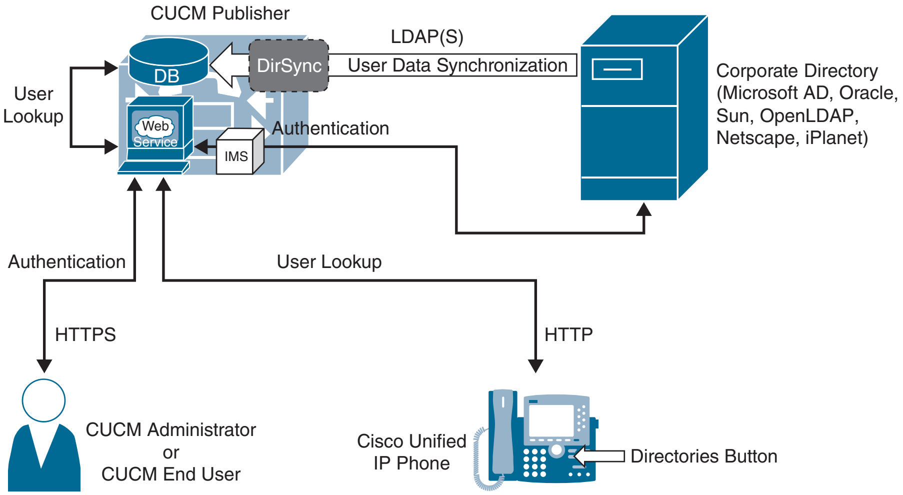


Figure 16-7 *LDAP Authentication Mechanisms and Process*

To enable authentication, a single authentication agreement may be defined for the entire cluster. The authentication agreement supports configuration of up to three LDAP servers for redundancy and also supports secure connections of LDAP over SSL/TLS (SLDAP) if desired. Although synchronization can be used without authentication, the opposite is not true. Authentication can be enabled only after LDAP synchronization is properly configured and used. LDAP authentication configuration is overridden by enabling SSO. With SSO enabled, end users are always authenticated using SSO, and LDAP authentication configuration is ignored. Use the following steps to configure authentication on the Cisco Unified Communications Manager:

Step 1. Navigate to **System > LDAP > LDAP Authentication**.

Step 2. Check the box beside **Use LDAP Authentication for End Users.**

Step 3. Enter the LDAP Manager Distinguished Name followed by the LDAP Password and Confirm Password.

Step 4. The LDAP User Search Base should be the main search base for the whole domain. Any users in the LDAP directory that have not been synchronized with the Cisco Unified Communications Manager will not be able to log in.

Step 5. Finally, enter the address for the LDAP server in the Host Name or IP Address for Server field. Enter the LDAP Port and check the **Use TLS** box if a secure connection is being used for LDAP authentication.

Step 6. Click **Save** when finished.

The following statements describe the Cisco Unified Communications Manager's behavior when authentication is enabled:

- End-user passwords of users imported from LDAP are authenticated against the corporate directory by a simple bind operation.
- End-user passwords for local users are authenticated against the Cisco Unified Communications Manager database.
- Application-user passwords are authenticated against the Cisco Unified Communications Manager database.
- End-user PINs are authenticated against the Cisco Unified Communications Manager database.

This behavior is in line with the guiding principle of providing single logon functionality for end users while making the operation of the real-time Unified Communications system independent of the availability of the corporate directory. The following steps outline how the Cisco Unified Communications Manager authenticates an end user synchronized from LDAP against a corporate LDAP directory:

Key Topic

1. A user connects to the Cisco Unified Communications Manager User Options page via HTTPS and attempts to authenticate with a username and password.
2. If the user is a local user, the password is checked against the local database.

The following steps apply only to LDAP synchronized users:

1. If the user is an LDAP synchronized user, the Cisco Unified Communications Manager issues an LDAP query for the username, using the value specified in the LDAP Search Base on the LDAP Authentication configuration page as the scope for this query. If SLDAP is enabled, this query travels over an SSL connection.

2. The corporate directory server replies via LDAP with the full distinguished name (DN) of the user; for example, for jsmith, DN would return the value "cn=jsmith, ou=Users, dc=karat&stic, dc=com".
3. The Cisco Unified Communications Manager then attempts to validate the user's credentials by using an LDAP bind operation to pass the full DN and password provided by the user.
4. If the LDAP bind is successful, the Cisco Unified Communications Manager allows the user to proceed to the configuration page requested.

Design Considerations for LDAP Authentication

Just as with LDAP synchronization, LDAP authentication also has design considerations that must be taken into account. Observe the following design and implementation best practices when deploying LDAP authentication with the Cisco Unified Communications Manager:

- Create a specific account within the corporate directory to allow the Cisco Unified Communications Manager to connect and authenticate to it. Cisco recommends that you use an account dedicated to the Cisco Unified Communications Manager, with minimum permissions set to "read" all user objects within the desired search base and with a password set to never expire. The password for this account in the directory must be kept in synchronization with the password configuration of the account in the Cisco Unified Communications Manager. If the account password changes in the directory, be sure to update the account configuration in the Cisco Unified Communications Manager. You can use the same account for both authentication and synchronization functions.

- Enable LDAP authentication on the Cisco Unified Communications Manager by specifying the credentials of the aforementioned account under LDAP Manager Distinguished Name and LDAP Password, and by specifying the directory subtree where all the users reside under LDAP User Search Base.

- This method provides single logon functionality to all end users synchronized from LDAP. They can then use their corporate directory credentials to log in to the Cisco Unified Communications Manager User Options page.

- Manage end-user passwords for LDAP synchronized users from within the corporate directory interface. Note that the password field is no longer displayed for LDAP synchronized users in the Cisco Unified Communications Manager Administration pages when authentication is enabled.

- Manage end-user PINs from the Cisco Unified Communications Manager Administration web page or from the Cisco Unified Communications Manager User Options page.

- Manage application-user passwords from the Cisco Unified Communications Manager Administration web pages. Remember that these application users facilitate communication and remote call control with other Cisco Unified Communications applications and are not associated with real people.

- Enable single logon for the Cisco Unified Communications Manager administrators by adding their corresponding end users to the Cisco Unified Communications Manager Super Users user group from the Cisco Unified Communications Manager Administration web pages. Multiple levels of administrator rights can be defined by creating customized user groups and roles.

Additional Considerations for Microsoft AD

In environments that employ a distributed AD topology with multiple domain controllers geographically distributed, authentication speed might be unacceptable. When the domain controller for the authentication agreement does not contain a user account, a search must occur for that user across other domain controllers. If this configuration applies, and login speed is unacceptable, it is possible to set the authentication configuration to use a global catalog server. Unfortunately, an important restriction exists. A global catalog does not carry the employeeNumber attribute by default. In that case, you should either use domain controllers for authentication or update the global catalog to include the employeeNumber attribute. Refer to Microsoft Active Directory documentation for details.

To enable queries against the global catalog, you simply configure the LDAP Server Information in the LDAP Authentication page to point to the IP address or host name of a domain controller that has the global catalog role enabled and configure the LDAP port as 3268.

The use of a global catalog for authentication becomes even more efficient if the users synchronized from Microsoft AD belong to multiple domains because it allows the Cisco Unified Communications Manager to authenticate users immediately without having to follow referrals. For these cases, point the Cisco Unified Communications Manager to a global catalog server and set the LDAP user search base to the top of the root domain.

In the case of a Microsoft AD forest that encompasses multiple trees, some additional considerations apply. Because a single LDAP search base cannot cover multiple namespaces, the Cisco Unified Communications Manager must use a different mechanism to authenticate users across these discontiguous namespaces. To support synchronization with an AD forest that has multiple trees, the UserPrincipalName (UPN) attribute should be used as the user ID within the Cisco Unified Communications Manager. When the user ID is the UPN, the LDAP authentication configuration page within the Cisco Unified Communications Manager Administration does not allow you to enter the LDAP Search Base field, but instead it displays the message "LDAP user search base is formed using userid information."

Support for LDAP authentication with Microsoft AD forests containing multiple trees relies exclusively on the approach described here. Therefore, support is limited to deployments where the UPN suffix of a user corresponds to the root domain of the tree where the user resides. AD allows the use of aliases, which allows a different UPN suffix. If the UPN suffix is disjointed from the actual namespace of the tree, it is not possible to authenticate the Cisco Unified Communications Manager users against the entire Microsoft Active Directory forest. It is, however, still possible to use a different attribute as user ID and limit the integration to a single tree within the forest.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 16-5 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 16-5 Key Topics for Chapter 16

Key Topic Element	Description	Page Number
List	End User Attributes	373
Table 16-2	Default Application Users in the CUCM	374
Paragraph	End Users and Application Users with LDAP	376
Table 16-3	LDAP Directory Attribute Map	379
List	Synchronization Mechanism in the CUCM	383
Table 16-4	Directory Number Creation Using Masks with LDAP Integration	384
List	Enterprise Group Support Settings Available on Cisco Jabber Clients	386
List	Design and Implementation Best Practices for LDAP Synchronization	387
List	LDAP Authentication Steps by the CUCM	390

Define Key Terms

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

AD, AD Forest, AD LDS, AD Tree, ADAM, Application Users, CN, DC, Directory, Directory Schema, DirSync, End Users, Identity Management, IMS, LDAP, LDAP Authentication, LDAP Manager Distinguished Name, LDAP Synchronization, OU, SLDAP, SSO, Synchronization Agreement, UPN

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the attributes that are associated with end users.
2. List the steps to enabling LDAP synchronization in the Cisco Unified Communications Manager.
3. List the steps to enable LDAP authentication in the Cisco Unified Communications Manager.

CHAPTER 17

Registering SIP Endpoints to the Cisco Unified Communications Manager

This chapter covers the following topics:

Manual Registration Process: This topic will explain how users and devices can be added to the Cisco Unified Communications Manager manually by an administrator.

Self-Provisioning: This topic will examine an alternative option to the manual process within the Cisco Unified Communications Manager for adding devices. This process involves setting up auto-registration prior to configuring Self-Provisioning.

Bulk Administration Tool (BAT): This topic will examine yet another option for provisioning multiple devices within the Cisco Unified Communications Manager. This method will also allow an administrator to modify existing settings on phones and within user profiles.

Device Onboarding with Activation Codes: This topic will examine how devices can register to the Cisco Unified Communications Manager by entering an activation code on the phone or Telepresence endpoint.

Provisioning can loosely be defined as mass configuration and mass deployment. The idea behind provisioning is to configure a baseline that can be pushed out to multiple devices, thus making the job of deployment much easier. One of the key functions within the Cisco Unified Communications Manager is to enable the provisioning of devices. This chapter will explain how to manually configure a single device and how to provision multiple devices using the Self-Provisioning and BAT options built into the Cisco Unified Communications Manager. This chapter will also examine how device onboarding can be achieved using activation codes whether you have one device or thousands of them. Topics discussed in this chapter include the following:

- Manual Registration Process
- Self-Provisioning
- Bulk Administration Tool (BAT)
- Device Onboarding with Activation Codes (On-Premises)

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.0 (CLCOR 350-801) exam:

- 2.3 Deploy SIP endpoints
  - 2.3.a Manual
    - 2.3.b Self provisioning
    - 2.3.c Bulk Administration Tool (BAT)
    - 2.3.e Device Onboarding with Activation Codes

"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
Manual Registration Process	1–3
Self-Provisioning	4–6
Bulk Administration Tool (BAT)	7–9
Device Onboarding with Activation Codes	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 settings should be configured in the CUCM before an end user is created?
   a. Phone profile
   b. User profile
   c. Device profile
   d. Phone
2. Which of the following settings allows a date/time group, region, and location to be grouped together?
   a. Common phone profile
   b. Common device configuration
   c. Phone button template
   d. Device pool

3. How does the CUCM identify a phone for registration?
   - a. IP address
   - b. MAC address
   - c. Serial number
   - d. tftp.cnf file
4. Which two of the following services must be enabled to use Self-Provisioning? (Choose two.)
   - a. Cisco Unified Mobile Voice Access Service
   - b. Cisco IP Voice Media Streaming App
   - c. Cisco CTI Manager
   - d. Cisco Extended Functions
   - e. Cisco Directory Number Alias Sync
   - f. Cisco UP Manager Assistant
   - g. Cisco WebDialer Web Service
   - h. Self-Provisioning IVR
5. When you are configuring Self-Provisioning in the CUCM, which of the following steps should be configured first?
   - a. Create an application user.
   - b. Create a CTI route point.
   - c. Configure a dial-in extension.
   - d. Configure auto-registration.
6. When you are creating an application user for Self-Provisioning, which of the following permission groups is required to add before Self-Provisioning can be set up?
   - a. Standard CTI Enabled
   - b. Standard CCM Admin User
   - c. Standard CTI Allow Control of All Devices
   - d. Standard CCM Super Users
7. When a bulk transaction is performed using BAT, what is the maximum number of records that can be included?
   - a. 1200
   - b. 12,000
   - c. 120,000
   - d. There is no limit
8. Which of the following statements is true regarding CSV files for BAT administration?
   - a. Data in a CSV will overwrite conflicting data in a BAT template.
   - b. Data in a BAT template will overwrite conflicting data in a CSV template.
   - c. Data in CSV template and data in a BAT template are universally unique from one another and so will never be conflicting.
   - d. Data in a CSV template and data in a BAT template must be reconciled before it can be used, or else all attempts to use them will fail.

9. When you are creating CSV files, what behavior will result in leaving a row blank?

- **a.** That field will be removed if anything is configured there.
- **b.** Nothing will change in that field.
- **c.** The system treats blank rows in the spreadsheet as end-of-file markers and discards subsequent records.
- **d.** The BAT.xlt file encloses that field entry in double quotation marks when you export to BAT format.

10. Which of the following must be configured to enable the use of activation codes for endpoint registration on a Cisco Unified Communications Manager?

- **a.** The Onboarding Method must be set to Auto Registration.
- **b.** Auto Registration must be removed from the Onboarding Method settings.
- **c.** The Cisco Device Activation Service must be activated.
- **d.** MAC addresses must still be used in the Phone profile, even with activation codes enabled.

- **Explanation:** *You must activate the Cisco Device Activation Service and switch the Onboarding Method from Auto Registration to Activation Code before device activation codes can be used for endpoint registrations. Therefore, the correct answer is* "The Cisco Device Activation Service must be activated."

Foundation Topics

Key Topic

Before a phone or endpoint can register to the Cisco Unified Communications Manager, an administrator must create the phone's configuration within the Cisco Unified Communications Manager Administration settings first. The phone's configuration contains all the TFTP configuration file information that is provisioned to the phone prior to registration. When it comes to creating a phone's configuration in the Cisco Unified Communications Manager, there are two types of phones the administrator can create. A user phone is a device configuration that is associated with a specific end user. A Cisco Unified IP phone, a personal Telepresence endpoint, or the Jabber soft client can be used for a user phone. The second type of phone an administrator can create is a room phone. These types of phones are not associated with any particular end user, and they can be any model of Cisco Unified IP phone or Telepresence endpoint, but they cannot be the Jabber soft client.

A user phone is the most common type of phone created in the Cisco Unified Communications Manager. These phone types must be associated with an end user; therefore, it is essential that the end users are created or imported into the Cisco Unified Communications Manager before the phones are created. The preceding chapter discussed at great length the process of using LDAP synchronization and authentication to import and authenticate end users with their passwords. Therefore, the following steps outline how to manually add a new end user into the Cisco Unified Communications Manager and configure that end user with an access control group and a primary line extension.

Before beginning, you should verify that a user profile has been configured and includes a universal line template. If a new extension needs to be configured, the Cisco Unified Communications Manager uses settings from the universal line template to configure the primary extension.

Key Topic

Step 1. In the Cisco Unified Communications Manager Administration, navigate to **User Management > User/Phone Add > Quick User/Phone Add.**

Step 2. Click **Add New**, and then enter the User ID and Last Name.

Step 3. From the Feature Group Template drop-down list, select a feature group template.

Step 4. Click Save.

Step 5. From the User Profile drop-down list, verify that the selected user profile includes a universal line template.

Step 6. From the Access Control Group Membership section, click the **+** icon.

Step 7. From the User Is a Member Of drop-down list, select an access control group. Most end users will be part of the Standard CCM End Users group.

Step 8. Under Primary Extension, click the **+** icon.

Step 9. From the Extension drop-down list, select a directory number (DN) that displays as (available).

Step 10. If all line extensions display as (used), perform the following steps:

a. Click the **New** button. The Add New Extension popup displays.

b. In the Directory Number field, enter a new line extension.

c. From the Line Template drop-down list box, select a universal line template.

d. Click **Add**.

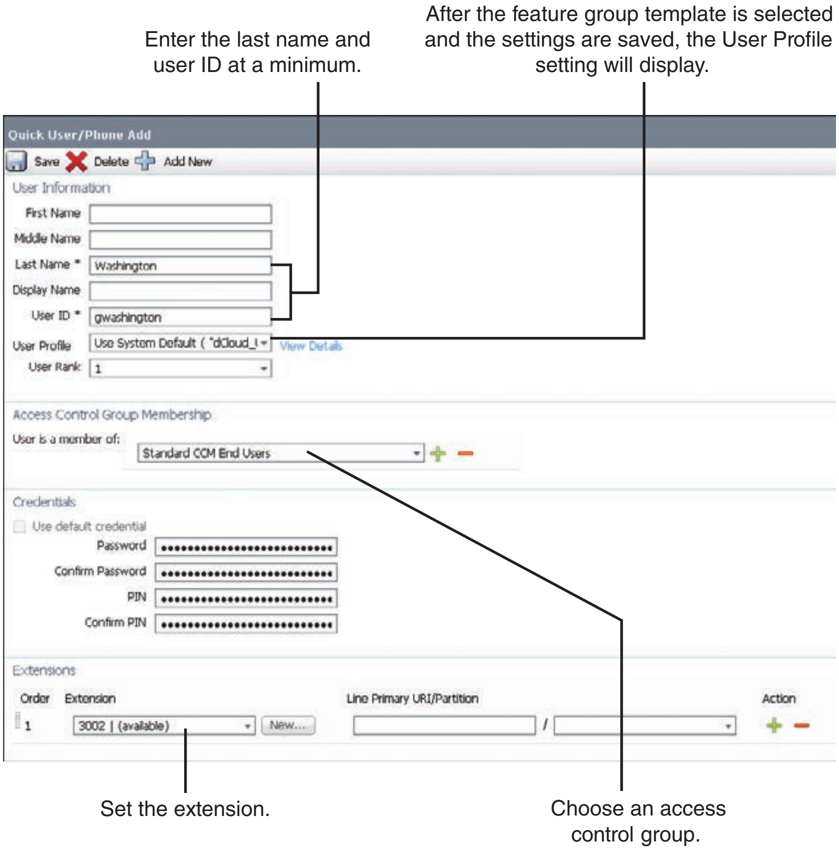
The Cisco Unified Communications Manager configures the directory number with the settings from the universal line template.

Step 11. (Optional) Complete any additional fields in the Quick User/Phone Add configuration window.

Step 12. Click Save.

There are other ways to add end users to the Cisco Unified Communications Manager, but this method will create the end user and associate the DN to this user prior to creating the phone in the Cisco Unified Communications Manager. Figure 17-1 illustrates the different fields from the Quick User/Phone Add dialog.

After an end user is created in the Cisco Unified Communications Manager, a phone can be created as well. Phones and end users can be provisioned separately, independent of each other, or collectively together. Chapter 15, "Cisco Unified Communications Manager Setup," delved into a lot of different settings that are required not only for basic Cisco Unified Communications Manager operations but also for endpoint registration. Because so many different settings need to be configured on Cisco Unified Communications Manager registered phones and endpoints, many tools within the Cisco Unified Communications Manager Administration menus allow administrations to group common settings together. The device pool is a perfect example, where the Cisco Unified Communications Manager Group, Date/Time Group, Regions, Location, and many other settings can all be grouped together for phones and endpoints that share a common geographical region. Other grouped settings include the phone button template, common phone profile, and common device configuration. Review Chapter 15 for more detailed information on most of these settings.



Enter the last name and user ID at a minimum.

After the feature group template is selected and the settings are saved, the User Profile setting will display.

Quick User/Phone Add

User Information

First Name
Middle Name
Last Name * Washington
Display Name
User ID * gwashington
User Profile Use System Default ("dCloud_(View Details
User Rank 1

Access Control Group Membership

User is a member of: Standard CCM End Users

Credentials

□ Use default credential
Password ••••••••••••••••••••••••••
Confirm Password ••••••••••••••••••••••••••
PIN ••••••••••••••••••••••••••
Confirm PIN ••••••••••••••••••••••••••

Extensions

Order	Extension		Line Primary URI/Partition		Action
1	3002 | (available)	New...		/	+ −

Set the extension.

Choose an access control group.

Figure 17-1 *Quick User/Phone Add Fields*

When it comes to adding phones to the Cisco Unified Communications Manager, several options are available to the administrator. Phones can be added manually, one at a time. This is a great option if a room phone is being added, or a single or few new employees need a phone set up for use. There is even a Copy option when adding a new phone, if the new phone being added will share settings with another phone of the same model. However, when an administrator needs to add a lot of phones, such as a hundred or a thousand or even ten thousand phones, the manual approach is not the way to add these phones, even with the Copy button. Several other methods are available to add a mass number of phones to the Cisco Unified Communications Manager. Auto-registration is the foundation for the other methods that will be discussed in this chapter, and this approach can be used independent of any other method if all phones within the enterprise are being configured the exact same way. However, since that is not usually the case, the administrator also can use the Self-Provisioning method and the Bulk Administration Tool (BAT) method. These two mass provisioning methods will be examined later in this chapter. First, it is important to understand the manual method of adding phones to the Cisco Unified Communications Manager.

You can perform the following procedure to manually add a new phone for a new or existing end user. First, make sure that the user profile for the end user includes a universal device template. Cisco Unified Communications Manager uses the universal device template settings to configure the phone. Before you begin, make sure an end user has already been created, as outlined earlier in this chapter. Also, the Cisco Unified Communications Manager identifies phones trying to register through the MAC address, so be sure to identify the MAC address of the phone prior to setting up registration.

Key Topic

Step 1. In the Cisco Unified Communications Manager Administration, navigate to **User Management > User/Phone Add > Quick/User Phone Add**.

Step 2. Click **Find** and select the end user for whom you want to add a new phone.

Step 3. Click the **Manage Devices** button. The Manage Devices window appears.

Step 4. Click **Add New Phone.** The Add Phone to User popup displays.

Step 5. From the Product Type drop-down list, select the phone model.

Step 6. From the Device Protocol drop-down, select **SIP** or **SCCP** as the protocol. Note that some Cisco phones and endpoints support only SIP, so SCCP will not be an option.

Step 7. In the Device Name text box, enter the device MAC address.

Step 8. From the Universal Device Template drop-down list, select a universal device template.

Step 9. (Optional) If the phone supports expansion modules, enter the number of expansion modules that you want to deploy.

Step 10. If you want to use Extension Mobility to access the phone, check the **Is Extension Mobility Template** check box.

Step 11. Click **Add Phone**. The Add New Phone popup closes. The Cisco Unified Communications Manager adds the phone to the user and uses the universal device template to configure the phone.

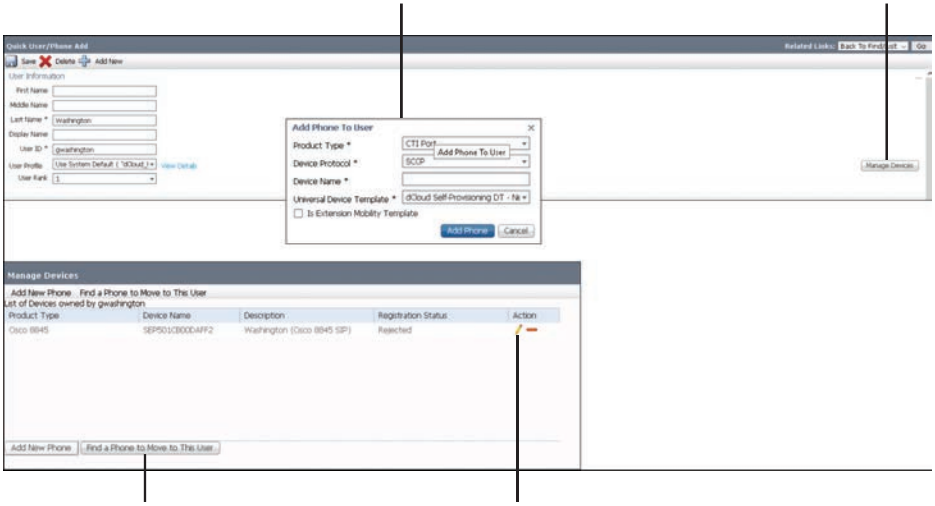
Step 12. If you want to make additional edits to the phone configuration, click the corresponding Pencil icon to open the phone in the Phone Configuration window.

An alternative way to add a phone manually to the Cisco Unified Communications Manager is to navigate to **Device > Phone**, click **Add New**, and enter all the appropriate phone settings. This method is used more often for phones and endpoints in rooms rather than for end users. Figure 17-2 illustrates the dialogs covered in the preceding steps for adding a phone to an existing end user.

The Self-Provisioning feature allows phones to be provisioned across the network by enabling end users to provision their own phones without contacting an administrator. If the system is configured for Self-Provisioning, and an individual end user is enabled for Self-Provisioning, then the end user can provision a new phone by plugging the phone into the network and following a few specified prompts. The Cisco Unified Communications Manager configures the phone and the phone line by applying preconfigured templates.

Enter the phone details.

Click Manage Devices.



User Information

First Name:
Middle Name:
Last Name *: Washington
Display Name:
User ID *: gwashington
User Profile: Use System Default ("dCloud_)
User Rank: 1

Add Phone To User

Product Type *: CTI Port
Device Protocol *: SCCP
Device Name *:
Universal Device Template *: dCloud Self-Provisioning DT - Ni
☐ Is Extension Mobility Template

List of Devices owned by gwashington

Product Type	Device Name	Description	Registration Status	Action
Cisco 8845	SEP501CB00DAFF2	Washington (Cisco 8845 SIP)	Rejected	✎ —

Search for an existing phone rather than creating a new phone.

Use the Pencil icon to edit settings on the phone.

Figure 17-2 *Adding a Phone to an End User Through the Quick User/Phone Add Dialogs*

Self-Provisioning is supported whether the cluster security setting is in nonsecure or mixed mode. In secure mode, users or administrators must be authenticated in order to access Self-Provisioning. End users can be authenticated against their password or PIN. Administrators can enter a preconfigured authentication code. In nonsecure mode, users or administrators can enter their user ID, or a Self-Provisioning ID, to associate the phone to a user account. Nonsecure mode is not recommended for day-to-day use.

Self-Provisioning uses the universal line template and universal device template configurations to configure provisioned phones and phone lines for an end user. When a user provisions his or her own phone, the system references the user profile for that user and applies the associated universal line template to the provisioned phone line and the universal device template to the provisioned phone. Once the Self-Provisioning feature is configured, you can provision a phone by doing the following:

Key Topic

Step 1. Plug the phone into the network and allow the phone to register to the Cisco Unified Communications Manager using auto-registration.

Step 2. Once the phone is registered, dial the Self Provisioning IVR extension.

Step 3. Follow the prompts to configure the phone and associate the phone with an end user. Depending on how Self-Provisioning has been configured, the end user may need to enter the user password, PIN, or an administrative authentication code.

Before end users can use Self-Provisioning, they must be configured with a primary extension. They must also be associated with a user profile or feature group template that includes a universal line template and a universal device template, and the user profile must be enabled for Self-Provisioning. If an administrator is provisioning a large number of phones on behalf of the end users, Cisco suggests also configuring a speed dial on the universal device template that will forward a call to the Self Provisioning IVR extension.

The task of setting up Self-Provisioning is not easy for the administrator. Several settings under many different menus must be configured before Self-Provisioning can be used. However, all of the required settings need to be configured only once, and after Self-Provisioning is set up, the process of provisioning phones through this service is quite simple. Use the following steps to configure the various aspects of Self-Provisioning. Figures 17-3 through 17-8 follow each of the steps in order to provide a visual example of the settings the steps describe.

Key Topic

Step 1. Before Self-Provisioning can be configured, you must activate some services first. Use the following steps to activate the services that support the Self-Provisioning feature, as shown in Figure 17-3. Both the Self-Provisioning IVR and Cisco CTI Manager services must be running.

a. From Cisco Unified Serviceability, navigate to **Tools > Service Activation**.

b. From the Server drop-down list, select the publisher node and click **Go**.

c. Under CM Services, check **Cisco CTI Manager**.

d. Under CTI Services, check **Self-Provisioning IVR**.

e. Click **Save** and then ensure the services are activated and running.

Key Topic

Step 2. After services have been activated, the next step is to configure the auto-registration parameters on the publisher, as shown in Figure 17-4.

a. From Cisco Unified Communications Manager Administration, navigate to **System > Cisco Unified CM**. Click **Find**, and then click on the publisher node.

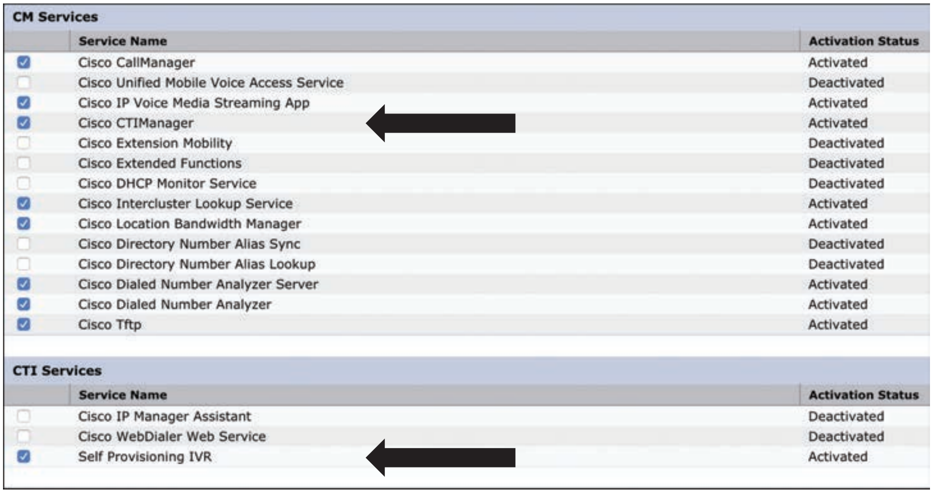
b. Select the Universal Device Template that you want to be applied to provisioned phones.

c. Select the Universal Line Template that you want to be applied to the phone lines for provisioned phones.

d. Use the Starting Directory Number and Ending Directory Number fields to enter a range of directory numbers to apply to provisioned phones. Make sure the range is broad enough to encompass all the phones within the enterprise network. If this pool runs out of DNs, then phones trying to auto-register will fail.

e. Uncheck the **Auto-registration Disabled** check box on the Cisco Unified Communications Manager.

f. Click **Save**.



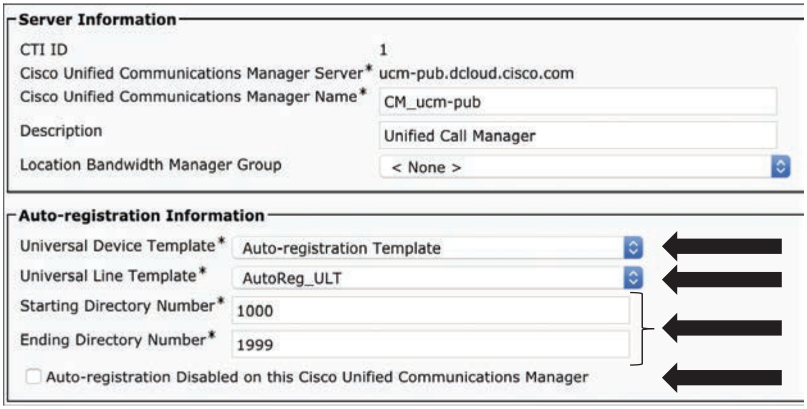
CM Services

	Service Name	Activation Status
☑	Cisco CallManager	Activated
☐	Cisco Unified Mobile Voice Access Service	Deactivated
☑	Cisco IP Voice Media Streaming App	Activated
☑	Cisco CTIManager	Activated
☐	Cisco Extension Mobility	Deactivated
☐	Cisco Extended Functions	Deactivated
☐	Cisco DHCP Monitor Service	Deactivated
☑	Cisco Intercluster Lookup Service	Activated
☑	Cisco Location Bandwidth Manager	Activated
☐	Cisco Directory Number Alias Sync	Deactivated
☐	Cisco Directory Number Alias Lookup	Deactivated
☑	Cisco Dialed Number Analyzer Server	Activated
☑	Cisco Dialed Number Analyzer	Activated
☑	Cisco Tftp	Activated

CTI Services

	Service Name	Activation Status
☐	Cisco IP Manager Assistant	Deactivated
☐	Cisco WebDialer Web Service	Deactivated
☑	Self Provisioning IVR	Activated

Figure 17-3 *Self-Provisioning IVR and Cisco CTI Manager Services*



Server Information

CTI ID 1
Cisco Unified Communications Manager Server* ucm-pub.dcloud.cisco.com
Cisco Unified Communications Manager Name* CM_ucm-pub
Description Unified Call Manager
Location Bandwidth Manager Group < None >

Auto-registration Information

Universal Device Template* Auto-registration Template
Universal Line Template* AutoReg_ULT
Starting Directory Number* 1000
Ending Directory Number* 1999
☐ Auto-registration Disabled on this Cisco Unified Communications Manager

Figure 17-4 *Auto-registration Settings on the Cisco Unified Communications Manager*

Key Topic

Step 3. Now that auto-registration is set up, the next step is to configure a CTI route point for the Self-Provisioning IVR (see Figure 17-5).

a. From Cisco Unified Communications Manager Administration, navigate to **Device > CTI Route Points**.

b. Complete either of the following steps: Click **Find** and select an existing CTI route point, or click **Add New** to create a new CTI route point.

c. In the Device Name field, enter a unique name to identify the route point.

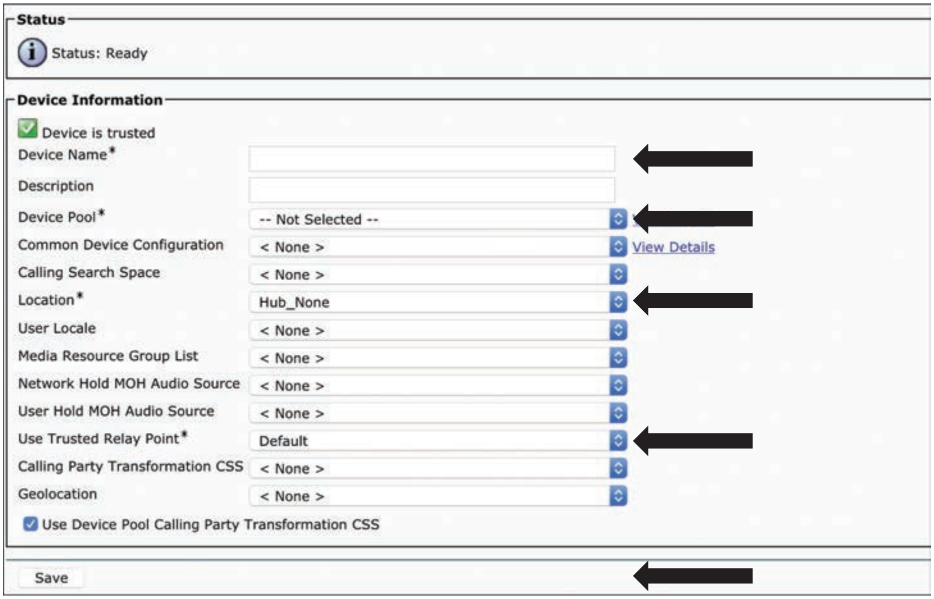
d. From the Device Pool drop-down list box, select the device pool that specifies the properties for this device.

e. From the Location drop-down list box, select the appropriate location for this CTI route point.

f. From the Use Trusted Relay Point drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. The Default setting is to use the Common Device Configuration setting that is associated with this device.

g. Complete the remaining fields in the CTI Route Point Configuration window. For help with the fields and their settings, refer to the online help.

h. Click **Save**.



Status

Status: Ready

Device Information

☑ Device is trusted

Device Name*	
Description	
Device Pool*	-- Not Selected --
Common Device Configuration	< None >
Calling Search Space	< None >
Location*	Hub_None
User Locale	< None >
Media Resource Group List	< None >
Network Hold MOH Audio Source	< None >
User Hold MOH Audio Source	< None >
Use Trusted Relay Point*	Default
Calling Party Transformation CSS	< None >
Geolocation	< None >

☑ Use Device Pool Calling Party Transformation CSS

Figure 17-5 *Create CTI Route Point for Self-Provisioning IVR*

Key Topic

Step 4. The administrator needs to set up the extension that users will dial to access the Self-Provisioning IVR. You must associate this extension to the CTI route point that you want to use for Self-Provisioning, which is why the CTI route point needs to be configured first (see Figure 17-6).

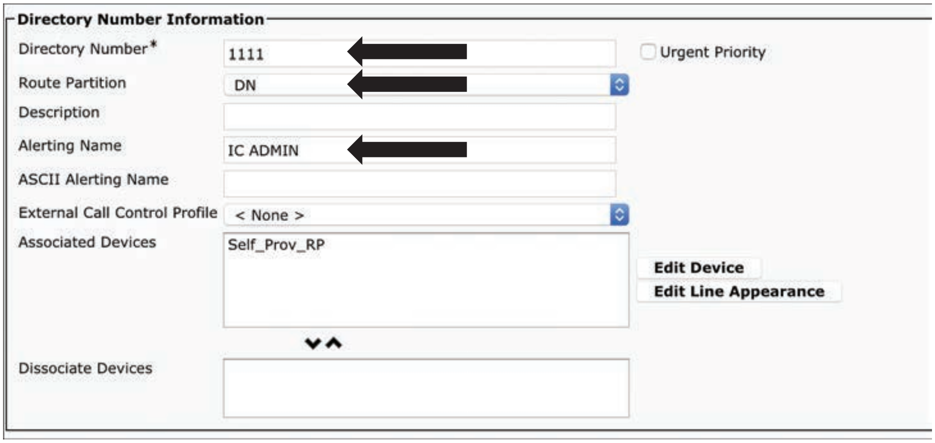
a. From the same CTI route point that was created in the previous step, scroll to the bottom of the page under the Association section. Click **Line [1] - Add a new DN**. The Directory Number Information window displays.

b. In the Directory Number field, enter the extension that you want users to dial to access the Self-Provisioning IVR service.

c. Click outside the box or press the Tab key.

d. Once the page refreshes, complete the remaining fields in the Directory Number Configuration window. For help with the fields and their settings, refer to the online help.

e. Click **Save** when finished.



Directory Number Information

Directory Number*	1111	□ Urgent Priority
Route Partition	DN	
Description		
Alerting Name	IC ADMIN	
ASCII Alerting Name		
External Call Control Profile	< None >	
Associated Devices	Self_Prov_RP	
Dissociate Devices		

Figure 17-6 *Dial-In Extensions for Self-Provisioning IVR*

Key Topic

Step 5. Next, the administrator needs to set up an application user for the Self-Provisioning IVR and associate the CTI route point that was created with the application user (see Figure 17-7).

a. From Cisco Unified Communications Manager Administration, navigate to **User Management > Application User.**

b. Perform either of the following steps: To select an existing application user, click **Find** and select the application user, or to create a new application user, click **Add New.**

c. In the User ID text box, enter a unique ID for the application user.

d. Select a BLF Presence Group for the application user.

e. Associate the CTI route point that you created to the application user by performing the following steps:

- If the CTI route point that you created does not appear in the Available Devices list box, then click **Find More Route Points.**

- If the CTI route point that you created does display as an available device, then in the Available Devices list box, select the CTI route point that you created for Self-Provisioning and click the down arrow.

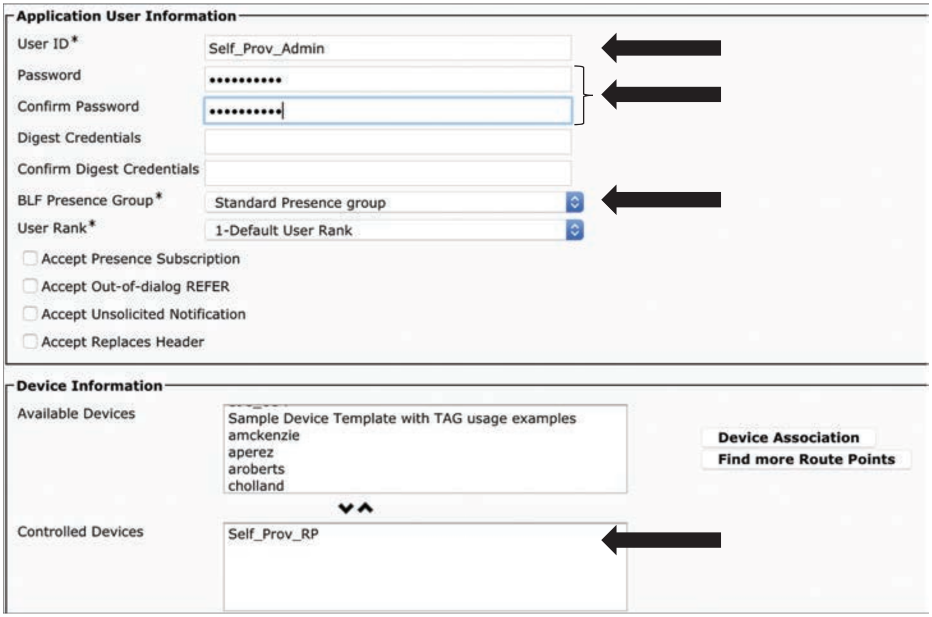
f. The CTI route point displays in the Controlled Devices list box.

g. Under the Permissions Information section, click the **Add to Access Control Group** button.

h. Check the box beside **Standard CTI Enabled** and then click the **Add Selected** button at the top of the page.

i. Complete the remaining fields in the Application User Configuration window. For help with the fields and their settings, refer to the online help.

j. Click **Save.**



Application User Information

User ID*	Self_Prov_Admin
Password	••••••••••
Confirm Password	••••••••••
Digest Credentials	
Confirm Digest Credentials	
BLF Presence Group*	Standard Presence group
User Rank*	1-Default User Rank

□ Accept Presence Subscription

□ Accept Out-of-dialog REFER

□ Accept Unsolicited Notification

□ Accept Replaces Header

Device Information

Available Devices: Sample Device Template with TAG usage examples, amckenzie, aperez, aroberts, cholland

Controlled Devices: Self_Prov_RP

Figure 17-7 *Application User Settings for Self-Provisioning IVR*

Key Topic

Step 6. Self-provisioning enables users in your network to add their own desk phone or soft client through an IVR system, without contacting an administrator. Use this procedure to configure your system for Self-Provisioning, but remember that in order to use the Self-Provisioning feature, end users must also have the feature enabled in their user profiles (see Figure 17-8).

a. From Cisco Unified Communications Manager Administration, navigate to **User Management > Self-Provisioning**.

b. Configure whether you want the Self-Provisioning IVR to authenticate end users by clicking one of the following radio buttons:

- **Require Authentication:** To use the Self-Provisioning IVR, end users must enter their password, PIN, or a system authentication code.
- **No Authentication Required:** End users can access the Self-Provisioning IVR without authenticating.

c. If the Self-Provisioning IVR is configured to require authentication, then click one of the following radio buttons to configure the method whereby the IVR authenticates end users:

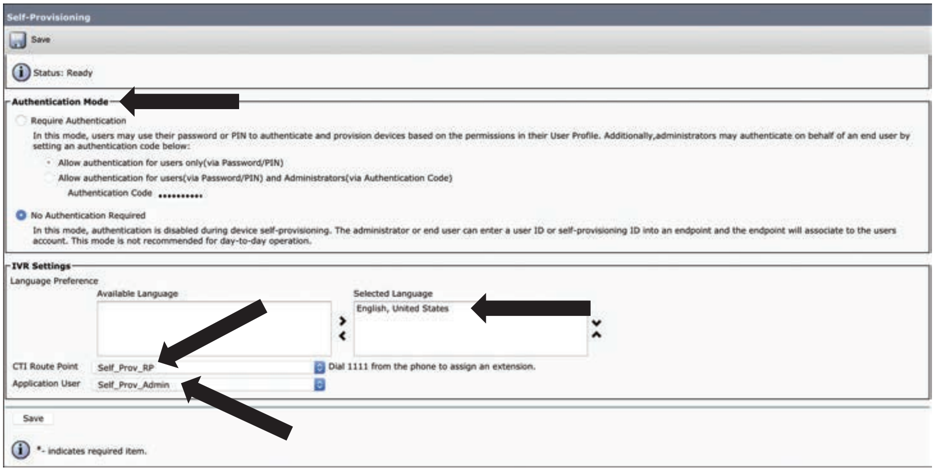
- **Allow Authentication for Users Only:** End users must enter their password or PIN.
- **Allow Authentication for Users (via Password/PIN) and Administrators (via Authentication Code):** End users must enter an authentication code. If you choose this option, configure the authentication code by entering an integer between 0 and 20 digits in the Authentication Code text box.

d. In the IVR Settings list boxes, use the arrows to select the language that you prefer to use for IVR prompts. The list of available languages depends on the language packs that you have installed on your system. Refer to the Downloads section of https://cisco.com if you want to download additional language packs.

e. From the CTI Route Point drop-down list, choose the CTI route point that you have configured for your Self-Provisioning IVR.

f. From the Application User drop-down list box, choose the application user that you have configured for Self-Provisioning.

g. Click **Save**.



Self-Provisioning

Save

Status: Ready

Authentication Mode

○ Require Authentication

In this mode, users may use their password or PIN to authenticate and provision devices based on the permissions in their User Profile. Additionally,administrators may authenticate on behalf of an end user by setting an authentication code below:

● Allow authentication for users only(via Password/PIN)

○ Allow authentication for users(via Password/PIN) and Administrators(via Authentication Code)

Authentication Code ••••••••••

● No Authentication Required

In this mode, authentication is disabled during device self-provisioning. The administrator or end user can enter a user ID or self-provisioning ID into an endpoint and the endpoint will associate to the users account. This mode is not recommended for day-to-day operation.

IVR Settings

Language Preference

Available Language

Selected Language: English, United States

CTI Route Point: Self_Prov_RP — Dial 1111 from the phone to assign an extension.

Application User: Self_Prov_Admin

Save

*- indicates required item.

Figure 17-8 *Configure the System for Self-Provisioning*

Bulk Administration Tool (BAT)

The Cisco Unified Communications Manager Bulk Administration Tool (BAT) is a web-based application that can be used to perform bulk transactions to the Cisco Unified Communications Manager database. BAT is installed as part of the Cisco Unified Communications Manager Administration and can be used to automate the manual process of creating phones and users to more quickly add, update, or delete a larger number of similar phones, users, or ports at the same time.

The Bulk Administration menu is visible only on the first node of a Cisco Unified Communications Manager cluster. Bulk Provision Service (BPS) administers and maintains all jobs that are submitted through the Bulk Administration menu of the Cisco Unified Communications Manager Administration. You can start this service from Cisco Unified Serviceability. The BPS Server service parameter determines whether the service is activated on a particular server. You need to activate BPS only on the first node of a Cisco Unified Communications Manager cluster. BAT can be used to work with the following types of devices and records:

Key Topic

- Add, update, and delete Cisco Unified IP phones including voice gateway (VG) phones, computer telephony interface (CTI) ports, and H.323 clients, and migrate phones from Skinny Client Control Protocol (SCCP) to Session Initiation Protocol (SIP)

- Add, update, and delete users
- Add, update, and delete user device profiles
- Add, update, and delete Cisco Unified Communications Manager Assistant and Manager associations
- Add, update, and delete ports on a Cisco Catalyst 6000 FXS Analog Interface Module
- Add or delete Cisco VG200 and Cisco VG224 analog gateways and ports
- Add or delete forced authorization codes
- Add or delete client matter codes
- Add or delete call pickup groups
- Update or export CUP/CUPC users
- Populate or depopulate the region matrix
- Insert, delete, or export the access list
- Export or import configuration
  - Insert, delete, or export remote destination and remote destination profiles
- Add infrastructure devices

As you can see from this list, BAT works not only with physical devices but also in combination with the user information. For example, when an administrator adds CTI ports and users, he or she can use BAT to choose the Enable CTI Application Use option. This setting saves time when users are added who have applications that require a CTI port, such as a Cisco IP soft phone. When a bulk transaction is performed, the number should be limited to a maximum of 12,000 records. This number applies whether BAT is used to insert, update, delete, or query any records. BAT can also be used to modify batch changes for users, phones, and device profiles.

The Auto-Registration Phone Tool and Self-Provisioning are optional components of BAT that can further reduce the time and effort involved in administering a large system. To add a large block of new phones, an administrator can use BAT to add the devices with dummy MAC addresses instead of entering each MAC address in the data input file. After the phones are registered using the Auto-Registration Phone Tool, the phone users or the administrator can call the Self-Provisioning IVR extension, follow the voice prompts, and download the correct user device profiles for their phones.

Every device includes a multitude of individual attributes, settings, and information fields that enable the device to function in the network and provide its telephony features. Many devices have the same attributes and settings in common, while other values, such as the directory number, are unique to a user or to a device. To condense the BAT data input file contents, BAT uses templates for settings that devices usually have in common.

For bulk configuration transactions on the Cisco Unified Communications Manager database, the BAT process uses two components: a template for the device type and a data file in comma-separated value (CSV) format that contains the unique values for configuring a new device or updating an existing record in the database. The CSV data file works in conjunction with the device template. For instance, when you create a bulk transaction for a group of Cisco IP phones, you set up the CSV data file that contains the unique information for each phone, such as the directory number and MAC address. In addition, you set up or choose the BAT template that contains the common settings for all phones in the transaction, such as a Cisco IP Phone 7841 template. Along these same lines, if BAT is being used to omit data from a field, you can type **NULL** into the field, but do not leave the field blank. BAT uses a multistep process to prepare the bulk configuration transaction, and it uses the Bulk Administration menu options to guide you through the configuration tasks. The BAT process includes these tasks:

1. Set up the template for data input.
2. Define a format for the CSV data file.
3. Collect the data for each device in the bulk transaction.
4. Upload the data files choosing the relevant target and function for the transaction.
5. Validate the data input files with the Cisco Unified Communications Manager database.
6. Submit jobs for execution.
7. Schedule jobs.
8. Execute jobs to insert the devices into the Cisco Unified Communications Manager database.

BAT Configuration Templates

For the first task in the BAT configuration process, an administrator needs to set up a template for the devices that are being configured. The administrator should specify the type of phone or device to add or modify, and then create a BAT template that has features that are common to all the phones or devices in that bulk transaction. BAT templates can be created for the following types of device options:

- **Phones:** All Cisco Unified IP phones and Cisco ATA 186, Cisco VGC phones, CTI ports, and H.323 clients
- **Gateways:** Cisco VG200 and Cisco Catalyst 6000 FXS Analog Interface Module
- **User Device Profiles:** Cisco Unified IP Phone 7900 series and Cisco Softphone

Prior to creating the BAT template, you should make sure settings such as device pools, locations, calling search spaces, phone button templates, and softkey templates have already been configured in the Cisco Unified Communications Manager Administration. Define a BAT template by specifying values in the template fields that will be common to all the devices in the bulk transaction. The BAT template fields require similar values to those that are entered when adding a device manually in the Cisco Unified Communications Manager Administration. After a BAT template has been created, save it with a name. Later in the configuration process, the template name will be associated with the CSV data file. The system stores the templates, so they are reusable for future bulk transactions. If an administrator configured a Cisco IP Phone 8841 template with a specific button template and calling search space for a small deployment, when that administrator needs to add a large number of phones later with the same basic configuration components, he or she can reuse the existing BAT template.

When adding a group of phones that have multiple lines, you can create a master phone template that provides multiple lines and the most common values for a specific phone model. The master template can then be used to add phones that have differing number of lines, but you should not exceed the number of lines in the master phone template. The Cisco Unified IP Phone 8841 is a good example. Even though the phone looks as though it can support eight lines, it can support only four. Therefore, the creation of a master phone template for a Cisco Unified IP Phone 8841 requires only four possible lines. If phones that had between one and four lines were added to the Cisco Unified Communications Manager, then this master template could accommodate them all.

CSV Data File Formats

The CSV data file contains the unique settings and information for each individual device, such as its directory number, MAC address, and description. Make sure that all phones and devices in a CSV data file are the same phone or device model and match the BAT template. The CSV data file can contain duplicates of some values from the BAT template, but values in the CSV data file will override any values that were set in the BAT template. You can use the override feature for special configuration cases. For example, if an administrator wants most of the phones in the bulk transaction to be redirected to a voice-messaging system, the Call Forward Busy for Both Internal and External (CFB) and Call Forward No Answer for Both Internal and External (CFNA) fields can be set to the voice-messaging number in the BAT phone template. However, if a few phones in the bulk transaction need to be redirected to, say, an office administrator or lobby ambassador instead of to a voice-messaging system, then that person’s directory number could be set in the CFB and CFNA fields in the CSV data file. All of the phones will use the CFB and CFNA values from the BAT phone template, except for those specific phones where the directory number of the office administrator or lobby ambassador was specified in the CSV data file.

The CSV data file for phones can also contain multiple directory numbers. Keep in mind, however, that the number of directory numbers that are entered in the CSV data file must not exceed the number of lines that are configured in the BAT phone template; otherwise, an error will result.

When you are adding new devices to the system, you can use the Microsoft Excel spreadsheet that was designed to use with BAT. The BAT spreadsheet assists you with the following features:

Key Topic

- Data file templates with macros for the different devices
- Customized file format definition
- Support for multiple phone lines
- Record error checking
- File conversion to CSV format

When you are creating new records, use the BAT spreadsheet, which is named BAT.xlt, because the data gets validated automatically when you export to the CSV format. BAT.xlt validates data only for valid characters, data types, and field length for particular fields. For experienced BAT users who are comfortable working in a CSV-formatted file, you can use a text editor to create a CSV data file by following the sample text file that is provided on the device insert task window. To modify or update existing phones and devices, you need to locate the records for these devices. BAT provides two methods for locating phones, gateways, and device profiles. You can search by using a customized query or by using a custom file. You can also extract a group of phone records from the Cisco Unified Communications Manager database for inclusion in a CSV data file by using the export utility.

- **Customized Query Searches:** BAT provides a window for defining your query criteria. You can choose the specific device model or choose criteria from a list of device details and a list of line details. To locate all devices of a specific device model, you choose the model but add no other criteria for the search. You get the records for all the Cisco Unified IP phones that are configured in the database.
- **Custom File Searches:** When no common attribute for a query exists, BAT provides the custom file option. A custom file includes device names or directory numbers. You can build a custom text file by putting each record on a separate line. The search gives you all the records that match the criteria.
- **Export Phone Records to CSV Data File:** When you need to move a group of phones, you can use the export utility. You use the export utility to extract existing records from the Cisco Unified Communications Manager database to move them into a CSV data file. When you move phones, use the Export Phones with the All Phone Details option. This option generates an export file that contains records with all the information, including the device attributes, line attributes, and services, that is associated with that phone. You can also export phone records with specific details when phones have similar line configurations and you want to use a template. CSV data files comprise a string of device attributes and information in a comma-separated value (CSV) format. To insert data records into the Cisco Unified Communications Manager database, ensure that each data file is in the CSV format.

The first row of every CSV data file shows the file format by displaying the name of each field that the CSV file includes. The file format information makes it easier to locate the entry for a specific field in the CSV data file. Example 17-1 demonstrates sample output of an exported CSV file. In the CSV file, USER ID represents the fourth field in the header, and the fourth field in the CSV file for the phone shows Johns.

Example 17-1 *Sample Output of a CSV Export*

```
MAC ADDRESS,DESCRIPTION,LOCATION,USER ID,DIRECTORY NUMBER 1,DISPLAY 1,LINE TEXT
LABEL 1,FORWARD BUSY EXTERNAL 1,FORWARD NO ANSWER EXTERNAL 1,FORWARD NO COVERAGE
EXTERNAL 1,FORWARD BUSY INTERNAL 1,FORWARD NO ANSWER INTERNAL 1,FORWARD NO COVERAGE
INTERNAL 1,CALL PICKUP GROUP 1,SPEED DIAL NUMBER 1,SPEED DIAL LABEL 1, 1231123245AB,
SEP1231123245AB,Dallas,Johns,9728437154,9728437154,Mike,9728437172,9728437196, 9728
437127,9728437154,9728437178,9728437189,9728437121/TollByPass,1230000000,Helpdesk,
9728437127,9728437154,9728437178,9728437189,Marketing,1230000000,Helpdesk
```

Now, the file format for the CSV data file can be customized by using the Create Phone File Format Configuration window. You can add attributes to your file format that are also in the BAT template. This allows you to override the template entry with a specific attribute for a device. For instance, you can choose the route partition attribute for your file format and enter different partitions for each phone in the CSV data file. From this window, you can choose specific attributes from the Device and Line fields. The MAC Address and Description device attributes always remain in each file format. The File Format Configuration dialog makes it easy to choose the device attribute in the Device Field box and click an arrow to move the attribute into the Selected Device Field box. You can select multiple attributes at the same time by holding down the Ctrl key. Rearrange the order of the device attribute fields and line attribute fields in the file format by using the up and down arrows. Select an attribute and then click the up arrow to move the item closer to the first record, or click the down arrow to move the item further away from the first record. However, line attributes cannot be moved before device attributes, nor can the order of speed dials be changed.

When a text editor is being used to create a CSV data file, create a customized file format and then enter values in the same order as specified by that file format. Before the text-based CSV data file that uses the customized file format is inserted, the file format name must be associated with the CSV data file. Only one file format can be associated with a single CSV data file. Use the following steps to perform this task:

Step 1. In the Add File Format window, choose the name of the CSV data file <*CSVfilename*>.txt from the File Name drop-down list.

Step 2. Choose a file format from the File Format Name drop-down list. The data in the CSV data file must match the custom file format that is chosen.

BAT Spreadsheet Data Collection for CSV Data File Creation

The BAT spreadsheet simplifies the creation of CSV data files. You can add multiple devices and view the records for each device in a spreadsheet format. The BAT spreadsheet allows you to customize the file format within the spreadsheet and provides validation and error checking automatically to help reduce configuration errors. The BAT spreadsheet also includes tabs along the bottom of the spreadsheet for access to the required data input fields for the various devices and user combinations in BAT. BAT.xlt validates data only for valid characters, data types, and field length for particular fields.

When the Cisco Unified Communications Manager is installed, the Microsoft Excel file for the BAT spreadsheet gets placed on the first node database server. That file must be downloaded from the first node database server to the administrator's computer where Microsoft Excel is installed. To use the BAT.xlt spreadsheet to create a CSV data file, locate and double-click the BAT.xlt file. You must choose Enable Macros when you open the BAT spreadsheet. If the Enable Macros option is not displayed while you are opening the spreadsheet, macro security on the Excel program may be set too high. Ensure that macro security is medium or low for the macros to run. To set the macro security to medium, do the following:

Key Topic

Step 1. Navigate to **Tools > Macro > Security** from the Excel menu.

Step 2. Set the security level to **medium**.

Step 3. Close the Excel program and open it again. This action should give you the Enable Macros option when you open the spreadsheet the next time.

When the spreadsheet opens, it will display a set of columns with attribute headings that specify the BAT field names, whether the field is required or optional, and the maximum number of characters that are allowed in the field. Tabs for every device are displayed along the bottom of the spreadsheet. Click the tab for the type of device to work with, and the columns will adjust to display all relevant fields for the chosen device. For example, to add phones and users all at once, click the tab marked Phones-Users.

Next, define the file format for the CSV data file by clicking the Create File Format button. Use the Field Selection dialog to choose items and their order in your CSV data file. Click Create and the columns in the spreadsheet will adjust to the new file format. In the first row, enter data for a device in all mandatory fields and any relevant optional fields. Enter data in a new row for each device. The system treats blank rows in the spreadsheet as end-of-file markers and discards subsequent records. If you enter a comma in one of the fields, BAT.xlt encloses that field entry in double quotation marks when you export to BAT format.

After all device records are completed, you export the BAT spreadsheet data to the CSV file format that BAT must use to perform the bulk transaction with the Cisco Unified Communications Manager first node database. The system saves the CSV-formatted file as a text file to a folder chosen by the administrator. The filename format should appear as <*tabname*><*timestamp*>.txt, where <*tabname*> represents the type of device input file that was created, such as phones or user device profiles, and <*timestamp*> represents the precise date and time that the file was created. Next, upload the converted CSV data file back to the Cisco Unified Communications Manager database server by choosing **Bulk Administration > Upload/Download Files** in Cisco Unified Communications Manager Administration.

Validate the Data Input Files

The system runs a validation routine to check for errors in the CSV data file and the BAT template against the first node database. These checks include the following items:

Key Topic

- Fields, such as Description, Display Text, and Speed-Dial Label that do not have a dependency on a database table, use valid characters.
- The BAT Validate Transaction validates only data type, length, and relational dependency. Consider the following example:

  ```
  MAC ADDRESS,DESCRIPTION,PARTITION
  AABBCC112233,Lab Phone,Dallas
  ```

  If the Partition does not exist, Validate displays an error saying “Dallas is not an existing PARTITION.”
- The number of lines that are configured on a device matches the device template (only for specific details).

Validation does not check for the existence of a user or for mandatory or optional fields that are BAT defined, such as the dummy MAC address. The following steps define how to run validation on the Cisco Unified Communications Manager.

Step 1. Select the **Validate File** option and choose the file name of the CSV data input file, the BAT template for the device, and the model, if applicable. The CSV data file should contain all details.

Step 2. Select the validation method.

a. Choose **Specific Details** for validating records that follow the Default or Custom file format.

b. Choose **All Details** for validating records from a file that was generated from the export utility using the All Details option.

Step 3. Click **Submit** when ready to validate the file.

After the transaction is complete, click the Log File Name link in the Job Configuration window to see a log file that displays the devices that could not be validated successfully and the error code.

Insert BAT Data Input File Records into Database

When the data input file has passed validation, you are ready to use the Insert window to add the device records into the Cisco Unified Communications Manager first node database. The CSV data input file must be valid. If any line information for a phone record fails, BAT does not insert that phone record. Use the following steps to insert BAT data input file records into the Cisco Unified Communications Manager database.

Key Topic

Step 1. In the Insert window, choose the name of the CSV data input file, the BAT template for the device, and the model, if applicable. The CSV data file should contain all details and be valid.

Step 2. Select the insert method.

a. Choose **Specific Details** to insert records that use a customized file format.

b. Choose **All Details** to insert records from a file that was generated from the export utility using the All Details option.

Step 3. Enter Job Information details and click **Submit**. This creates a job that can be accessed using the Job Scheduler option in the Bulk Administration menu.

Step 4. Use the Job Configuration window to view the status and to schedule and activate the job.

If any line information for a phone record fails, BAT does not insert that phone record. After the transaction is complete, click the Log File Name link in the Job Configuration window to see a log file that displays the number of records that were added and the number of records that failed, including an error code.

Device Onboarding with Activation Codes

The method of onboarding devices using activation codes was first developed in the Cisco Spark cloud calling solution. When a phone was set to cloud registration mode, there was a prompt on the screen after the phone fully booted that allowed the user to enter a 16-digit activation code. Typically, this code was emailed to the user from the cloud management platform prompted by an administrator. It also came with a QR code, so if the phone was a video phone, you could use the camera to scan the QR code, which would enter the 16-digit access code for you. Once the access code was entered into the phone, it would proceed to register to that same cloud management platform. Spark later became Webex, and that cloud management platform became the Webex Control Hub, but the process of registering a phone to the Webex Control Hub still uses the 16-digit access code. It is a proven and effective method of registering phones. It's so effective that Cisco decided to implement it into the on-premises Cisco Unified Communications solution. Activation codes provide a simple method for provisioning and onboarding phones without requiring an administrator to collect and input the MAC address for each phone manually. This method is a simple alternative to Auto Registration that can be used to provision a large number of phones or just a single phone. It can even be used to re-register existing phones.

Activation codes provide many great benefits. Onboarding using activation codes ensures that all newly provisioned phones or untrusted phones have their Manufacturing installed certificate (MIC) assessed and verified by Cisco Unified Communications Manager. Bear in mind that Cisco Manufacturing Root certificates must be present in the CallManager-trust store to perform this onboarding activity. Phone users can obtain their activation codes via the Self Care Portal, provided the **Show Phones Ready to Activate** enterprise parameter is set to **True**. Otherwise, administrators must provide the codes to the phone users.

Another benefit to using activation codes is that there's no need to manually enter actual MAC addresses. Administrators can use dummy MAC addresses, and the phone updates the configuration automatically with the real MAC address during registration. When you provision with dummy MAC addresses, activation codes are tied to the phone model. You must enter an activation code that matches the phone model in order to activate the phone. For added security, you can provision the phone with its actual MAC address. This option involves more configuration because the administrator must gather and input each phone's MAC address during provisioning, but it provides greater security because users must enter the activation code that matches the actual MAC address on their phone. There's also no need to deploy an IVR, such as TAPS, to convert phone names from BAT to SEP.

Key Topic

The process for setting up device onboarding with activation codes is pretty straightforward. The following process outlines the basic steps to complete when dummy MAC addresses are used:

1. The administrator sets the configuration to require the user to enter an activation code for onboarding.
2. The administrator provisions and configures the phone. If dummy MAC addresses are being used, the administrator does not enter the actual MAC address.
3. The phone gets an IP address for TFTP via a DHCP option 150, or from an alternate TFTP as configured in Phone settings. The phone downloads the XMLDefault file and detects that an activation code is in use.
4. The user enters the activation code on the phone.
5. The phone authenticates to the Cisco Unified Communications Manager via the activation code and manufacturing installed certificate.

6. The phone requires the TVS service when the activation code is used for onboarding phones. The ITL file provides this TVS function, which contains the certificate of the TVS service that runs on the Cisco Unified Communications Manager server's TCP port 2445.
7. Cisco Unified Communications Manager updates the device configuration with the actual MAC address. The TFTP server sends the device configuration to the phone, allowing the phone to register. Note that device registration can take up to 5 minutes.

As of Cisco Unified Communications Manager release 12.5(1), the following Cisco IP Phone models support onboarding via activation codes: 7811, 7821, 7832, 7841, 7861, 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, and 8865NR. If you plan to have your users use the Self Care Portal to onboard their phones, you need to set the portal up beforehand so that your users will have access to it. Now that you have a basic understanding how onboarding with activation codes works, let's take a deeper look behind the curtain to see how to set it up.

Steps to Set Up Device Onboarding with Activation Codes

Key Topic

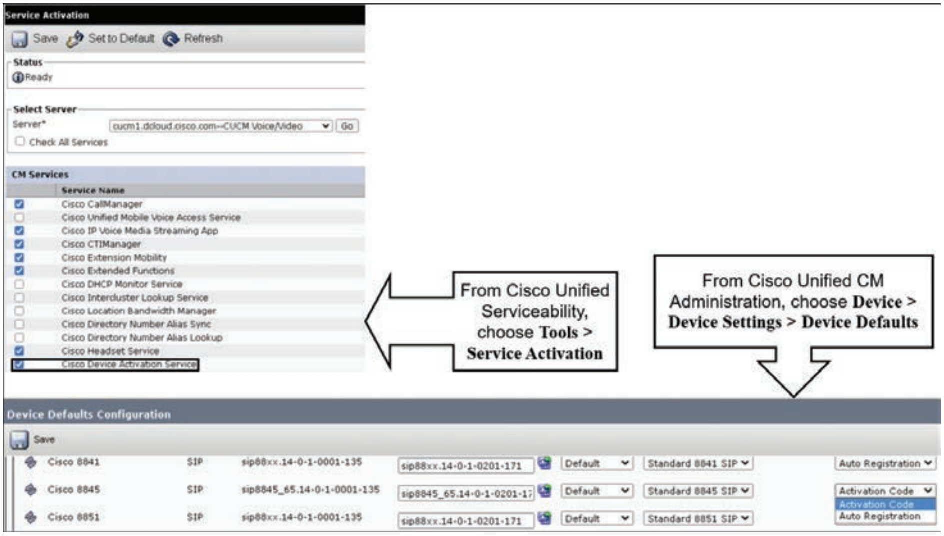
To use activation codes, the **Cisco Device Activation Service** must be running in Cisco Unified Serviceability. From Cisco Unified Serviceability, choose **Tools > Service Activation**. From the **Server** drop-down, choose the Unified Communications Manager publisher node and click **Go**. Under **CM Services**, confirm that the **Status** setting of the **Cisco Device Activation Service** says **Activated.** If the service is not running, check the adjacent check box and click **Save**.

Once you've ensured the Cisco Device Activation Service is running, you can adjust the system defaults so that phones of a specific model type will use activation codes to register with Unified Communications Manager. This procedure applies for the onboarding of on-premises endpoints only. The Onboarding Method setting under **Device Defaults** does not apply for onboarding of Mobile and Remote Access endpoints using activation codes. From Cisco Unified CM Administration, choose **Device > Device Settings > Device Defaults.** In the **Device Defaults Configuration** window, select the device type that will use activation codes for registration in the **Dual Bank Information** section, change **Onboarding Method** from **Auto Registration** to **Activation Code**, and then click **Save.** When device default is set to Activation Code, and if Auto Registration was used earlier for phone types, the subsequent addition of new phones should follow Activation Code Onboarding or Manual Configuration of Phone (Using MAC address) and Registration. Figure 17-9 illustrates the fields where you can configure the Cisco Device Activation Service and set the onboarding method to Activation Code.

You should now be ready to provision a new phone with an activation code requirement. You can configure Universal Device and Line Templates with the settings that you want to apply, as it makes the provisioning process faster. However, if you choose not to use templates, you can add a new phone and configure settings manually, or you can add settings via a BAT Template. In each case, the **Requires Activation Code for Onboarding** check box must be checked in the **Phone Configuration** window.

From Cisco Unified CM Administration, choose **Device > Phone.** Click **Add New From Template** to add settings from a universal line or device template. From the **Phone Type** drop-down menu, select the phone model. In the **MAC Address** field, enter a MAC address.

With activation codes, you can use a dummy MAC address or the phone’s actual MAC address. You can modify the MAC address of a phone in the following scenarios:



Status
Ready

Select Server
Server* cucm1.dcloud.cisco.com--CUCM Voice/Video Go
□ Check All Services

CM Services

	Service Name
☑	Cisco CallManager
□	Cisco Unified Mobile Voice Access Service
☑	Cisco IP Voice Media Streaming App
☑	Cisco CTIManager
☑	Cisco Extension Mobility
☑	Cisco Extended Functions
□	Cisco DHCP Monitor Service
□	Cisco Intercluster Lookup Service
□	Cisco Location Bandwidth Manager
□	Cisco Directory Number Alias Sync
□	Cisco Directory Number Alias Lookup
☑	Cisco Headset Service
☑	Cisco Device Activation Service

From Cisco Unified Serviceability, choose **Tools > Service Activation**

From Cisco Unified CM Administration, choose **Device > Device Settings > Device Defaults**

Cisco 8841	SIP	sip88xx.14-0-1-0001-135	sip88xx.14-0-1-0201-171	Default	Standard 8841 SIP	Auto Registration
Cisco 8845	SIP	sip8845_65.14-0-1-0001-135	sip8845_65.14-0-1-0201-17	Default	Standard 8845 SIP	Activation Code Activation Code Auto Registration
Cisco 8851	SIP	sip88xx.14-0-1-0001-135	sip88xx.14-0-1-0201-171	Default	Standard 8851 SIP	

Figure 17-9 *Cisco Device Activation Service and Onboarding Method Fields*

Key Topic

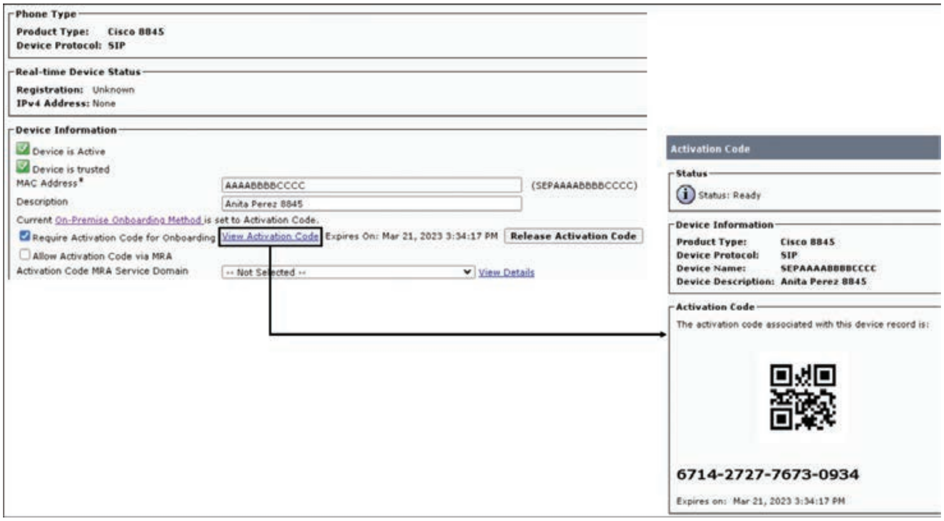
- **BAT{mac}->SEP{mac}:** You should know the exact device name for prefix to change from ?BAT? to ?SEP? upon clicking **Save**.
- **SEP{mac}->BAT{mac}:** You can blank out the MAC address for prefix to change from ?SEP? to ?BAT? and a new device name with a prefix of ?BAT?.

From the **Device Template** drop-down, select a template such as an existing Universal Device Template with the settings you want to apply. From the **Directory Number** field, select an existing directory number or click **New** and do the following:

Step 1. In the **Add New Extension** popup, enter a new directory number and a Line Template that contains the settings you want to apply.

Step 2. Click **Save** and then click **Close**.

The new extension should now appear in the **Directory Number** field. From the **User** field, select the user ID you want to apply to this phone and then click **Add**. Now you need to check the **Requires Activation Code for Onboarding** check box. You should also configure any other settings you want to apply. Once you’re finished, click **Save** and then click **OK**. The **Phone Configuration** will automatically generate the new activation code. Click **View Activation Code** if you want to view the code. Figure 17-10 illustrates how some of these fields should look once the phone is set up to use an activation code.



Phone Type
Product Type: Cisco 8845
Device Protocol: SIP

Real-time Device Status
Registration: Unknown
IPv4 Address: None

Device Information
☑ Device is Active
☑ Device is trusted
MAC Address* AAAABBBBCCCC (SEPAAAABBBBCCCC)
Description Anita Perez 8845
Current On-Premise Onboarding Method is set to Activation Code.
☑ Require Activation Code for Onboarding View Activation Code Expires On: Mar 21, 2023 3:34:17 PM Release Activation Code
☐ Allow Activation Code via MRA
Activation Code MRA Service Domain -- Not Selected -- View Details

Activation Code

Status
Status: Ready

Device Information
Product Type: Cisco 8845
Device Protocol: SIP
Device Name: SEPAAAABBBBCCCC
Device Description: Anita Perez 8845

Activation Code
The activation code associated with this device record is:

6714-2727-7673-0934

Expires on: Mar 21, 2023 3:34:17 PM

Figure 17-10 *Cisco Phone Settings with Activation Code Enabled*

Using BAT with Activation Codes

You can provision many phones to register using activation codes by leveraging the Bulk Administration Tool's Insert Phones feature to provision a large number of phones in a single operation. These phones will use activation codes for registration. You can use this procedure to create a phone template with common settings that you can apply via Bulk Administration to newly provisioned phones of a specific phone model. This procedure assumes that your users are already deployed on the system and that you have already set up device pools, SIP profiles, and phone security profiles that meet your needs.

From Cisco Unified CM Administration, choose **Bulk Administration** > **Phones** > **Phone Template** and click **Add New**. From the **Phone Type** drop-down, select the phone model for which you want to create a template and then enter a **Template Name**. Check the **Require Activation Code for Onboarding** check box and configure values for the following mandatory fields:

- Device Pool
- Phone Button Template
- Owner User ID
- Device Security Profile
- SIP Profile

Complete any remaining fields in the **Phone Template Configuration** window and click **Save**.

Once you've completed your phone template, you need to create a new .csv file with your new phones. From Cisco Unified CM Administration, choose **Bulk Administration** > **Upload/Download Files** and click **Find**. Select and download the **bat.xlt** spreadsheet. Open the spreadsheet and go to the **Phones** tab. Add your new phone details to the spreadsheet. If you are using dummy MAC addresses, leave the MAC Address field empty. When you are done, click **Export to BAT Format**.

From Cisco Unified CM Administration, choose **Bulk Administration** > **Upload/Download Files**. Upload the .csv file by clicking **Add New**. Click **Choose File** and select the .csv file for uploading. Select **Phones** as the target. Select **Insert Phones – Specific Details** for the transaction type and then click **Save**.

Now you can insert new phones from the .csv file by going to **Bulk Administration** > **Phones** > **Insert Phones**. From the **File Name** drop-down, select your .csv file. From the **Phone Template Name** drop-down, select the provisioning template you created. Check the **Create Dummy MAC Address** check box.

For added security, you can add actual MAC addresses to the .csv file such that the activation code works only for the phone with the matching MAC address. In this instance, leave this check box unchecked.

Check the **Run Immediately** check box to run the job right away. If you choose to run the job later, you must schedule the job in the Bulk Administration Tool's Job Scheduler. Click **Submit**, and now you are ready to activate your phones.

Activate Phones

The administrator of the Cisco Unified Communications solution is not going to want to go around and activate hundreds or thousands of phones. It's better to put the tools in the hands of the users to activate their own phones. After you complete the provisioning process, distribute activation codes to your phone users so that they can activate their own phones. Two options exist for gathering and distributing activation codes.

Phone users can log in to the Self Care Portal in order obtain the activation code that applies to their phone. They can either key in the 16-digit code on the phone manually or use their phone's video camera to scan the QR code that displays in Self Care. Either method will work. To use Self Care to activate the phone, the **Show Phones Ready to Activate** enterprise parameter must be set to **True** in Cisco Unified Communications Manager (this is the default setting). Figure 17-11 illustrates a Cisco 8845 Unified IP Phone with the activation code screen ready to receive input.

Alternatively, you can also export the list of outstanding users and activation codes to a .csv file, which you can then distribute to your users via email. Phone users must enter the activation code on their phones in order to use them. After a phone user enters the correct activation code on their phone, the following occurs:

Key Topic

- Their phone authenticates with Cisco Unified Communications Manager.
- The phone configuration in Cisco Unified Communications Manager updates with the actual MAC address of the phone.
- The phone downloads the configuration file and any other relevant files from the TFTP server and registers with Cisco Unified Communications Manager.
- The phone is now ready to use.

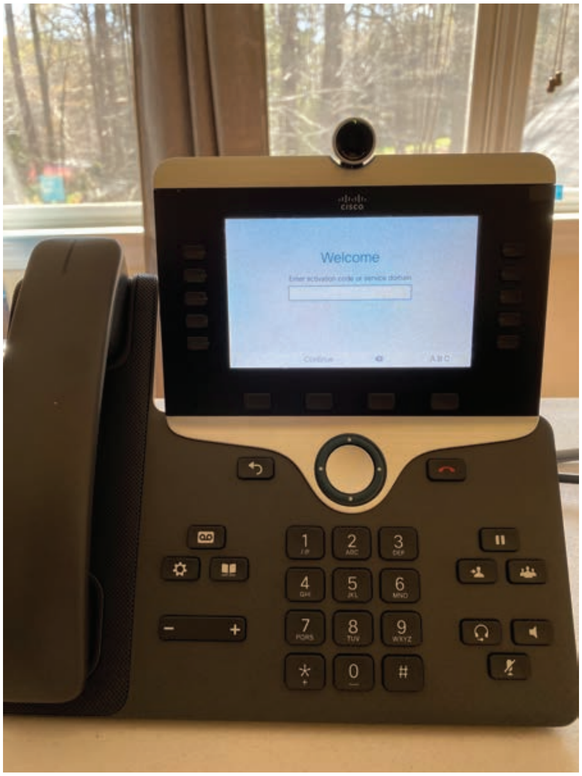


Figure 17-11 *Activation Code Screen on Cisco 8845*

You can export a .csv file of activation codes along with their corresponding phones and users by following these two simple steps. From Cisco Unified CM Administration, choose **Device** > **Phone**. From **Related Links**, select **Export Activation Codes** and click **Go**. A file will be exported to your desktop that you can now use to distribute activation codes to your users.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 17-2 lists a reference of these key topics and the page numbers on which each is found.

Table 17-2 Key Topics for Chapter 17

Key Topic Element	Description	Page Number
Paragraph	Two Types of Phones in the CUCM	397
Steps	Manually Creating Users Within CUCM	398
Steps	Manually Add Phone to End-User Account in CUCM	400
Steps	Self-Provisioning Basic Steps	401
Steps	Enable Services for Self-Provisioning	402
Steps	Auto-registration Settings on CUCM	402
Steps	CTI Route Point for Self-Provisioning IVR	403
Steps	Dial-in Extension for Self-Provisioning IVR	404
Steps	Application User for Self-Provisioning IVR	405
Steps	Configure System for Self-Provisioning	406
List	Devices and Records Used with BAT	407
Paragraph	Two Components Used by BAT	409
List	Tasks to Set Up the BAT Process	409
List	BAT Spreadsheet Feature Assistance	410
Steps	Changing Macro Security Levels in Excel	412
List	Validation Routine Checklist for BAT CSV Files	413
Steps	Insert BAT Data into Database	414
Steps	Setup Process for Activation Codes Using Dummy MAC addresses	415
Paragraphs	Device Activation Service and Enabling Activation Codes	416
List	Modifying MAC Address Scenarios with Activation Codes	417
Section	Using BAT with Activation Codes	418
List	Process of Phone After Activation Codes Are Entered	419

Define Key Terms

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

Auto-registration, BAT, BPS, CSV, DN, IVR, Self-Provisioning

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the steps to manually add a phone to an end user in the Cisco Unified Communications Manager.
2. List the main steps for Self-Provisioning.
3. List the steps to set up and use BAT on the CUCM.

This page intentionally left blank

CHAPTER 18

Cisco Unified Communications Manager Call Admission Control (CAC)

This chapter covers the following topics:

Endpoint Addressing: This topic will overview dial plan components on the Cisco Unified Communications Manager and explain directory numbers and directory URIs.

Call Privileges: This topic will introduce how partitions and calling search spaces within the Cisco Unified Communications Manager can be used for a controlled cost of service (COS) (not to be confused with class of service [CoS]) to prevent hairpinning and establish privileges for different users. This section will also cover how to control calls through bandwidth management using location-based Call Admission Control (CAC).

Call Coverage: This topic will illustrate how to use hunt pilots, hunt lists, line groups, shared lines, and call forward settings in the Cisco Unified Communications Manager to establish better call coverage within a production environment.

The preceding three chapters discussed how to set up the Cisco Unified Communications Manager initially, how to import users, and how to register endpoints. This chapter will begin examining how to control the voice and video communications environment using cost of service (COS) and Call Admission Control (CAC) tools built into the Cisco Unified Communications Manager. Topics discussed in this chapter include the following:

- Endpoint Addressing
- Numeric Addresses
  - Alphanumeric Addresses
- Call Privileges
- Partitions and Calling Search Spaces (CSS)
  - Time of Day (ToD) Routing
  - Location-Based CAC Bandwidth Requirements
- Call Coverage
- Hunting (Line Group Members, Hunt Lists, Line Groups, Hunt Pilots)
  - Call Hunting Operation and Call Flow
  - Call Queuing Settings

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 4.1 Describe the Cisco UCM digit analysis process
- 4.2 Implement toll fraud prevention on Cisco UCM
- 4.3 Configure globalized call routing in Cisco UCM
- 4.3.a Route patterns (traditional and +E.164 format)
    - 4.3.e SIP route patterns

"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 18-1 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 18-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Endpoint Addressing	1–3
Call Privileges	4–6
Call Coverage	7–10

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 tool exists on Cisco IOS gateways to allow administrators to implement call privileges?
    a. Partitions
    b. CSSs
    c. COR
    d. Call Policy
2. Which of the following is a method of mapping PSTN numbers to DNs using translation patterns on the CUCM?
    a. +E.164 addressing
    b. Two-stage dialing
    c. E.164 addressing
    d. Off-net dialing

3. What is the maximum number of directory URIs that can be set per DN?

- **a.** 1
- **b.** 2
- **c.** 5
- **d.** 10

4. Which of the following is an application of call privileges in the CUCM?

- **a.** Used to control per-call bandwidth and total bandwidth throughout the enterprise network
- **b.** Used to group endpoints together so that incoming calls are not dropped
- **c.** Used to give priority over some calling devices, such as a manager's phone, over others during high congestion times
- **d.** Used to route calls to the same number in different ways based on different calling devices

5. If both line and device CSSs are configured on a CTI port, what order are aliases and route patterns searched?

- **a.** Line CSS partitions based on order listed, then device CSS based on order listed
- **b.** Line CSS partitions, then device CSSs, but the order listed does not matter
- **c.** Device CSS partitions based on order listed, then line CSSs based on order listed
- **d.** Device CSS partitions, then line CSS, but the order listed does not matter

6. What location should be used for inter-cluster trunks on the CUCM?

- **a.** Hub_None
- **b.** Shadow
- **c.** Phantom
- **d.** Custom

7. Which of the following call coverage areas are features typically implemented for individuals? (Choose three.)

- **a.** Call Forward
- **b.** Shared Lines
- **c.** Call Pickup
- **d.** Hunting
- **e.** Partitions
- **f.** Calling Search Spaces

8. What is the correct order of configuration for hunting on the Cisco Unified Communications Manager?

- **a.** Line Group Members > Line Groups > Hunt List > Hunt Pilot
- **b.** Hunt Pilot > Hunt List > Line Group > Line Group Members
- **c.** Line Group Members > Hunt List > Line Group > Hunt Pilot
- **d.** Hunt Pilot > Line Group > Hunt List > Line Group Members

9. When hunting is used on the CUCM from a call forward, and all possible line group members have been searched without making a connection, which of the following final forwarding options is likely to be used?

- **a.** All calls will stop hunting, regardless of any other setting.
- **b.** A final forwarding number must be configured in the hunt pilot.
- **c.** The call will return to the call forwarding hunt pilot number that initiated the hunt, and the whole process will start over again.
- **d.** If Use Personal Preference is selected, the call is routed to the number that is -configured for CFNC on the phone line that invoked the call to the pilot number.

10. When you use queuing with hunting, which of the following reasons could cause the call to be disconnected and never placed in the queue?

- **a.** A line group member becomes available while in the queue.
- **b.** No line group members are logged in or registered.
- **c.** Hunt pilot maximum wait time in the queue has expired.
- **d.** The queue will never disconnect callers for any reason.

Foundation Topics

Endpoint Addressing

In my experience, when I mention the term *dial plan*, many people are not acquainted with the term. However, all people use dial plans daily. A dial plan is a carefully planned design for reaching devices and services in a Collaboration network and in the public switched telephone network (PSTN). Endpoint addressing covers how you assign individual or blocks of telephone numbers or URIs to endpoints. A dial plan must include information on how to call other endpoints. These dial rules typically differ depending on the type of call, whether it be an intra-site, inter-site, external, emergency, or other type of call. The dial plan specifies the format in which connected parties are presented and determines the dial plan features and applications such as classes of service and call coverage. Finally, a dial plan defines how calls are routed. This process includes analyzing the received digits, finding the best-matching entry in the call-routing table, choosing the device to which the call should be sent, and determining what to do if that device is busy or not reachable.

The larger an enterprise deployment and the more different dialing domains exist, the more an engineer has to know to design an appropriate dial plan. In general, an engineer must know about the possible types of endpoint addressing, such as numbers versus URIs, how internal and external numbers relate to each other, and the E.164 format that is used in the PSTN. In addition, the engineer must be able to assess the dialing habits of all the dialing domains that exist locally in the enterprise deployment and how to identify and avoid overlapping numbers. The engineer must also have the skills to analyze emergency dialing requirements and to implement methods for PSTN cost avoidance.

Dial plans can be very complex and involve a lot of different geographic areas and devices. Therefore, good documentation is required and should include information that is relevant to end users as well as implementation details that are relevant for administrators and support personnel. Information that is relevant to end users includes the dial habits that are applicable to their site, the dial habits that apply when they roam to another site, and their calling privileges. Documentation is useful only when it is up to date, accessible, and when everyone knows where to find it and when it has been updated. Therefore, you should make sure that all documentation is well defined and that clear responsibilities and processes are in place to ensure that the documentation is accurate; simple to understand; and available to users, administrators, and support teams.

Two aspects must be included in any dial plan documentation: the person who is responsible for each part of the documentation and how changes are approved, implemented, and communicated. Accurate documentation is the basis for troubleshooting, monitoring, planning changes and enhancements, and redesigning.

Key Topic

The North American Numbering Plan (NANP) is a standardized national dial plan that assigns individual or blocks of telephone numbers, which are called E.164 addresses, to physical lines or circuits. This telephone network is based on a 10-digit dial plan that consists of 3-digit area codes and a 7-digit subscriber number known as the telephone number. That 7-digit subscriber number can be further broken down into a 3-digit Central Office Code and a 4-digit line number, also referred to as the subscriber number.

Features within a telephone switch, such as Centrex, support a custom 5-digit dial plan for specific customers who subscribe to that service. PBXs also support variable-length dial plans that contain from 3 to 11 digits. Dialing internationally will also require variable-length numbers to be dialed depending on the country being called. Dial plans contain specific dialing patterns so that users can reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of dialed digits are all part of any particular dial plan. Dial plans that are used within voice-capable routers specify how to determine which digits and how many digits to store in each configuration. If the dialed digits match the configured number and patterns, the call is processed for forwarding.

Dial plan design requires knowledge of the network topology, current telephone-number dialing patterns, proposed router and gateway locations, and traffic-routing requirements. No standard protocol is defined for the dynamic routing of E.164 telephony addresses. VoIP dial plans are configured statically and are managed on call processing devices such as the Cisco Unified Communications Manager, Cisco gateways, and the Cisco Unified Border Element (CUBE). A well-designed dial plan consists of the following components:

Key Topic

- **Endpoint Addressing (Numbering Plan):** Assigning directory numbers (DNs) to all endpoints (such as IP phones, fax machines, and analog phones) and applications (such as voicemail systems, auto attendants, and conferencing systems) enables you to access internal and external destinations.
- **Call Routing and Path Selection:** Depending on the calling device, you can select different paths to reach the same destination. You can also use a secondary path when the primary path is unavailable, such as transparently rerouting a call over the PSTN during an IP WAN failure.
- **Digit Manipulation:** In some cases, the dialed string must be manipulated before routing a call, such as when a call that was originally dialed by using the on-net access code is rerouted over the PSTN. Another example is when an abbreviated code, such as 0 for the operator, is expanded to an extension. This necessity can occur before or after a routing decision is made.

- **Calling Privileges:** You can assign different groups of devices to different classes of service, by granting or denying access to certain destinations. For example, you might allow lobby phones to reach only internal and local PSTN destinations but give executive phones unrestricted PSTN access.
- **Call Coverage:** You can create special groups of devices to process incoming calls for a certain service, according to different rules (top-down, circular hunt, longest idle, or broadcast). This approach also ensures that calls are not dropped without being answered.

Call routing and path selection along with digit manipulation will be covered in more detail in the next chapter. Figure 18-1 illustrates the essence of a scalable endpoint-addressing scheme that logically includes geographical information as part of the endpoint directory number.

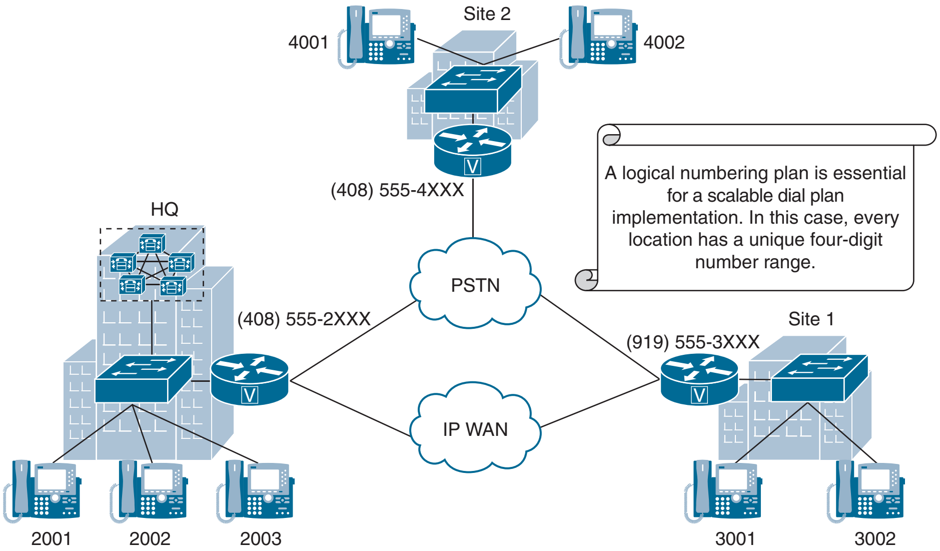

Site 2
4001
4002
(408) 555-4XXX
A logical numbering plan is essential for a scalable dial plan implementation. In this case, every location has a unique four-digit number range.
HQ
PSTN
(408) 555-2XXX
(919) 555-3XXX
Site 1
IP WAN
2001
2002
2003
3001
3002

Figure 18-1 *Dial Plan Components and Functions*

In Figure 18-1, the first digit of every endpoint's assigned directory number also represents its location. The digit 2 represents Headquarters, 3 represents Site 1, and 4 represents Site 2. All endpoints use the same extension length of four digits. Variable extension lengths and overlapping endpoint addresses can make call routing, path selection, or general dial plan implementation much more complex. Therefore, it is best to avoid such dial plans, as demonstrated in this figure.

An important part of every dial plan implementation is call routing and path selection. Many factors can be considered when deciding which path to take to connect two endpoints via WAN or PSTN. In Figure 18-1, the WAN connection has priority when establishing calls between Headquarters and Site 1. If the WAN is unavailable or its bandwidth is exhausted, calls can be rerouted via the PSTN gateway.

The measure of a good dial plan implementation is realized when the end user does not realize which path was taken to establish the call. A core function to provide this transparency is digit manipulation. Many situations require manipulation of called- or calling-party numbers. Figure 18-2 illustrates two scenarios where digit manipulation is required. In the first scenario, a user on phone 2003 may dial 4002 to reach a user in Site 2. Headquarters and Site 2 are connected via PSTN only, so the dialed number 4002 must be expanded to a complete PSTN number so that the PSTN can successfully route the call. Consider the second scenario where an outside PSTN phone dials (919) 555-3001. That complete PSTN called-party number of an incoming call at Site 1 would need to be trimmed to the 3001-extension length of four digits.

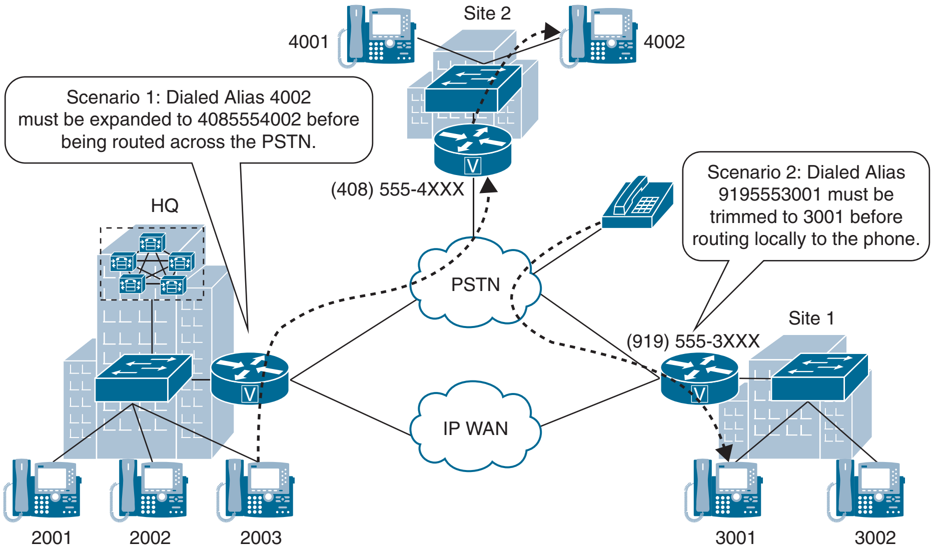

Site 2
4001
4002
Scenario 1: Dialed Alias 4002 must be expanded to 4085554002 before being routed across the PSTN.
(408) 555-4XXX
Scenario 2: Dialed Alias 9195553001 must be trimmed to 3001 before routing locally to the phone.
HQ
PSTN
Site 1
(919) 555-3XXX
IP WAN
2001
2002
2003
3001
3002

Figure 18-2 *Digit Manipulation Scenarios*

In most collaboration infrastructure deployments, some type of calling privilege is implemented within a location, between locations, and for calls to the PSTN. Calling privileges are typically implemented according to the called and calling numbers. Using Figure 18-2 as an example, the user on phone 2001 could be configured to allow the establishment of a call to Site 2 via the PSTN, whereas the user on phone 2002 could be restricted to not have sufficient privileges to establish calls via the PSTN.

Some call coverage settings provide functions to process calls that would otherwise be unanswered or provide service numbers through which calls can be distributed among a group of people. Hunt pilot numbers can be created so that calls to a pilot number are distributed among all members of a group based on a defined hunting algorithm. Call coverage can also be configured to forward calls to different numbers, depending on the reason for not being able to process the call, such as Busy, No Answer, and so on, and based on the origin of the call, such as on-net or off-net.

This chapter will delve deeper into the endpoint addressing, call privilege, and call coverage components of a dial plan. Table 18-2 compares the dial plan configuration elements of the Cisco Unified Communications Manager, a Cisco IOS gateway, and the Cisco Expressway series per main component.

Table 18-2 Comparison of Dial Plan Configuration Elements

Dial Plan Component	Cisco Unified Communications Manager	Cisco IOS Gateway	Cisco Expressway Series
Endpoint Addressing	Directory Number, Directory URI	ephone-dn, voice register pool	IP Address, H.323 ID, E.164 Alias, Directory URI, Service Prefix
Call Routing and Path Selection	Route Patterns, SIP Route Patterns, Route Groups, Route Lists, Trunks	Dial Peers	Search Rules, Zones
Digit Manipulation	Translation Patterns, Transformation Patterns, Route Patterns	Voice Translation Profiles and Rules, Dial Peer Settings	Transforms, Call Policy, FindMe
Call Privileges	Partitions, Calling Search Spaces, ToD	COR	Call Policy
Call Coverage	Hunt Pilots, Line Groups, Hunt Lists, Shared Lines, Call Forward settings	Dial Peers, Hunt Groups, Call Applications	FindMe

Numeric Addresses

To reach internal endpoints such as IP phones, fax machines, and applications, such as voicemail systems, auto-attendants, and conferencing systems, an engineer must assign at least one directory number to each endpoint. In addition, directory URIs can be added as aliases to directory numbers. Calling a configured directory number or directory URI will allow a user to reach the corresponding device.

The first decision an engineer must make is the length of the internally used extension. The number of required extensions influences whether the engineer will choose longer or shorter extensions. Four-digit extensions allow up to 10,000 endpoints to be addressed within a single enterprise deployment. Typically, the phones should also be reachable from the PSTN. Internal endpoint addressing can be mapped to PSTN numbers for off-net connectivity in two ways:

- **Two-Stage Dialing:** With two-stage dialing, all endpoints share a single PSTN number. When a PSTN user wants to call an internal endpoint, the PSTN user calls the PSTN number of the target company. The communications system, such as the Cisco Unified Communications Manager, accepts the call either by routing the call to an attendant's extension or by answering the call with an IVR script that allows the caller to then enter the extension of the desired internal user.
- **Direct Inward Dialing (DID):** With DID, each internal phone has its own PSTN number. Ideally, the least significant digits of the external DID range match the internally used extension numbers (1:1 mapping). If a corresponding DID range is not

available and your PSTN provider assigns different external numbers to you, you must map each external number to an internal extension and translate the number accordingly.

The E.164 number format is used in the PSTN environment. E.164 numbers start with a country code, and they can have a maximum of 15 digits. International phone numbers are usually written with a plus sign (+) before the phone number to indicate that the number is in international E.164 format. Such numbers are referred to as +E.164 numbers. H.323 does not support +E.164 dialing. To actually dial a PSTN number from a normal fixed-line phone, you must use the appropriate access code. Every country has both a national access code, which is used to dial a national number without the country code, and an international access code, which is used to dial out of the country. To indicate that an IP call should be sent to the PSTN from an IP PBX, such as the Cisco Unified Communications Manager, instead of being routed within the enterprise network, a PSTN access code is often configured and must be dialed first to reach an outside line. Calls within an enterprise IP network are referred to as *on-net calls*. Calls that leave the IP network and traverse the PSTN network are referred to as *off-net calls*. Figure 18-3 illustrates how 4-digit internal directory numbers are mapped 1:1 to external +E.164 numbers.

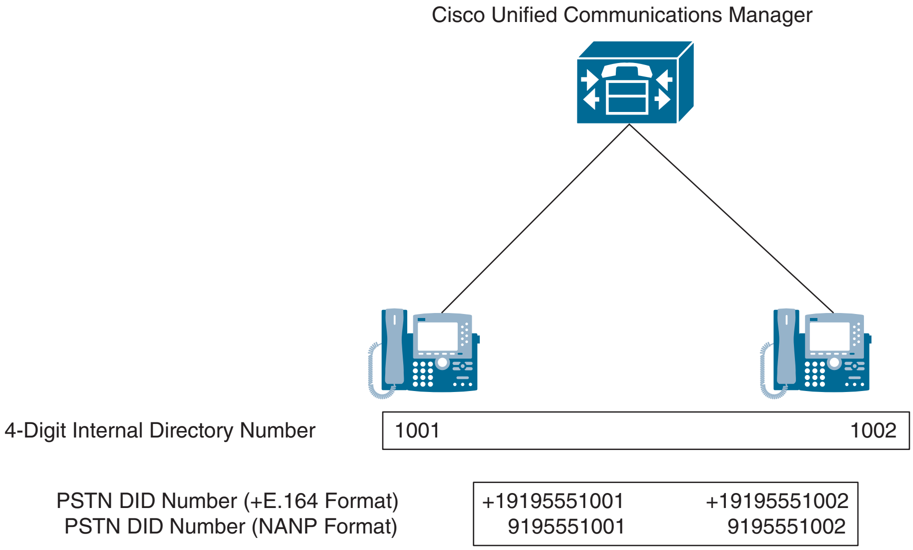

Cisco Unified Communications Manager
4-Digit Internal Directory Number
1001
1002
PSTN DID Number (+E.164 Format)
PSTN DID Number (NANP Format)
+19195551001
9195551001
+19195551002
9195551002

Figure 18-3 *Endpoint Addressing by Numbers*

Alphanumeric Addresses

Directory numbers are assigned to a phone line, and then directory URIs are assigned to a directory number. Therefore, a directory URI cannot exist unless a directory number exists first. The format of a standard URI is different from the format of a URI in the Cisco Unified Communications Manager. A standard URI takes the form *host@<Fully_Qualified_Domain_Name>*, such as *john@cisco.com*. Email addresses are a common use of standard URIs where the domain must be qualified against an authoritative server, such as the mail server. A directory URI on the Cisco Unified Communications Manager has the same look as a standard URI, but it takes the form *user@domain* or *user@ip_address*. Because a directory URI is not assigned to a phone, the "domain" portion of the alias does not have to be qualified. The behavior of a directory URI is also slightly different on the Cisco Unified Communications Manager than standard URIs in a typical networked environment. Cisco has renamed the components that make up a directory URI. The domain portion of the directory URI is also referred to as the "host" portion within the Cisco Unified Communications Manager.

Out of the box, the user portion of a directory URI is case sensitive. This has to do with the characters that are considered digits within the Cisco Unified Communications Manager. Any digit 0–9; plus special characters question mark (?), dollar sign ($), exclamation mark (!), percent sign (%), ampersand (&), underscore (_), tilde (~), equal sign (=), backslash (\), brackets ([ ]), plus sign (+), dash (-), caret (^), asterisk (*), comma (,), dot (.), forward slash (/), and pound sign (#); and the capital letters *A–D* are all considered to be of numeric value. Under Cisco Unified Communications Manager Administration, in the Enterprise Parameters Configuration menu, there is a parameter called URI Lookup Policy. The default value to this setting is Case Sensitive, which is what makes the letters A–D represent numbers. Changing this setting to Case Insensitive changes the user portion of the directory URI so that it's case insensitive, therefore also changing the letters *A–D* away from numeric status.

The host, or domain, portion of the directory URI is always case insensitive. Acceptable characters in the host portion of the directory URI include the letters *a–z*, *A–Z*, numbers 0–9, hyphens, and dots. The host portion must contain at least two characters, it cannot start or end with the hyphen character, nor can it contain two consecutive dots. Table 18-3 identifies all the characters that are supported in both the user and domain portions of a directory URI.

Key Topic

Table 18-3 Directory URI Characters Supported

	User Portion	Domain (Host) Portion
Letters	a–z, A–Z	a–z, A–Z
Special Characters	! $ % & * _ + ~ - = \ ? ' , . /	- .
Numbers	0–9	0–9

There are two ways to place calls to URIs from endpoints that support URI dialing. The first method is by dialing a full directory URI. This method of dialing uses both the user and domain portions of the URI address and is always supported. This method is required when calling the URI of an endpoint outside of the enterprise domain, such as Webex.com. The second method of dialing by URI is by dialing only the user portion. The Cisco Unified Communications Manager will not allow URIs to be dialed by only the user portion unless the organization top-level domain (OTLD) is configured under the enterprise parameters. This is where the case sensitivity setting comes into play. If a user were to dial **BAD2003**, and the URI Lookup Policy was set to Case Sensitive, the Cisco Unified Communications Manager would see this alias as a directory number, not a directory URI, and no domain would be appended to it. This may impact call routing if the alias only existed within a directory URI. However, changing the URI Lookup Policy to Case Insensitive would allow this alias to be routed as a directory URI. The domain that existed in the OTLD would be appended, and the call would be routed providing a match was found. Ideally, all URIs that are applied to endpoints of a Cisco Unified Communications Manager cluster use the same, globally unique host portion. If you use the same host portion in different clusters, calls between these clusters work only if you implement URI synchronization. URI synchronization is an application of the ILS and GDPR.

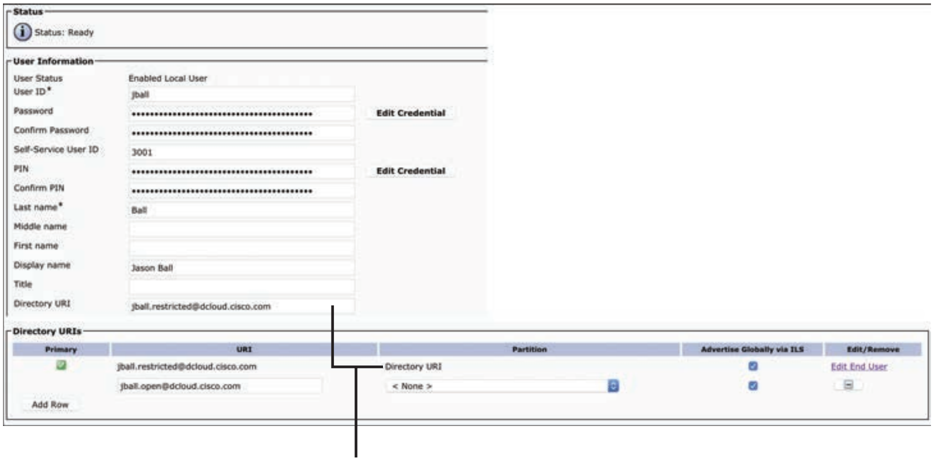
Key Topic

As mentioned before, URIs are not directly applied to a phone or phone line, but they are associated with a directory number. When a call is placed to a locally configured URI, the Cisco Unified Communications Manager routes the call to the associated directory number. There are two places where directory URIs can be configured in the Cisco Unified Communications Manager. Directory URIs are assigned at the Directory Number configuration page or at the End User configuration page. Directory URIs set at the End User configuration page will be placed automatically in the Device URI partition, which is a default partition that exists within the Cisco Unified Communications Manager, and this setting cannot be changed. URIs set at the Directory Number configuration page allow you to set the partition to anything, including the None partition, and you can change this setting at any time. You can also set up to five directory URIs per directory number, as long as one of the directory URIs is set as the primary.

Directory numbers can be individually managed under Cisco Unified Communications Manager Administration by navigating to **Call Routing > Directory Number**. Search for a specific directory number or click Find to view all the available entries. Click the Add New button to configure a new directory number.

After the directory number has been configured, whether with the provisioned phone, end user, or manually, other line settings can now be configured. Many of these settings will be discussed as this chapter progresses. Scroll down to the Directory URIs section. Enter a full URI address in the URI box, and select a partition from the Partition drop-down box. Click on the Add Row button when finished. A new line appears, but the directory URI is added to this directory number. Click Save when finished.

To add a directory URI to an end user, navigate to **User Management > End User**. Select the end user to be modified, whether this is an LDAP synchronized user or not. In the User Information section, locate the directory URI setting and enter the appropriate value in the box beside it. Click Save after the setting has been configured. Figure 18-4 illustrates where to configure the directory URI settings on the Cisco Unified Communications Manager.



Status

Status: Ready

User Information

User Status	Enabled Local User	
User ID*	jball	
Password	**	Edit Credential
Confirm Password	**	
Self-Service User ID	3001	
PIN	**	Edit Credential
Confirm PIN	**	
Last name*	Ball	
Middle name		
First name		
Display name	Jason Ball	
Title		
Directory URI	jball.restricted@dcloud.cisco.com	

Directory URIs

Primary	URI	Partition	Advertise Globally via ILS	Edit/Remove
☑	jball.restricted@dcloud.cisco.com	Directory URI	☑	Edit End User
	jball.open@dcloud.cisco.com	< None >	☑	⊟

Add Row

Directory URI Setting configured at the End User page will set
the Partition to Directory URI and this setting cannot be changed.

Figure 18-4 *Directory URI Settings on the CUCM*

Call Privileges

Calling privileges are configured to control which call-routing table entries are accessible from a particular endpoint, such as a phone, gateway, or trunk. The primary application of calling privileges is the implementation of cost of service (COS). Cost of service (COS) should not be confused with class of service (CoS). Class of service is a Layer 2 QoS mechanism that is specific to IP routing across the network. Cost of service (COS) is specific to the Cisco Unified Communications Manager, and it is typically used to control telephony charges when calls are routed through the PSTN by blocking costly service numbers and international calls for some users. COS is also used to protect the privacy of some users, such as to disallow direct calls to managers except through their assistants.

Calling privileges can also be used to implement special applications, such as routing calls to the same number in different ways based on different calling devices. For example, in a selective PSTN breakout in a multisite environment with PSTN gateways at each site, PSTN route patterns should always be directed toward the associated local PSTN gateway. Therefore, the same route patterns must exist multiple times—once per site, in this example. Only the site-specific route patterns should be accessible by the devices at their respective site. Another application is time-of-day routing, in which calls take different paths depending on when the call is placed. Figure 18-5 illustrates the concept of using calling privileges for implementing special applications.

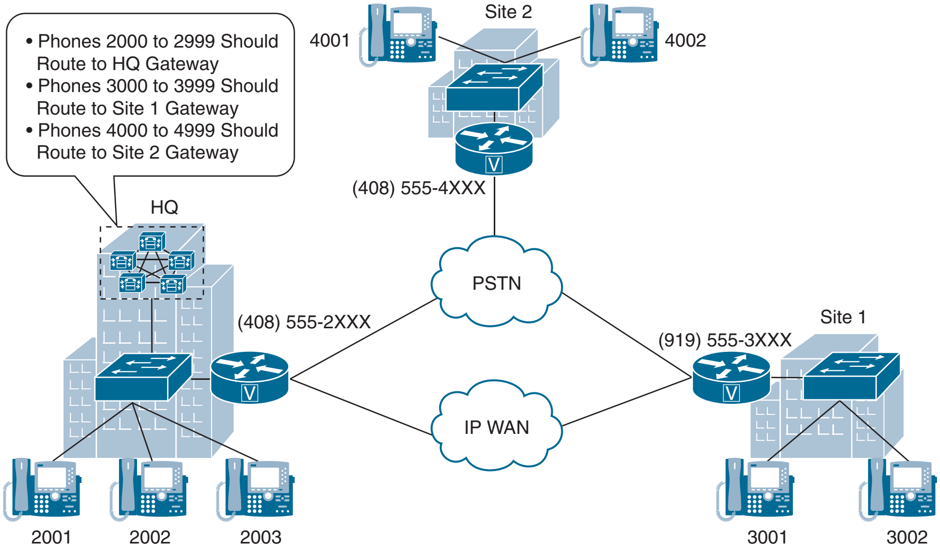

• Phones 2000 to 2999 Should Route to HQ Gateway
• Phones 3000 to 3999 Should Route to Site 1 Gateway
• Phones 4000 to 4999 Should Route to Site 2 Gateway
Site 2
4001
4002
(408) 555-4XXX
HQ
PSTN
(408) 555-2XXX
Site 1
(919) 555-3XXX
IP WAN
2001
2002
2003
3001
3002

Figure 18-5 *Using Calling Privileges for Implementing Special Applications*

Calling classes are most commonly used to control tolled calling environments, so that employees are only capable of placing tolled calls depending on what their position in the company requires. Tolled calls can be divided into four categories: Internal, Local, Long Distance, and International. A typical COS implementation will align each of these privilege classes with its allowed destinations. Each calling privilege class can then be assigned to specific devices or users. Table 18-4 identifies each calling privilege class and its associated allowed destinations.

Table 18-4 PSTN Calling Privilege Class Map

Calling Privilege Class (COS)	Allowed Destinations
Internal	Internal Emergency
Local	Internal Emergency Local PSTN
Long Distance	Internal Emergency Local PSTN Long-Distance PSTN
International	Internal Emergency Local PSTN Long-Distance PSTN International PSTN

In Table 18-4, internal calls are IP-based and have no cost associated with them. Therefore, every class has internal access as an allowed destination for calling. The Internal class is also allowed emergency calls across the PSTN for obvious reasons, but all other PSTN access is restricted. The Local class adds permission for local PSTN calls but is still restricted from placing long-distance or international calls across the PSTN. The Long Distance class is also allowed long-distance PSTN calls, and the International class is not restricted from any type of PSTN call.

Partitions and Calling Search Spaces

A *partition* is a group of dialable patterns with identical accessibility. A calling search space (CSS) defines which partitions are accessible to a particular device. Another way of looking at partitions and CSSs is that partitions affect inbound called numbers, whereas CSSs affect outbound calling devices. A device can call only those call-routing table entries that are in partitions included in the CSS of the device. Partitions are assigned to call-routing targets—that is, any entry of the call-routing table, including voicemail ports, directory numbers, route patterns, and translation patterns. CSSs are assigned to the sources of call-routing requests, such as phone lines, gateways, trunks, voicemail ports, and applications. By default, all entities that can be configured with a partition are automatically in the <None> partition, also referred to as the *null partition*, and all entities that can be configured with a CSS are automatically assigned the <None> CSS. The <None> partition allows access to any call-routing sources regardless of the CSS of that call-routing source, and the <None> CSS provides access to no partitions except the <None> partition. By default, no partitions or CSSs are assigned, and all entities are associated with the null partition and <None> CSS. Therefore, all calls are possible for all calling sources by default. Figure 18-6 illustrates how partitions and CSSs operate within the Cisco Unified Communications Manager environment.

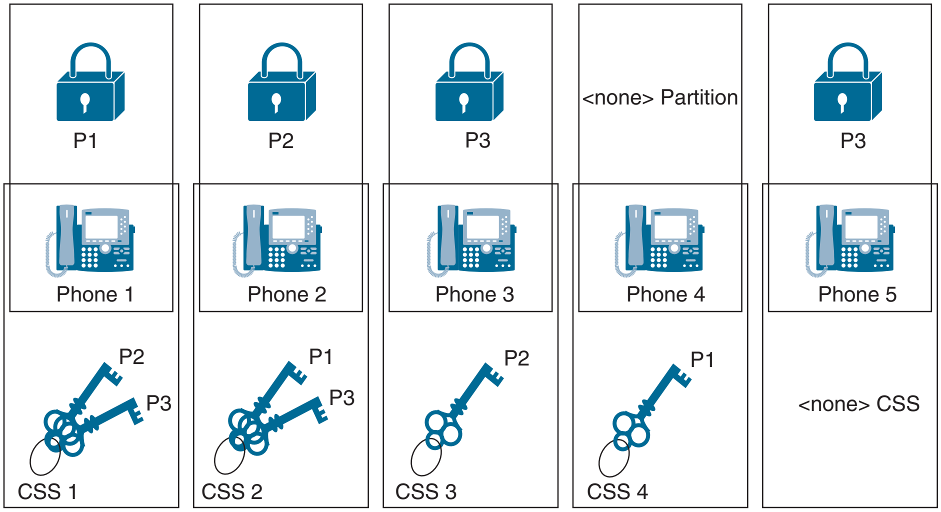


Figure 18-6 *Partition and CSS Operation in the CUCM*

Several analogies have been created over the years to try to explain the relationship between partitions and CSSs. None have conveyed this information as well as the analogy of locks and key rings, as illustrated in Figure 18-6. The locks represent partitions that an administrator has applied to phone lines. The key rings represent the CSSs. Each key on a key ring represents a different partition associated with that CSS and therefore provides access to that partition. CSSs can be applied to either the phone line or to the phone itself.

In Figure 18-6, Phone 1 is configured as a member of the P1 partition, Phone 2 is in the P2 partition, and Phone 3 and Phone 5 are in the P3 partition. Phone 4 remains in the <none> partition because this phone has not been assigned to any other partition. Following the analogy of locks and keys, there are three different locks (P1, P2, and P3). Locks are a great symbol for partitions because when a phone is assigned to a partition, that phone is secured so that no other phone can call it without appropriate permission. With only the partitions (locks) in place, none of the phones can contact any of the other phones except for Phone 4, which is in the <none> partition. Any device in the <none> partition can be contacted by any other device under any circumstance. Even though Phone 3 and Phone 4 are in the same partition, they cannot call one another because neither phone has permission to call P3. To assign calling privileges, CSSs must also be assigned to each phone.

The CSSs are represented as key rings. Each key on a key ring represents the partition that key ring can access. Phone 1 has a key ring with P2 and P3 keys. Phone 2 has a key ring with P1 and P3 keys. Phone 3 has a key ring with only one key to P2. Phone 4 has a key ring with only one key to P1, and Phone 5 has no keys. As a result of this implementation of partitions and CSSs, the following effective permissions apply:

- **Phone 1:** Phone 1 has access to all devices in the <none> partition, which includes Phone 4 from this example. In addition, Phone 1 can access devices in the P2 and P3 partitions because it has the appropriate keys. Therefore, Phone 1 can access Phone 2, Phone 3, Phone 4, and Phone 5. However, Phone 1 cannot access any other devices in the P1 partition if any existed.

- **Phone 2:** Like Phone 1, Phone 2 has access to all devices in the <none> partition, which includes Phone 4 from this example. In addition, Phone 2 can access devices in the P1 and P3 partitions because it has the appropriate keys. Therefore, Phone 2 can access Phone 1, Phone 3, Phone 4, and Phone 5. However, Phone 2 cannot access any other devices in the P2 partition if any existed.

- **Phone 3:** Like all other phones, Phone 3 has access to all devices in the <none> partition, which includes Phone 4 from this example. In addition, Phone 3 can access devices in the P2 partition because it has the appropriate key. Therefore, Phone 3 can access Phone 2 and Phone 4. However, Phone 3 cannot access any devices in the P1 or P3 partitions.

- **Phone 4:** Like all other phones, Phone 4 has access to all devices in the <none> partition, which includes itself from this example. In addition, Phone 4 can access devices in the P1 partition because it has the appropriate key. Therefore, Phone 4 can access Phone 1 and itself, which is of no practical importance because phones don't usually place a call to themselves.

- **Phone 5:** Like all other phones, Phone 5 has access to all devices in the <none> partition, which includes Phone 4 from this example. Phone 5 cannot access any other partitions because it is still part of the <none> CSS. Therefore, Phone 5 can access only Phone 4.

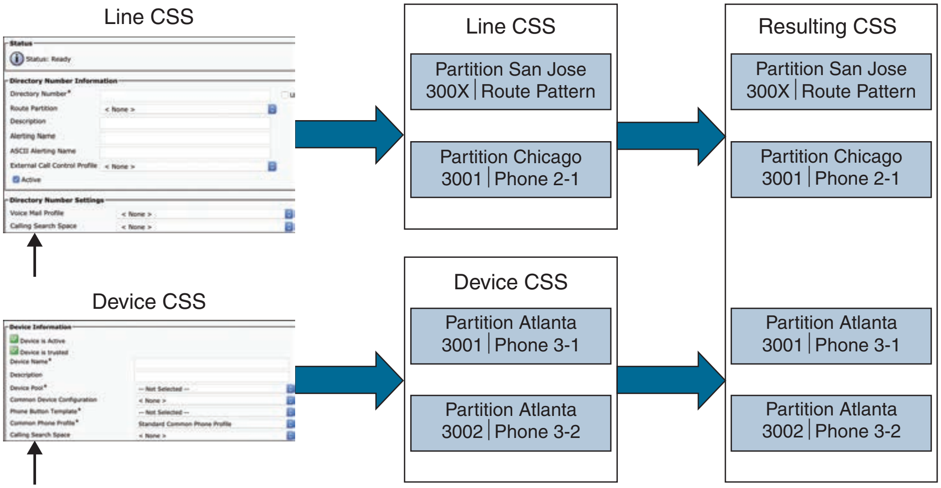
To summarize the analogy that is used in Figure 18-6: partitions are like locks, which can be unlocked only by an appropriate key. CSSs are like key rings that include the specified keys for the appropriately assigned partitions. If no partition (lock) is applied to a device, all other devices can access that device. If no CSS (key ring) is present, only devices that do not have a partition (lock) assigned can be accessed.

Now that we've established a basic understanding of partitions and CSSs, it is important to understand how these COS mechanisms affect call-routing decisions within the Cisco Unified Communications Manager. Assume a phone has a CSS containing two partitions called Chicago and San Jose. The Chicago Partition contains a phone with the directory number 3001 assigned to Phone 2-1. The San Jose partition contains a phone with the directory number 2001 assigned to Phone 1-1. When the user with the CSS assigned to it places a call to directory number 3001, which is the directory number of Phone 2-1, the Cisco Unified Communications Manager performs a call-routing lookup of the number 3001 through the partitions that are configured in the CSS of the calling phone: Chicago and San Jose. The Cisco Unified Communications Manager finds a match in the Chicago partition because the directory number 3001 of Phone 2-1 is assigned to this partition. Because no other matches exist, routing is complete, and Phone 2-1 rings. This example is pretty straightforward and in line with how call routing has been explained up to this point.

A CSS is an ordered list of partitions from the top down. The partition that is listed first has higher priority over a partition that is listed later. When the Cisco Unified Communications Manager performs a call-routing lookup, all accessible entities are considered by best-match logic. Accessible entities include all targets that reside in a partition that is listed in the CSS of the calling phone and all targets that do not have an applied partition (the <none> partition). Multiple identical entities can exist in the call-routing table, but they must be in different partitions. One exception to this rule is phone directory numbers. When two or more devices share the same directory number within the same partition, the directory number is called a *shared line*. If no single best match is found, the Cisco Unified Communications Manager uses the entry of the call-routing table whose partition is listed first in the CSS of the calling device. So, the call-routing table entry is chosen based on the following order:

1. The best match is chosen.
2. If multiple equally qualified matches exist, the order of the partition in the CSS of the calling device is the tiebreaker. In other words, if there is no single best match, the match that is found in the earlier listed partition in the device CSS is chosen.

On most sources of a call-routing request, such as a trunk, gateway, or translation pattern, only one CSS can be configured. On IP phones, however, a CSS can be applied per line and once at the device level. If both line and device CSSs are configured, the CSS of the line from which the call is placed is considered first. In other words, the CSS that is used is composed of the partitions that are listed in the line CSS, followed by the partitions of the device CSS. The exception to this rule is on CTI ports, where the line CSS and the device CSS are placed in reverse order. The partitions of the device CSS are placed before the partitions of the line CSS. Figure 18-7 illustrates the typical order of line CSSs being listed before device CSSs.



Status
Status: Ready
Directory Number Information
Directory Number*
Route Partition < None >
Description
Alerting Name
ASCII Alerting Name
External Call Control Profile < None >
☑ Active
Directory Number Settings
Voice Mail Profile < None >
Calling Search Space < None >

Device Information
☑ Device is Active
☑ Device is trusted
Device Name*
Description
Device Pool* -- Not Selected --
Common Device Configuration < None >
Phone Button Template* -- Not Selected --
Common Phone Profile* Standard Common Phone Profile
Calling Search Space < None >

Figure 18-7 *Line CSS and Device CSS Order on a Single Phone*

In the example from Figure 18-7, the line CSS of the calling phone includes the San Jose and Chicago partitions, and the device CSS of the calling phone includes the Atlanta partition. Route pattern 300X is in the San Jose partition, directory number 3001 is used at Phone 2-1 in the Chicago partition, and the same directory number 3001 is used at Phone 3-1 in the Atlanta partition. If the calling phone dials 3001, the Cisco Unified Communications Manager interprets the dialed digits and searches for the closest match.

The route pattern 300X represents 10 possible numbers and is therefore not a "closest match," as compared to the two directory numbers of 3001. Out of the two equally matched directory numbers, the number of Phone 2-1 is used to extend the call because it is in the partition that is listed first from the line CSS. Based on this current configuration, Phone 3-1 can never be reached from the phone with these CSSs. Site codes would be needed in order to reach Phone 3-1.

The importance of this example is to illustrate that the line CSS has higher priority over the device CSS. If the line CSS and device CSS were reversed, the call would be sent to Phone 3-1. Although route pattern 300X matches the dialed number and is listed in the first partition, it is not used to route the call in this example. The first priority for the call-routing decision is the best match; the order of partitions is important only if multiple best matches exist.

A common misunderstanding is that the first matching pattern found when searching through the partitions in the order that is specified in the CSS is used for call routing, regardless of the quality of the match. If this scenario were true, subsequent partitions of the CSS would be looked at only if no match was found in the earlier partitions. However, all partitions are immediately considered for best-match logic. The partition order is relevant only if multiple best matches exist.

When you are creating partitions and CSSs, you should always create partitions first. Use the following steps to configure partitions and CSSs on the Cisco Unified Communications Manager:

Step 1. Create partitions.

- **a.** From Cisco Unified Communications Manager Administration, navigate to **Call Routing > Class of Control > Partition.**
- **b.** Click **Add New** and enter a name for the partition.

NOTE To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions; the names and descriptions can have up to a total of 1475 characters. The partition name cannot exceed 50 characters. Use a comma (,) to separate the partition name and description on each line. If a description is not entered, Cisco Unified Communications Manager uses the partition name as the description.

- **c.** Click **Save** when finished.
- **d.** Once partitions have been created, they can be assigned to dialable patterns such as directory numbers, route patterns, or translation patterns.

Step 2. Create CSSs.

- **a.** Navigate to **Call Routing > Class of Control > Calling Search Space**.
- **b.** Choose one of the following options:

NOTE Several CSSs exist by default in the Cisco Unified Communications Manager. After partitions have been configured, the administrator may choose to modify an existing CSS or create new ones.

Click **Add New** to add a new calling search space.

Click **Find** and select an existing CSS.

c. From the Calling Search Space Configuration page, enter a Name and optionally a Description for the CSS.

d. From the Available Partitions box, select the partitions to be added to this CSS, and then click the down arrow. These partitions will be searched based on the order they are listed. Use the up- and down-arrow keys to the right of the Selected Partitions box to change the order of any selected partition.

e. Click **Save** once the CSS has been configured.

f. Once all the CSSs have been configured, assign the appropriate CSS to entities that can request lookups to the call-routing table to route a call. Examples of such entities are phones and phone lines, trunks, gateways, and translation patterns.

A translation pattern can support both a partition as a called entity and a CSS as the calling entity. The translation pattern is a dialable pattern in the call-routing table as the target of a call-routing request. If matched, the pattern invokes a new call-routing request for the translated pattern. The partition at the translation pattern specifies who can match the pattern. The partition is required in the CSS of the calling device. The CSS at the translation pattern specifies the entries of the call-routing table that the translation pattern can see for its call-routing request when trying to find the translated pattern in the call-routing table.

Time of Day (ToD) Routing

Time of day (ToD) routing is a practical means of controlling when calls across a PSTN are allowed, in addition to who is allowed to place those calls. For example, a company noticed its phone bill increased significantly during recent months. Upon closer investigation, the staff realized that multiple international calls were being placed after closing hours during the week. That company had recently contracted a new cleaning company to come in after hours to clean the office. The cleaning personnel were making international calls during their shifts. The Collaboration administrators were able to resolve this issue and prevent after-hours calls from being made by simply introducing ToD routing to the existing network.

You can use ToD routing to define time periods. You can define a start time and an end time, and also specify repetition intervals either as days of the week or a specified date on the yearly calendar. The following steps outline how to configure ToD routing in the Cisco Unified Communications Manager:

Key Topic

Step 1. Configure a time period.

a. From Cisco Unified Communications Manager Administration, navigate to **Call Routing > Class of Control > Time Period.**

b. Click **Add New** and configure the following fields in the Time Period Configuration window:

Name: Enter a name for the time period.

Time of Day Start: Choose a start time from the drop-down menu.

Time of Day End: Choose an end time from the drop-down menu.

Repeat Every: Optionally choose a start and end date based on weeks or years.

c. Click **Save.**

Step 2. Configure a time schedule. The time periods that were configured in the preceding step are building blocks for this schedule. Time periods can be assigned to multiple schedules.

- **a.** Navigate to **Call Routing > Class of Control > Time Schedule**.
- **b.** Click **Add New** and enter a Name for the new time schedule.
- **c.** Click **Save**.
- **d.** In the Time Schedule Configuration window, the Time Period Information box will appear. Select the time periods that should be added to this time schedule from the Available Time Periods box and use the down-arrow key to move them to the Selected Time Periods box. This is an ordered list from top down, so the order can be changed using the up- and down-arrow keys to the right of the box.
- **e.** Click **Save**.

Step 3. Associate time schedules with partitions to determine where calling devices search when they are attempting to complete a call during a particular time of day.

- **a.** Navigate to Call Routing > Class of Control > Partition.
- **b.** Click **Find**, and select a partition to modify from the list.
- **c.** From the Partition Configuration page, use the Time Schedule drop-down list to choose a time schedule to associate with this partition. The time schedule specifies when the partition is available to receive incoming calls. If you choose <None>, the partition remains active at all times.
- **d.** Click **Save**.

Location-Based CAC Bandwidth Requirements

An enterprise network uses bandwidth for many different purposes, and all IP-based communication usually crosses the same network edge. You could have voice and video traffic crossing the WAN, while large files are being transferred to an FTP server at a remote location, while other devices are accessing email or other services in the cloud. The result is that each device is competing for bandwidth across the company's network. Individual sites of a multisite deployment are usually interconnected by an IP WAN. Bandwidth on WAN links is limited and relatively expensive. Therefore, the goal is to use the available bandwidth as efficiently as possible. You should discourage unnecessary traffic, such as social media sites and personal use, and consider implementing methods for bandwidth optimization. Figure 18-8 illustrates the dichotomy of an unmanaged enterprise network across a WAN.

Implementing QoS policies will certainly help during high congestion times across the network, but QoS will not prevent overutilization of bandwidth. Imagine a scenario where a corporate WAN can handle up to 1 Mbps total bandwidth. If two endpoints place an audio-only call using the G.711 codec for audio, they will consume 87.2 kbps: 64 kb are for the payload, and 23.2 kb are for headers. That means that this WAN link can support up to roughly 11 audio-only calls, assuming there is no other network traffic consuming bandwidth at the time of the calls. Now imagine what happens when the eleventh call attempt is placed. The call isn't dropped. Rather, this call leg will begin barrowing bandwidth from the other existing calls, and everyone will suffer quality loss during their calls, even if proper

QoS has been implemented. This is where Call Admission Control (CAC) comes into the picture.

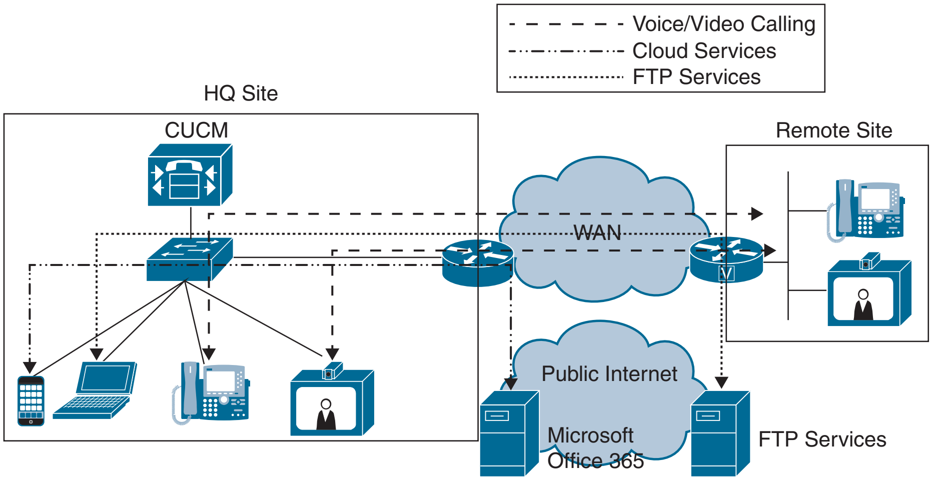


Figure 18-8 *Network Issues Across a WAN*

Cisco has several Call Admission Control mechanisms that can be implemented to control how bandwidth is used across your network. Using CAC in the Cisco Unified Communications Manager allows administrators to control the codec used on a per-call basis depending on the sites between which calls are placed, as well as the overall bandwidth used when calls are placed across the WAN.

Regions are the first settings on the Cisco Unified Communications Manager that an administrator should configure for Call Admission Control. Regions, which were discussed in previous chapters, control the codecs used between endpoints when calls are set up. There is a specific bandwidth allocation associated with each audio codec, so you can easily plan and predict how much bandwidth is going to be consumed. G.711 is an uncompressed codec and consumes 87.2 kbps per call with average audio quality. G.729 is a compressed audio codec that consumes only 31.2 kbps but suffers from poorer quality. Other codecs can be compressed or uncompressed and will have varying levels of quality accordingly.

Compression involves utilizing encoding algorithms to reduce the size of digital data. Compressed data must also be decompressed before it can be used. This extra processing imposes computational or other costs into the transmission hardware. *Lossless* and *lossy* are descriptive terms used to describe whether or not the data in question can be recovered exactly bit-for-bit when the file is uncompressed or whether the data will be reduced by permanently altering or eliminating certain bits, especially redundant bits. Lossless compression searches content for statistically redundant information that can be represented in a compressed state without losing any original information. By contrast, lossy compression searches for nonessential content that can be deleted to conserve storage space.

By contrast to audio, video is very greedy and bursty when it comes to bandwidth consumption. Video codecs do not have a specific set bandwidth rate to them like audio codecs. You can place a video call using 480p30 resolution at 384 kbps or at 2 Mbps. However, using a higher codec can provided better efficiency and thus consume less bandwidth. Therefore, when you are configuring regions in the CUCM, you do not select a codec specifically;

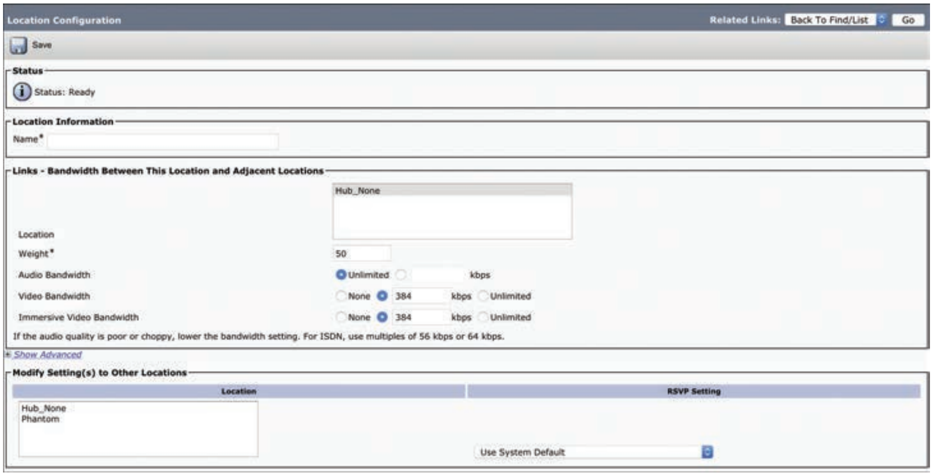
rather, you set the per-call bandwidth rate that is allowed between each site. There are two fields to configure video bit rates in the Regions settings page. The Video Calls column has to do with UC endpoints that can place video calls, such as 8845 and 8865 IP video phones and the Cisco Jabber client. The Immersive Video Calls column has to do with any Cisco Telepresence video endpoint, such as the DX80, MX700, SX80, or Webex endpoints.

Whereas regions deal more with a per-call bandwidth, locations control total bandwidth consumption. The following three locations are predefined in the Cisco Unified Communications Manager:

- **Hub_None:** This is a sample location that typically serves as a hub linking two or more locations. It is configured by default with the Unlimited intra-location bandwidth allocations for audio, video, and immersive bandwidth, but you can specify bandwidth allocations for each of these. By default, devices not assigned to other locations are assigned to Hub_None automatically.
- **Phantom:** This location specifies unlimited bandwidth for audio, video, and immersive calls. Specify this location to allow successful Call Admission Control for calls across inter-cluster trunks that use the H.323 or SIP trunks to certain destinations that support the earlier location CAC feature.
- **Shadow:** This is a system location created for inter-cluster enhanced location CAC. To pass locations across clusters, the SIP inter-cluster trunk (ICT) must be assigned to the Shadow system location.

An administrator can create custom locations as well. When setting up locations, remember that the bandwidth rate is total bandwidth, not per call. Also, overhead is not calculated automatically, so you will have to include overhead when setting the bandwidth limitations. For video calls, add 20 percent to each call rate and then multiply by the number of calls allowed. If the call rate is 384 kb, add 20 percent to give a total of 460 kbps. If you wanted to support 10 calls, then 460 × 10 = 4600 kbps.

Use the following steps to configure location-based CAC on the Cisco Unified Communications Manager. Figure 18-9 illustrates the Location Configuration window.


Location Configuration
Related Links: Back To Find/List
Go
Save
Status
Location Information
Links - Bandwidth Between This Location and Adjacent Locations
Show Advanced
Modify Setting(s) to Other Locations

Status: Ready

Name*

Location: Hub_None

Weight* 50

Audio Bandwidth ● Unlimited ○ kbps

Video Bandwidth ○ None ● 384 kbps ○ Unlimited

Immersive Video Bandwidth ○ None ● 384 kbps ○ Unlimited

If the audio quality is poor or choppy, lower the bandwidth setting. For ISDN, use multiples of 56 kbps or 64 kbps.

Location	RSVP Setting
Hub_None Phantom	Use System Default

Figure 18-9 *Location Configuration Window on CUCM*

Step 1. Configure locations on the Cisco Unified Communications Manager.

a. From Cisco Unified Communications Manager Administration, navigate to **System > Location Info > Location**.

b. Click **Add New** and enter the following information in the Location Configuration window.

- **Name:** Enter a name for the location.
- **Location:** Select a location from the list.
- **Weight:** Enter the relative priority of this link in forming the effective path between any pair of locations. The effective path has the least cumulative weight of all possible paths. Valid values are 0–100.
- **Audio Bandwidth:** Enter the maximum amount of audio bandwidth in kbps that is available for all audio calls on the link between this location and other locations. For audio calls, the audio bandwidth includes overhead.
- **Video Bandwidth:** Enter the maximum amount of video bandwidth in kbps that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead.
- **Immersive Video:** Enter the maximum amount of immersive video bandwidth in kbps that is available for all immersive video calls on the link within this location. For video calls, the immersive video bandwidth does not include overhead.

c. Click **Save** when finished.

Locations can be assigned to phones directly, or they can be added to device pools, which is the recommended method. Each phone is automatically assigned the Hub_None location. However, location settings in the device pool override location settings on the phone.

Step 2. Assign locations to device pools.

a. Navigate to **System > Device Pool**.

b. Choose one of the following options:

- Click **Add New** to add a new device pool.
- Click **Find** and choose a device pool from the resulting list to modify the settings for an existing device pool.

c. On the Device Pool Configuration page, under the Roaming Sensitive Settings section, locate the Locations menu option and use the drop-down list to select the appropriate location.

d. Click **Save**. If an existing device pool has been modified, click the **Apply Config** button so that the changes will be pushed to any phones already configured with this device pool.

Call Coverage

Call coverage is part of the dial plan and ensures that all incoming calls are answered. The following call coverage features are typically implemented for individuals:

Key Topic

- **Call Forward:** If the called phone does not answer the call, the call should be forwarded to another phone or voicemail. Call forward options include Call Forward Busy (CFB) internal and external, Call Forward No Answer (CFNA) internal and external, Call Forward No Coverage (CFNC) internal and external, plus several others.
- **Shared Lines:** A shared line is a directory number that is assigned to more than one device within the same partition, allowing the call to be accepted on more than one phone.
- **Call Pickup:** Call pickup allows a call that is ringing on a phone to be picked up at another phone.

Call hunting is another complex and flexible feature that provides call coverage. Call hunting is based on a pilot number that, if called directly or used as a call forward target, allows hunting through multiple line groups. Several hunting algorithms exist, ranging from a round-robin selection of group members to a broadcast option that rings all members of a line group.

Call queuing allows hunt pilot callers to be held in a queue while they wait for an agent to become available. It enables customers to provide a professional call coverage solution without the need to deploy a Cisco Unified Contact Center product if the rich features of a contact center solution are not required.

Hunting

The Cisco Unified Communications Manager call hunting implementation is composed of four main components. They are hunt pilots, hunt lists, line groups, and line group members. A user can dial a hunt pilot number, which will direct the call to a hunt list, that in turn selects a line group, which contains a prioritized list of line group members. Though this is the order of operation for hunting in the Cisco Unified Communications Manager, the order of configuration for each of these components must be in the reverse order. Figure 18-10 illustrates the order of operation for hunting on the Cisco Unified Communications Manager.

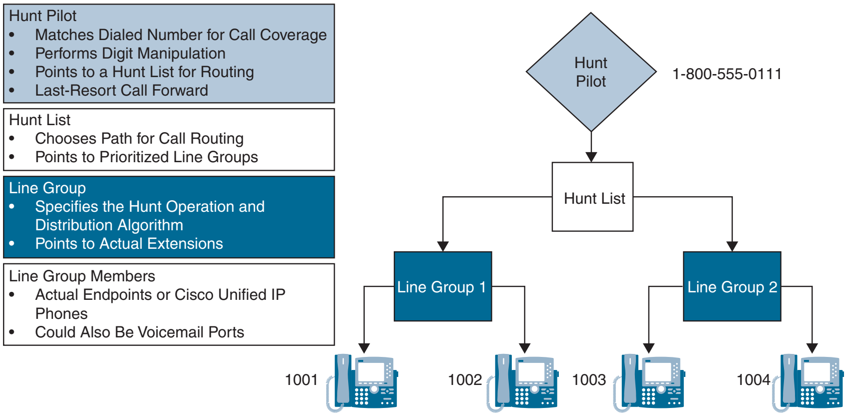

Hunt Pilot
• Matches Dialed Number for Call Coverage
• Performs Digit Manipulation
• Points to a Hunt List for Routing
• Last-Resort Call Forward
Hunt List
• Chooses Path for Call Routing
• Points to Prioritized Line Groups
Line Group
• Specifies the Hunt Operation and Distribution Algorithm
• Points to Actual Extensions
Line Group Members
• Actual Endpoints or Cisco Unified IP Phones
• Could Also Be Voicemail Ports
Hunt Pilot
1-800-555-0111
Hunt List
Line Group 1
Line Group 2
1001
1002
1003
1004

Figure 18-10 *CUCM Hunting Order of Operation*

Line Group Members

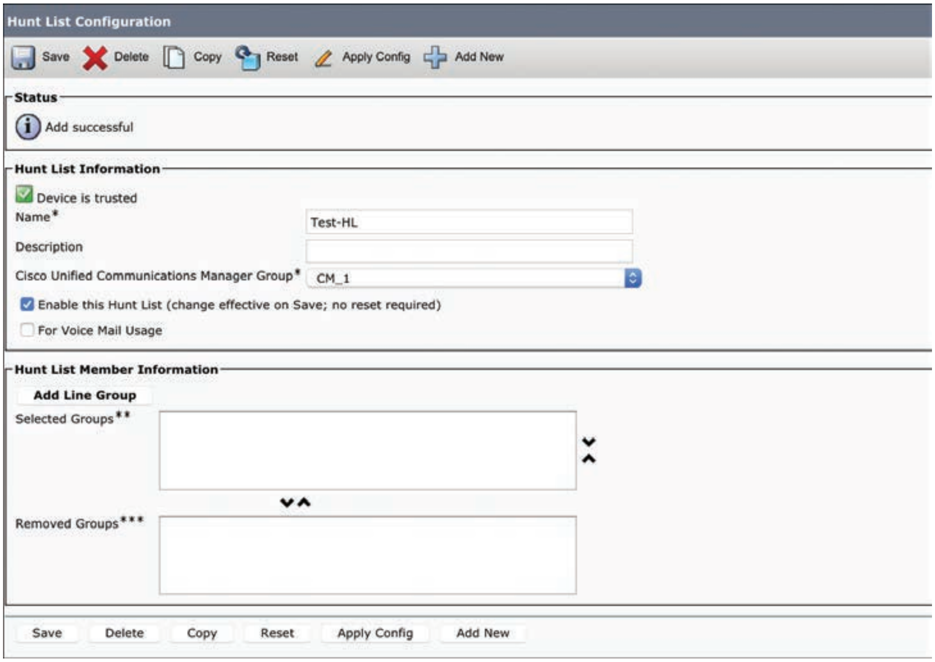
A line group member could be the directory numbers or voicemail ports assigned to line groups. Line group members are the Cisco Unified IP phones or Cisco Telepresence endpoints that a line group can access. These endpoints can be numbers or voicemail ports. CTI ports and CTI route points cannot be added to a line group. Therefore, calls cannot be distributed to endpoints that are controlled through CTI applications. Obviously, endpoints must be configured in, and preferably registered to, the Cisco Unified Communications Manager before they can be added to a line group.

Hunt Lists

A hunt list is an ordered list of line groups that are used for call coverage. Hunt lists have the following characteristics:

- Multiple hunt pilots can point to the same hunt list.
- Multiple hunt lists can contain the same line group.
- A hunt list is a prioritized list of line groups; line groups are hunted in the order of their configuration in the hunt list.
- A hunt list does not perform digit manipulation.

Hunt lists are assigned to hunt pilots. Figure 18-11 illustrates the configuration menus for hunt lists on the Cisco Unified Communications Manager.



Status

Add successful

Hunt List Information

☑ Device is trusted

Name* Test-HL

Description

Cisco Unified Communications Manager Group* CM_1

☑ Enable this Hunt List (change effective on Save; no reset required)

☐ For Voice Mail Usage

Hunt List Member Information

Add Line Group

Selected Groups**

Removed Groups***

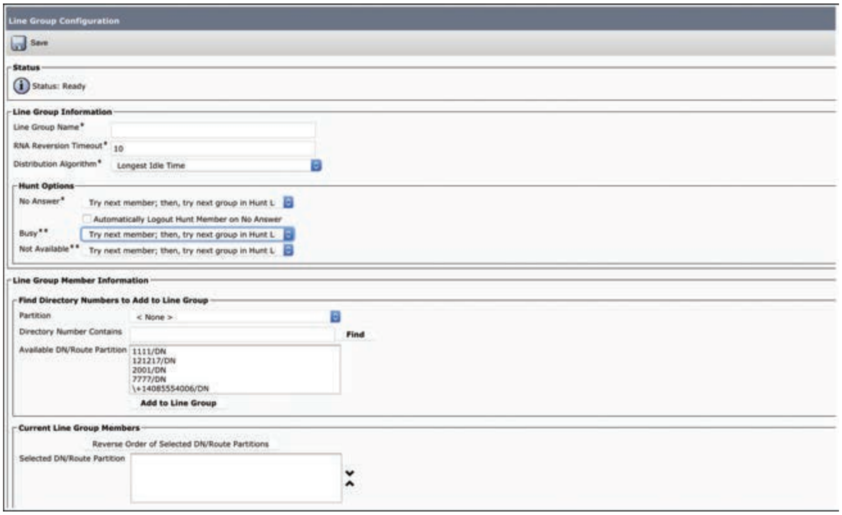
Figure 18-11 *Configuration Options for Hunt Lists on the CUCM*

Line Groups

Line groups are assigned to hunt lists and are composed of a list of line group members. A hunt list can have one or more line groups. At the line group, hunt options and distribution algorithms can be specified to define how call hunting should be performed for the members of a line group. Line groups control the order in which a call is distributed, and they have these characteristics:

- The RNA Reversion Timeout specifies how long the hunting algorithm rings a member of the line group before proceeding to hunt according to the Line Group No Answer hunt option setting.
- Line groups are configured with hunt options, which describe how hunting should be continued after trying the first member of the line group. The hunt options are configured based on per-hunt failure events, such as No Answer, Busy, or Not Available.
- Line groups are configured with a global distribution algorithm, which is used to select the next line group member for hunting. The algorithm options include the following:
- Try Next Member; Then Try Next Group in Hunt List
    - Try Next Member, but Do Not Go to Next Group
    - Skip Remaining Members, and Go Directly to Next Group
    - Stop Hunting
- Line groups point to specific extensions, which are typically IP phone extensions or voicemail ports.
- The same extension may be present in multiple line groups.

Figure 18-12 shows the configuration options for line groups.



Status

Status: Ready

Line Group Information

Line Group Name*

RNA Reversion Timeout* 10

Distribution Algorithm* Longest Idle Time

Hunt Options

No Answer* Try next member; then, try next group in Hunt L

□ Automatically Logout Hunt Member on No Answer

Busy** Try next member; then, try next group in Hunt L

Not Available** Try next member; then, try next group in Hunt L

Line Group Member Information

Find Directory Numbers to Add to Line Group

Partition < None >

Directory Number Contains

Available DN/Route Partition
1111/DN
121217/DN
2001/DN
7777/DN
+14085554006/DN

Current Line Group Members

Selected DN/Route Partition

Figure 18-12 *Configuration Options for Line Groups on the CUCM*

Hunt Pilots

Hunt pilots are dialable patterns, such as route patterns and directory numbers, in the call-routing table. The hunt pilot points directly to a hunt list. Hunt lists point to line groups, which point to endpoints. A hunt pilot can be called directly, such as to provide a certain service to customers. Alternatively, an IP phone can be configured to forward unanswered or busy call attempts that it receives to the hunt pilot to provide call coverage.

If the directory number of the phone is dialed directly and the call is busy or not answered, the forwarding configuration of the line (CFB or CFNA setting) can forward the call to a hunt pilot. However, while hunting, the forwarding configuration of line group members is ignored. If the hunting algorithm rings a phone and the call is not answered, the CFNA setting of that phone is ignored. The hunting algorithm goes on to the next line group member.

At the hunt list, digit manipulation can be configured to transform the calling and called number before the call is passed on to line group members. Calls can also be redirected to a final destination when the hunting fails because of one or both of these reasons:

- All hunting options have been exhausted and the call still is not answered.
- A maximum hunt timer that is configured at the hunt list has expired.

This call redirection is configured in the Hunt Call Treatment Settings section of the Hunt Pilot Configuration page, and the destination for this redirect can be either of these options:

Key Topic

- **Forward Unanswered Calls to Destination or Forward Busy Calls to Destination:** A specific destination that is configured globally at the hunt pilot.
- **User Forward Settings of Line Group Member:** A personal preference that is configured at the phone line of the originally called number, when hunting on behalf of that number fails. The personal preference is configured by using the Call Forward No Coverage (CFNC) settings at the phone line.

You can implement the personal preferences option. To do so, configure a user phone so that the Forward No Answer field redirects the call to a hunt pilot, which searches for someone else to answer the call. If call hunting fails because all the hunting options are exhausted or because a timeout period expires, the call can be sent to a personalized destination for the person who was originally called. For example, if you set the Forward No Coverage field in the Directory Number Configuration page to a voicemail number, the call will be sent to the voice mailbox of that person if hunting fails.

These considerations apply to calls that are processed by hunt pilots:

- Call Pickup and Group Call Pickup are not supported on calls that a hunt pilot distributes. A member of the line group cannot pick up a hunt pilot call that is offered to another member in the line group, even if both members belong to the same Call Pickup group.
- The hunt pilot can distribute calls to any of its line group members, regardless of the calling privileges implementation of the line group members. If line group members are configured with a partition, the hunt pilot overcomes all partitions and CSS restrictions.

Call Hunting Operation and Call Flow

Now that you have a basic understanding of the components involved with call hunting, a description of the call hunting operation is in order. The call hunting flow in the Cisco Unified Communications Manager call hunting configuration is as follows:

1. Either a direct call is placed to the hunt pilot number, or a call is forwarded from a phone to the hunt pilot number.
2. The hunt pilot that is configured with the appropriate hunt pilot number starts the maximum hunt timer to monitor the overall hunting time. If the timer expires, hunting stops. The hunt pilot is associated with a hunt list.
3. The hunt list that is associated with the hunt pilot sends the call to the first line group that is configured in the hunt list.
4. The line group sends the call to the first line group member, based on the distribution algorithm that is configured for the line group. The possible distribution methods are as follows:
   - Top down
     - Circular
     - Longest idle time
     - Broadcast
5. If the line group member (or members, in case of broadcast) that the distribution algorithm selects does not answer the call, the hunt option specifies how hunting should continue. The hunt option is configured independently, per hunt failure reason, for the line group. Possible hunt failure reasons are No Answer, Busy, and Not Available. In hunt failures that result in No Answer, assumedly the RNAR timer that is configured for the line group has expired.
   - If the hunt option that is configured for the appropriate hunt failure reason is Stop Hunting, hunting stops.
   - If the hunt option that is configured for the appropriate hunt failure reason is Skip Remaining Members and Go Directly to Next Group, and there are no more line groups, hunting stops. If there are additional line groups, the process continues with the next line group (step 4).
   - If the hunt option that is configured for the appropriate hunt failure reason is Try Next Member Then Try Next Group in Hunt List, and there are additional line group members, the process continues with the next line group member (step 4). If there are no additional line group members, the next line group is used. If there are additional line groups, the process continues with the next line group (step 4). If there are no more line groups, hunting stops.

   When hunting stops, the following are possible reasons:

   - Stop Hunting is the hunt option that was applied after a call was not accepted by the last attempted line group member.
   - After hunting tried the last line group member, there were no other line group members or other line groups to be used. This reason is known as *hunt exhaustion*.

- The maximum hunt timer that is configured for the hunt pilot expired.

Once the process has exhausted all hunting options, the hunt pilot continues with the following actions.

6. Review the hunt pilot configuration for its final forwarding settings. If the hunt pilot is not configured for final forwarding, the call fails and a reorder tone is played.
7. Review the final forwarding destination settings that are configured for the hunt pilot:
   - If a Final Forwarding number is specified for the hunt pilot, route the call to the specified number.
   - If Use Personal Preference is selected, route the call to the number that is configured for CFNC on the phone line that invoked the call to the pilot number.

Figure 18-13 illustrates the call hunting flow on the Cisco Unified Communications Manager.

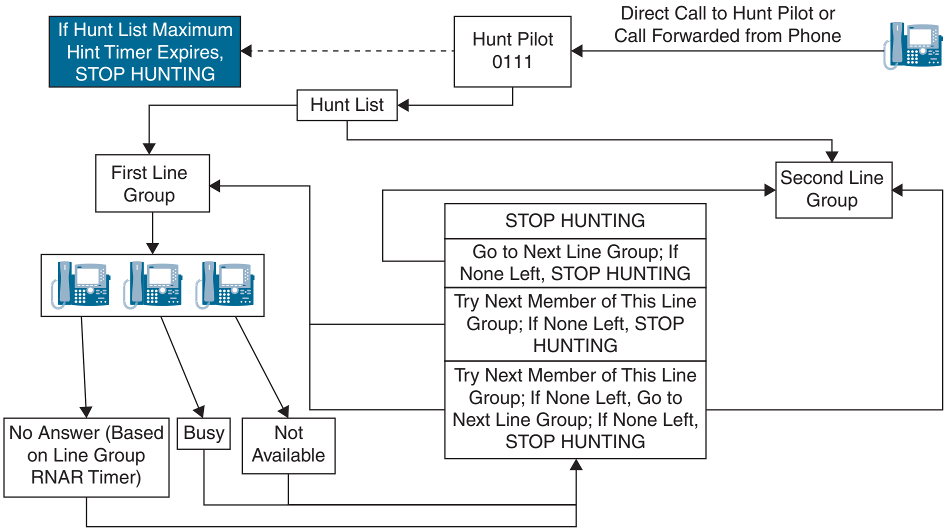

If Hunt List Maximum Hint Timer Expires, STOP HUNTING
Hunt Pilot 0111
Direct Call to Hunt Pilot or Call Forwarded from Phone
Hunt List
First Line Group
Second Line Group
STOP HUNTING
Go to Next Line Group; If None Left, STOP HUNTING
Try Next Member of This Line Group; If None Left, STOP HUNTING
Try Next Member of This Line Group; If None Left, Go to Next Line Group; If None Left, STOP HUNTING
No Answer (Based on Line Group RNAR Timer)
Busy
Not Available

Figure 18-13 *Call Hunting Flow*

Call Queuing Settings

Call queuing allows hunt pilot callers to be held in a queue while they wait for an agent to become available. Call queuing is based on the existing call distribution capabilities that are provided by hunt lists and hunt pilots. It enables calls to a hunt pilot to be redirected to a queue if all agents that are associated with the hunt pilot are busy, logged out, unregistered, or do not answer. In call queuing, a line group member may be referred to as an agent. However, call queuing does not support an agent desktop application, routing based on agent skills, or similar contact center features. Agents can be part of multiple hunt pilots in which queuing is enabled. When an agent does not answer an offered call, the agent is automatically logged out of the hunt group. This action also applies to shared line appearances. The auto-logout occurs after expiration of the RNAR timer. An agent becomes idle after logging in to a hunt group or after finishing a call. When an agent becomes idle, the following process occurs:

- The Cisco Unified Communications Manager checks all queues to which the agent is currently subscribed for waiting callers.
- Out of these queued callers, the caller that has been waiting the longest is routed to the agent.

Call queuing supports announcements while calls are queued. The Cisco Unified Communications Manager has preinstalled announcements in U.S. English, but custom announcements can be uploaded. Uploading custom announcements is similar to uploading custom Music On Hold (MOH) audio files. Announcements are configured at the MOH Audio Source configuration page. The announcement to be played is chosen by referring to an MOH audio source at the Hunt Pilot Configuration page. Two different announcement types are available through the Cisco Unified Communications Manager:

Key Topic

- **Initial announcement:** This announcement is played once at the beginning of the call. It can be configured to be played before or after the call is queued.
- **Periodic announcement:** This announcement is played at a configurable interval while the call is held in the queue.

You can configure an agent phone with the Queue Status IP phone feature button. If pressed, this feature button provides information about the hunt pilot number, the number of queued calls, and the longest waiting time. For call queuing to work over SIP trunks, PRACK must be enabled on the SIP trunk.

The actual hunting process can stop because of hunt exhaustion, expiration of the hunt list maximum hunt timer, or because of running into a configured stop-hunting condition. Queuing can be enabled as another option for call management after the Cisco Unified Communications Manager stops hunting. The other two previously existing options—attempt final forwarding to a configured number or disconnect the call—are still configurable, but they are mutually exclusive. In other words, only one option can be chosen per hunt pilot. Figure 18-14 illustrates the call queuing process on the Cisco Unified Communications Manager.

When a caller is to be placed into a queue, the Cisco Unified Communications Manager first checks whether any hunt members are logged in or registered. If no hunt members are logged in or registered, the caller is not put into the queue of the called hunt pilot. Then the Cisco Unified Communications Manager checks whether the queue of the hunt pilot is already full. The Maximum Number of Callers Allowed in Queue hunt pilot configuration setting is used to decide whether the new caller can be added to the queue. If both checks are passed successfully, the caller is added to the queue. A timer is started to monitor the time that this caller spends in the queue. If the queued call cannot be delivered to an agent before expiration of the configured Maximum Wait Time in Queue, the call is removed from the queue at expiration of the timer.

If a call is not queued at all or is removed from the queue, a final call management option must be configured. A call is not queued if there are no logged-in or registered agents or if the maximum number of queued calls is reached. A call is removed from the queue at the expiration of the maximum wait timer. The default is to disconnect the call. This setting can be changed independently according to the individual scenario by specifying a secondary destination to which the call should be routed. This secondary destination is similar to the final forwarding configuration at the hunt pilot when call queuing is not enabled.

A secondary destination can be a directory number, a voicemail number, a shared line, or another hunt pilot that may or may not have queuing enabled. Be aware that sending the call to another queuing-enabled hunt pilot can result in long queuing times. This situation is especially important when cascading multiple hunt pilots.

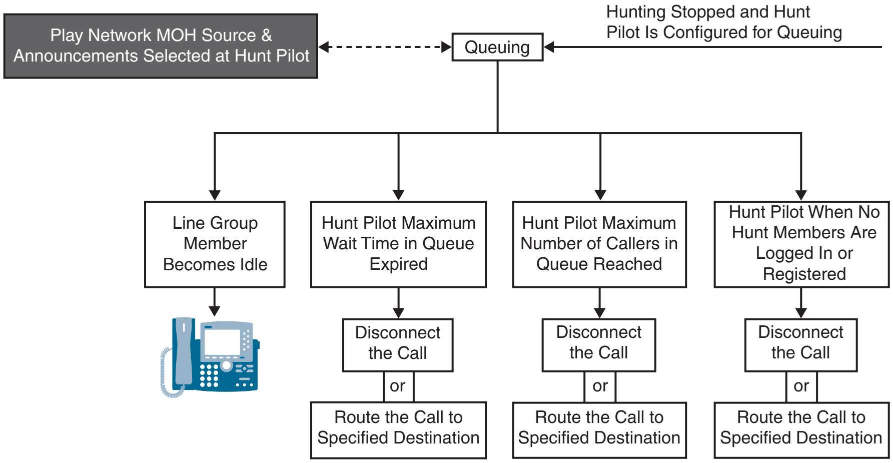
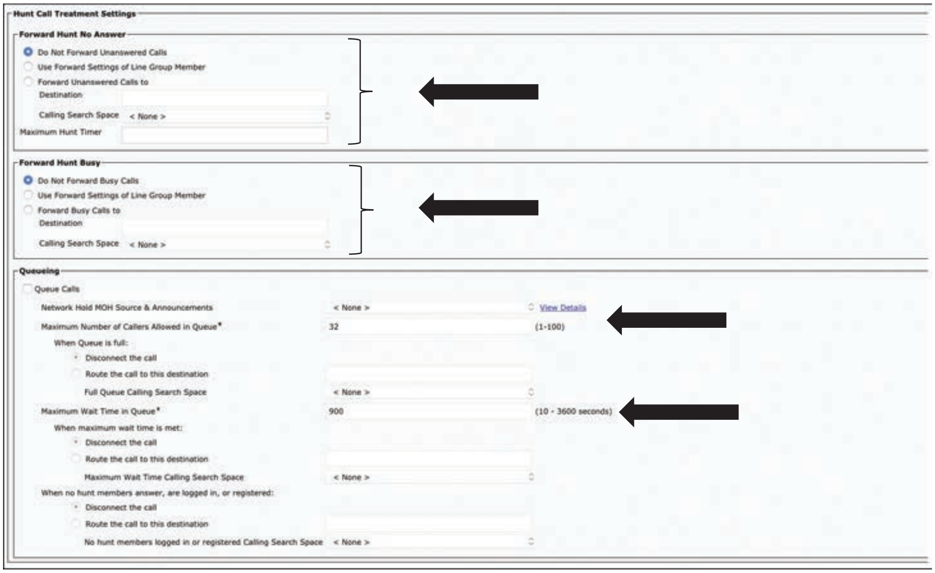

Hunting Stopped and Hunt Pilot Is Configured for Queuing
Play Network MOH Source & Announcements Selected at Hunt Pilot
Queuing
Line Group Member Becomes Idle
Hunt Pilot Maximum Wait Time in Queue Expired
Hunt Pilot Maximum Number of Callers in Queue Reached
Hunt Pilot When No Hunt Members Are Logged In or Registered
Disconnect the Call
or
Route the Call to Specified Destination
Disconnect the Call
or
Route the Call to Specified Destination
Disconnect the Call
or
Route the Call to Specified Destination

Figure 18-14 *Call Queuing Process*

The Maximum Number of Callers Allowed in Queue parameter is configurable from 1 to 100, and the default is 32. The Maximum Wait Time in Queue parameter is configurable from 0 to 3600 seconds, and the default for this setting is 900. Each value is configurable per hunt pilot. Call queuing supports the playing of announcements once at the beginning of a call and periodically while a call is held in a queue. Figure 18-15 illustrates the configuration procedures for hunt call treatment and queuing settings.



Hunt Call Treatment Settings

Forward Hunt No Answer

● Do Not Forward Unanswered Calls
○ Use Forward Settings of Line Group Member
○ Forward Unanswered Calls to
Destination
Calling Search Space < None >
Maximum Hunt Timer

Forward Hunt Busy

● Do Not Forward Busy Calls
○ Use Forward Settings of Line Group Member
○ Forward Busy Calls to
Destination
Calling Search Space < None >

Queueing

□ Queue Calls
Network Hold MOH Source & Announcements < None > View Details
Maximum Number of Callers Allowed in Queue* 32 (1-100)
When Queue is full:
● Disconnect the call
○ Route the call to this destination
Full Queue Calling Search Space < None >
Maximum Wait Time in Queue* 900 (10 - 3600 seconds)
When maximum wait time is met:
● Disconnect the call
○ Route the call to this destination
Maximum Wait Time Calling Search Space < None >
When no hunt members answer, are logged in, or registered:
● Disconnect the call
○ Route the call to this destination
No hunt members logged in or registered Calling Search Space < None >

Figure 18-15 *Hunt Call Treatment and Queuing Configuration Settings*

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 35, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 18-5 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 18-5 Key Topics for Chapter 18

Key Topic Element	Description	Page Number
Paragraph	NANP E.164 Address Patterns	428
List	Components of a Dial Plan	428
Table 18-2	Comparison of Dial Plan Configuration Elements	431
List	Two Ways to Address Internal Endpoints for PSTN Mapping	431
Table 18-3	Directory URI Characters Supported	433
Paragraph	Configuring Directory URIs in the CUCM	434
Table 18-4	PSTN Calling Privilege Class Map	436
Paragraph	None Partition and CSS	436
List	Call-Routing Order with COS	439
Steps	Steps to Configuring ToD Settings	441
List	Call Coverage Features for Individuals	446
List	Characteristics of Line Groups on CUCM	448
List	Designation for the Redirect of Hunt Call Treatment Settings	449
List	Hunt Distribution Methods	450
List	Announcement Types for Call Queuing	452

Define Key Terms

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

CAC, Call Queuing, COS, CSS, Dial Plan, DID, Directory URI, DN, +E.164 Alias, E.164 Alias, Hub_None, Hunt Exhaustion, Hunting, NANP, Off-net, On-net, Partition, Phantom, RNAR, Shadow, ToD, Two-Stage Dialing

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the five components of a well-designed dial plan.
2. List all the mechanisms in the CUCM to which partitions and CSS can be applied.
3. List the four different hunt distribution algorithms that can be configured on a line group.

This page intentionally left blank

CHAPTER 19

Configuring Globalized Call Routing in Cisco Unified Communications Manager

This chapter covers the following topics:

Call Routing and Path Selection: This topic will examine Cisco Unified Communications Manager call-routing tools, such as route patterns, SIP route patterns, route groups, and route lists.

Digit Manipulation: This topic will explain how translation patterns, route patterns, and transformation patterns are used in the Cisco Unified Communications Manager to manipulate the dial plan when necessary.

Continuing the same thread of call routing discussed in the preceding chapter, this chapter discusses two other very important aspects to call routing. The idea of a globalized call-routing plan is to implement tools that will allow calls to be routed between Cisco Unified Communications Manager clusters within an enterprise network, route calls outside an enterprise network over IP, and route calls from an IP network out across the PSTN. Routing calls in so many different environments will inevitably require aliases to be manipulated from their original form. This concept of digit manipulation is also part of a globalized call-routing plan. Topics discussed in this chapter include the following:

- Call Routing and Path Selection
- Route Groups and Local Route Groups
  - Route Lists
  - Route Patterns and SIP Route Patterns
- Digit Manipulation
- Translation Patterns
  - Transformation Patterns

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 4.3 Configure globalized call routing in Cisco UCM
- 4.3.a Route patterns (traditional and +E.164 format)
  - 4.3.b Translation patterns

- 4.3.c Standard local route group
- 4.3.d Transforms
- 4.3.e SIP route patterns

“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 19-1 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 19-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Call Routing and Path Selection	1–4
Digit Manipulation	5–7

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. Which of the following call-routing components of the CUCM is considered a source component?

a. Call park number

b. Route pattern

c. Directory number

d. Translation pattern

2. Which of the following are the main three components of route planning on the CUCM?

a. Route patterns, route lists, and route groups

b. Route patterns, route filters, and route groups

c. Route patterns, route lists, and local route groups

d. Route patterns, route filters, and local route groups

3. Which of the following components can be included in a route list?

a. Route pattern

b. SIP route pattern

c. Local route group

d. Route filter

4. Which of the following wildcards can be used in a route pattern to match all National Numbering Plan numbers?

- **a.** !
- **b.** @
- **c.** +
- **d.** \+

5. Which of the following are uses for transformation patterns?

- **a.** Discard digits.
- **b.** Prefix digits.
- **c.** Add a calling party transformation mask.
- **d.** Control the presentation of the calling party number.
- **e.** All of these answers are correct.

6. Which of the following statements about translation patterns on the CUCM is true?

- **a.** Partition, route filter, and numbering plan must all be unique,
- **b.** Partition and route filter must be unique.
- **c.** Partition and numbering plan must be unique.
- **d.** Route filter and numbering plan must be unique.

7. How many different types of transformation patterns can be created in the CUCM?

- **a.** 1
- **b.** 2
- **c.** 4
- **d.** 8

Foundation Topics

Call Routing and Path Selection

Chapter 18, "Cisco Unified Communications Manager Call Admission Control (CAC)," introduced the concept of call routing within the Cisco Unified Communications Manager. Routing calls involves several aspects, some of which were covered in that chapter. Chapter 18 covered how to allow or block calls based on the Class of Service of the calling entity, and began identifying dialing habits based on the structure of the dial string. This chapter will expand on these concepts as calls reach beyond the local call control system. Call routing is about selecting a route to the called destination, establishing the call, and presenting the identity of the parties involved in the expected format. Route selection also involves selecting alternate routes if the primary route is not available for some reason. It also involves applying modifications to the dial string and applying modifications to the calling party identification. An end-to-end enterprise dial plan needs to consider all of these aspects and is not limited only to establishing a route between the calling and called entities. Calls must be routed and interconnected according to the dialed number. There are three main types of call routing:

- **Intrasite routing:** This type of call routing occurs within a single site.
- **Intersite routing:** This type of call routing occurs between multiple sites.

- A translation pattern is used for both centralized and distributed call-processing deployment models.
  - A route pattern is used only for a distributed call-processing deployment.
- **PSTN routing:** This type of call routing occurs between a site and the PSTN.

The Cisco Unified Communications Manager can automatically route calls to internal destinations within the same cluster because Cisco Unified Communications Manager is configured with the directory numbers of its associated devices. For external destinations, an explicit route—called a *route pattern*—must be configured. External destinations are PSTN destinations or other VoIP domains such as an ITSP or another Cisco Unified Communications Manager cluster. PSTN destinations can include off-net intersite calls, which are effectively PSTN destinations because they are addressed by their PSTN numbers. The Cisco Unified Communications Manager call-routing table is built using connected devices. The table consists of directory numbers of registered IP phones and of statically entered route patterns that point to external destinations. Regardless of the call-routing type, the call-routing process itself can be summarized as follows:

Key Topic

1. Cisco Unified Communications Manager receives a call setup request from a local endpoint or from another call control system such as a remote Cisco Unified Communications Manager cluster or a PSTN gateway.
2. Cisco Unified Communications Manager analyzes the target of the received request to find the best matching entry in its call-routing table. The type of analysis depends on the addressing method that is used by the source of the call setup request (digit-by-digit or en bloc) and the address type (number versus URI).
3. Cisco Unified Communications Manager forwards the call setup request to the destination device that is associated with the matched call-routing table entry. This destination device can be a local endpoint or another remote call control system.

Many different settings within the Cisco Unified Communications Manager require an administrator to understand the difference between call-routing sources and call-routing targets. Five different sources of call-routing requests require a call-routing table lookup. The simplest are the IP phone, gateways, and trunks. The following sources of call-routing requests also require a call-routing table lookup:

- **Translation patterns:** A translation pattern is like a route pattern. A translation pattern includes a pattern that when matched provides an entry to the call-routing table. If the dialed number matches the pattern, another number, which is the translated number that is configured at the translation pattern, is looked up in the call-routing table. A translation pattern, therefore, combines both roles in one entity. The translation pattern is both a call-routing table target when it is matched by a dialed number and the basis of a second lookup for the translated number.
- **Voicemail ports:** When a call is sent to a voicemail system, that system can request that the call be transferred to another directory number, to a PSTN destination, such as the cell phone of a user, or to an assistant. In all these scenarios, the voicemail port is the entity that requests the call that the Cisco Unified Communications Manager is routing.

By contrast, several other components within the Cisco Unified Communications Manager are call-routing targets, such as directory numbers, route patterns, translation patterns, and more. Table 19-2 identifies components that are call-routing sources and targets. If a dialed number matches one of these entries, the call is routed to the appropriate entity. That entity can be a phone line, a trunk, a gateway, a feature, or an application. For URI-based call routing, only directory URIs and SIP route patterns are applicable. All other components refer to call routing for numbered targets. However, calls placed to directory URIs can be routed only to a local phone, if the directory URI is associated with a directory number.

Key Topic

Table 19-2 Call-Routing Source and Target Components

Routing Component	Description	Call-Routing Source, Target, or Both
IP Phones	A number dialed by an IP phone is looked up in the call-routing table.	Source
Trunks	A call request received through a trunk is looked up in the call-routing table.	Source
Gateways	A call request received from a gateway is looked up in the call-routing table.	Source
Translation Patterns	After a translation pattern is best matched (as a target of a call-routing table lookup), the transformed number is looked up again in the call-routing table. The entry that generates this lookup is the translation pattern.	Both
Voicemail Ports	A voicemail system can be configured to allow calling of other extensions or PSTN numbers (such as the mobile phone of an employee). In these cases, the call-routing request is received from the voicemail port of the CUCM.	Both
Directory Numbers	Assigned to endpoints.	Target
Directory URIs	Assigned to directory numbers.	Target
Route Patterns, SIP Route Patterns	Used to route calls to off-net destinations (via a gateway) or to other CUCM clusters via a trunk.	Target
Call Park Numbers	Allows a call on hold to be sent to a number and retrieved from another phone by dialing that number.	Target

When a number is dialed, the Cisco Unified Communications Manager uses closest-match logic to select which pattern to match from among all the patterns in its call-routing table. In practice, when multiple potentially matching patterns are present, the destination pattern is chosen based on the following criteria:

- The pattern matches the dialed string.
- The pattern represents the smallest number of endpoints.

Some entries of the call-routing table can include wildcards, such as an X in a numbered pattern that represents one digit. If the exclamation point (!) is used in a numbered pattern, it stands for one or more digits. Figure 19-1 illustrates an example in which the call-routing table includes the numbered patterns 12XX, 121X, and 1234.

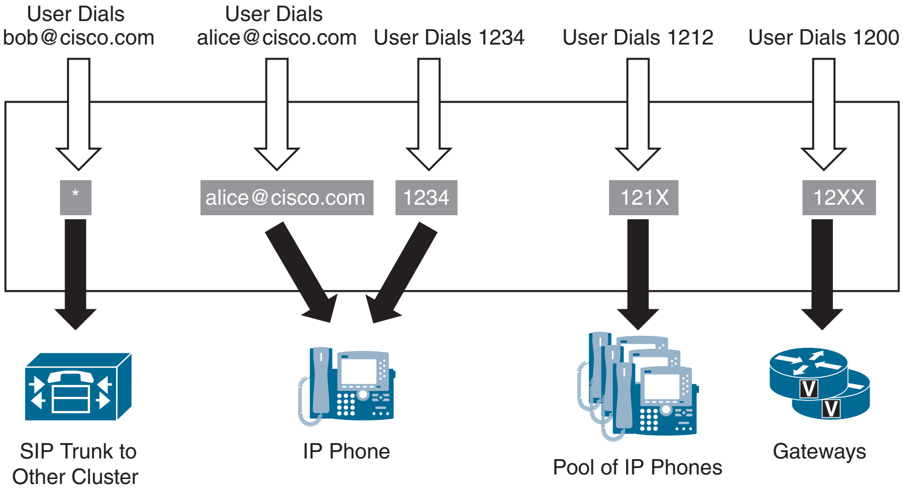


Figure 19-1 *Closest-Match Logic*

When a user dials the string 1234, the Cisco Unified Communications Manager compares the string to the patterns in its call-routing table. In this case, there are two potentially matching patterns: **12XX** and **1234**. Both of these patterns match the dialed string, but **12XX** matches a total of 100 numbers from 1200 to 1299, whereas 1234 does not include any wildcard characters and therefore is one exact number. Therefore, **1234** is selected as the destination of this call because it is the closest match. When a user dials the string 1210, then pattern **121X** is chosen because out of the two potential matches, **121X** and **12XX**, **121X** is the better match as it represents only 10 possible numbers while **12XX** represents 100 possible numbers. The same is also true for URI pattern matching. When a user dials the URI alice@cisco.com, the Cisco Unified Communications Manager chooses the locally configured URI that is an exact match of the dialed URI. However, when a user dials the URI bob@cisco.com, the only match is the SIP route pattern *, which stands for any URI. If there were a SIP route pattern ***.cisco.com**, then a call to bob@cisco.com would find a better match in the ***.cisco.com** SIP route pattern because it is more specific than the * SIP route pattern.

From the phone that is placing the call, there are different dialing methods as to how dialed aliases are sent to the Cisco Unified Communications Manager. In SIP, you can use *en bloc* dialing or *KPML*. In en bloc dialing, the whole dialed string is sent in a single SIP INVITE message. KPML allows digits to be sent one by one. SIP dial rules are also supported, which allow part of the call attempt to be processed inside the SIP phone. Therefore, a SIP phone can detect invalid numbers and play a reorder tone, without sending any signaling messages to the Cisco Unified Communications Manager. If dialed digits match an entry of a SIP dial rule, the dialed string is sent in a single SIP INVITE message to the Cisco Unified Communications Manager en bloc. If the Cisco Unified Communications Manager requires more digits, KPML can be used to send the remaining digits one by one from the SIP phone to the Cisco Unified Communications Manager.

Trunks, gateways, and ISDN PRIs can be configured for *overlap sending and receiving*, in addition to *en bloc*, allowing digits to be sent or received one by one over an ISDN PRI. The difference between trunks and gateways in regard to addressing methods is the protocols each supports. So, the Cisco Unified Communications Manager does not always receive all dialed digits at once. Table 19-3 shows the addressing methods that the Cisco Unified Communications Manager supports for different devices.

Table 19-3 Addressing Methods for Destination Numbers

Device Type	Signaling Protocol(s)	Addressing Method
IP Phones	SCCP	Digit-by-digit analysis
		En bloc (not on type-A phones)
	SIP	En bloc
		KPML (not on type-A phones)
		SIP dial rules
Gateways	MGCP, SIP, H.323	En bloc
		Overlap sending and receiving
Trunks	SIP, H.323	En bloc
		Overlap sending and receiving

Be aware that if a phone sends dialed digits one by one, the Cisco Unified Communications Manager starts digit analysis immediately upon receiving the first digit. In fact, digit analysis starts one step earlier, when a phone indicates an off-hook state to the Cisco Unified Communications Manager. At that point, the Cisco Unified Communications Manager looks up a null string dialed number that matches all available routes in the call-routing table. By analyzing each additional digit that is received, the Cisco Unified Communications Manager can reduce the list of potential matches within the call-routing table. After a single entry is matched, such as the directory number 1234 from Figure 19-1, the call is then sent to the corresponding device. The Cisco Unified Communications Manager does not always receive dialed digits one by one. If digits are received en bloc, the whole received dial string is checked at once against the call-routing table.

An international call prefix or dial-out code is a trunk prefix used to select an international telephone circuit for placing an international call. It is now called an International Direct Dialing (IDD) prefix. A country will typically have a National Direct Dialing (NDD) prefix as well. The ITU recommends the sequence 00 as a standard for an IDD prefix, and this sequence has been implemented by most countries, but not all of them. Calls for any country that follows the North American Numbering Plan (NANP), such as the United States and Canada, use 011 as the IDD. Japan uses 010, Australia uses 0011, and Russia uses a predefined international call operator with 810. International destinations are usually configured by using the exclamation point (!) wildcard, which represents any quantity of digits, also referred to as variable-length patterns. In North America, the route pattern 9.011! is typically configured for international calls. The 9. (note the dot) is significant because the 9 is representative of an IP PBX prefix used to obtain an outside line. Dialing behaviors called "pre dot" that can be configured in the Cisco Unified Communications Manager allow any digits that precede a dot in a dial pattern to be stripped off. Therefore, the 9 is used to obtain an outside line and then removed from the dial string so that it does not interfere with how the call should be routed. The 011 is the IDD number in this same example, and the exclamation point (!) is the wildcard signifying any additional digits that are dialed, regardless of how long or short the dial string is. In most European countries, the same result is accomplished by using the 0.00! route pattern.

When phone numbers are published for use abroad, they typically show a plus sign (+) prefix in place of any international call prefix, to signify that callers should use the prefix code appropriate for their country. Many phones allow the plus sign to be entered in their saved number lists. Holding down the zero (0) key will enter a plus sign on most GSM mobile phones, while other phones, such as Cisco Unified IP phones, require two consecutive presses of the star (*) key. When a call is made, the system then automatically converts the plus sign to the correct IDD prefix, depending on where the phone is being used. This enables callers to use the same stored number when calling from either their own country or any other.

When matching a variable-length pattern, the Cisco Unified Communications Manager does not know when dialing is complete, so it will wait for 15 seconds by default before processing the call. This post-dial delay can be reduced or eliminated as follows:

- Reduce the Cisco CallManager service parameter called the T302 Timer to allow earlier detection of the end of dialing. However, do not set this timer to less than 4 seconds, to prevent premature transmission of the call before the user finishes dialing.
- Configure a second route pattern, followed by the pound sign (#) wildcard, such as **9.011!#** for North America or **0.00!#** for Europe. Then educate users that they can indicate end of dialing by terminating the number with the # key. This action is analogous to pressing the Send button on a cell phone.

The implementation of the interdigit timeout termination in the Cisco Unified Communications Manager is different from the implementation in Cisco IOS dial peers. In the Cisco Unified Communications Manager, the # is not only the instruction to stop digit collection but is also part of the dialed number. Therefore, if you use the # to avoid waiting for the expiration of the interdigit timeout, all route patterns must be configured twice—once with the # and once without.

A dial plan may include overlaps. Overlaps occur when a pattern overlaps with another, longer pattern. Figure 19-2 illustrates an overlap scenario within a dial plan: 131 overlaps with 13!.

Digit collection is stopped as soon as an entry in the call-routing table is matched in its complete length and no other potential matches exist. In Figure 19-2, a user dials 13115. The Cisco Unified Communications Manager interprets the number digit by digit as the user enters the digits on the keypad of the phone. After all received digits are analyzed, the only match is 13!. Although there is only a single matching pattern, the Cisco Unified Communications Manager must wait for additional digits because the matched pattern is of variable length. The (!) wildcard represents one or more digits. The call can be sent to the device that is associated with pattern 13! only after the interdigit timeout expires. In this scenario, you could lower the T302 timer or add a pattern 13!# to reduce or eliminate post-dial delays. If the user dials 131, the user will also experience a post-dial delay. After these three digits are analyzed, two longer potential matches remain (1[2–4]XX and 13!). The Cisco Unified Communications Manager detects that the end user finished dialing and that the longer matches are not applicable only after the interdigit timeout expires. If the user dials 1415, the only matching pattern is 1[2–4]XX. This pattern does not include the (!) wildcard, and the Cisco Unified Communications Manager does not have to wait for additional dialed digits. The call to 1415 can be routed immediately after receiving the fourth digit.

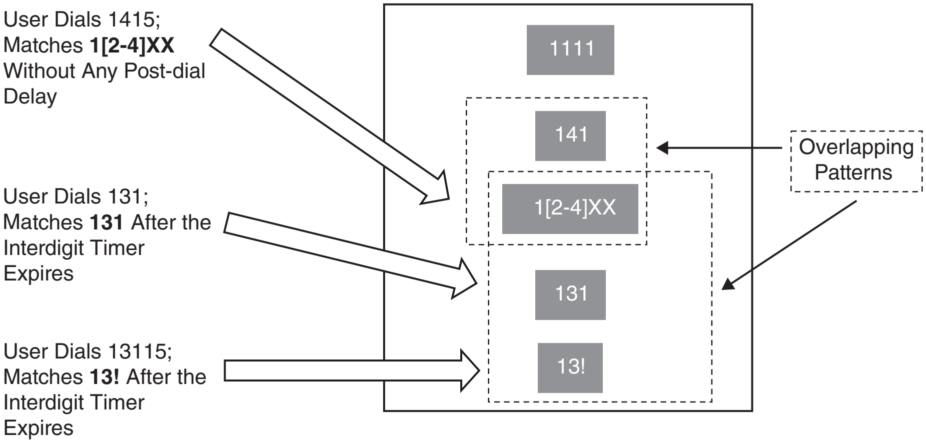

User Dials 1415; Matches **1[2-4]XX** Without Any Post-dial Delay
User Dials 131; Matches **131** After the Interdigit Timer Expires
User Dials 13115; Matches **13!** After the Interdigit Timer Expires
1111
141
1[2-4]XX
131
13!
Overlapping Patterns

Figure 19-2 *Overlaps and Interdigit Timeout*

Route patterns, translation patterns, and directory numbers have a check box labeled Urgent Priority. The Urgent Priority check box can be used to force immediate routing of certain calls as soon as a match is detected, without waiting for the interdigit timeout to expire when additional longer potential matches exist. The most applicable scenario in North America pertains to emergency 911 calls. If the patterns 9.911 and 9.[2–9]XXXXXX are configured and a user dials 9911, the Cisco Unified Communications Manager must wait for the interdigit timeout before routing the call because further digits might cause the 9.[2–9]XXXXXX pattern to match. However, when urgent priority is enabled for the 9.911 route pattern, the Cisco Unified Communications Manager makes its routing decision as soon as the user has finished dialing 9911, without causing any post-dial delay. When urgent priority has been enabled, the specified route pattern is excluded from other, longer route pattern matches. If en bloc dialing is used and the provided number is longer than the urgent pattern, the urgent pattern is not considered.

Route Groups and Local Route Groups

In larger enterprise networks, a number of IP PBXs might be deployed over several clusters. These independent IP PBX or PBX clusters are interconnected using trunks. The possible topologies include hub and spoke, full mesh, or many different combinations of these. Each one of these IP PBXs is capable of independently routing calls initiated by either endpoints, applications registered locally, or internal and external trunks. Connections to voice gateways, session border controllers, and other devices can also provide connections between the enterprise IP network and the PSTN for business-to-business (B2B) communications. Some structural method must be used to map out how these complex systems can communicate successfully with one another.

The Cisco Unified Communications Manager uses route plans to determine how to route calls between clusters and how to route external calls to a private network or to the public switched telephone network (PSTN). The route plan configured specifies the path that the system uses to route each type of call. For example, a route plan can be created to use the IP network for on-net calls and then use one carrier for local PSTN calls and a different carrier for international calls. The Cisco Unified Communications Manager has a three-tiered approach to route planning that uses the following components:

Key Topic

- **Route Patterns:** The system searches for a configured route pattern that matches the external dialed string and uses it to select a gateway or a corresponding route list.
- **Route Lists:** These are prioritized lists of the available paths for the call.
- **Route Groups:** These are the available paths; the route group distributes the call to gateways and trunks.

In addition to these building blocks, the route plan can also include the following components. Not all of these additional routing components will be discussed in this section:

- **Local Route Groups:** Decouple the location of a PSTN gateway from the route patterns that are used to access the gateway.
- **Route Filters:** Restrict certain numbers that are otherwise allowed by the route pattern.
- **Automated Alternate Routing (AAR):** Automatically reroute calls through the PSTN or another network when the system blocks a call due to insufficient bandwidth.
- **Time-of-Day Routing:** Create a time schedule that specifies when a partition is available to receive incoming calls. This topic will be discussed more later in a section on call privileges.

A local route group can reduce the number of route lists that are required within an enterprise network. Route lists point to the PSTN gateway that the system uses to route the call, based on the location of the PSTN gateway. As an alternative, you can use local route groups to decouple the location of a PSTN gateway from the route patterns that are used to access the gateway. This configuration allows phones and other devices from different locations to use a single set of route patterns, while the Cisco Unified Communications Manager selects the correct gateway to route the call.

The Cisco Unified Communications Manager provides a default local route group called *standard local route group*, but additional local route groups can be configured. To configure new local route groups, follow these steps:

Step 1. Configure local route group names.

a. From Cisco Unified CM Administration, navigate to **Call Routing > Route/Hunt > Local Route Group Names**.

b. Click **Add Row**.

c. Enter a name and description for the new local route group, and then click **Save**.

Step 2. Associate a local route group with a device pool.

- **a.** Navigate to **System > Device Pool**.
- **b.** Enter search criteria if necessary, and then click **Find**. Select a device pool from the resulting list.
- **c.** In the Local Route Group Settings area, select a route group from the Standard Local Route Group drop-down list.
- **d.** Click **Save**.

Step 3. Add a local route group to a route list.

- **a.** Navigate to **Call Routing > Route/Hunt > Route List**.
- **b.** Choose one of the following options:
  - Click the **Add New** button to add a new route list.
  - Click **Find** and select a route list from the resulting list to modify the settings for an existing route list.
- **c.** The Route List Configuration window appears. To add a local route group to the route list, click the **Add Route Group** button.
- **d.** From the Route Group drop-down list, select a local route group to add to the route list. You can add the standard local route group, or you can add a custom local route group that you have created.
- **e.** Click **Save**, and then click **Apply Config**.

A route group can be configured to prioritize the order in which the Cisco Unified Communications Manager selects gateways for outgoing calls. Use the following procedure to group together gateways that have similar characteristics, so that any gateway in the group can dial the call. The Cisco Unified Communications Manager will select a gateway to use based on the order that was specified when the route group was configured. A single gateway or other device can be assigned to multiple route groups.

Step 1. From Cisco Unified CM Administration, navigate to **Call Routing > Route/Hunt > Route Group**.

Step 2. Choose one of the following options:

- Click **Add New** to add a new route group.
- Click **Find** and choose a route group from the resulting list to modify the settings for an existing route group.

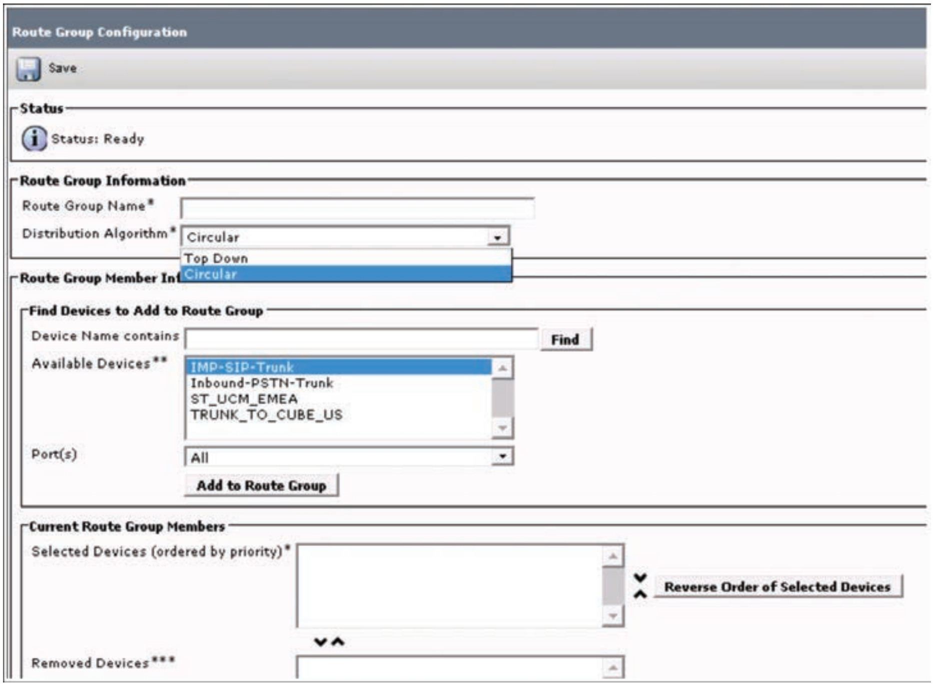
Step 3. When the Route Group Configuration window appears, configure the following fields:

- **Route Group Name:** Enter a name for the route group.
- **Distribution Algorithm:** Choose between Circular and Top Down.
- **Find Devices to Add to Route Group:** There will be a list of available trunks and gateways in the Available Devices window. You can search this list by using the Device Name Contains menu option. Select a gateway from the list, and then click the **Add to Route Group** button.

- **Current Route Group Members:** Any devices added to the route group will be added to this box. This is a prioritized list and will be searched based on the Distribution Algorithm configuration. Select a device from the list and use the arrow keys to the right of the box to change the order within the list.

Step 4. Click **Save**.

Figure 19-3 illustrates the Route Group Configuration menu options.



Route Group Configuration

Save

Status

Status: Ready

Route Group Information

Route Group Name*

Distribution Algorithm* Circular

Top Down
Circular

Route Group Member Inf

Find Devices to Add to Route Group

Device Name contains

Find

Available Devices**

IMP-SIP-Trunk
Inbound-PSTN-Trunk
ST_UCM_EMEA
TRUNK_TO_CUBE_US

Port(s) All

Add to Route Group

Current Route Group Members

Selected Devices (ordered by priority)*

Reverse Order of Selected Devices

Removed Devices***

Figure 19-3 *Route Group Configuration Menu*

Route Lists

A route list can be configured to identify a set of route groups and order them by priority. The Cisco Unified Communications Manager uses the order in the route list to search for available devices for outgoing calls. If you configure a route list, you must configure at least one route group first. A route list can contain only route groups and local route groups.

When an outbound call is sent through a route list, the route list process locks the outbound device to prevent sending an alert message before the call is completed. After the outbound device is locked, the hunt list, if any is configured, will stop hunting down the incoming calls. Use the following steps to configure a route list in the Cisco Unified Communications Manager:

Step 1. From Cisco Unified CM Administration, navigate to **Call Routing > Route/ Hunt > Route List.**

Step 2. Choose one of the following options:

- Click **Add New** to add a new route list.
- Click **Find** and select a route list from the resulting list to modify the settings for an existing route list.

Step 3. Configure the following fields in the Route List Configuration window.

- Name
- Description (Optional)
- Cisco Unified Communications Manager Group
- Enable This Route List check box
- Run on All Active Unified CM Nodes check box

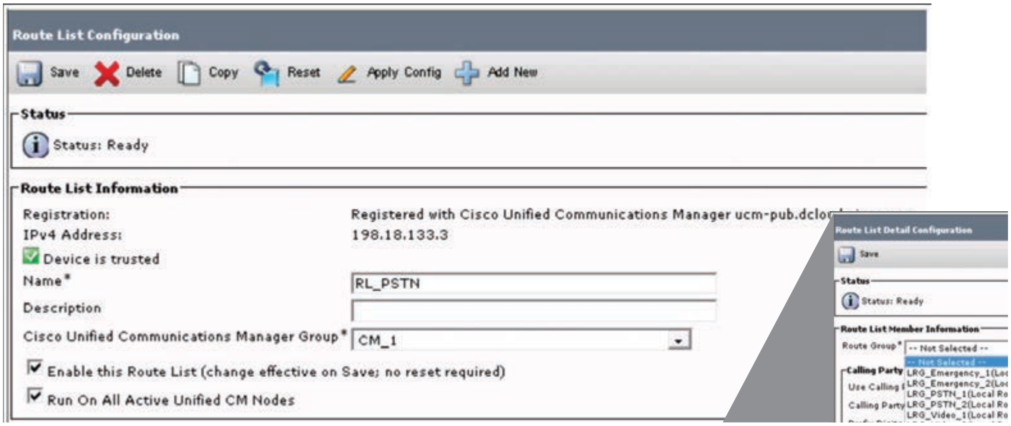
Step 4. To add a route group to the route list, click the **Add Route Group** button.

Step 5. From the Route Group drop-down list, choose a route group to add to the route list.

Step 6. Click **Save**.

Step 7. Click **Apply Config**.

Figure 19-4 illustrates the Route List Configuration menu options.



Status: Ready

Registration: Registered with Cisco Unified Communications Manager ucm-pub.dclo

IPv4 Address: 198.18.133.3

☑ Device is trusted

Name* RL_PSTN

Description

Cisco Unified Communications Manager Group* CM_1

☑ Enable this Route List (change effective on Save; no reset required)

☑ Run On All Active Unified CM Nodes

Status: Ready

Route Group* -- Not Selected --

-- Not Selected --
LRG_Emergency_1(Loc
LRG_Emergency_2(Loc
LRG_PSTN_1(Local Ro
LRG_PSTN_2(Local Ro
LRG_Video_1(Local Ro

Figure 19-4 *Route List Configuration Menu*

Route Patterns and SIP Route Patterns

As mentioned in the previous section, the Cisco Unified Communications Manager does not require route patterns or SIP route patterns when routing locally within the Cisco Unified Communications Manager itself. These pattern types are used to match dialed aliases intended to route outside the Cisco Unified Communications Manager, whether that call attempt is on-net or off-net. Route patterns are used to route numeric digits only. SIP route patterns are used to route SIP URIs only. The following instructions describe the basic settings needed to configure each of these pattern types in the Cisco Unified Communications Manager. Although the route pattern can point directly to a gateway, Cisco does recommend that route patterns be configured with route lists and route groups. This approach provides the greatest flexibility in call routing and scalability.

Step 1. From Cisco Unified CM Administration, navigate to **Call Routing > Route/Hunt > Route Pattern**.

Step 2. Perform one of the following:

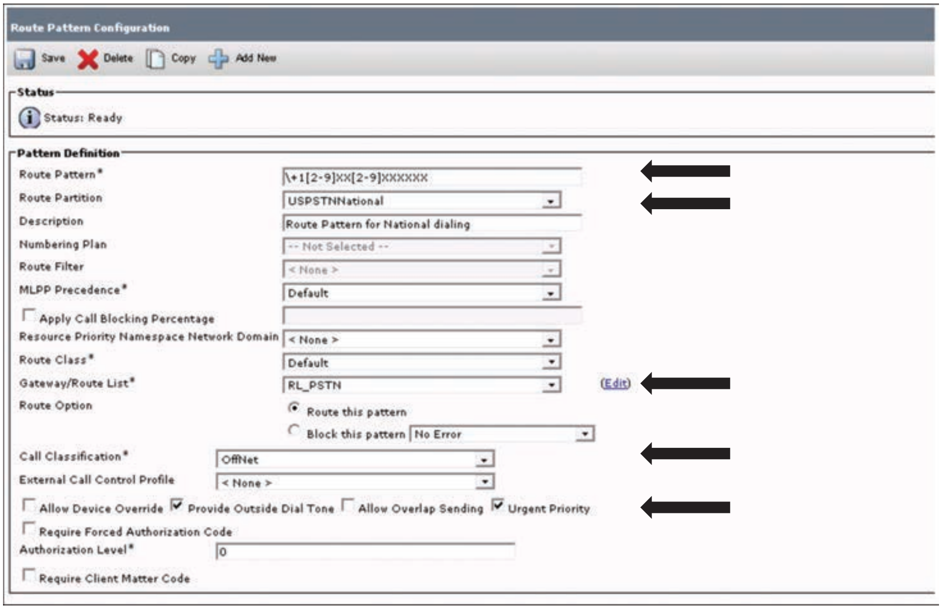
- Click **Add New** to create a new route pattern.
- Click **Find** and select an existing route pattern.

Step 3. The Route Pattern Configuration window appears. Configure the following fields at a minimum:

- In the Route Pattern field, enter the number pattern that the dial string must match.
- From the Gateway/Route drop-down list, select the destination where you want to send calls that match this route pattern.
- Complete the remaining fields in the Route Pattern Configuration window. For more information on the fields and their configuration options, see the system's Online Help.

Step 4. Click **Save**.

Figure 19-5 illustrates the Route Pattern Configuration menu options.



Status
Status: Ready

Pattern Definition
Route Pattern* \+1[2-9]XX[2-9]XXXXXX
Route Partition USPSTNNational
Description Route Pattern for National dialing
Numbering Plan -- Not Selected --
Route Filter < None >
MLPP Precedence* Default
□ Apply Call Blocking Percentage
Resource Priority Namespace Network Domain < None >
Route Class* Default
Gateway/Route List* RL_PSTN
Route Option ● Route this pattern
○ Block this pattern No Error
Call Classification* OffNet
External Call Control Profile < None >
□ Allow Device Override ☑ Provide Outside Dial Tone □ Allow Overlap Sending ☑ Urgent Priority
□ Require Forced Authorization Code
Authorization Level* 0
□ Require Client Matter Code

Figure 19-5 *Route Pattern Configuration Menu*

Wildcards and special characters in route patterns allow a single route pattern to match a range of numbers (addresses). You can use these wildcards and special characters to build instructions that enable the Cisco Unified Communications Manager to manipulate a number before sending it to an adjacent system. Table 19-4 describes the wildcards and special characters that Cisco Unified Communications Manager supports.

SIP route patterns are configured in the Cisco Unified Communications Manager to route or block calls to external entities based on the host portion, otherwise known as the domain portion, of directory URIs. A SIP route pattern can point directly to a SIP trunk or point to a route list that then refers to one or more route groups and finally to SIP trunks. The use of the full SIP route pattern, route list, route group construct is highly recommended because it offers more flexibility.

Key Topic

Table 19-4 Wildcards and Special Characters in Route Patterns

Character	Description
@	The at symbol (@) wildcard matches all National Numbering Plan numbers. Each route pattern can have only one @ wildcard.
X	The X wildcard matches any single digit in the range 0 through 9.
!	The exclamation point (!) wildcard matches one or more digits in the range 0 through 9.
?	The question mark (?) wildcard matches zero or more occurrences of the preceding digit or wildcard value.
+	The plus sign (+) wildcard matches one or more occurrences of the preceding digit or wildcard value.
[ ]	The square bracket ([ ]) characters enclose a range of values. Only one value in the range can represent a dialed character.
-	The hyphen (-) character, used with the square brackets, denotes a range of values.
^	The circumflex (^) character, used with the square brackets, negates a range of values. Ensure that it is the first character following the opening bracket ([). Each route pattern can have only one ^ character.
.	The dot (.) character, used as a delimiter, separates the Cisco Unified Communications Manager access code from the directory number. Use this special character, with the discard digits instructions, to strip off the Cisco Unified Communications Manager access code before sending the number to an adjacent system. Each route pattern can have only one dot (.) character.
*	The asterisk (*) character can provide an extra digit for special dialed numbers.
#	The octothorpe (#) character, often called the pound sign, generally identifies the end of the dialing sequence. Ensure the # character is the last character in the pattern.
\+	A plus sign preceded by a backslash, that is, \+, indicates that you want to configure the international escape character +. Using \+ means that the international escape character + is used as a dialable digit, not as a wildcard.

SIP route patterns matching on the host part of the directory URI can match on a domain name or an IP address, both of which can be configured after the @ on directory URIs. Wildcards can be used in the *IPv4 patterns* to match on multiple domains, such as *.cisco.com and ccm[1-4].uc.cisco.com. In IP address SIP route patterns, a subnet notation can be used, such as 192.168.10.0/24. To create a SIP route pattern that matches any domain, you can just put * (star) in the pattern string field.

Digit Manipulation

The two primary methods for digit manipulation are translation patterns and transformation patterns. Translation patterns can be configured in the Cisco Unified Communications Manager to manipulate digits for any type of call. Translation patterns follow the same general rules and use the same wildcards as route patterns. As with route patterns, translation patterns are assigned to a partition. However, when the dialed digits match the translation pattern, the Cisco Unified Communications Manager does not route the call to an outside entity such as a gateway; instead, it performs the translation first and then routes the call again, this time using the calling search space configured within the translation pattern.

Key Topic

Transformation patterns determine how the system manipulates the digits that were dialed in an incoming or outgoing call. Transformation patterns are configured when the calling or called number needs to be changed before the system sends it to the phone or the PSTN. You can use transformation patterns to discard digits, prefix digits, add a calling party transformation mask, and control the presentation of the calling party number. Consider the following transformation pattern associations with calling search spaces (CSS):

- Associate a calling party transformation pattern with a called party transformation CSS.
- Associate a called party transformation pattern with a calling party transformation CSS.

Translation Patterns

For each translation pattern that you create, ensure that the combination of partition, route filter, and numbering plan is unique. If you receive an error that indicates duplicate entries, check the route pattern or hunt pilot, translation pattern, directory number, call park number, call pickup number, or meet-me number configuration windows. Configure translation patterns to apply digit manipulations to the calling and called numbers when the dial string matches the pattern. The system completes the digit translation and then reroutes the call. Use the following steps to configure translation patterns on the Cisco Unified Communications Manager.

Step 1. From Cisco Unified CM Administration, navigate to **Call Routing > Translation Pattern**.

Step 2. Choose one of the following options:

- Click **Add New** to add a new translation pattern.
- Click **Find** and select an existing translation pattern.

Step 3. In the Translation Pattern field, enter the pattern that you want the system to match to dial strings that use this pattern.

Step 4. From the Partition drop-down list, select the partition where you want to assign this pattern.

Step 5. Complete the remaining fields in the Translation Pattern Configuration window. For more information on the fields and their configuration options, see the system's Online Help.

Step 6. Click **Save**.

Transformation Patterns

There are three main steps to configuring transformation patterns in the Cisco Unified Communications Manager. You can configure calling party transformation patterns to transform the calling number. For example, you can configure a transformation pattern that replaces a caller's extension with the office's main number when calling the PSTN. You also can configure called party transformation patterns to transform the called number. For example, you can configure a transformation pattern that retains only the last five digits of a call dialed as a ten-digit number. Optionally, you can configure transformation profiles, but you should use this procedure only if you are using Cisco Intercompany Media Engine (Cisco IME). You must configure a transformation profile to convert dialed numbers into the E.164 format. Use the following steps to configure transformation patterns on the Cisco Unified Communications Manager:

Step 1. Configure calling party transformation patterns:

a. From Cisco Unified CM Administration, navigate to **Call Routing > Transformation > Transformation Pattern > Calling Party Transformation Pattern**.

b. Choose one of the following options:

- Click **Add New** to add a new calling party transformation pattern.
- Click **Find** and select an existing pattern.

c. From the Pattern field, enter the pattern that you want to match to the calling party number.

d. Complete the remaining fields in the Calling Party Transformation Pattern Configuration window. For more information on the fields and their configuration options, see the system's Online Help.

e. Click **Save**.

Step 2. Configure called party transformation patterns:

a. Navigate to **Call Routing > Transformation > Transformation Pattern > Called Party Transformation Pattern**.

b. Choose one of the following options:

- Click **Add New** to add a new called party transformation pattern.
- Click **Find** and select an existing pattern.

c. From the Pattern field, enter the pattern that you want to match to the called number.

d. Complete the remaining fields in the Called Party Transformation Pattern Configuration window. For more information on the fields and their configuration options, see the system's Online Help.

e. Click **Save**.

Step 3. Configure transformation profiles. Perform this procedure only if you are using Cisco Intercompany Media Engine (Cisco IME). You must configure a transformation profile to convert dialed numbers into the E.164 format. The E.164 format includes the international + prefix; for example, +14085551212.

a. Navigate to **Call Routing > Transformation > Transformation Profile.**

b. Choose one of the following options:

- Click **Add New** to add a new transformation profile.
- Click **Find** and choose a pattern from the resulting list to modify the settings for an existing transformation profile.

c. The Transformation Profile Configuration window appears. Configure the fields in the Transformation Profile Configuration window. For more information on the fields and their configuration options, see the system's Online Help.

d. Click **Save**.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 19-5 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 19-5 Key Topics for Chapter 19

Key Topic Element	Description	Page Number
Steps	Call-Routing Process	459
Table 19-2	Call-Routing Source and Target Components	460
Table 19-3	Addressing Methods for Destination Numbers	462
Paragraph	Use of +E.164 Addresses	463
List	CUCM Route Plan Components	465
Table 19-4	Wildcards and Special Characters in Route Patterns	470
Paragraph	Use of Transformation Patterns	471

Define Key Terms

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

AAR, CAC, Digit-by-Digit Analysis, +E.164 Alias, E.164 Alias, En Bloc, IDD, IME, Intersite Routing, Intrasite Routing, KPML, Local Route Group, Off-net, On-net, Overlap Sending and Receiving, PSTN Routing, Route Filter, Route Group, Route List, Route Pattern, ToD, Translation Patterns, Voicemail Port

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the five call-routing source components.
2. List the six call-routing target components.
3. List the three main steps to configuring transformation patterns on the CUCM.

This page intentionally left blank

This part covers the following topics:

- **Chapter 20, Introduction to Cisco Edge Services:** This chapter will introduce three Edge products in the Cisco Collaboration architecture. The Cisco Expressway Series provides an Edge connection across the IP Internet network. The Cisco Voice Gateway Elements offer TDM direct access from the Enterprise edge IP network out to the PSTN. Finally, the Cisco Unified Border Element offers an IP-to-ISDN connection through a third-party service provider.
- **Chapter 21, Mobile and Remote Access (MRA):** This chapter will describe the different elements required to set up a complete Mobile and Remote Access solution in a Cisco Collaboration environment, including security settings, infrastructure configuration steps, and interconnecting trunks between all the various components involved. This chapter will also cover how to configure device onboarding with activation codes over MRA.

Part V

Edge Services

CHAPTER 20

Introduction to Cisco Edge Services

This chapter covers the following topics:

Cisco Expressway: This topic will provide a brief history of how the Expressway evolved from the VCS and explain the role the Expressway plays in a Cisco collaboration network today.

Cisco Voice/Video Gateway Elements: This topic will discuss some of the legacy products used for analog voice gateway communications and introduce new products that can be used for both voice and video gateway communication.

Cisco Unified Border Element: This topic will briefly introduce the CUBE software that is available in Cisco IOS XE software-based routers.

This world is changing with the introduction of new technology. Business is moving at a faster speed, and companies have to be able to make informed decisions faster to be competitive in today's market. Smaller companies have turned to various solutions to provide the edge they needed but have created technology silos in the process. The Cisco Collaboration Edge products provide connections between these silos for any sized business to be productive outside the office. These connections come from various third-party solutions, such as Microsoft Skype-for-Business (S4B) (now Microsoft Teams) interoperability, to key partnerships with companies such as Apple, AWS, IBM, and Google. Cisco Collaboration Edge solutions also provide connections for cloud-hosted solutions, such as Webex and BroadSoft, as well as IP-to-IP connections through the firewall, and IP-to-PSTN connections. Cisco allows this extension of rich collaboration capabilities to anyone, anywhere, in any pocket, using Cisco phones or endpoint, or third-party systems, and even on personal smartphones, tablets, and computers. This standards-based interoperability provides investment protection for companies of any size willing to procure this technology advantage.

You can create highly secure, reliable branch office collaboration by using a range of UC and Telepresence endpoints. You also can create relationships with your customers and business partners by collaborating in the way that they want, whether it is through voice, instant messaging, video, or content sharing. The Cisco Collaboration Edge architecture is designed to deliver unified communications across borders. Topics discussed in this chapter include the following:

- Cisco Expressway
- Cisco Voice Gateway Elements
- Cisco Unified Border Element

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 1.2 Describe the purpose of Edge devices in the Cisco Collaboration architecture such as Expressway and Cisco Unified Border Element
- 4.4 Describe Mobile and Remote Access (MRA)

"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 20-1 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 20-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Cisco Expressway	1–3
Cisco Voice Gateway Elements	4–5
Cisco Unified Border Element	6

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 feature capability of the Cisco VCS was the main reason Cisco used this product to design the Cisco Expressway?
   a. H.323 and SIP interworking
   b. IPv4 and IPv6 interworking
   c. NAT and firewall traversal
   d. Microsoft interoperability
2. What license is required on the Cisco Expressway before a personal endpoint, such as the DX80, can register?
   a. RMS License
   b. H.323/SIP Registration License
   c. Room Registration License
   d. Device Registration License

3. What license is required on the Cisco Expressway for B2B calls?
   a. RMS License
   b. Non-Traversal Call License
   c. Traversal Call License
   d. No extra licenses are needed for B2B calls.
4. Which of the following is an analog voice gateway?
   a. ISR2900
   b. VG204XM
   c. PVDM4
   d. ATA188
5. What operating system of Cisco routers should be used when running gateway services?
   a. IOS
   b. IOS XE
   c. ASR
   d. ISR
6. Where does the ISDN SIP trunk from the service provider terminate when setting up CUBE on an enterprise router?
   a. TDoS
   b. B2BUA
   c. TDM Circuit
   d. SBC

Foundation Topics

Cisco Expressway

No matter what line of business exists, extending to branch offices is a fundamental approach to reaching a wider market. Cisco's next-gen routers offer incredible routing capabilities across network borders. However, these complicated network deployments can falter, leaving communication gaps at critical times. Additionally, not all companies use a modern IP solution for communication. Yet companies that have moved to an IP-based communications solution still need to be able to communicate with businesses and consumers who have not yet made this move. The Cisco Edge products allow communication to be unified and uninterrupted regardless of location or disruption.

In today's everchanging workplace, businesses are no longer tied to the four walls of the office space. Employees are now allowed and encouraged to work from home, which reduces company overhead expenses and increases employee productivity. However, with these changes to the corporate environment, there are many challenges to overcome as well. One such challenge pertains to how employees communicate with one another from many different remote locations. Cisco has designed a solution to this communication dilemma called Mobile and Remote Access (MRA). This distinctive platform allows employees to leverage the same great Cisco collaboration solution from anywhere in the world without a VPN while maintaining the same level of security that employees experience within the corporate network.

The Cisco Expressway Series product portfolio is an evolved solution that originated in the Tandberg Video Communications Server (VCS) products. After Cisco acquired Tandberg, the company used these extraordinary products as the foundation of an even greater-reaching solution known as Mobile and Remote Access (MRA). To fully understand the Expressway series, it is essential to first understand the VCSs.

The Video Communications Server is a product developed by a company called Tandberg, which was acquired by Cisco in 2010. For Tandberg, the VCS was the central call control product for video telecommunications, just as the Cisco Unified Communications Manager is the central call control product in a Cisco-preferred designed architecture today. Part of what made the VCS such a great product, and why Cisco still utilizes this product today, is its capability to securely handle NAT and firewall traversal, unlike any other product on the market. Tandberg climbed this ladder to success much the same way as Cisco, by acquiring key companies that possessed the technology it needed for the time. In 2004, Tandberg acquired a company called Ridgeway Systems and Software, which was a UK-based software company specializing in firewall and NAT traversal. Ridgeway had developed a proprietary traversal protocol called Assent.

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 was initiated from inside the firewall with this keepalive message. Now the ports allocated can be used after the call setup has completed. Another great aspect to this solution is that only two ports are required to be opened on the firewall that can handle all the media and signaling because Assent will multiplex this data. So, 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 into the protocol as well.

Assent is such a powerful tool that the ITU used it as the basis to develop two H.323 traversal standards known as H.460.18 and H.460.19. By the summer of 2005, the standards were completed and in full use. H.460.17, which was a predecessor protocol, performs firewall traversal by carrying the media over TCP ports instead of UDP. H.460.18 works just like Assent, except it requires ports 50000 to 52400 to be opened on the firewall. In conjunction with H.460.18, H.460.19 multiplexes the media ports so that 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. Another advantage to Assent over the ITU standards is that it can support both H.323 and SIP calls, as well as interworking calls between the two protocols.

The Cisco VCS-centric firewall and NAT traversal solution comes in two server platforms. 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.

Cisco released the Cisco Expressway Series products after the Tandberg merger, and they share the same source code as the Cisco VCSs. Because the menus on the Expressway Series are identical to the menus on the Cisco VCS, there has been some confusion as to why Cisco released these products and what the differences between them are. This brief explanation of the Expressway Series will shed some light on this confusing solution.

Key Topic

Cisco first launched the Expressway Series in version X8.1. Expressways are built on the same firmware as the VCSs but offer an alternative solution for existing Cisco Unified Communications Manager customers, providing them with a low-cost traversal solution without having to buy a Cisco VCS Control and VCS Expressway with licenses. Because these servers could be virtualized, customers who were already running the Cisco Unified Communications Manager could install the Expressway Series for free, gaining the ability to do secure firewall traversal for IP communications. The Expressway Series also offered a secure VPN-less solution for unified communications, known as Mobile and Remote Access (MRA). The X8.1 version of the Expressway could not support registrations directly, but MRA allows endpoints outside the firewall to register to an internal Cisco Unified Communications Manager from anywhere outside the corporate network through a proxied registration rather than through a VPN. This limits the need for small and medium-sized businesses to install complex VPN routers and improves the media flow of calls between internal endpoints and external endpoints. Because some companies had already made the investment for a VCS solution, MRA was also made available through these products.

Like the VCSs, the Expressway Series solution is composed of two devices: the Expressway Core and Expressway Edge. The Expressway Series offers the capability 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) and business-to-consumer (B2C) communications. B2B and B2C communication is an optional feature on the Expressway Series, and as such requires Rich Media Session (RMS) licenses. Also, the recommended deployment is to use a dedicated Expressway C and Expressway E for Mobile and Remote Access, while a separate set should be used for B2B and B2C communication. A third set should be used if a Webex Hybrid integration is being deployed, but that topic is outside the scope of this book.

In August 2016, Cisco released version X8.9, which allows for registrations directly to the Expressway Core. With this version the Expressway Edge can still handle only proxied registrations and only using SIP. However, the Expressway Core can handle direct registration via SIP or H.323. This confused a lot of people because direct registration was the only distinguishing factor between the VCS and the Expressway Series. However, there is still another distinguishing factor, and it involves licenses. The VCS uses device-based licensing, whereas the Expressway Series uses the same user-based licensing model as the Cisco Unified Communications Manager. Also, these licenses can be migrated should a customer decide to move to a Cisco Unified Communications Manager–centered call control platform. On the Cisco Expressway Core, one user license is equivalent to one *Device Registration* license, which will allow personal devices to register, such as the DX80. Additional *Room*

Registration licenses can be purchased for common meeting room devices, such as MX, SX, or Webex Room endpoints. There have been several more upgrades since X8.9, and the Cisco Expressway Edge can now support both H.323 and SIP registration. Proxied registration still supports only SIP. Table 20-2 outlines the differences between the licensing available on these two server platforms. Note that for "Local Call Licenses," there is no distinction between traversal and non-traversal calls on the Cisco Expressway. The Cisco VCS went end-of-sale June 30, 2020, and will go end-of-life December 31, 2023.

Key Topic

Table 20-2 Licensing on the Cisco VCS Compared to the Expressway Series

	VCS Control	VCS Expressway	Expressway Core	Expressway Edge
Registration Licenses	SIP/H.323 Registration	SIP/H.323 Registration	SIP.H.323 Device Registration Room Registration	SIP.H.323 Device Registration Room Registration SIP Proxy Registration Only
Calling Licenses	Non-Traversal Call Licenses	Non-Traversal Call Licenses	Local Call Licenses Included	Local Call Licenses Included
	Traversal Call Licenses	Traversal Call Licenses	RMS Licenses for B2B and B2C Calls	RMS Licenses for B2B and B2C Calls
FindMe	FindMe Option Key	FindMe Option Key	FindMe Option Key	FindMe Option Key
Microsoft Interop	Microsoft Interop Option Key	Microsoft Interop Option Key	Microsoft Interop Included with RMS	Microsoft Interop Included with RMS
Device Provisioning	Device Provisioning Option Key	Device Provisioning Option Key	Device Provisioning Option Key	Device Provisioning Option Key
Cloud Call Connectors	Installed from Webex Cloud Management Portal	Installed from Webex Cloud Management Portal	Installed from Webex Cloud Management Portal	Installed from Webex Cloud Management Portal

Cisco Voice Gateway Elements

IP-to-PSTN communication can be achieved through many different solutions. Gateways provide a number of methods for connecting a network of collaboration endpoints to the public switched telephone network (PSTN), a legacy PBX, or external systems. Voice and video gateways range from entry-level and standalone platforms to high-end, feature-rich integrated routers, chassis-based systems, and virtualized applications.

During the 1990s and early 2000s, the only way for an enterprise to connect its internal voice and video network to services outside the enterprise was by means of TDM or serial gateways to the traditional PSTN. Cisco still offers a full range of TDM and serial gateways with analog and digital connections to the PSTN as well as to PBXs and external systems. TDM connectivity covers a wide variety of low-density analog (FXS and FXO), low-density digital (BRI), and high-density digital (T1, E1, and T3) interface choices. Starting around

2006, new voice and video service options to an enterprise became available from service providers, often as SIP trunk services. Using a SIP trunk for connecting to the PSTN and other destinations outside the enterprise involves an IP-to-IP connection at the edge of the enterprise's network. The same functions traditionally fulfilled by a TDM or serial gateway are still needed at this interconnect point, including demarcation, call admission control, quality of service, troubleshooting boundary, security checks, and so forth. For voice and video SIP trunk connections, the Cisco Unified Border Element and the Cisco Expressway Series fulfill these functions as an interconnection point between the enterprise and the service provider network.

The two types of Cisco TDM gateways are analog and digital. Both types support voice calls, but only digital gateways support video. There are two categories of Cisco analog gateways: station gateways and trunk gateways. Analog station gateways connect the Cisco Unified Communications Manager to plain old telephone service (POTS) analog telephones, interactive voice response (IVR) systems, fax machines, and voicemail systems. Station gateways provide Foreign Exchange Station (FXS) ports. Analog trunk gateways connect the Cisco Unified Communications Manager to PSTN central office (CO) or PBX trunks. Analog trunk gateways provide Foreign Exchange Office (FXO) ports for access to the PSTN, PBXs, or key systems, and E&M (recEive and transMit, or ear and mouth) ports for analog trunk connection to a legacy PBX. Analog direct inward dialing (DID) and Centralized Automated Message Accounting (CAMA) are also available for PSTN connectivity. Cisco analog gateways are available on the following products and series:

Key Topic

- Cisco Analog Voice Gateways VG204XM and VG300 Series (VG310, VG320, VG350) all support SCCP.
- Cisco Integrated Services Routers Generation 2 (ISR G2) 2900, 3900, 3900E, and 4000 Series (4300 and 4400) with appropriate Packet Voice Digital Signal Processor Modules (PVDMs) and service modules or cards. PVDM4s utilized by ISR 4000 Series do not support video today.
- Cisco Analog Telephone Adapter (ATA) 190 (SIP only) provides a replacement for the ATA188.

A Cisco digital trunk gateway connects the Cisco Unified Communications Manager to the PSTN or to a PBX via digital trunks such as Primary Rate Interface (PRI), Basic Rate Interface (BRI), serial interfaces (V.35, RS-449, and EIA-530), or through T1/E1 Channel Associated Signaling (CAS). Digital T1 PRI and BRI trunks can be used for both video and audio-only calls. Cisco digital trunk gateways have traditionally been available on the following products and series:

- Cisco Integrated Services Routers Generation 2 (ISR G2) 1900, 2900, 3900, 3900E, 4300, and 4400 Series with appropriate PVDMs and service modules or cards (The PVDM2 cards are end of life as of June 30, 2019. Cisco recommends using the PVDM3 or PVDM4 cards on appropriate routers.)
- Cisco Telepresence ISDN GW 3241 and MSE 8321 (These products are end of sale as of May 2, 2017.)
- Cisco Telepresence Serial GW 3340 and MSE 8330 (This product is end of sale as of May 2, 2017.)

As you can see, most of these products are no longer available. Cisco has been introducing a dynamic shift in its product portfolio to both reduce the number of products available to a manageable amount and to offer more feature-rich products that can more easily support a modern collaboration solution. One of the significant advancements Cisco has changed is the software that runs on enterprise switches, wireless controllers, aggregation and edge routers, and branch routers. This new software is called IOS XE. Internetwork Operating System (IOS) XE is a combination of a Linux kernel and a monolithic application that runs on top of this kernel, whereas the IOS predecessor is a monolithic operating system that runs directly on the hardware itself. The IOS software runs on top of the Linux kernel so the commands are the same as before, but this also allows for other applications to run on the hardware at the same time.

Along with new software, Cisco has released a new series of switches and routers. The routers are called ASRs, and they were discussed in Chapter 12, "Cisco Core Network Components." Refer to that chapter if you need a review of the information. Either ASR or ISR routers can be used as the gateway product for a company, depending on the size of the company; the focus here should be on the software rather than the hardware. Both router platforms support the PVDM and PRI service modules, as well as the CUBE software, which will be discussed in the next section.

The Cisco Telepresence ISDN link is a compact appliance that provides Cisco Telepresence endpoints direct ISDN and external IP network connectivity. This unit is supported on all Cisco Telepresence endpoints running TC or CE software. While traditional voice and video gateways are shared resources that provide connectivity between the IP network and the PSTN for many endpoints, each Cisco ISDN link is paired with a single Cisco endpoint for direct ISDN access. This product is worth mentioning but will not be discussed any further because there is only a small market of people who use this product.

Cisco Unified Border Element

Cisco has invested a lot of resources in researching and developing another solution that is cost effective, scalable, sustainable, and easy to deploy and support. The result is the Cisco Unified Border Element (CUBE), which allows IP communication to be integrated with more traditional PSTN communication. Instead of organizations investing in, installing, and supporting all the necessary infrastructure needed for an expensive ISDN solution on-premises, a simple SIP trunk can be created from the Cisco router to a service provider using the CUBE service on the router. The service provider then makes the transition from IP to PSTN and vice versa. This takes the complication and much of the expense out of the hands of an organization while maintaining an open communications solution regardless of the medium through which people collaborate.

Innovations in collaboration services have delivered significant improvements in employee productivity, and enterprises are widely deploying IP-based Unified Communications, for both internal calling within the enterprise and external PSTN access. This has resulted in significant migration from TDM-based circuits, by both enterprises and telephony service providers, to IP-based trunks for Unified Communications. At the heart of IP-based telephony trunks lies the Session Initiation Protocol (SIP), which is an industry standard communications protocol based on RFC 3261 and is widely used for controlling multimedia communication sessions and applications such as voice, video, unified messaging, voicemail, and conferencing.

Key Topic

These PSTN SIP trunks terminate on a Session Border Controller (SBC) at the enterprise, which serves as a demarcation point between the enterprise and the service provider IP networks, similar to how firewalls separate two data networks. The CUBE Enterprise is Cisco's SBC offering, and it enables rich multimedia communications for enterprises by providing session control through call admission control, trunk routing, QoS, statistics, billing, redundancy, scalability, and voice quality monitoring. It offers security through encryption, authentication, registration, SIP protection, voice policy, toll fraud prevention, and telephony denial of service (TDoS) attack protection. CUBE offers interworking through various SIP and H.323 stack interoperability, SIP normalization, DTMF, transcoding, transrating, and codec filtering. Finally, CUBE offers demarcation through fault isolation, topology and address hiding, and L5/L7 protocol demarcation, and it provides a network border.

CUBE provides essential capabilities that ensure interoperability, security, and service assurance when carrying IP traffic via SIP trunks across various enterprises and service provider networks. It is a back-to-back user agent (B2BUA) and is part of the Cisco IOS infrastructure on Cisco ISR G2 800 Series platforms, Cisco IOS-XE for the ASR 1000 Series, Cisco ISR 4000 Series, and CUBE on the Cisco Cloud Services Router (CSR) 1000V Series (virtual CUBE, or vCUBE).

Information is sacred in the business world. Companies need to be able to communicate while protecting the information that is shared. The Cisco Collaboration Edge architectures offer simple, highly secure deployments. They enable you to build multiservice solutions to connect the enterprise to outside users through highly secure, encrypted firewall traversal and connectivity to the PSTN. The Collaboration Edge Architecture supports a variety of use cases. Teleworkers and mobile Jabber users can collaborate easily on any device with no VPN client required. B2B and B2C collaboration can revolutionize interactions with other organizations and consumers through browser and mobile-based collaboration. You can then communicate with anyone using service provider time-division multiplexing (TDM) or SIP trunking. You also can provide Intra-enterprise connectivity to help users collaborate on legacy private branch exchanges (PBXs), IP PBXs, and third-party devices. Finally, you can connect to the cloud for benefits such as Cisco Webex and Cisco Telepresence technologies together.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 20-3 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 20-3 Key Topics for Chapter 20

Key Topic Element	Description	Page Number
Paragraph	Value of the VCS	481
Paragraph	Assent Compared to H.460 ITU Standards	481
Paragraph	Explain MRA	482
Table 20-2	Licensing on the Cisco VCS Compared to the Expressway Series	483
List	Cisco Analog Gateway Product Series	484
Paragraph	Define CUBE	486

Define Key Terms

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

ASR, Assent, B2B, B2BUA, B2C, CAS, CUBE, DID, DMZ, E&M, FXO, FXS, IOS XE, ISR, IVR, MRA, PBX, POTS, PSTN, RMS, SBC, TDM, TDoS, VCS

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What are the two firewall traversal protocols supported on the Expressway Series?
2. What services come with the RMS license on the Cisco Expressway?
3. What are the two router models that support TDM direct access to the PSTN for an on-premises solution?

CHAPTER 21

Mobile and Remote Access (MRA)

This chapter covers the following topics:

Requirements for MRA: This topic will examine the different prerequisites that must be configured before an MRA solution can be deployed. These requirements include DNS settings, firewall ports and considerations, certificate requirements, HTTPS reverse proxy settings, and the service discovery.

Cisco Unified Communications Manager Settings for MRA: This topic will examine settings that should be configured on the Cisco Unified Communications Manager in support of endpoints registering over MRA.

TLS Verify Requirements: This topic will identify the certificate requirements for an MRA deployment using the Cisco Unified Communications Manager, the Cisco Expressway Core, and the Cisco Expressway Edge servers.

Initializing MRA on Expressway Servers: This topic will walk through the steps to enable MRA on the Expressway Core and Edge servers.

Collaboration Traversal Zones and Search Rules: This topic will walk through the steps to configure the appropriate traversal zones required to support the MRA solution.

Device Onboarding with Activation Codes over MRA: This topic will walk through the steps to configure device onboarding with activation codes over a Mobile and Remote Access deployment.

Virtual private networks have a long-time tradition of connecting remote locations with an enterprise network. However, VPNs are very complex and require a lot of resources to operate. Additionally, the modern workplace is not always located in an office environment. Companies are now encouraging their employees to work from home, which complicates how these employees communicate with each other and the outside world. Cisco's out-of-the-box thinking has brought about a solution to many of the problems created by the modern workplace mindset. The Mobile and Remote Access (MRA) solution is a unique deployment that incorporates many facets of the more traditional traversal solution discussed in the preceding chapter. Communication devices can operate from any network at any location without the use of VPNs. Employees can leverage these communication devices from a home office without the need to set up and store another router in their home. Additionally, all the features and capabilities that employees would have from a communications device located in an office are still at their disposal from their remote location using this MRA solution. Topics discussed in this chapter include the following:

- Requirements for MRA
  - DNS A-Records and SRV Records
  - Firewall Ports and Considerations

    - Certificate Requirements and Recommendations
    - HTTPS Reverse Proxy Settings
    - Service Discovery
- Cisco Unified Communications Manager Settings for MRA
- TLS Verify Requirements
    - Cisco Expressway Certificates
    - Cisco Unified Communications Manager Certificates
    - Creating Certificates for MRA
- Initializing MRA on Expressway Servers
- Collaboration Traversal Zones and Search Rules
- Device Onboarding with Activation Codes over MRA

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.0 (CLCOR 350-801) exam:

- 1.2 Describe the purpose of Edge devices in the Cisco Collaboration architecture such as Expressway and Cisco Unified Border Element
- 2.3.e Device Onboarding with Activation Codes (MRA)
- 4.4 Describe Mobile and Remote Access (MRA)

"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 21-1 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 21-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Requirements for MRA	1–5
Cisco Unified Communications Manager Settings for MRA	6
TLS Verify Requirements	7–9
Initializing MRA on Expressway Servers	10–11
Collaboration Traversal Zones and Search Rules	12
Device Onboarding with Activation Codes over MRA	13

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 is an SRV record that's needed on the public DNS for an enterprise MRA deployment?
   - a. *_collab-edge._tls.<domain>*
   - b. *_cisco-uds._tcp.<domain>*
   - c. *_cuplogin._tcp.<domain>*
   - d. *_sip._tcp.<domain>*
2. Which of the following ports needs to be opened between the DMZ and the public Internet for an MRA deployment?
   - a. TCP 7001
   - b. UDP 36000–36001
   - c. TCP 2222
   - d. TCP 8443
3. Which of the following certificate pairs are required for an MRA deployment? (Choose two.)
   - a. Public or enterprise CA certificate chain used to sign Expressway Core certificate
   - b. Public or enterprise CA certificate chain used to sign Expressway Edge certificate
   - c. CUCM Tomcat certificates or CA chain
   - d. CUCM CallManager certificates or CA chain
   - e. IMP Tomcat certificate or CA chain
   - f. CUCM CAPF certificates
4. What two ports are used with reverse proxy to allow inbound authenticated HTTPS requests for TFTP file download and SOAP API requests on the CUCM?
   - a. TCP 2222 and TCP 8443
   - b. TCP 6970 and TCP 8443
   - c. TCP 7400 and TCP 8443
   - d. TCP 5222 and TCP 8443
5. When an endpoint located outside the corporate network is configured to register to the CUCM using MRA, what is the first communication sent by that endpoint?
   - a. TLS handshake with the Expressway Edge to establish a trusted certificate verification
   - b. Registration request sent to the CUCM through the Expressway Core and Edge servers
   - c. DNS SRV Lookup for *_collab-edge._tcp.<domain>*
   - d. DNS SRV Lookup for *_cisco-uds._tcp.<domain>*

6. What service on the Cisco Unified Communications Manager should be enabled for MRA?
   - a. Cisco CallManager Service
   - b. Cisco TFTP Service
   - c. Cisco AXL Web Service
   - d. Cisco CTI Service

7. Which of the following certificate options should be used on the Cisco Expressways for an MRA deployment?
   - a. Self-signed certificates
   - b. Single host/domain certificate
   - c. Multiple subdomain wildcard certificates
   - d. All of these answers are correct.

8. What CUCM certificates are significant for Mobile and Remote Access? (Choose two.)
   - a. Public or enterprise CA certificate chain used to sign Expressway Core certificate
   - b. Public or enterprise CA certificate chain used to sign Expressway Edge certificate
   - c. CUCM Tomcat certificates or CA chain
   - d. CUCM CallManager certificates or CA chain
   - e. IMP Tomcat certificate or CA chain
   - f. CUCM CAPF certificates

9. What is the recommended format for certificates on the Expressway servers for an MRA deployment?
   - a. .cer or .crt format
   - b. DER-encoded or Base64-encoded format
   - c. DER-encoded format
   - d. Base64-encoded format
   - e. Any format can be used; there is no recommended format.

10. Which of the following statements is true when configuring an MRA solution?
    - a. Enabling MRA on the Expressway-C involves turning it on and configuring MRA Access Control settings, but enabling MRA on the Expressway-E only involves turning it on.
    - b. Enabling MRA on the Expressway-E involves turning it on and configuring MRA Access Control settings, but enabling MRA on the Expressway-C only involves turning it on.
    - c. MRA needs to be enabled only on the Expressway-C, not the Expressway-E.
    - d. MRA needs to be enabled only on the Expressway-E, not the Expressway-C.
    - e. Enabling MRA is exactly the same on both the Expressway-C and the Expressway-E.

11. When nodes are being discovered on the Expressway-C for an MRA deployment, which of the following statements is true?
    - a. The CUCM and CUCM IM and Presence nodes will not show Active until the traversal zones are configured and active.
    - b. The CUCM IM and Presence nodes will not show Active until the traversal zones are configured and active.

   c. The CUCM node will not show Active until the traversal zones are configured and active.

   d. The CUCM and CUCM IM and Presence nodes will show Active immediately after they are discovered.

12. What zone type should be selected on the Cisco Expressway Edge server when setting up the traversal component of the MRA solution?

   a. Traversal client zone

   b. Neighbor zone

   c. Traversal server zone

   d. Unified Communications Traversal

   e. DNS zone

   f. ENUM zone

13. Which of the following must be configured in the Cisco Unified Communications Manager before device onboarding with activation codes over MRA can be used?

   a. OAuth Refresh Login Flow must be enabled.

   b. The _collab_edge SRV records must point to the Expressway Cluster.

   c. Go to **Configuration > Unified Communications > Configuration > MRA Access Control** and set **Authorize by OAuth token with refresh** to **On**.

   d. Go to **Configuration > Unified Communications > Configuration** and set **Allow activation code onboarding** to **Yes**.

Foundation Topics

Requirements for MRA

Cisco Collaboration Mobile and Remote Access (MRA) is a core part of the Cisco Collaboration Edge architecture. MRA allows endpoints, such as Cisco Jabber, UC phones, and CE software-based Telepresence endpoints, to securely utilize registration, call control, provisioning, messaging, and presence services that are provided by Cisco Unified Communications Manager when the endpoint is not within the enterprise network. Cisco Expressway series components are used to provide secure access and firewall traversal to the endpoints that register with the Cisco Unified Communications Manager.

Key Topic

Although the MRA solution operates in a similar fashion to a standard firewall traversal solution for B2B communications, there are some significant differences between them. First, MRA is only supported for SIP; there is no H.323 support in the MRA solution. Second, certificates are required for MRA; there is no way to build the traversal zones with a basic TLS or TCP SIP connection. TLS Verify is required for MRA. Third, some specific settings must be configured to enable MRA on the Expressway servers. Fourth, the zones created between the Cisco Expressway Core and Cisco Expressway Edge servers are not the same traversal client zone and traversal server zone used in a standard firewall traversal solution. Finally, the DNS SRV records that need to be created are different from what is required for a traditional firewall traversal solution.

MRA consists of four main components. One of the components is Firewall Traversal Services. MRA supports internal firewalls between Cisco Expressway Core and Cisco

Expressway Edge, and an external firewall between Cisco Expressway Edge and the Internet. The firewall traversal capabilities of MRA use the same Assent traversal protocol of standard firewall traversal, but traversal chaining is not supported with MRA. Another component is DNS records. Internal and external DNS records are essential to enable endpoints to detect whether they should register directly with Cisco Unified Communications Manager or proxy registration through the MRA deployment. Certificates are another component of MRA. This solution provides secure communication over Transport Layer Security (TLS). Trust between TLS entities is established based on certificates. Implementing the necessary certificates for a public key infrastructure (PKI) is an important part of Cisco Collaboration MRA implementation. The last component in an MRA solution is reverse HTTPS proxy. To support secure data services, such as visual voicemail, contact photo retrieval, Cisco Jabber custom tabs, and so on, a reverse HTTPS proxy runs on the Cisco Expressway Edge server. If these services are not needed in an enterprise deployment of MRA, this component does not need to be set up. Once these components are set up, the MRA deployment can support two main features:

- **Off-Premises Access:** Cisco Collaboration MRA offers a consistent experience to clients, such as Cisco Jabber; UC phones; and Cisco DX, MX, SX, and Webex series endpoints, regardless of whether they are in the internal network or on an external network.
- **Business-to-Business Communications:** Cisco Collaboration Mobile and Remote Access offers secure communication to other businesses.

DNS A-Records and SRV Records

The DNS A-records and SRV records required for an MRA deployment are different from those required for a traditional firewall traversal solution. Additionally, different records need to be configured on an internal DNS and an external DNS. Before deploying an MRA solution, you will need to set up DNS first. Certificates cannot be created until DNS is configured because the PKI certificates depend on the DNS records of the different servers.

Cisco endpoints, especially Jabber, are programmed to use DNS so that they always search for the CUCM SRV record first. If the CUCM cannot be reached, they search for the Expressway-E. The Expressway-E can be located with an SRV lookup whether the endpoint is internal or external to the network, but the endpoint should not search for the Expressway unless it's external to the corporate network. The endpoint should be able to locate the CUCM using an SRV lookup only if the endpoint is located within the corporate network. This is the reason that the endpoint will always search for the CUCM first. If that path fails, there is an alternative path for the endpoint to register through the Expressway servers using MRA.

The external DNS server must be configured with a *_collab-edge._tls.<domain>* service record so that external endpoints can discover that they should use Cisco Expressway-E for Mobile and Remote Access. Service records for secure SIP are also required, not specifically for Mobile and Remote Access, but for deploying a secure SIP service on the Internet. The service records must point to each cluster member of the Cisco Expressway-E server. Table 21-2 provides examples of the service records needed on a public DNS for two Cisco Expressway Edge servers clustered together.

Key Topic

Table 21-2 Public DNS SRV Records for Expressway-E Cluster

Service	Protocol	Domains	Priority	Weight	Port	Target
_Collab-edge.	_tls.	Cisco.com	10	10	8443	Exp-e1.cisco.com
_Collab-edge.	_tls.	Cisco.com	10	10	8443	Exp-e2.cisco.com
_sips.	_tcp.	Cisco.com	10	10	5061	Exp-e1.cisco.com
_sips.	_tcp.	Cisco.com	10	10	5061	Exp-e2.cisco.com

The internal DNS server must be configured with a *_cisco-uds._tcp.<domain>* SRV record so that internal endpoints can discover that they should use Cisco Unified Communications Manager for direct registration. When using Cisco Unified Communications Manager IM and Presence Services, a *_cuplogin._tcp.<domain>* SRV record is also required on the internal DNS server. Just as the public DNS SRV records must refer to the Cisco Expressway-E servers, the internal DNS SRV records must refer to all call processing nodes of a Cisco Unified Communications Manager cluster, as well as with all Cisco Unified Communications Manager IM and Presence server SRV records. The internal DNS records must be available to all internal endpoints and to the Cisco Expressway Core. The Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence server SRV records must not be resolvable from outside the internal network. Otherwise, Cisco endpoints and soft clients will not use the necessary Mobile and Remote Access registration via Cisco Expressway-E. Table 21-3 provides examples of the SRV records needed on a private DNS for two Cisco Unified Communications Managers and two Cisco Unified Communications Manager IM and Presence servers clustered together.

Key Topic

Table 21-3 Private DNS SRV Records for CUCM and CUCM IMP Clusters

Service	Protocol	Domains	Priority	Weight	Port	Target
_cisco-uds.	_tcp.	Cisco.com	10	10	8443	cucm1.cisco.com
_cisco-uds.	_tcp.	Cisco.com	10	10	8443	cucm2.cisco.com
_cuplogin.	_tcp.	Cisco.com	10	10	5061	imp1.cisco.com
_cuplogin.	_tcp.	Cisco.com	10	10	5061	imp2.cisco.com

Firewall Ports and Considerations

Cisco MRA uses a firewall traversal connection to allow inbound and outbound-initiated packet exchange, such as registration and call setup messages. MRA uses the Cisco Expressway Edge as the traversal server that is installed in a demilitarized zone (DMZ), and the Expressway Core is the traversal client that is installed on the internal network. Firewall traversal offers secure communication across firewalls as follows:

Key Topic

1. The Cisco Expressway-C initiates an outbound traversal connection through the internal firewall to specific ports on the Cisco Expressway-E with secure authentication credentials to establish a connection between the two servers.
2. Once the connection has been established, the Cisco Expressway-C sends keepalive packets periodically to Cisco Expressway-E to maintain the connection.
3. When Cisco Expressway-E receives an incoming message, whether it's a registration or call setup message, from an outside endpoint, it sends the request to the Cisco Expressway-C through the existing traversal connection.

4. The Cisco Expressway-C then sends the message, such as a call setup request, to the Cisco Unified Communications Manager.
5. The Cisco Unified Communications Manager processes the call, and media streams are set up over the existing traversal connection.

For communication to flow through the firewall, appropriate ports must be opened to allow the flow of packets. The following ports must be opened on the internal firewall between the Expressway Core and the Expressway Edge:

Key Topic

- **SIP:** TCP 7001
- **Traversal Media:** UDP 36000 to 36001 (for small to medium VM deployments)
- **Extensible Messaging and Presence Protocol (XMPP):** TCP 7400
- **HTTPS (Tunneled over Secure Shell [SSH] between Expressway-C and Expressway-E):** TCP 2222

The following ports must be opened on the external firewall between the public Internet and the Cisco Expressway Edge in the DMZ:

- **SIP:** TCP 5061
- **HTTPS:** TCP 8443
- **XMPP:** TCP 5222
- **TURN Server Control and Media:** UDP 36012 to 59999 (if TURN relays are being used only)

The firewall administrator should open all of the ports from the preceding list before traversal zones are set up between the Expressway-C and the Expressway-E. Certificates must also be set up before traversal zones are created. Whether firewall ports are opened or certificates are established first doesn't matter as long as both tasks are completed before configuring the traversal zones.

Certificate Requirements and Recommendations

Six different certificate pairs can be configured in an MRA deployment. However, only two pairs are required to set up the solution. The other four exist in an ideal environment for absolute security pertaining to registration and calling. The first certificate required is a public or enterprise CA certificate chain used to sign the Expressway-C. This is required to establish the traversal client zone connection. The second certificate required is a public or enterprise CA certificate chain used to sign the Expressway-E. This is also required to establish the traversal server zone connection. Both are absolutely required for TLS Verify to operate successfully. The traversal zones used for an MRA deployment will not work without these two certificate pairs. The root CA certificate for the Expressway-C certificate should be added to both the Expressway-C and the Expressway-E. The root CA certificate for the Expressway-E certificate should be added to both the Expressway-E and the Expressway-C. If both servers were signed by the same CA, then they will use the same root CA certificate; therefore, it needs to be added to each server only once.

The next optional certificate is the Cisco Unified Communications Manager Tomcat certificate or CA chain. The Tomcat certificate is for Tomcat trust. This certificate is used for MRA only when the Expressway-C is configured to use TLS Verify mode on Cisco Unified Communications Manager discovery. The Tomcat CA should be added to the Expressway-C, and the root CA certificate for the Expressway-C should be added to the Cisco Unified Communications Manager. If TLS Verify is not used on the Expressway-C for Cisco Unified Communications Manager discovery, this certificate is not needed.

Another optional certificate is the Cisco Unified Communications Manager certificate or CA chain used when the Cisco Unified Communications Manager is in mixed mode for end-to-end TLS. If this certificate is used, the Cisco Unified Communications Manager CA should be added to the Expressway-C, and the certificate CA for the Expressway-C should be added to the Cisco Unified Communications Manager.

The Cisco Unified Communications Manager IM and Presence Tomcat certificate or CA chain is similar to the Cisco Unified Communications Manager Tomcat certificate or CA chain. This certificate is used only when the Expressway-C is configured to use TLS Verify mode on Cisco Unified Communications Manager IM and Presence discovery. The Tomcat CA should be added to the Expressway-C, and the certificate CA for the Expressway-C should be added to the Cisco Unified Communications Manager IM and Presence server. If TLS Verify is not used on the Expressway-C for Cisco Unified Communications Manager IM and Presence discovery, this certificate is not needed.

The last optional certificate is the Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) certificate. This certificate is used when remote endpoints authenticate using a Locally Significant Certificate (LSC). By default, LSC is signed by the CAPF, so the CAPF is the CA for phones in this scenario. However, when the CAPF is signed by an external CA, then the CAPF in this scenario acts as a subordinate CA or intermediate CA. The difference between a self-signed CAPF and CA-signed CAPF is that the CAPF is the root CA to LSC when doing a self-signed CAPF, but the CAPF is the subordinate or intermediate CA to LSC when doing a CA-signed CAPF. Table 21-4 identifies each of the six certificate pairs used in an MRA deployment.

Key Topic

Table 21-4 Certificate Pairs Used in an MRA Deployment

Certificate Type	Core	Edge	Required
Public or enterprise CA certificate chain used to sign Expressway Core certificate	Yes	Yes	Yes
Public or enterprise CA certificate chain used to sign Expressway Edge certificate	Yes	Yes	Yes
CUCM Tomcat certificates or CA chain	Yes	No	No
CUCM CallManager certificates or CA chain	Yes	No	No
IMP Tomcat certificate or CA chain	Yes	No	No
CUCM CAPF certificates	No	Yes	No

HTTPS Reverse Proxy Settings

The Cisco MRA reverse proxy settings provide a mechanism to support visual voicemail access, contact photo retrieval, Cisco Jabber custom tabs, and other data applications. HTTPS reverse proxy is a function that is provided by the Cisco Expressway-E using port

TCP 8443 for HTTPS traffic. Initial MRA configuration allows inbound authenticated HTTPS requests to the following destinations:

Key Topic

- TCP 6970 (TFTP file download) and TCP 8443 (SOAP API) to all discovered Cisco Unified Communications Manager nodes
- TCP 7400 (XCP router) and TCP 8443 (SOAP API) to all Cisco Unified Communications Manager IM and Presence nodes

Additional hosts can be added to the allow list on the Cisco Expressway-C.

Service Discovery

Before we show how to configure an MRA solution, we should more closely examine the MRA service discovery operation. This discussion will help administrators deploying this solution fully understand the dependencies between the components involved with an MRA solution. Figure 21-1 illustrates the way Cisco MRA service discovery operates on the public network. This example is for a Cisco Jabber client in phone-only mode. Additional steps involving the Cisco Unified Communications Manager IM and Presence Services would need to be included if additional Cisco Jabber services were being utilized.

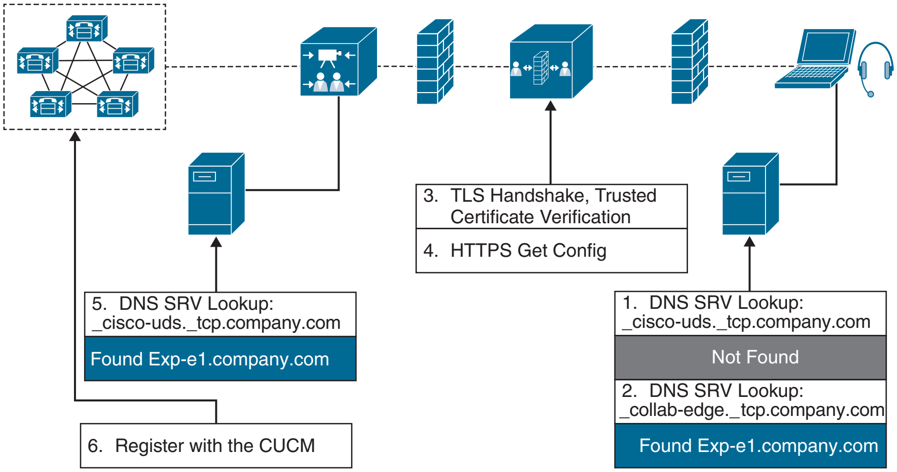

3. TLS Handshake, Trusted Certificate Verification
4. HTTPS Get Config
5. DNS SRV Lookup: _cisco-uds._tcp.company.com
Found Exp-e1.company.com
6. Register with the CUCM
1. DNS SRV Lookup: _cisco-uds._tcp.company.com
Not Found
2. DNS SRV Lookup: _collab-edge._tcp.company.com
Found Exp-e1.company.com

Figure 21-1 *Cisco MRA Service Discovery Operation*

Figure 21-1 assumes that the initiating endpoint, or Jabber client in this case, does not connect to the corporate network over a VPN. This is the reason that the initial DNS SRV lookup for the *_cisco-uds._tcp.domain* record fails. The service discovery occurs as follows. First, a Cisco Jabber client located outside the corporate network, and without a VPN connection, sends a DNS SRV record lookup for *_cisco-uds._tcp.company.com* to a public DNS server. The public enterprise DNS that manages company.com should not have such an SRV record, and therefore, the lookup fails. Next, the Cisco Jabber client sends another DNS SRV record lookup for *_collab-edge._tls.company.com*. This time the lookup is successful, and the address of the Cisco Expressway Edge is provided to the Jabber client in the DNS response.

Now the Cisco Jabber client can start the Mobile and Remote Access negotiation with the Cisco Expressway Edge server. A certificate is presented to Cisco Jabber and may need to be manually trusted by the user if it is not signed by a certificate authority server that the client

PC already trusts. A TLS handshake is exchanged to establish a secure connection. The Cisco Expressway Edge will then act as a proxy for the Cisco Jabber client by passing messages that it receives from Cisco Jabber to Cisco Expressway Core through the firewall traversal connection and return messages from the Expressway Core to the Jabber client.

When a trusted 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 Communications Manager. The Cisco Expressway Core will send a DNS SRV record lookup for *_cisco-uds._tcp.company.com* to the internal DNS. The internal DNS will respond with the address of the Cisco Unified Communications Manager. The Cisco Expressway Core will then forward the registration request from the Cisco Jabber client to the Cisco Unified Communications Manager. The Cisco Expressway Core will act as the proxy for messages between the Cisco Unified Communications Manager and the Expressway Edge.

Cisco Unified Communications Manager Settings for MRA

After an administrator has ensured that all the prerequisite components have been configured, which were covered in the first section of this chapter, the process for configuring MRA in a corporate network begins on the Cisco Unified Communications Manager. The following seven steps must be completed to deploy Mobile and Remote Access endpoints.

Step 1. Make sure that the Cisco AXL Web Service is activated on the publisher node.

- **a.** From Cisco Unified Serviceability, navigate to **Tools > Service Activation**.
- **b.** From the **Server** drop-down menu, select the publisher node and click **Go**.
- **c.** Under the Database and Admin Services section, confirm that the Cisco AXL Web Service is Activated.
- **d.** If the service is not activated, check the corresponding check box and click **Save** to activate the service.

Step 2. Optionally, configure region-specific settings for MRA endpoints. The default settings may be sufficient in many cases, but if you expect MRA endpoints to use video, you may want to increase the Maximum Session Bit Rate for Video Calls within your region configuration. The default setting of 384 kbps may be too low for some video endpoints, such as the DX series.

- **a.** From Cisco Unified CM Administration, navigate to **System > Region Information > Region**.
- **b.** Perform any one of the following:
  - Click **Find** and select a region to edit the bit rates.
  - Click **Add New** to create a new region.
- **c.** In the Modify Relationship to Other Regions section, configure a new setting for the Maximum Session Bit Rate for Video Calls, such as 6000 kbps.
- **d.** Configure other fields in the Region Configuration window as necessary. For more information on the fields and their configuration options, see the system's online help.
- **e.** Click **Save**.

Step 3. After you have created a new region, assign your region to the device pool that your MRA endpoints use.

- **a.** From Cisco Unified CM Administration, navigate to **System > Device Pool.**
- **b.** Do either of the following:
  - Click **Find** and select the existing device pool to edit.
  - Click **Add New** to create a new device pool.
- **c.** Enter a device pool **Name.**
- **d.** Select a redundant Cisco Unified Communications Manager Group.
- **e.** Assign a Date/Time Group. This group includes the Phone NTP references that may have been set up for MRA endpoints.
- **f.** Assign a region from the Region drop-down menu to the device pool that MRA endpoints will use.
- **g.** Complete the remaining fields in the Device Pool Configuration window as necessary. For more information on the fields and their configuration options, see the system's online help.
- **h.** Click **Save.**

Step 4. Use this procedure to set up a Phone Security Profile to be used by MRA endpoints. You must apply this profile to the phone configuration for each of your MRA endpoints.

- **a.** From Cisco Unified CM Administration, navigate to **System > Security > Phone Security Profile.**
- **b.** Click **Add New.**
- **c.** From the Phone Security Profile Type drop-down list, select your device type, such as the Cisco Unified Client Service Framework for a Jabber application.
- **d.** Click **Next.**
- **e.** Enter a Name for the profile. For MRA, the name must be in FQDN format and must include the enterprise domain.
- **f.** From the Device Security Mode drop-down list, select **Encrypted.** This field must be set to Encrypted; otherwise, Expressway will reject the communication.
- **g.** Set the Transport Type to **TLS.**
- **h.** Leave the TFTP Encrypted Config check box unchecked for the following phones because MRA will not work for these phones with this option enabled: DX Series, IP Phone 7800, or IP Phone 8811, 8841, 8845, 8861 and 8865.
- **i.** Complete the remaining fields in the Phone Security Profile Configuration window. For more information on the fields and their configuration options, see the system's online help.
- **j.** Click **Save.**

Step 5. This step is for Cisco Jabber only. Set up an MRA Access Policy for Cisco Jabber users. Cisco Jabber users must be enabled with MRA access within their user profiles in order to use the MRA feature. The Jabber desktop client includes Cisco Jabber for Windows users and Cisco Jabber for Mac users. The Jabber mobile client includes Cisco Jabber for iPad and iPhone users and Cisco Jabber for Android users.

a. In Cisco Unified CM Administration, navigate to **User Management > User Settings > User Profile**.

b. Click **Add New**.

c. Enter a Name and Description for the user profile.

d. Assign a Universal Device Template to apply to users' Desk Phones, Mobile and Desktop Devices, and Remote Destination/Device Profiles.

e. Assign a Universal Line Template to apply to the phone lines for users in this user profile.

f. If you want the users in this user profile to be able to use the self-provisioning feature to provision their own phones, do the following:

- Check the **Allow End User to Provision Their Own Phones** check box.
- In the Limit Provisioning Once End User Has This Many Phones field, enter a maximum number of phones the user is allowed to provision. The maximum is 20.

g. If you want Cisco Jabber users associated with this user profile to be able to use the Mobile and Remote Access feature, check the **Enable Mobile and Remote Access** check box. By default, this check box is selected. When you uncheck this check box, the Jabber Policies section is disabled, and the No Service Client Policy option is selected by default. This setting is mandatory only for Cisco Jabber users. Non-Jabber users do not need this setting to be able to use MRA.

h. Assign the Jabber policies for this user profile. From the Jabber Desktop Client Policy and Jabber Mobile Client Policy drop-down list, choose one of the following options:

- **No Service:** This policy disables access to all Cisco Jabber services.
- **IM & Presence Only:** This policy enables only instant messaging and presence capabilities.
- **IM & Presence, Voice and Video Calls:** This policy enables instant messaging, presence, voicemail, and conferencing capabilities for all users with audio or video devices. This is the default option.

i. Click **Save**.

Step 6. This step is also for Cisco Jabber users only. The user policy that was set up previously must be applied to the appropriate end user. Remember from Chapter 16, "LDAP Integration with Cisco Unified Communications Manager," and Chapter 17, "Registering SIP Endpoints to the Cisco Unified Communications Manager," that end users can be set up manually, from an import using LDAP or using BAT. Because each method was covered in these chapters, we will not cover the steps to apply the user policy to the end user at this point in the book. Refer to these other chapters if a review is necessary.

Step 7. Configure and provision endpoints that will use the MRA feature. This step is achieved by ensuring the corresponding settings above are applied to the phone through TFTP when registration is attempted. Refer to Chapter 7, "Cisco Unified Communications Phones," Chapter 8, "Cisco Telepresence Endpoints," and Chapter 9, "Endpoint Registration," for a review in configuring endpoints registering to the Cisco Unified Communications Manager.

High volumes of Mobile and Remote Access calls may trigger denial of service thresholds on the Cisco Unified Communications Manager. The reason is that all the calls arriving at the Cisco Unified Communications Manager are from the same Expressway-C cluster. If necessary, Cisco recommends that you increase the level of the SIP Station TCP Port Throttle Threshold to 750 kbps. To make this change from Cisco Unified CM Administration, navigate to **System > Service Parameters**, and select the Cisco CallManager service.

Key Topic

Another requirement on the Cisco Unified Communications Manager must be configured before MRA is set up on the Expressway Core. An application user must be configured on the Cisco Unified Communications Manager that has been assigned the *AXL API Access* role. The Cisco Expressway Core will need this level of access into the Cisco Unified Communications Manager; otherwise, communication will fail. The default administrator account can be used, but Cisco recommends a new application user account be created for each application service that's set up with the Cisco Unified Communications Manager. The same is also true for MRA deployments that include the Cisco Unified Communications Manager IM and Presence services. The corresponding IM and Presence user must have the *Standard AXL API Access* role assigned.

TLS Verify Requirements

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both frequently referred to as "SSL," are cryptographic protocols that provide communications security over a computer network. This TCP protocol aims primarily to provide privacy and data integrity between two communicating hosts or applications.

Client/server applications such as web browsers, email, and VoIP commonly use the TLS protocol to prevent eavesdropping and tampering of information. The protocols these applications use must choose to use or not to use TLS. The easiest way to segregate the information is to use different port numbers for unencrypted traffic, such as port 80 for HTTP, and TLS-encrypted traffic, such as port 443 for HTTPS. The connection is secure because symmetric cryptography is used to encrypt the transmitted data. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiation at the start of the session. The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. Identification is usually in the form of digital "certificates" that contain the server name, the trusted certificate authority (CA), and the server's public encryption key. The identity of the communicating parties can be authenticated using this public-key cryptography (asymmetric cryptography) to ensure only the intended recipient can decrypt the traffic. The negotiation of a shared secret is both secure and reliable against eavesdroppers and attacks, including man-in-the-middle attacks. The connection ensures integrity because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

Once the client and server have agreed to use TLS, they negotiate a stateful connection by using a handshake procedure. The handshake begins when a client connects to a TLS-enabled server requesting a secure connection and presents a list of supported ciphers and hash functions. From this list, the server picks a cipher and hash function that it also supports, and it informs the client of the decision. The server then identifies itself with its digital certificate, which can contain the server name, the trusted certificate authority, and the server's public encryption key. The client then validates the certificate before proceeding. Public-key encryption is used to share the pre-master secret via the use of RSA or Diffie-Hellman key exchange. This process generates a random and unique session key for encryption and decryption that has the additional property of forward secrecy, which protects past sessions against future compromises of secret keys or passwords.

Remember that the server is validated because the client initiates the secure connection. The client side confirms that the server is who it claims to be and whether it can be trusted with the use of certificates. The client receives the digital certificate from the server side of the TLS negotiation, but the identity must be verified before proceeding. The server certificate may contain the name of the certificate holder. This name is checked against the Common Name (CN) or the Subject Alternative Name (SAN). Also, additional information like a serial number, expiration dates, revocation status, a copy of the certificate holder's public key (which is used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority. This information identifies to the client that the certificate is signed by a certificate authority. If you trust this certificate authority, you can verify using the CA's public key that it really did sign the server's certificate. To sign a certificate yourself, you need the private key, which is only known to the CA of your choice. This way an attacker cannot sign a certificate himself and falsely claim to be the server. When the certificate has been modified, the sign will be incorrect, and the client will reject it. Figure 21-2 illustrates the steps involved with a security handshake between a client and a server.

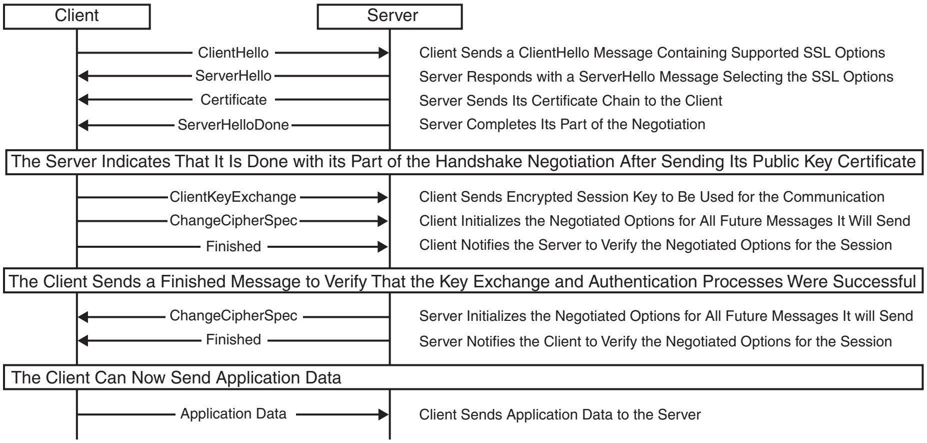

Client
Server
ClientHello
Client Sends a ClientHello Message Containing Supported SSL Options
ServerHello
Server Responds with a ServerHello Message Selecting the SSL Options
Certificate
Server Sends Its Certificate Chain to the Client
ServerHelloDone
Server Completes Its Part of the Negotiation
The Server Indicates That It Is Done with its Part of the Handshake Negotiation After Sending Its Public Key Certificate
ClientKeyExchange
Client Sends Encrypted Session Key to Be Used for the Communication
ChangeCipherSpec
Client Initializes the Negotiated Options for All Future Messages It Will Send
Finished
Client Notifies the Server to Verify the Negotiated Options for the Session
The Client Sends a Finished Message to Verify That the Key Exchange and Authentication Processes Were Successful
ChangeCipherSpec
Server Initializes the Negotiated Options for All Future Messages It will Send
Finished
Server Notifies the Client to Verify the Negotiated Options for the Session
The Client Can Now Send Application Data
Application Data
Client Sends Application Data to the Server

Figure 21-2 *TLS Security Handshake Between a Client and Server*

Mutual TLS authentication is also an option that can be chosen. In this type of authentication, both parties authenticate each other through verifying the provided digital certificate so that both parties are assured of the others' identity. Mutual TLS is very similar to the normal process of the client handling the verification of the server's certification but including the additional step of the client providing a certificate. This process allows the server side to authenticate the client, allowing both parties to trust each other.

Server-to-server connections rely on mutual TLS for mutual authentication. In the Cisco Collaboration infrastructure, some examples would be a secure connection between endpoints and the Cisco Unified Communications Manager, Cisco Unified Communications Manager SIP trunks to other clusters, and even Cisco Unified Communications Manager SIP trunks with a Cisco Expressway Core.

To secure voice and video traffic, you must understand multiple technologies. Remember, the most common VoIP communication used today is SIP. For secure transmissions of SIP messages, the protocol may be encrypted with TLS. Media identification and negotiation are achieved with the Session Description Protocol (SDP). SDP can also be used for the master key exchange. For the transmission of media streams, SIP employs the Real-time Transport Protocol (RTP) or Secure Real-time Transport Protocol (SRTP). Unencrypted SIP generally uses port 5060, whereas TLS-encrypted SIP utilizes port 5061.

Trusted certificates are very important to create secure connections. This part of the process is where the certificate authority comes into the solution. These certificate authorities are widely used both on the public Internet and private networks to issue digital certificates containing identity credentials binding them to SSL or TLS cryptography keys. However, because these CAs are trust anchors, they must conduct several checks into the identity of the applicant. The checks correlate to the class and type of certificate being applied for. Table 21-5 identifies each of these classes of certificates available and which of these certificates are supported on Cisco Collaboration servers.

Key Topic

Table 21-5 Classes of Certificates on Cisco Collaboration Servers

Options	Types			Support Info
	DV	OV	EV	
Single Host/Domain	Yes	Yes	Yes	Supported on all Cisco Collaboration servers
UCC/Multiple SAN/Cert	Yes	Yes	Yes	Supported on all Cisco Collaboration servers
Multiple Subdomain Wildcard Cert	Yes	Yes	No	Not supported at all on Cisco Expressways

For domain validation (DV) certificates, the CA checks only the right of the applicant to use a specific domain name. No company identity information is vetted, and no information is displayed other than encryption information within the Secure Site Seal. For organization validation (OV) certificates, the CA checks the right of the applicant to use a specific domain name and conducts some vetting of the organization. Additional vetted company information is displayed to customers when clicking the Secure Site Seal, giving enhanced visibility into who is behind the site and associated enhanced trust. For extended validation (EV) certificates, the certificate authority checks the right of the applicant to use a specific domain name, and in addition, it conducts a thorough vetting of the organization. The issuance process of EV certificates is strictly defined in the EV guidelines, as formally ratified by the CA/Browser Forum in 2007, that specify all the steps that are required for a CA before issuing a certificate. They include

- Verifying the legal, physical, and operational existence of the entity
- Verifying that the identity of the entity matches official records

- Verifying that the entity has exclusive rights to use the domain that is specified in the EV SSL certificate
- Verifying that the entity has properly authorized the issuance of the EV SSL certificate

EV certificates are available for all types of businesses, including government entities and both incorporated and unincorporated businesses. A second set of guidelines, the EV Audit Guidelines, specify the criteria under which a CA needs to be successfully audited before issuing EV certificates. The audits are repeated yearly to ensure the integrity of the issuance process.

Because people are constantly searching the Internet, the browsers constantly are checking the websites that are visited against a CA to authenticate web pages. As an example, web browsers like Google Chrome, Firefox, and Internet Explorer maintain lists of certificate authorities they consider trustworthy. When you access what should be a secure website, the site presents its security certificate to your browser. If the certificate is up-to-date and from a trusted certificate authority, you will see the trusted secure connection. If the certificate lacks any of the requirements, you will see that your web browser will not establish a connection until you accept the risks and proceed.

With the Cisco Collaboration products, only certain certificate options are supported. The Expressway-E will require a public certificate because it is the most public-facing part of the Cisco Collaboration solution and needs to be trusted by outside sources like clients and other businesses. A single host/domain certificate option will suffice with any type of validation desired. If multiple hosts, domains, or subdomains need to be covered, multiple Subject Alternative Name (SAN) certificates are required. Note that the wildcard certification is not supported on the Cisco Expressway series.

In the Cisco Collaboration architecture, it is easy to secure all enterprise network information simply by creating a private network behind the security of a firewall. However, companies may need to work with other businesses or clients for their day-to-day operations. To place voice and video calls outside the network and connect to other networks securely, Cisco offers the Expressway Series. This robust and secure solution comes equipped with Cisco's proprietary Assent protocol that allows secure firewall-traversal technology for any-to-any collaboration.

Cisco Expressway Certificates

Best practice for setting up the Expressway Series begins with the Expressway Edge, which is usually placed in between two firewalls in a separate network from the private enterprise network and the public outside network. This subnetwork is known as a demilitarized zone (DMZ). First, you can add authentication credentials and build a traversal server zone on the Expressway Edge. All zones also require search rules that will determine when and how they are searched. Next, you can configure the Expressway Core to use a traversal client zone. This zone initiates a secure traversal connection through the firewall on a specific keepalive port and authenticates against the authentication database configured on the Expressway Edge. Once a connection is established, the Expressway Core preserves the connection by continuously sending UDP keepalive packets over that same port to the Expressway Edge. This allows endpoints to both place calls out of the network and receive incoming calls as well. When a call comes into the network, the call setup is forwarded from the Expressway Edge to the Expressway Core and ultimately to the Cisco Unified Communications Manager to search for a user or endpoint. Once call setup has completed, both the call signaling and media will securely traverse through the firewall using the traversal zones previously created.

The process described here can use a standard TLS verification, which uses a single self-signed certificate on the Expressway Edge, or it can use the more secure TLS Verify mode where both Expressways have to validate each other's certificates. The TLS Verify mode can be set to enabled or disabled on the Zone settings page, which will decide which mode is used. When the zone is configured with the TLS Verify mode set to OFF, the Expressway Edge declines to verify the host name and signature of a certificate from the Expressway Core. The Expressway Core still verifies the certificate of the Expressway Edge's self-signed certificate, but this certificate does not use domain verification; therefore, this configuration also allows for the use of IP addresses for the peers. With TLS Verify mode set to ON, Mutual TLS (MTLS) is activated, and both client and server will match the CN or SAN against the peer address.

When using the TLS Verify mode in the ON configuration on an Expressway-E, the CA and SAN must match the TLS Verify Subject Name field in the zone configuration. As a result, this configuration is commonly used in closed or federated systems. For open B2B searches to other nonfederated enterprises, TLS Verify mode on the Expressway-E needs to be in the OFF mode. When you are setting up traversal zones for MRA, TLS Verify mode is required to be turned ON. MRA will not work if TLS Verify mode is set to OFF.

Cisco Unified Communications Manager Certificates

Two Cisco Unified Communications Manager certificates are significant for Mobile and Remote Access. They are the CallManager certificate and the Tomcat certificate. These certificates are automatically installed on the Cisco Unified Communications Manager, and by default, they are self-signed and have the same Common Name (CN). Cisco recommends using CA-signed certificates. However, if self-signed certificates are used, the two certificates must have different Common Names. The Expressway does not allow two self-signed certificates with the same CN. If the CallManager and Tomcat self-signed certificates have the same CN in the Expressway's trusted CA list, the Expressway can trust only one of them. This means that either secure HTTP or secure SIP between Expressway-C and Cisco Unified Communications Manager will fail.

Two IM and Presence Service certificates are significant if you use XMPP. They are the cup-xmpp certificate and tomcat certificate. Cisco recommends using CA-signed certificates. However, if self-signed certificates are used, these two certificates must also have different Common Names. The Expressway does not allow two self-signed certificates with the same CN. If the cup-xmpp and tomcat (self-signed) certificates have the same CN, Expressway trusts only one of them, and some TLS attempts between Cisco Expressway-E and IM and Presence Service servers will fail.

Although Expressway certificates were discussed in the previous section, some important settings on the Cisco Unified Communications Manager can affect how the Expressway Core certificates are set up. The Expressway Core server certificate needs to include the following elements in its list of subject alternate names:

- **Unified CM Phone Security Profile Names:** The names of the phone security profiles in the Cisco Unified Communications Manager that are configured for encrypted TLS and are used for devices requiring remote access. Use the FQDN format and separate multiple entries with commas. Having the secure phone profiles as alternative names means that the Cisco Unified Communications Manager can communicate via TLS with the Expressway-C when it is forwarding messages from devices that use those profiles.

- **IM and Presence Chat Node Aliases (Federated Group Chat):** The chat node aliases that are configured on the IM and Presence Service servers. These are required only for Unified Communications XMPP federation deployments that intend to support group chat over TLS with federated contacts. The Expressway-C automatically includes the chat node aliases in the CSR, providing it has discovered a set of IM and Presence Service servers. Cisco recommends using DNS format for the chat node aliases when generating the CSR. The same chat node aliases must be used in the Expressway Edge server certificate's alternative names (SANs).

The Expressway Edge server certificate needs to include the following elements in its list of Subject Alternative Names (SANs):

- **Cisco Unified Communications Manager Registrations Domains:** All of the domains that are configured on the Expressway Core for Cisco Unified Communications Manager registrations. Required for secure communications between endpoint devices and the Expressway Edge.
- **XMPP Federation Domains:** The domains used for point-to-point XMPP federation. These are configured on the IM and Presence Service servers and should also be configured on the Expressway-C as domains for XMPP federation. Select the DNS format and manually specify the required FQDNs. Separate the FQDNs with commas if you need multiple domains. Do not use the XMPPAddress format because your CA may not support it, and it may be discontinued in future versions of the Expressway software.
- **IM and Presence Chat Node Aliases (Federated Group Chat):** The same set of chat node aliases as entered on the Expressway-C's certificate. They are required only for voice and presence deployments that will support group chat over TLS with federated contacts. Note that you can copy the list of chat node aliases from the equivalent Generate CSR page on the Expressway-C.

The Cisco Unified Communications Manager registration domains used in the Expressway configuration and Expressway-E certificate are used by Mobile and Remote Access clients to look up the *_collab-edge* DNS SRV record during service discovery. They enable MRA registrations on the Cisco Unified Communications Manager and are primarily for service discovery. These service discovery domains may or may not match the SIP registration domains. It depends on the deployment, and they don't have to match. One example is a deployment that uses a *.local* or similar private domain with Cisco Unified Communications Manager on the internal network, and public domain names for the Expressway-E FQDN and service discovery. In this case, you need to include the public domain names in the Expressway-E certificate as SANs. There is no need to include the private domain names used on the Cisco Unified Communications Manager. Only the edge domain needs to be listed as a SAN. Select the DNS format and manually specify the required FQDNs. Separate the FQDNs with commas if you need multiple domains. You may select *CollabEdgeDNS* format instead, which simply adds the prefix *collab-edge* to the domain that you enter. This format is recommended if you do not want to include your top-level domain as a SAN.

Creating Certificates for MRA

The Cisco Unified Communications Manager does not require an MTLS connection to the Expressway Core for the MRA deployment; therefore, this section will cover only the detailed steps on how to sign and load certificates on the Expressway Core and Edge servers. Once all

MRA settings have been configured on the Expressway-C, traversal zones can be configured between the Expressway-E and the Expressway-C. TLS Verify is required for these zones, so certificates must be used. If the certificates come from the same CA, the root CA will be the same on both Expressway servers. However, if a different CA is used for the Expressway Core than what is used on the Expressway Edge, the root CA certificate must be uploaded to both Expressways to identify where the certificates were signed. Information required when signing certificates is the same regardless of the CA being used. The instructions provided in this book on how to sign certificates are through a Microsoft certificate server.

The Expressway-C and Expressway-E have a tool built into them that can generate a certificate signing request (CSR). The CSR contains all the information the CA will need to sign the certificate. When the CA signs the certificate, it's important that it is done with a template that contains the server and client authentication extensions. The certificate generation process seems to confuse a lot of customers and engineers. The basic requirement to get this set up is fairly straightforward. The first consideration is what to use for a CA. There are two commonly used approaches. One method is to use OpenSSL, and the other is to use Active Directory Certificate Services (ADCS). Setting up ADCS in a Microsoft environment is very complex and would warrant discussion that goes beyond the scope of this book. The OpenSSL method is well defined in the *VCS Certificate Creation and Use Deployment Guide*; therefore, this section will focus only on how to use an ADCS after it has already been configured on a Windows server.

Step 1. On the Expressway, generate a certificate signing request (CSR). For the most part, the following steps pertain to both the Expressway-C and Expressway-E servers.

a. On the Expressway, navigate to **Maintenance > Security > Server Certificate.**

b. Click **Generate CSR** to access the Generate CSR page.

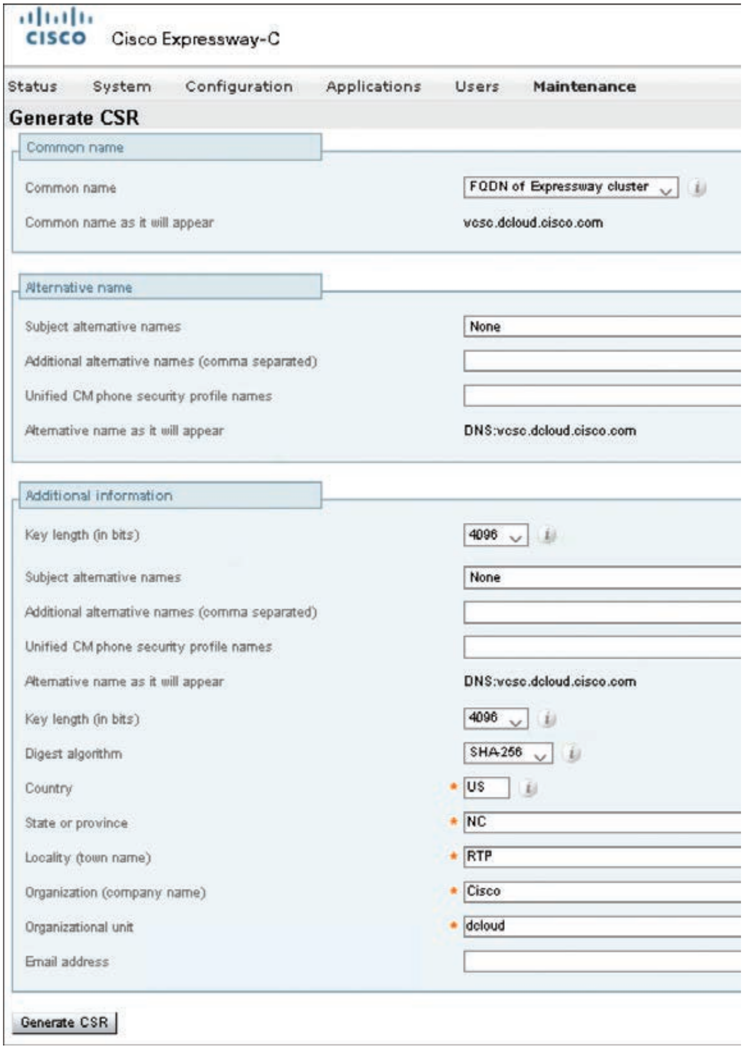
c. Fill out the appropriate details, and then click the **Generate CSR** button:

- **Key Length:** (Recommended to use 2048 or higher)
- **Country:** (Optional) Abbreviations OK
- **State or Province:** (Optional) Abbreviations OK
- **Locality (Town Name):** (Optional)
- **Organization (Company Name):** (Optional)
- **Organization Unit:** (Optional)

Key Topic

Make a note of the Common Name that is autopopulated on the Generate CSR page. This is automatically created using the DNS settings, so the DNS settings on the Expressway must be accurate. The Common Name on the Expressway-C will be used as the Subject Name when the traversal zone is configured on the Expressway-E. The Common Name on the Expressway-E will be used as the Peer address when the traversal zone is configured on the Expressway-C. There are a few points of interest for the Expressway-C certificate. If the IM and Presence Service has already been added to the Expressway-C, a prepopulated Chat Node Alias will appear. This is required for XMPP federation deployments that intend to use both TLS and group chat, such as *conference-2-StandAlone-Cluster5ad9a.%yourdomain%*. Also, if the solution is being deployed using TLS between the Expressway-C and Cisco Unified Communications Manager, ensure that the Subject Alternative Name on the certificate contains the names in FQDN format of all the phone security profiles in the Cisco Unified Communications Manager that are configured for encrypted TLS, such as *CSFJabber.tftp.com*.

d. Under the Certificate Signing Request section, click **Show (PEM file)**. Copy the entire contents of the PEM file to a notepad. Be sure to include the -----Begin Certificate Request----- and -----End Certificate Request----- lines. The contents of this PEM file will be used to sign the Expressway-C certificate using Microsoft ADCS. Figure 21-3 illustrates the settings that need to be configured when generating a CSR.



Common name

Common name	FQDN of Expressway cluster
Common name as it will appear	vcsc.dcloud.cisco.com

Alternative name

Subject alternative names	None
Additional alternative names (comma separated)	
Unified CM phone security profile names	
Alternative name as it will appear	DNS:vcsc.dcloud.cisco.com

Additional information

Key length (in bits)	4096
Subject alternative names	None
Additional alternative names (comma separated)	
Unified CM phone security profile names	
Alternative name as it will appear	DNS:vcsc.dcloud.cisco.com
Key length (in bits)	4096
Digest algorithm	SHA-256
Country	* US
State or province	* NC
Locality (town name)	* RTP
Organization (company name)	* Cisco
Organizational unit	* dcloud
Email address	

Figure 21-3 *Generate CSR Page in an Expressway Server*

Step 2. Sign the CSR with the Microsoft ADCS.

a. Browse to the ADCS web interface at **https://***<IP_address>***/certsrv**.

b. Log in and select **Request a Certificate**.

c. Click the **Submit a Certificate Request by Using a Base-64-Encoded CMC or PKCS #10 File**, or **Submit a Renewal Request by Using a Base-64-Encoded PKCS #7 File** option.

d. Paste the copied contents from the Expressway-C Server PEM file into the Base-64-Encoded Certificate Request box.

e. Some ADCS servers have a Certificate Template field. If this option is available, choose the most appropriate one for your certificate purpose, and then click **Submit**.

Key Topic

f. The next page that appears will allow you to download the signed certificate in either a DER-encoded or Base64-encoded format. DER stands for Distinguished Encoding Rules, which is a binary format. Base64 is an encoding method that converts binary to plain ASCII text. Some scenarios prevent copying and transferring data in binary, so plain text is needed. Therefore, it is recommended to choose the **Base 64 Encoded** option before downloading the certificate.

Key Topic

g. After the signed certificate has been downloaded, a copy of the root CA certificate will need to be downloaded as well. The root CA certificate establishes a trusted chain that begins at the root CA, or in this case the ADCS, through the root CA certificate, and ends at the certificate that was signed. The use of the root CA certificate provides an added level of security. From the ADCS page, click **Home** in the top-right corner of the screen.

h. Click the **Download a CA Certificate, Certificate Chain or CRL** link.

i. Select the **Base 64** radio button and click **Download CA Certificate**.

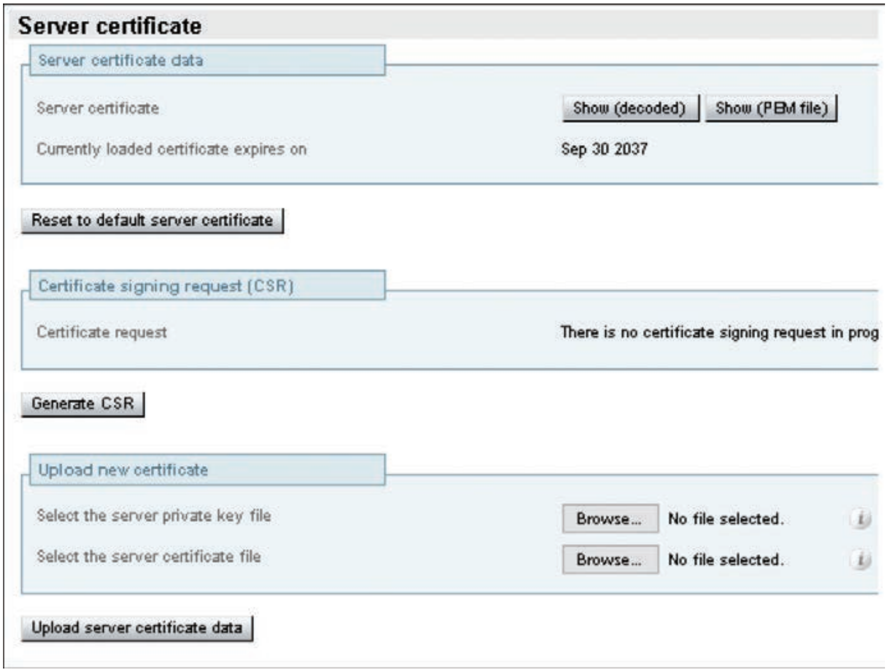
j. When prompted, save the certificate into the same location as the signed server certificate.

Step 3. After both certificates have been obtained, return to the Expressway and apply the certificates.

a. Navigate to **Maintenance > Security > Server Certificate**. This is the same page where the CSR request was generated.

b. Scroll to the bottom of the page, select **Browse**, and choose the server certificate that was just signed by ADCS.

c. Click **Upload Server Certificate Data**. Depending on what version of Expressway is being used, the web browser may prompt the administrator to reauthenticate again. A restart may also be required to complete the certificate installation. If so, do not restart the Expressway until the root CA has been installed. Figure 21-4 illustrates the Server Certificate page on an Expressway-C.



Server certificate

Server certificate data

Server certificate — Show (decoded) | Show (PEM file)

Currently loaded certificate expires on — Sep 30 2037

Reset to default server certificate

Certificate signing request (CSR)

Certificate request — There is no certificate signing request in prog

Generate CSR

Upload new certificate

Select the server private key file — Browse... No file selected.

Select the server certificate file — Browse... No file selected.

Upload server certificate data

Figure 21-4 *Expressway-C Server Certificate Page*

d. Navigate to **Maintenance > Security > Trusted CA Certificate.**

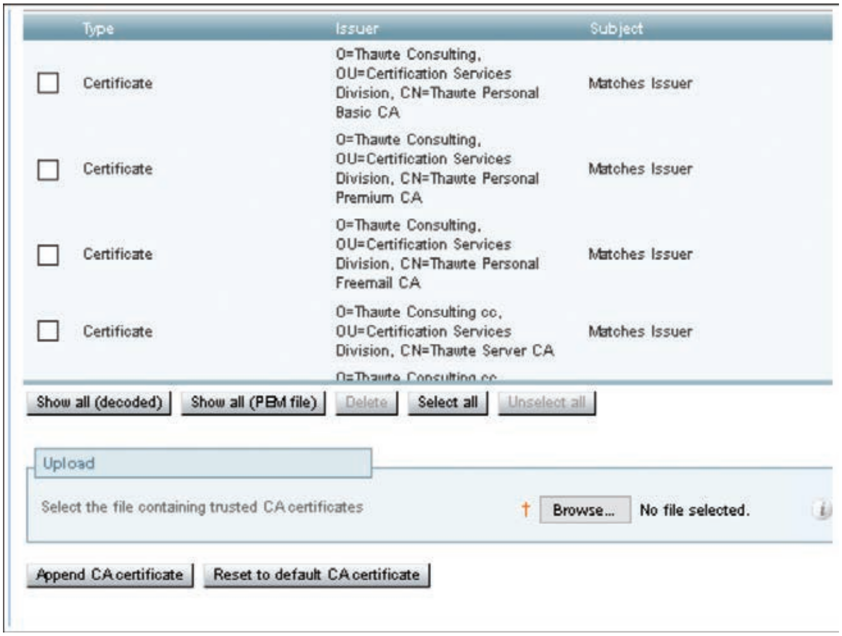
e. Select **Browse** and choose the root CA certificate that was downloaded from ADCS.

f. Click the **Append CA Certificate** button. A restart of the server may be required.

g. Navigate to **Maintenance > Restart Options** and click **Restart**. When prompted to confirm, click **OK**. The restart will take two to three minutes on the Expressways. Figure 21-5 illustrates the Trusted CA Certificate page.

Key Topic

Now you need to repeat all these steps on the other Expressway. There are some points of interest for the Expressway-E certificate. If multiple domains are being used, be sure that each domain configured for the Cisco Unified Communications Manager is a part of the Subject Alternative Name on the certificate. As with the Expressway-C certificate, if you are deploying the solution with XMPP federation, the same chat node aliases will be required. For successful validation of received certificates, the Cisco Expressway servers must trust the CA that issued certificates and will be exchanged during the TLS handshake. Therefore, if a different CA was used for the Expressway Core and Expressway Edge, the root CA certificate must be added to the counterpart server. For example, if an ADCS was used to sign the Expressway-C CSR, and a public CA was used to sign the Expressway-E CSR, the public root CA certificate will need to be loaded on both servers, as well as the ADCS root CA certificate.



	Type	Issuer	Subject
□	Certificate	O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Basic CA	Matches Issuer
□	Certificate	O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Premium CA	Matches Issuer
□	Certificate	O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Freemail CA	Matches Issuer
□	Certificate	O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA	Matches Issuer
		O=Thawte Consulting cc	

Select the file containing trusted CA certificates † Browse... No file selected.

Figure 21-5 *Expressway-C Trusted CA Certificate Page*

Initializing MRA on Expressway Servers

Before configuring a Cisco MRA solution, make sure certain settings are already configured within the Collaboration environment. All endpoints being used with the MRA solution need to be running a version of software that supports this feature. Cisco Jabber 9.7 or later must be used. Starting with this version, Cisco Collaboration Mobile and Remote Access functionality is enabled by default, and the client can identify that it must connect through Cisco Expressway Edge when there is no response to the *_cisco-uds._tcp.<domain>* DNS SRV record lookup request. Administrators should also ensure that the local DNS and public DNS servers are configured with the required SRV records for MRA functionality. The *_cisco-uds._tcp.<domain>* and *_cuplogin._tcp.<domain>* SRV records must not be resolvable from outside the internal network. The Cisco Expressway-C and Cisco Expressway-E should be configured with initial configurations, such as system name, DNS, and NTP at a minimum. Cisco Unified Communications Manager should be configured to allow registrations from Cisco Jabber clients.

Most of the configuration steps to deploy an MRA solution are performed on the Cisco Expressway Core and Cisco Expressway Edge servers. The Cisco Unified Communications Manager Tomcat certificate that must be installed on the Cisco Expressway Core must be obtained from the Cisco Unified Communications Manager server or servers. These certificates are required only if MTLS is being used between the Expressway Core and the Cisco Unified Communications Manager. The following is an overview of the steps to configure MRA on the Expressway servers:

Key Topic

Step 1. Enable MRA on both Cisco Expressways (Core and Edge).

Step 2. Configure MRA on the Cisco Expressway Core.

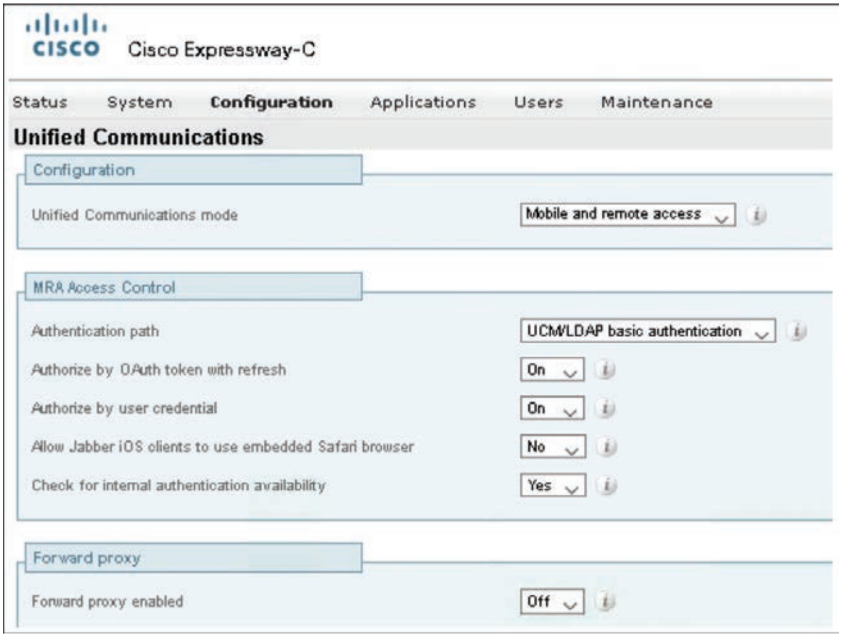
a. Configure a SIP domain to route registrations to the Cisco Unified Communications Manager.

- **b.** Install the Cisco Unified Communications Manager Tomcat certificate (if TLS Verify is being used).
- **c.** Discover the Cisco Unified Communications Manager from the Expressway Core.

Step 3. Configure a secure traversal zone connection between the Cisco Expressway Edge and the Cisco Expressway Core.

- **a.** Generate a CSR on both Expressways.
- **b.** Sign both CSRs.
- **c.** Install the signed CA and root CA on each respective Cisco Expressway (Core and Edge).
- **d.** Configure a Unified Communications Traversal (Server) Zone on the Expressway Edge.
- **e.** Configure a Unified Communications Traversal (Client) Zone on the Expressway Core.

To enable the Cisco Collaboration Mobile and Remote Access on the Expressway-C, navigate to **Configuration > Unified Communications > Configuration**. Change the Unified Communications Mode to Mobile and Remote Access. All other settings can be left as their defaults. Click Save when finished. On the Expressway-E, the menu path is the same to enable MRA, but the menu options are slightly different. Change the Unified Communications Mode to Mobile and Remote Access and leave all other settings as their defaults. Figure 21-6 illustrates some of the settings available when MRA is enabled on the Expressway-C. Figure 21-7 illustrates the settings available when MRA is enabled on the Expressway-E. Use these figures to compare and contrast the differences between the settings.



Unified Communications

Configuration

Unified Communications mode: Mobile and remote access

MRA Access Control

Authentication path: UCM/LDAP basic authentication

Authorize by OAuth token with refresh: On

Authorize by user credential: On

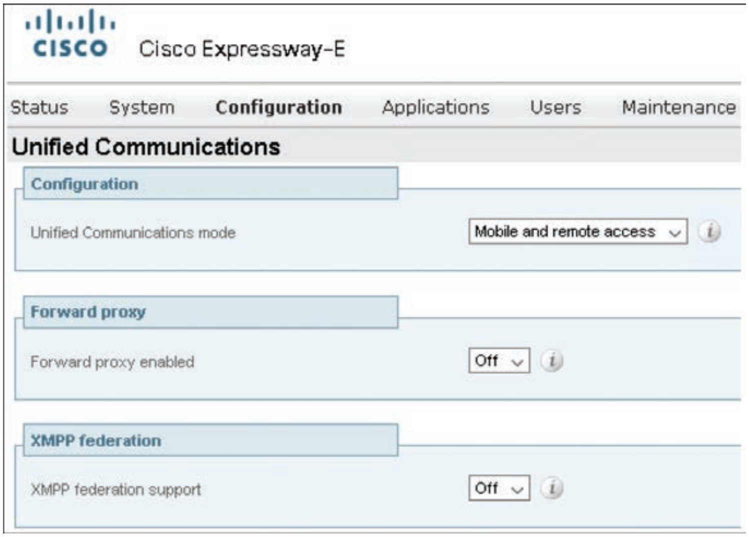
Allow Jabber iOS clients to use embedded Safari browser: No

Check for internal authentication availability: Yes

Forward proxy

Forward proxy enabled: Off

Figure 21-6 *Settings Used to Enable MRA on the Expressway-C*



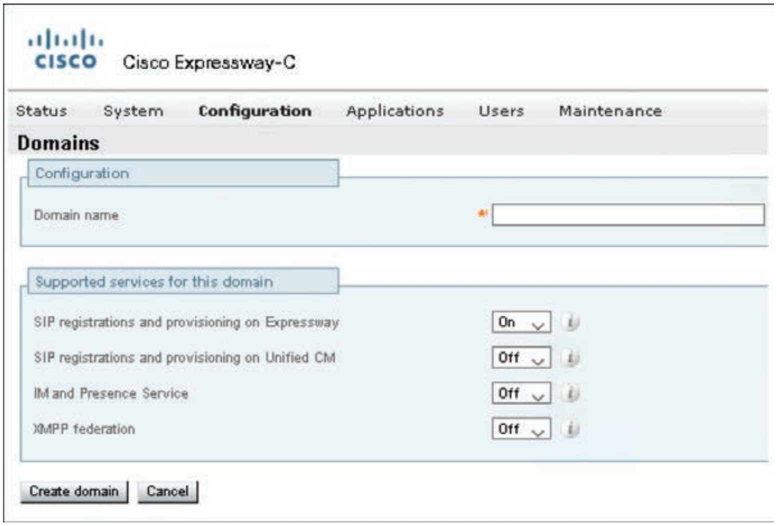
Unified Communications mode: Mobile and remote access

Forward proxy enabled: Off

XMPP federation support: Off

Figure 21-7 *Settings Used to Enable MRA on the Expressway-E*

No more MRA-specific settings have to be configured on the Expressway-E. However, several settings need to be configured on the Expressway-C. First, navigate to **Configuration > Domains**. If a domain was configured previously, an administrator can click that domain to edit the settings. If not, you will need to create a new domain by clicking the New button. When MRA is not in use, there is only one field to configure in the Domains menu; that is the domain itself. When MRA is enabled, several settings will need to be configured. First, configure the domain in the Domain Name field. In the next section, an administrator will need to enable all the services for this domain that will need to be supported using MRA. The options include SIP Registrations and Provisioning on Expressway, SIP Registrations and Provisioning on Unified CM, IM and Presence Service, and XMPP Federation. Figure 21-8 illustrates the DNS settings related to MRA on the Expressway-C.



Domain name: *

SIP registrations and provisioning on Expressway: On

SIP registrations and provisioning on Unified CM: Off

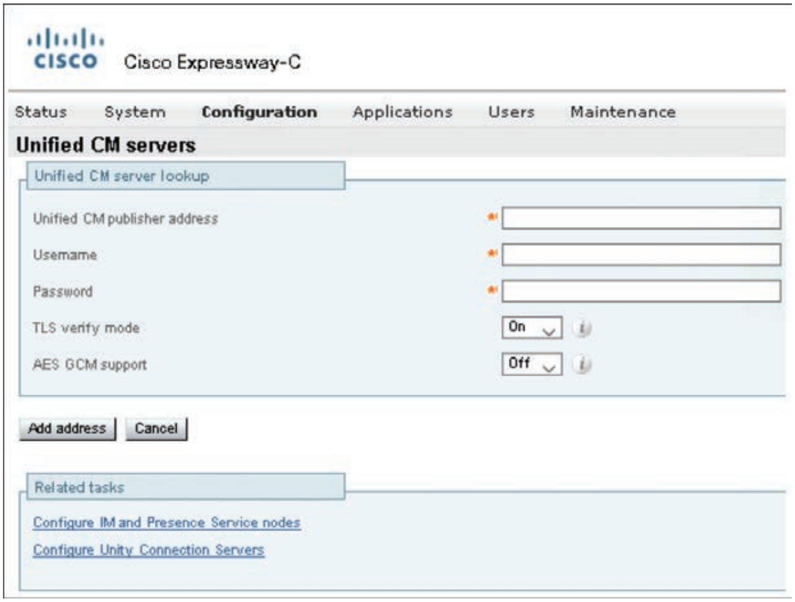
IM and Presence Service: Off

XMPP federation: Off

Figure 21-8 *DNS Settings on Expressway-C for MRA*

Before adding any servers to the Expressway-C, such as the Cisco Unified Communications Manager, you will need to add the Tomcat certificate first. This certificate needs to be added only if TLS Verify is being used for communication between the Cisco Unified Communications Manager and the Expressway-C. Navigate to **Maintenance > Security > Trusted CA Certificate.** Under the Upload section, click Browse and select the Tomcat certificate that's intended for this server. Click Open to return to the Trusted CA Certificate page and click the Append CA certificate button to load the certificates. Check the list of certificates to ensure the Tomcat certificate was uploaded successfully.

Now the Cisco Unified Communications Manager can be discovered by the Expressway-C. Navigate to **Configuration > Unified Communications > Unified CM Servers.** Click the Add button and enter the following parameters. If TLS Verify is being used, the Unified CM Publisher Address must be the URL of the Cisco Unified Communications Manager publisher. If TLS Verify is not being used, this address can be the URL or the IP address of the Cisco Unified Communications Manager Publisher. The Username and Password settings should correspond to the AXL application user credentials created on the Cisco Unified Communications Manager. Verify TLS Verify Mode is set to On if TLS Verify is being used. If not, change this setting to Off. When these settings are saved, the Expressway-C will automatically create a neighbor zone to the Cisco Unified Communications Manager. The last setting on this page is the AES GCM Support setting. If it is enabled, the neighbor zone generated for the Cisco Unified Communications Manager will support AES GCM algorithms to encrypt and decrypt media passing through the zone. The default is Off but can be switched to On depending on how the Cisco Unified Communications Manager is configured to handle media encryption. When finished, click the Add Address button. This will return you to the Unified CM Servers page. In the Currently Found Unified CM Nodes section, verify that the discovery status is displayed as Active. Figure 21-9 illustrates the settings that need to be configured when adding a Cisco Unified Communications Manager to the Expressway-C for discovery.



Unified CM servers

Unified CM server lookup

Unified CM publisher address	*
Username	*
Password	*
TLS verify mode	On
AES GCM support	Off

Related tasks

Configure IM and Presence Service nodes

Configure Unity Connection Servers

Figure 21-9 *CUCM Discovery Settings in the Expressway-C*

Key Topic

Administrators can navigate to **Configuration > Zones > Zones** and verify that the neighbor zone to the Cisco Unified Communications Manager has been created. Clicking into this zone will display all the settings, but they will be grayed out and cannot be changed. There is also a search rule associated with this zone that was automatically created. Navigate to **Configuration > Dial Plan > Search Rules** to verify this rule exists. These settings will also be grayed out. The Cisco Unified Communications Manager IM and Presence Service and Cisco Unity Connections servers can also be discovered by the Expressway-C if these servers are being used. However, be aware that the status will not show Active on these until the traversal zones are configured and active. Navigate to **Configuration > Unified Communications > IM and Presence Service Nodes** or **Configuration > Unified Communications > Unity Connection Servers** to configure the discovery settings for these servers in the same manner as the Cisco Unified Communications Manager.

Collaboration Traversal Zones and Search Rules

After the MRA settings have been configured and the certificates have been exchanged, the next step is to create traversal zones between the Expressway servers. Traversal zones should always be configured on the traversal server first, in this case the Cisco Expressway-E.

Step 1. Configure the traversal server zone on the Expressway E.

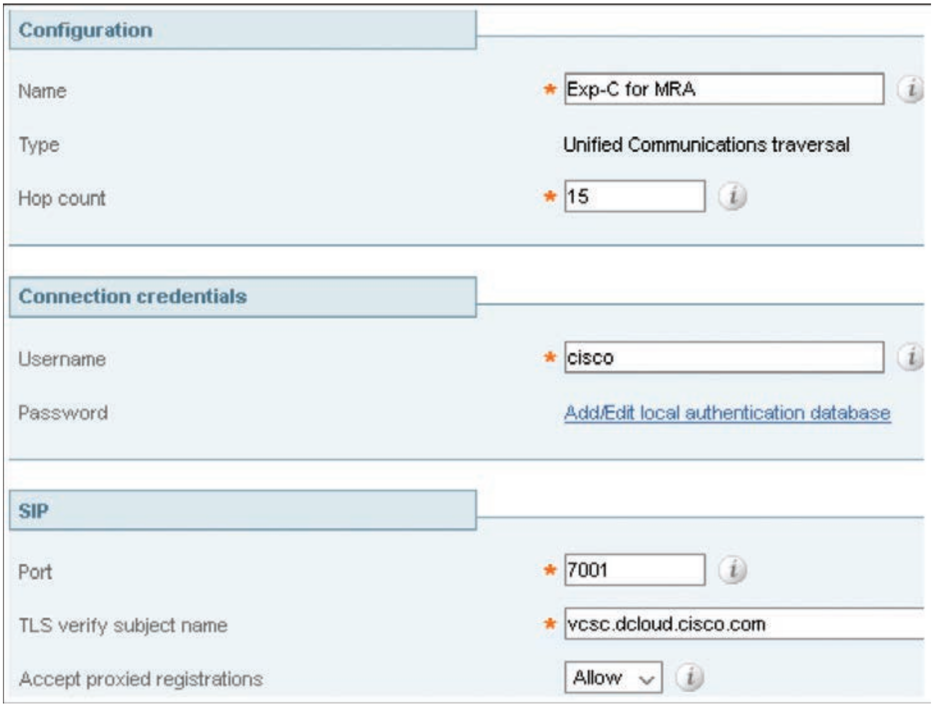
- **a.** On the Expressway-E, navigate to **Configuration > Authentication > Local Database** and add new credentials.
- **b.** Navigate to **Configuration > Zones > Zones** and add a new traversal server zone. Because this zone is specifically for MRA, the zone Type should be set to **Unified Communications Traversal**.
- **c.** Supply the username from the authentication database. Notice that no H.323 settings are available under this zone type. The reason is that H.323 is not supported using MRA. If H.323 calls are to be supported, another traversal zone must be established using the standard traversal zone setup.

  To enable Unified Communications Services on this traversal zone, you must configure the SIP settings to use TLS with TLS Verify Mode enabled, and Media Encryption Mode must be set to Force Encrypted. All of these settings default to the aforementioned parameters, and they cannot be changed. Therefore, these settings will not appear in the Unified Communications Traversal Zone settings page.
- **d.** Supply the SIP TLS Verify Subject Name. The Subject Name must match the subject name or the alternative subject name specified in the Cisco Expressway Core server security certificate. This is the Common Name you should have noted from the CSR of the Expressway Core. If you did not write it down, it is the full URL of the Expressway Core.
- **e.** Set the Accept Proxied Registrations setting to **Allow**.
- **f.** Set the Authentication Policy to **Treat as Authenticated.**
- **g.** Click **Create Zone** when finished.

Step 2. To route calls from the Expressway Edge to the Expressway Core through this traversal server zone, you need to configure a search rule as well.

- **a.** Navigate to **Configuration > Dial Plan > Search Rules.**

b. Click **New**, configure the settings, and then click **Create Search Rule.** Figure 21-10 illustrates some of the Unified Communications traversal zone settings on the Expressway-E.



Configuration

Name	* Exp-C for MRA
Type	Unified Communications traversal
Hop count	* 15

Connection credentials

Username	* cisco
Password	Add/Edit local authentication database

SIP

Port	* 7001
TLS verify subject name	* vcsc.dcloud.cisco.com
Accept proxied registrations	Allow

Figure 21-10 *Unified Communications Traversal Zone Settings on the Expressway-E*

Once you've configured the traversal server zone, you can configure the traversal client zone on the Cisco Expressway-C to initiate communication between the two servers.

Step 3. Configure the traversal server zone on the Expressway Core.

a. On the Expressway-C, navigate to **Configuration > Zones > Zones** and add a new traversal client zone. Again, since this zone is specifically for MRA, you should set Zone Type to **Unified Communications Traversal.**

b. Supply the Username and Password that were configured in the Authentication database on the Expressway-E.

c. Enter the port that will be used to establish a connection and keep the connection alive. This port needs to match the SIP keepalive port on the Expressway Edge.

d. Set the Accept Proxied Registrations setting to **Allow**.

e. Set the Authentication Policy to **Treat as Authenticated**.

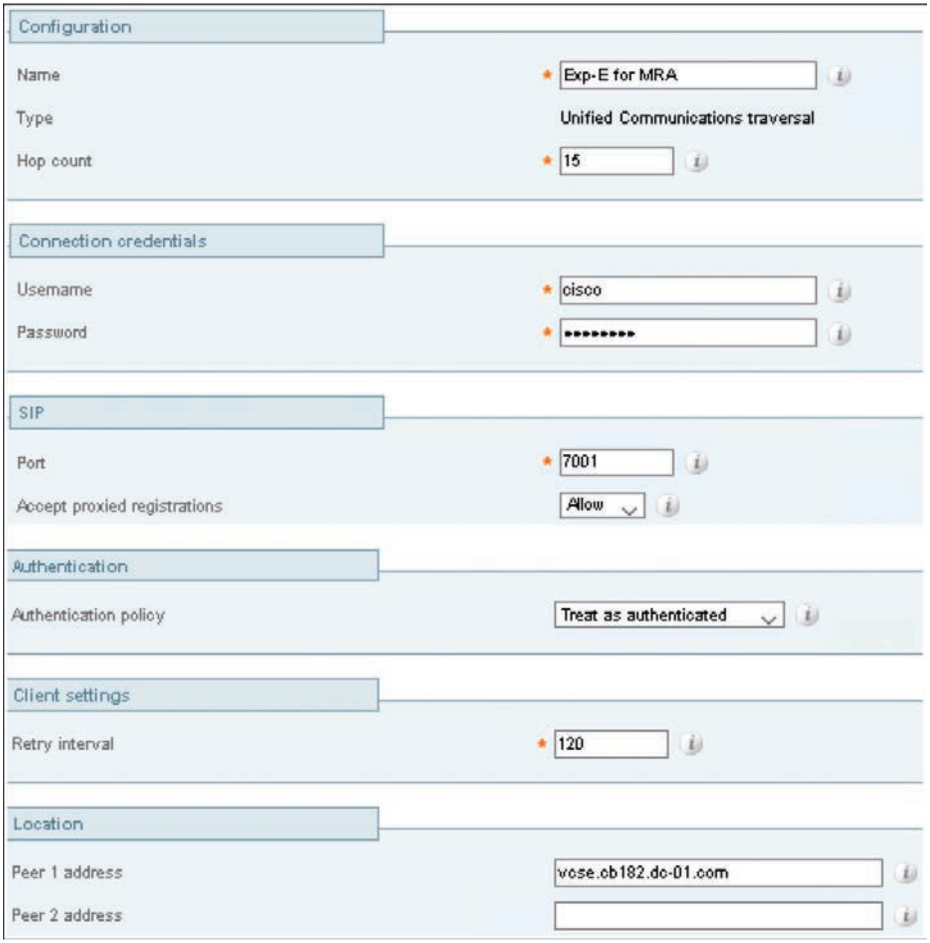
f. In the Location Peer 1 Address field, enter the URL of the Expressway Edge.

Because TLS Verify is being used, this setting must be in the URL format. It must also match the Common Name you should have noted from the CSR of the Expressway Edge. If the IP address of the Expressway-E is used, communication will fail between the traversal client and the traversal server.

g. Click **Create Zone** when finished.

h. Verify that the state of the zone is Active after saving the client zone.

Step 4. To route calls through the Expressway Edge using this traversal client zone, you need to configure a search rule here as well. However, because calls may be routed to any possible destination, you can use an Any Alias rule. Figure 21-11 illustrates some of the Unified Communications Traversal Zone settings on the Expressway-C.



Configuration	
Name	* Exp-E for MRA
Type	Unified Communications traversal
Hop count	* 15
Connection credentials	
Username	* cisco
Password	* •••••••••
SIP	
Port	* 7001
Accept proxied registrations	Allow
Authentication	
Authentication policy	Treat as authenticated
Client settings	
Retry interval	* 120
Location	
Peer 1 address	vcse.cb182.dc-01.com
Peer 2 address	

Figure 21-11 *Unified Communications Traversal Zone Settings on the Expressway-C*

The MRA deployment is now complete. You can test these settings by trying to register endpoints located both inside the enterprise network and outside the network. If the zones created will support calls as well, test the deployment by trying to place a few calls. Try calling between an internally registered endpoint and an externally registered endpoint. Then try calling between an internally registered endpoint and an endpoint located in another business network. Also, try calling between an externally registered endpoint and an endpoint located in another business network. You should try all call attempts from both directions: initiated from inside out, and initiated from outside in.

Device Onboarding with Activation Codes over MRA

Activation codes provide a simple and secure way to onboard remote endpoints for Mobile and Remote Access (MRA). This feature eliminates the need for an MRA user to be on-premises the first time they use their phones. Remote users can plug in the phone, enter the activation code, and then start placing calls. This feature leverages the Cisco cloud to handle onboarding. An administrator onboards Cisco Unified Communications Manager to the cloud, specifying the clusterwide MRA Activation Domain with the Expressway cluster to which all remote MRA users connect during the device activation process. If you have multiple Expressway clusters, MRA Service Domains let you specify which Expressway your phones register through. After the phone activates, the phone downloads its configuration file, which contains a redirect to the MRA Service Domain with the Expressway cluster assigned to that phone.

Activation codes were covered in Chapter 17. To review, an activation code is a single-use, 16-digit value that a user must enter on a phone before registering the phone. The user must enter the correct code; otherwise, the phone does not register. Activation codes provide a secure method to onboard phones without requiring an administrator to collect and input the MAC address for each phone manually.

If you want to use your own certificates, you can use the cloud to distribute certificates to MRA phones so that they can establish trust with Expressway. With this option, you must upload your certificates first to Expressway and then to the **PhoneEdge-trust** store on Cisco Unified Communications Manager. The certificates are uploaded to the Cisco cloud so that the phone can download them during the device activation process.

Prerequisites for Activation Codes with MRA

Before setting up device onboarding with activation codes over MRA, you should be sure you meet all the minimum prerequisites. The Cisco Expressways should be running version X12.5.1 or higher, and the Cisco Unified Communications Manager should be running version 12.5(1)SU1 or higher. The same phone models discussed in Chapter 17 are supported when using activation codes over MRA. However, you should be sure these phones are running Cisco IP Phone firmware version 12.5(1)SR3.

Key Topic

If you've upgraded the Expressways from a release prior to X12.5, refresh your Cisco Unified Communications Manager servers on Expressway-C before you configure this feature. On Expressway-C, go to **Configuration > Unified Communications > Unified CM servers** and click **Refresh servers**. All other settings discussed in Chapter 17 that pertain to setting up activation codes should be configured as well. Also, OAuth refresh logins must be enabled in Cisco Unified Communications Manager by setting the **OAuth Refresh Login Flow** enterprise parameter to **Enabled**.

If you want users to be able to use the Self Care Portal to activate their phones, you must set the **Show Phones Ready to Activate** enterprise parameter to **True** in Cisco Unified Communications Manager. End users require login access to the portal, so you will need to ensure all settings related to the Self Care Portal have been configured. Also note that the Self Care Portal is not supported over MRA, so remote users may need a VPN to access the portal from their computers.

Finally, for the MRA Activation Domain and any MRA Service Domains, you must configure *_collab_edge* SRVs that point to the appropriate Expressway clusters.

Configure Activation Codes with MRA

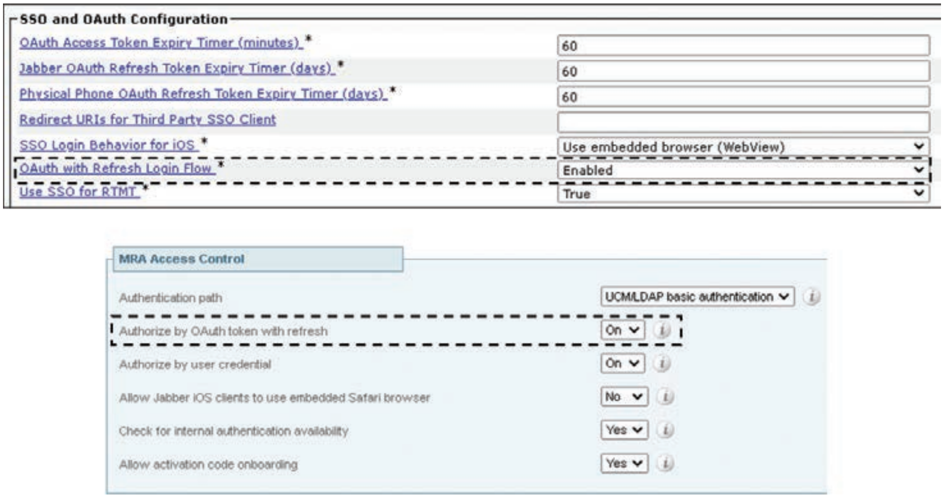
Key Topic

The following steps will walk you through how to configure device onboarding using activation codes in MRA mode.

Step 1. Enable OAuth Authentication in Cisco Unified Communications Manager and Expressway.

From Cisco Unified CM Administration, go to **System > Enterprise Parameters**. Set the **OAuth Refresh Login Flow** parameter to **Enabled** and click **Save**.

From the Expressway, go to **Configuration > Unified Communications > Configuration > MRA Access Control**. Set **Authorize by OAuth token with refresh** to **On** and click **Save**. Figure 21-12 illustrates how to configure OAuth Authentication.



SSO and OAuth Configuration

OAuth Access Token Expiry Timer (minutes) *	60
Jabber OAuth Refresh Token Expiry Timer (days) *	60
Physical Phone OAuth Refresh Token Expiry Timer (days) *	60
Redirect URIs for Third Party SSO Client	
SSO Login Behavior for iOS *	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Enabled
Use SSO for RTMT *	True

MRA Access Control

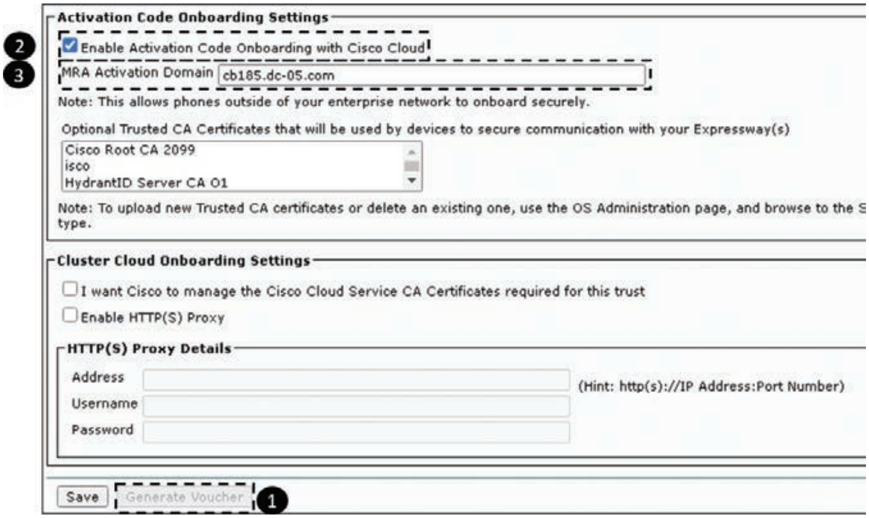
Authentication path	UCM/LDAP basic authentication
Authorize by OAuth token with refresh	On
Authorize by user credential	On
Allow Jabber iOS clients to use embedded Safari browser	No
Check for internal authentication availability	Yes
Allow activation code onboarding	Yes

Figure 21-12 *Unified Communications and Expressway-C OAuth Authentication Settings*

Step 2. Onboard Cisco Unified Communications Manager to the cloud for MRA activation code onboarding.

From Cisco Unified CM Administration, choose **Advanced Features > Cisco Cloud Onboarding.** Click the **Generate Voucher** button. Check the **Enable Activation Code Onboarding with Cisco Cloud** check box. Specify the **MRA Activation Domain** and click **Save**.

Collab-edge DNS records must exist for the MRA Activation Domain. There is a limit of one MRA Activation Domain per cluster. The MRA Activation Domain is added automatically to the list of MRA Service Domains. Figure 21-13 illustrates how to onboard Cisco Unified Communications Manager to the cloud for MRA activation code onboarding.



Activation Code Onboarding Settings

☑ Enable Activation Code Onboarding with Cisco Cloud

MRA Activation Domain: cb185.dc-05.com

Note: This allows phones outside of your enterprise network to onboard securely.

Optional Trusted CA Certificates that will be used by devices to secure communication with your Expressway(s)

Cisco Root CA 2099
isco
HydrantID Server CA O1

Note: To upload new Trusted CA certificates or delete an existing one, use the OS Administration page, and browse to the S
type.

Cluster Cloud Onboarding Settings

☐ I want Cisco to manage the Cisco Cloud Service CA Certificates required for this trust

☐ Enable HTTP(S) Proxy

HTTP(S) Proxy Details

Address: (Hint: http(s)://IP Address:Port Number)

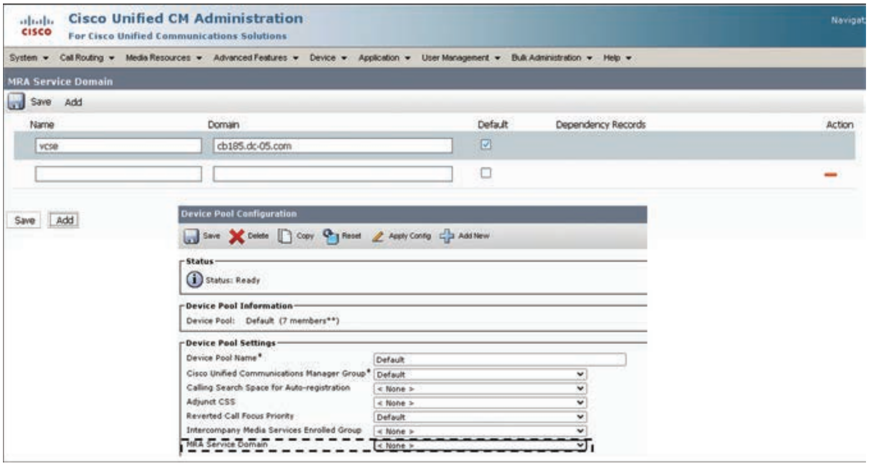
Username:

Password:

Figure 21-13 *Onboard Cisco Unified Communications Manager to the Cloud for MRA Activation Code Onboarding*

Step 3. Configure MRA Service Domains.

From Cisco Unified CM Administration, choose **Advanced Features > MRA Service Domains**. If you have multiple Expressway clusters, add each domain where your MRA endpoints will operate. Check the **Default** check box if you want a domain to be applied as a clusterwide default MRA Service domain. Click **Save**. Figure 21-14 illustrates how to configure MRA Service Domains.



MRA Service Domain

Name	Domain	Default	Dependency Records	Action
vcse	cb185.dc-05.com	☑		
		☐		—

Device Pool Configuration

Status

Status: Ready

Device Pool Information

Device Pool: Default (7 members**)

Device Pool Settings

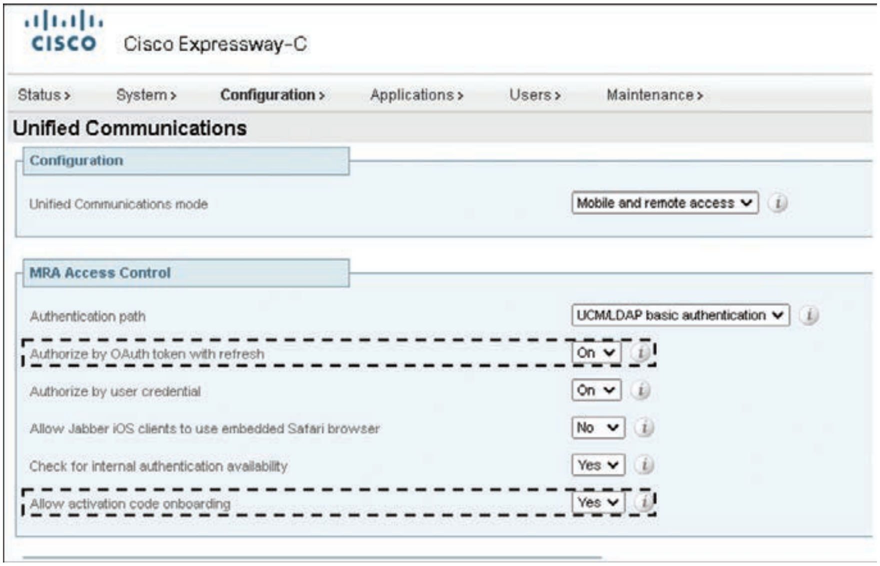
Device Pool Name*	Default
Cisco Unified Communications Manager Group*	Default
Calling Search Space for Auto-registration	< None >
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Intercompany Media Services Enrolled Group	< None >
MRA Service Domain	< None >

Figure 21-14 *MRA Service Domain*

Optionally, you can assign an MRA Service Domain to an existing device pool. This lets you assign a specific Expressway cluster to all MRA devices that use the device pool. From Cisco Unified CM Administration, choose **System > Device Pool**. Click **Find** and select the appropriate device pool. From the **MRA Service Domain** drop-down, select the domain you want to assign to devices that use this device pool and click Save.

Step 4. Configure MRA Access Control to allow activation code onboarding.

From Expressway-C, choose **Configuration > Unified Communications > Configuration**. Set **Authorize by OAuth token with refresh** to **On**. Set **Allow activation code onboarding** to **Yes**. Figure 21-15 illustrates how to configure MRA access control to allow activation code onboarding.



Unified Communications

Configuration

Unified Communications mode: Mobile and remote access

MRA Access Control

Authentication path: UCM/LDAP basic authentication

Authorize by OAuth token with refresh: On

Authorize by user credential: On

Allow Jabber iOS clients to use embedded Safari browser: No

Check for internal authentication availability: Yes

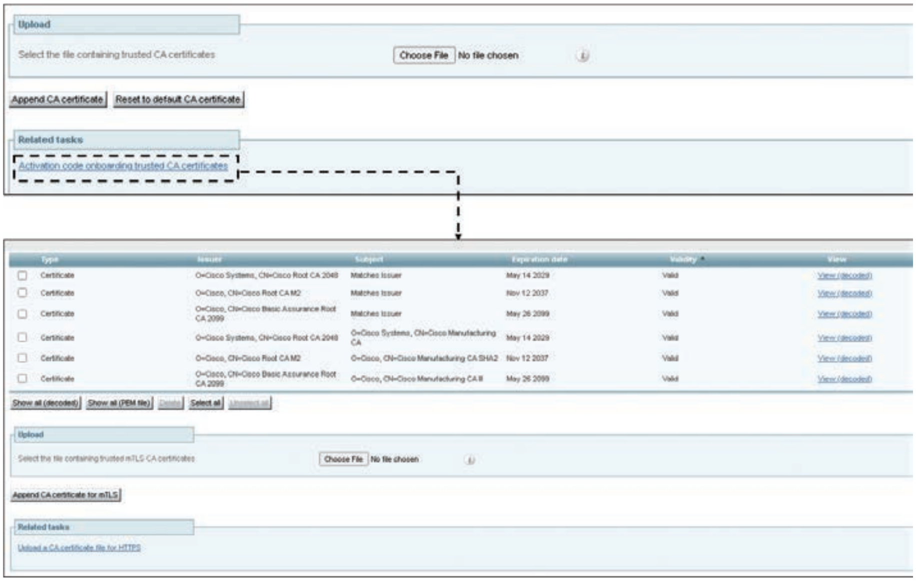
Allow activation code onboarding: Yes

Figure 21-15 *MRA Access Control to Allow Activation Code Onboarding*

Step 5. Check that the trusted Cisco manufacturing installed certificates (MICs) installed. They are required to access the activation code onboarding functionality.

On Expressway-E, choose **Maintenance > Security > Trusted CA certificates**. Click **Activate code onboarding trusted CA certificates**. Figure 21-16 illustrates how to check trusted MICs are installed.

Optionally, you can use your own custom certificates. Upload the certificates to Expressway. Upload certificates to PhoneEdge-trust on Cisco Unified Communications Manager. Cisco Unified Communications Manager uploads the certificates to the cloud. During the activation process, the phone downloads the certificates from the cloud, thereby ensuring that the phone can communicate with Expressway.



Upload

Select the file containing trusted CA certificates [Choose File] No file chosen

[Append CA certificate] [Reset to default CA certificate]

Related tasks

Activation code onboarding trusted CA certificates

	Type	Issuer	Subject	Expiration date	Validity	View
□	Certificate	O=Cisco Systems, CN=Cisco Root CA 2048	Matches Issuer	May 14 2029	Valid	View (decoded)
□	Certificate	O=Cisco, CN=Cisco Root CA M2	Matches Issuer	Nov 12 2037	Valid	View (decoded)
□	Certificate	O=Cisco, CN=Cisco Basic Assurance Root CA 2099	Matches Issuer	May 26 2099	Valid	View (decoded)
□	Certificate	O=Cisco Systems, CN=Cisco Root CA 2048	O=Cisco Systems, CN=Cisco Manufacturing CA	May 14 2029	Valid	View (decoded)
□	Certificate	O=Cisco, CN=Cisco Root CA M2	O=Cisco, CN=Cisco Manufacturing CA SHA2	Nov 12 2037	Valid	View (decoded)
□	Certificate	O=Cisco, CN=Cisco Basic Assurance Root CA 2099	O=Cisco, CN=Cisco Manufacturing CA III	May 26 2099	Valid	View (decoded)

[Show all (decoded)] [Show all (PEM file)] [Delete] [Select all] [Unselect all]

Upload

Select the file containing trusted mTLS CA certificates [Choose File] No file chosen

[Append CA certificate for mTLS]

Related tasks

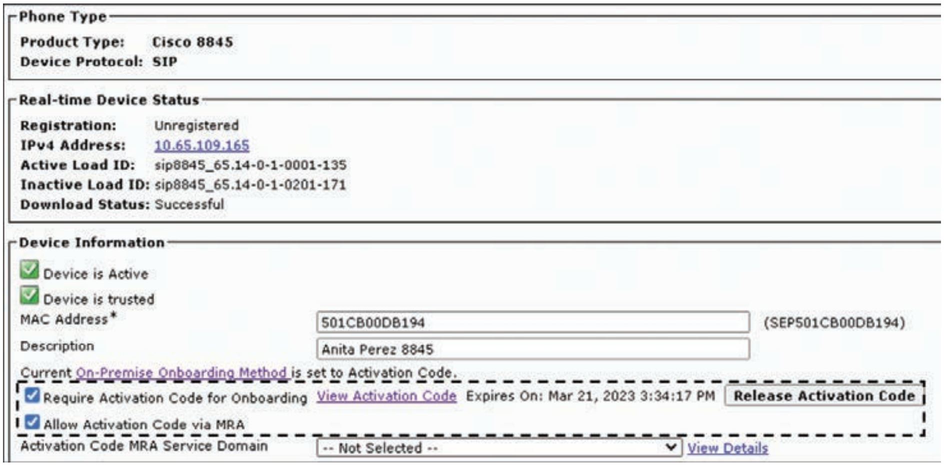
Upload a CA certificate file for HTTPS

Figure 21-16 *Check That Trusted Manufacturing Installed Certificates Are Installed*

Step 6. Provision the phone in the Cisco Unified Communications Manager database using any accepted provisioning method. No matter which option you choose, make sure that both of the following check boxes are checked:

- **Requires Activation Code Onboarding**
- **Allow Activation Code via MRA**

You can provision the phone with a dummy MAC address. The onboarding process updates the **Device Name** setting using the phone's actual MAC address. Figure 21-17 illustrates how to provision the phone in the Cisco Unified Communications Manager.



Phone Type

Product Type: Cisco 8845
Device Protocol: SIP

Real-time Device Status

Registration: Unregistered
IPv4 Address: 10.65.109.165
Active Load ID: sip8845_65.14-0-1-0001-135
Inactive Load ID: sip8845_65.14-0-1-0201-171
Download Status: Successful

Device Information

☑ Device is Active
☑ Device is trusted
MAC Address* 501CB00DB194 (SEP501CB00DB194)
Description Anita Perez 8845
Current On-Premise Onboarding Method is set to Activation Code.
☑ Require Activation Code for Onboarding View Activation Code Expires On: Mar 21, 2023 3:34:17 PM [Release Activation Code]
☑ Allow Activation Code via MRA
Activation Code MRA Service Domain -- Not Selected -- View Details

Figure 21-17 *Provision the Phone in the Cisco Unified Communications Manager*

Activate Phones over MRA

Administrators have two options for sending activation codes to phone users. Phone users can log in to the Self Care Portal to view their phone's activation code and an accompanying QR code. They can either key in the activation code to the phone or use the phone's video camera to scan the QR code—both methods work. Alternatively, administrators can export a .csv file from the Cisco Unified Communications Manager containing outstanding activation codes and associated users. They can use the contents of this file to notify MRA users with their activation codes.

To export a .csv file from Cisco Unified CM Administration, choose **Device > Phone**. From **Related Links**, select **Export Activation Codes** and click **Go**.

Activation codes have a default lifetime of 168 hours (7 days). You can reconfigure this value via the **Activation Time to Live (Hours)** service parameter in Cisco Unified Communications Manager. If the activation code expires, the administrator can click **Release Activation Code** and then **Generate New Activation Code** from the Phone Configuration window in order to reset the activation code.

When an MRA user plugs in their phone, they are prompted to enter the activation code. Once they enter the activation code, or scan the QR code that displays in the Self Care Portal, the phone onboards, downloads its configuration file, and registers. The phone is now ready to use.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 21-6 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 21-6 Key Topics for Chapter 21

Key Topic Element	Description	Page Number
Paragraph	Standard Traversal Solution versus MRA Traversal Solution	492
Table 21-2	Public DNS SRV Records for Expressway-E Cluster	494
Table 21-3	Private DNS SRV Records for CUCM and CUCM IMP Clusters	494
List	Firewall Traversal Communications Process	494
List	Firewall Ports for MRA	495
Table 21-4	Certificate Pairs Used for MRA Deployments	496
List	Reverse Proxy Ports	497
Paragraph	AXL User Needed on CUCM for MRA	501
Table 21-5	Classes of Certificates on Cisco Collaboration Servers	503

Key Topic Element	Description	Page Number
Paragraph	Points of Interest for Certificates on Expressway-C	507
Paragraph	DER and Base64 Comparison	509
Paragraph	Root CN Chaining Explained	509
Paragraph	Points of Interest for Certificates on Expressway-E	510
List	General Steps to Configure MRA	511
Paragraph	Autoconfigured Neighbor Zones for MRA	515
Paragraph	OAuth Refresh Logins for Device Activation Codes	518
Steps	Configure Activation Codes with MRA	519

Define Key Terms

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

A-Record, ADCS, Asymmetric Cryptography, Base64 Encoded Format, CA, CSR, DER Encoded Format, Diffie-Hellman Key Exchange, DNS, DV Certificates, EV Certificates, Firewall, HTTPS Reverse Proxy, MRA, OV Certificates, PKI, Root CA, Root CA Certificate, RSA, SRV, SSL, Symmetric Cryptography, TLS, TLS Verify, Traversal Chaining, Traversal Client Zone, Traversal Server Zone, Traversal Zone, Unified Communications Traversal Zone

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What are the five differences between a standard firewall traversal solution and MRA?
2. What are the four prerequisites that MRA depends on to be configured?
3. What are the six steps in a basic service discovery from an endpoint using the MRA solution?
4. What are the three main categories for deploying an MRA solution?
5. Summarize the six steps required to configure activations codes over MRA.

This page intentionally left blank

This part covers the following topics:

- **Chapter 22, Components of the Webex Solution:** This chapter will introduce the Webex cloud-based solution and provide an overview of the three main components that make up Webex.
- **Chapter 23, Adding Users and Devices in Webex Control Hub:** This chapter will explain the various methods available to add users and devices to the Webex Control Hub. This chapter will also describe the steps used to add users via the Directory Connector.
- **Chapter 24, Webex Calling Options:** This chapter will examine the different routers that support Webex Calling, as well as the various architecture models used to deploy this solution.
- **Chapter 25, Webex Calling Features:** This chapter will closely examine all the different Webex Calling features available to customers from the Webex Control Hub.
- **Chapter 26, Webex Calling Using a Local Gateway:** This chapter will describe the steps needed to configure the Webex Control Hub, a local gateway, and a Cisco Unified Border Element router to support Webex Calling.

Part VI

Webex Calling

Chapter 22: Components of the Webex Solution

Chapter 23: Adding Users and Devices in the Webex Control Hub

Chapter 24: Webex Calling Options

Chapter 25: Webex Calling Features

Chapter 26: Webex Calling Using a Local Gateway

CHAPTER 22

Components of the Webex Solution

This chapter covers the following topics:

Webex Meeting: This topic will introduce the three current Webex Meeting platforms available today, which are Webex Personal Rooms, Webex Webinars, and Webex Events.

Webex Messaging: This topic will discuss the features and benefits available to customers within Webex Messaging, which include Instant Messaging, Presence, document sharing, meeting joining and scheduling, and integrations and bots.

Webex Calling: This topic will briefly introduce the Webex Calling solution and the components required to support it. This topic will also introduce the features and phones supported in the Webex Calling solution.

Although Webex began as a cloud conferencing platform, the vision for what it could become was always something greater. Over the years, Cisco has managed to build a complete collaboration solution in the cloud fostered from the foundation of Webex. The complete Webex solution is formed upon three main pillars: meetings, messaging, and calling. In this chapter, you will learn the importance of these three pillars and how together they provide all the tools any sized company needs to be a disrupter within its market. Topics discussed in this chapter include the following:

- Webex Meeting
  - Webex Personal Rooms
  - Webex Webinars
  - Webex Events
  - Joining Webex Meetings
- Webex Messaging
  - Webex App Hub
  - Extension of Webex Meetings
- Webex Calling
  - Webex Calling Cloud Components
  - Features and Phones

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (350-801 CLCOR) exam:

- 1.5.c Directory Connector
- 2.3.d Onboarding cloud devices
- 3.4 Describe cloud calling hybrid local gateway
- 4.5 Describe Webex Calling dial plan features
  - 4.5.a Locations and numbers
  - 4.5.b Outgoing and incoming permissions
  - 4.5.c Transfer and forwarding restrictions

"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 22-1 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 22-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Webex Meeting	1–4
Webex Messaging	5–7
Webex Calling	8–10

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 the 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 is a type of Webex Meeting?

a. Personal Room

b. Webex Training

c. Webex Meeting

d. Webex Support

2. A Webex Webinar needs to be set up to support 50,000 people. What should an administrator do to support this need?

a. Order more licenses from the reseller.

b. Nothing needs to be done because Webinars support up to 100,000 attendees natively.

  - **c.** Enable Webcast when scheduling the Webinar.
  - **d.** Nothing can be done because Webinars will only support up to 10,000 attendees.

3. How many attendees can be supported in a Webex Webinar with Webcast enabled?

  - **a.** Up to 1000
  - **b.** Up to 3000
  - **c.** Up to 10,000
  - **d.** Up to 100,000

4. Which statement is correct?

  - **a.** The Webex Board can only join a Webex meeting for whiteboard content sharing.
  - **b.** The Webex Board can be used to join a Webex meeting like any other endpoint, with full audio, video, and content sharing.
  - **c.** The Webex Board cannot join a Webex meeting.
  - **d.** The Webex board requires a special license before it can join a Webex meeting with full audio, video, and content sharing capabilities.

5. Which of the following functions can be used on a message after it has been sent?

  - **a.** Add a reaction
  - **b.** Format text
  - **c.** Emoji
  - **d.** @mention

6. Which of the following functions can be used before sending an original message in the Webex client?

  - **a.** Start a thread
  - **b.** Add a reaction
  - **c.** Quote message
  - **d.** @mention

7. Which tool can be used to integrate with other apps and streamline work?

  - **a.** Control Hub
  - **b.** User Portal
  - **c.** App Hub
  - **d.** Webex app

8. What year did Cisco acquire BroadSoft?

  - **a.** 2017
  - **b.** 2018
  - **c.** 2019
  - **d.** 2020

9. What does a customer need to connect their on-premises environment with the Webex cloud for a Webex calling deployment?

  - **a.** Local gateway
  - **b.** Cisco UBE
  - **c.** ISR router with PRI cards
  - **d.** CCP

10. What does an approved Cisco phone need before it can register to the Webex Control Hub?
    a. Enterprise software installed
    b. FLEX license installed
    c. Nothing is needed to register phones
    d. MPP software installed

Foundation Topics

Webex Meeting

The humble beginnings of Webex started with meetings. A Webex Meeting provides a virtual space hosted in the cloud that anyone can join from any device anywhere they have an Internet connection. A great number of things have changed about Webex Meeting from its original design. Webex Meeting offers a more secure platform, with integrated audio, video, and content sharing from any device, anywhere. Intelligent features have been added such as noise removal and Webex Assistant, with real-time translations. Other features like People Insights automate meeting tasks to help you work smarter. These powerful analytics and intelligent context allow you to learn more about meeting participants.

Key Topic

There are different Webex Meeting platforms you can choose from, depending on what your needs require. Webex offers Personal Rooms, Webinars, and Events.

Webex Personal Rooms

Personal Rooms are Webex meeting rooms assigned to and used by specific users. They are always available and do not have to be scheduled, but they can be scheduled when needed. Personal preferences can be set up, such as the name, host PIN, and lobby notifications. Personal Rooms can also be locked to prevent uninvited people from joining.

You can make other participants a cohost of your Personal Room. A cohost is someone who has permission to host your scheduled meeting or Personal Room meeting when you cannot host it yourself. If you joined your meeting as the host but need to leave the room without ending the meeting, you can assign another participant the role of host before leaving from the meeting.

Webex Webinars

Webex Webinars, formerly known as Webex Events, is a best-in-class virtual Webinar experience that is video-centric, intelligent, and simple to use. Cisco has simplified the scheduling flow for event organizers with plans for 3000 or more users. Previously, organizers had two options when scheduling an event, Webinar, or Webcast. With this update, organizers can select Webcast view for attendees to allow attendee participation only through text-based chat, Q&A, and polling. Webcast view for attendees will be available with licenses that support 3000 or more attendees. For Webinars with more than 10,000 attendees, Webcast view for attendees is required.

With Webinars, a host can schedule a Webinar from either the <your_company>.webex.com site on the **Calendar** page or **Webinars** page or from the Webex app. The host can invite panelists, automatically start a practice session, and more. Webinars support up to 10,000 attendees or up to 100,000 attendees in Webcast view, depending on the Webinar plan you purchased. Regardless of what size or view you choose, the user experience is consistent:

- Presenters can share content optimized for motion and video with computer audio.
- All attendees can view the panelists' video and shared content.
- You can assign someone to be the cohost of your Webinar at the time of scheduling, or during a Webinar, to help manage attendees in a Webinar.
- Hosts can set a stage view for all attendees.

In Webinars, participants enjoy rich features that allow them to stay engaged and get the most out of the webinar. When enabled, all participants can send animated emoji reactions, select Music mode when they want to perform, or check out a panelist's profile with people insights profiles.

When your Webinar calls for a simpler attendee joining and viewing experience with limited interactions, you can host the Webinar in Webcast view. Once attendees receive the invite and join from the welcome page, they can stream the Webinar with a web browser instantly. Attendees can adjust volume, stop and resume video, and expand to full screen, as well as chat, participate in polls, and answer questions posted by the host. The host can specify the layout for attendees at any time during the Webinar.

Webex Events

Webex Events, formerly known as Socio, is the end-to-end event platform that powers continuous engagement to drive better results for virtual, in-person, and hybrid events:

- Build fully branded registration for virtual, in-person, and hybrid events in minutes. Flexible ticketing enables multiple ticket types, prices, groups, discount codes, and more—all with instant payouts.
- Onsite solutions allow you to power safe and seamless in-person experiences with the Webex Events event check-in and badge printing solution. With more onsite solutions like lead retrieval and live display, it's easy to deliver connected attendee experiences.
- The virtual event platform allows you to host more engaging, interactive virtual events that attendees love. The Webex Events virtual event platform comes standard with all the networking and engagement features you need to ensure active virtual participation and to drive better results.
- The mobile event app allows your attendees to access your event content in person or on the go from a simple and fully customizable app.
- Finally, Webex Events allows you to craft a branded community where like-minded individuals can meet for networking, thought leadership, and exclusive content.

Joining Webex Meetings

There are many different ways users can join a Webex Meeting. You can join a meeting from an email invitation, Personal Room, mobile device, and many other ways. You can start the Personal Room meeting though any supported video system or video application. You can also start a Personal Room meeting by phone without having to log in using the Webex application.

Personal devices, such as smartphones, tablets, and computers, can be used to join Webex meetings using the Webex application or a web browser. The Webex application is a similar experience to what users have traditionally experienced through the Webex Meeting web portal. Content can be shared by any participant in the meeting, annotation tools are available, and polling questions can be incorporated into a Webex Meeting.

Webex endpoints can also be used to join Webex Meetings. The Webex Board has an integrated camera, microphone, and speakers so that it can be used the same as any other Webex endpoint for joining meetings. Figure 22-1 illustrates a Webex Board and another Webex endpoint, each facing each other in a single meeting space. In this type of setup, the intelligence built into each of these endpoints allows them to detect one another during a call setup to the same meeting. The camera, microphone, and speakers of the Webex Board will not be used to call into the meeting, but the endpoint will still join so that the annotation features of the Webex Board can be used and shared with all participants in the meeting. This is just another great demonstration of the technology that sets Cisco apart from the competition.

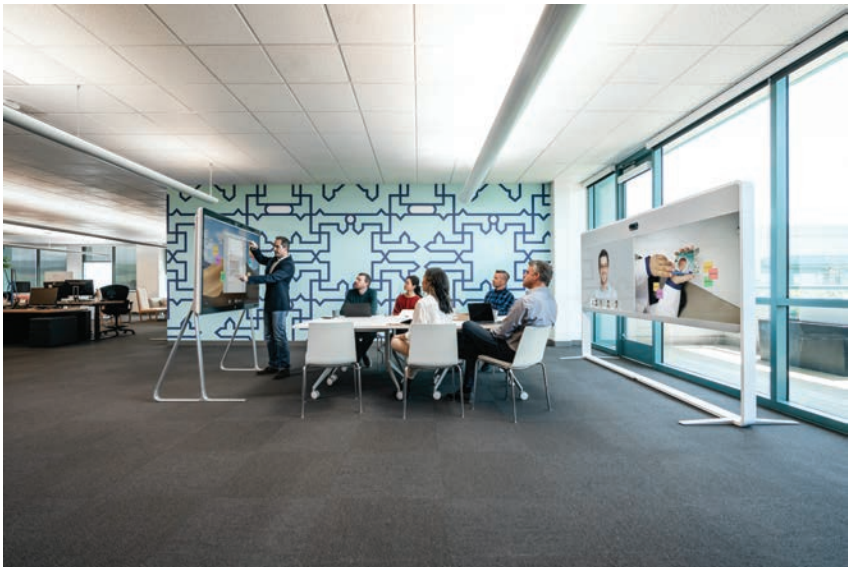


Figure 22-1 *Webex Intelligence Using a Webex Board and Another Webex Endpoint*

Webex Messaging

Key Topic

Webex Messaging is all about extending collaboration beyond the meeting. Messaging allows users to send someone a direct message or bring everyone together easily and quickly into a Webex Space. Messaging enables everyone to see and share all the information they need to work together productively in real time by sending messages, sharing files, and creating or editing whiteboards. Webex is built on a multilayer security model so that all information is kept private.

Additional interactive tools have been added to the Webex app, such as emojis, GIFs, and text formatting. You can also edit and delete messages after they have been sent, and you can start a thread within a space to track conversations more easily.

Webex App Hub

Use the Webex App Hub to easily integrate with other apps and streamline work. Integrate with other tools for an uninterrupted workflow. Webex delivers pre-built solutions with third-party applications from vendors such as Microsoft, Google Cloud, Miro, Salesforce, and more to deliver a complete collaboration experience. Further, users can share and edit files from Microsoft OneDrive and SharePoint Online right in Webex Spaces, eliminating app switching and file sprawl. Other integrations can be set up using the Webex App Hub to connect your team in Webex Messaging with the work happening in other tools, such as Service Now, Trello, Asana, Salesforce, and Jira.

Extension of Meetings

With Microsoft Office 365, Microsoft Exchange, and Google Calendar integrations, you can view your meeting list right in the Webex app, making it easy to stay on top of your upcoming appointments and join meetings with a single button push. New meetings are scheduled with ease, automatically including all the people you need and the join details.

Select the **Meetings** menu from the left column on the Webex app to view your scheduled meetings. Click the **Start a Personal Room meeting** button to start an ad hoc meeting. Click the **Schedule a meeting** button to schedule a meeting using your Personal Room or to schedule a Webinar. If you want to join a meeting you are not scheduled for, and you know the meeting number, you can click the **Join a meeting** button, enter the meeting number and password, if necessary, and join the meeting. If a scheduled meeting is active, which occurs 5 minutes before the scheduled start time, then a green join button will appear beside the entry in the meetings list. Figure 22-2 illustrates the Meetings section on the Webex App.

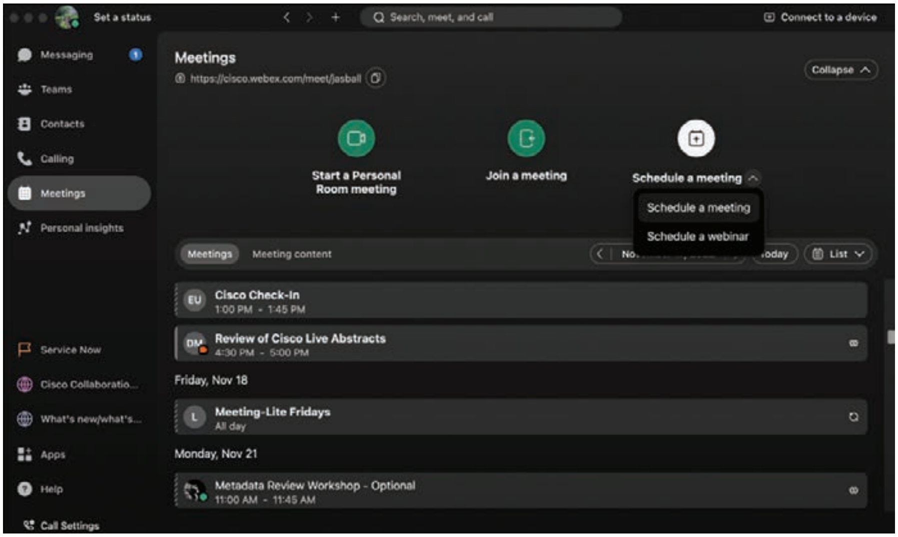


Figure 22-2 *Meetings Section on the Webex App*

You can also invite people within a space to a meeting by using the Personal Room Invite button. Clicking this button will provide a meeting link to your Personal Room in the chat window. Other participants in that space can click the link to join the meeting instantly.

Webex Calling

The companies Cisco acquired over the years are part of what makes Webex such a powerful solution. These acquisitions brought the right features needed to enhance Webex to what it is today. BroadSoft was a company Cisco acquired in 2018 for its calling capabilities. There were two autonomous cloud offerings to the BroadSoft solutions: BroadCloud and BroadWorks.

BroadSoft had a full cloud solution called BroadCloud that supported its calling solution called UC1. BroadCloud became the foundation for Webex Calling, which in turn became the backbone of the Cisco FLEX offering, which is Webex Calling for value-added resellers (VARs).

BroadSoft had a second product called BroadWorks, which is the technical name of the solution that BroadSoft sold to service providers (SPs). BroadWorks operates the same as BroadCloud, except it comes in a rack-mountable server that SPs can install and maintain. This allowed SPs to sell UC1 directly to customers from their own hosted data centers. BroadWorks is still used with SPs today.

BroadSoft also offered a contact center service called CC1. Cisco rebranded it to Customer Journey Platform and then changed it again to Webex Contact Center. This contact center solution was hosted from the same BroadCloud and BroadWorks platforms. However, Webex Contact Center can also be sold and leveraged without a subscription to Webex Calling by integrating it with an on-premises enterprise deployment using Cisco Unified Border Element (UBE). Either VARs or SPs can resell Webex Contact Center.

Webex Calling Cloud Components

Key Topic

The main concept to grasp with the Webex Calling solution is that phones and applications can place calls using either IP or the public switched telephone network (PSTN). Therefore, a connection between the IP cloud and the PSTN cloud needs to be established. This can be accomplished using multiple methods:

- A telephony provider can create what's called a Cloud-Connected PSTN (CCP) connection.
- The customer can provide a connection through their own telephony service provider via a routed connection from within their on-premises corporate network. This connection is typically established using Cisco Unified Border Element (UBE) or a Cisco Integrated Service Router (ISR) with Primary Rate Interface (PRI) cards.
- Cisco now has a PSTN option that's similar to CCP called Cisco PSTN.

Whichever routing option is used, a connection must also be established back to the Webex cloud. If a CCP or Cisco PSTN is being used, this is done on the customer's behalf by the CCP provider or Cisco. If the customer is providing their own connection to their preferred PSTN provider on-premises, then a local gateway must be set up. This will provide the connection back to the Webex cloud. Within the Webex cloud, remote session border controllers (SBCs) are configured to receive communications from the local gateway. Figure 22-3 illustrates the different components needed to establish a Webex Calling connection.

The Webex Control Hub will need to be configured to make all these parts work together. Security settings and local gateway settings can be created in the Control Hub. They will then need to be configured on the local gateway router to establish a connection with the Webex cloud. Calling features can also be configured from the Webex Control Hub. This will be covered with more detail in Chapter 26, "Webex Calling Using a Local Gateway."

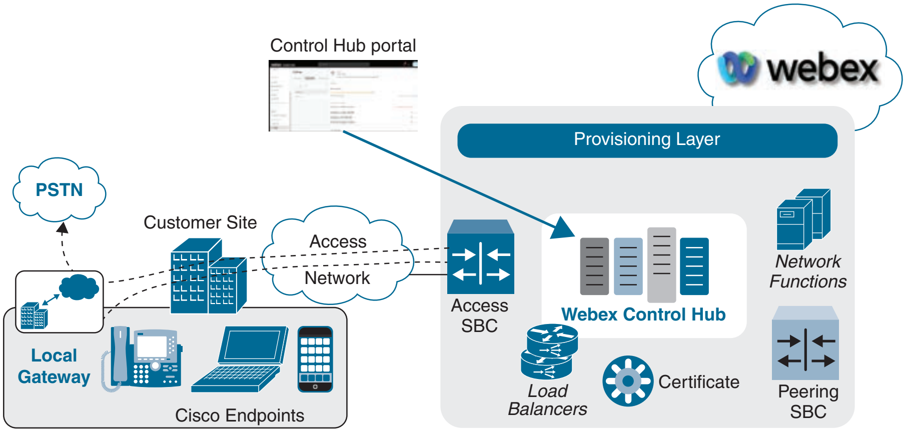


Figure 22-3 *The Required Webex Calling Components*

Features and Phone

Two categories of calling features are associated with Webex Calling, and each category can be configured per site. The first set of calling features can be configured only by an administrator from the Webex Control Hub administration portal. These features include the following:

- Auto Attendant
- Call Park Extensions
- Call Park Group
- Call Pickup
- Call Queue
- DECT Network
- Hunt Group
- Single Number Reach
- Paging Group
- Receptionist Client
- Virtual Extension
- Voicemail Group

The second set of calling features can be configured by an administrator from the Webex Control Hub administration portal or by the users themselves through the user portal. The Webex Control Hub administration portal can be accessed by navigating to https://admin.webex.com. The Webex user portal can be accessed by navigating to https://settings.webex.com. User-facing calling features include the following:

- Voicemail, fax, and announcement
- Language

- Call handling
  - Incoming call permissions
  - Outgoing call permissions
  - Call forwarding
  - Call waiting
  - Call intercept
- Between-user permissions
  - Monitoring
  - Barge in
  - Hoteling
  - Push-to-Talk
  - Privacy
  - Executive / Executive Assistant
- User call experience
  - In-call feature access
  - Application ringing and assignments
  - Compression options
  - Call recording
  - Reception client
- Agent Call Queue ID

All features will be covered with more detail in Chapter 25, "Webex Calling Features."

Key Topic

Webex Calling requires phones that register to the Webex Control Hub to be running the Multi-Platform Phone (MPP) software. Phones that register to the Cisco Unified CM must be running Enterprise software. Therefore, MPP phones can be ordered from Cisco with the software already installed for greenfield deployments, or existing Enterprise phones can be migrated to the MPP software for brownfield deployments. Migrating phones from MPP to Enterprise software, and vice versa, does require a migration license. The FLEX plan includes one migration license per user.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 22-2 lists a reference of these key topics and the page numbers on which each is found.

Table 22-2 Key Topics for Chapter 22

Key Topic Element	Description	Page Number
Paragraph	Types of Meetings	531
Paragraph	Message Capabilities	533
Paragraph	Calling Provider Options	535
Paragraph	MMP and Enterprise Phone Options	537

Define Key Terms

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

Webex Meeting, Personal Rooms, Webex Webinars, Webex Events, Webex Messaging, Webex App Hub, VAR, SP, CCP, MPP, Enterprise Software

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the three types of meetings available in a Webex solution.
2. List the three Webex Calling PSTN options.

This page intentionally left blank

CHAPTER 23

Adding Users and Devices in the Webex Control Hub

This chapter covers the following topics:

Webex Control Hub Overview: This topic looks at the various screens and dashboards available within the Cisco Webex Control Hub.

Methods of Adding Users to Webex Control Hub: This topic will examine five methods of adding users to the Webex Control Hub.

Directory Connector Configuration: This topic will describe the steps used to add users to the Webex Control Hub using the Directory Connector.

Adding Unified IP Phones to Webex Control Hub: This topic will describe the steps used to add Cisco Unified IP Phones to the Webex Control Hub.

Adding Webex Endpoints to Webex Control Hub: This topic will describe the steps used to add Webex endpoints to the Webex Control Hub.

Webex is a powerful cloud-based solution used to deploy and manage messaging, meeting, and calling for enterprise networks. The management tool used to administer all Webex operations through a single pane of glass is called the Webex Control Hub. This chapter will introduce you to the menus and capabilities of the Webex Control Hub and guide you through the process of adding users and registering devices. Topics discussed in this chapter include the following:

- Webex Control Hub Overview
  - Webex Control Hub Monitoring
  - Webex Control Hub Management
  - Webex Control Hub Services
- Methods of Adding Users to Webex Control Hub
  - Add Users Manually
  - Add Users with a CSV File
  - Claim Existing Webex Users
  - Directory Management
  - User Contact Synchronization
- Directory Connector Configuration
- Adding Unified IP Phones to Webex Control Hub
- Adding Webex Endpoints to Webex Control Hub

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (350-801 CLCOR) exam:

- 1.5.c Directory Connector
- 1.6 Describe Webex Control Hub features
- 2.3.d Onboarding cloud devices

"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 23-1 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 23-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Webex Control Hub Overview	1–2
Methods of Adding Users to Webex Control Hub	3–4
Directory Connector Configuration	5–6
Adding Unified IP Phones to Webex Control Hub	7–8
Adding Webex Devices to Webex Control Hub	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 the 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. The IT manager wants to show adoption of messaging in the Webex app. Where can you find the number of messages sent by users to assist with her efforts?
   a. **Monitoring > Webex Experience**
   b. **Management > Users**
   c. **Management > Apps**
   d. **Monitoring > Analytics**
2. You have been asked to add a user to Webex so you can build him a phone. Where would you go inside Webex Control Hub to accomplish the first step in this task?
   a. **Management > Devices**
   b. **Management > Workspaces**
   c. **Management > Users**
   d. **Management > Groups**

3. Which of the following is considered a "user" in Webex Control Hub?

- **a.** Workspaces.
- **b.** Service Numbers.
- **c.** Personal Contacts.
- **d.** All options are users.
- **e.** None of the options are users.

4. An administrator is trying to set up a directory synchronization with Azure AD. He downloaded the Directory Connector and configured all the settings, but the synchronization keeps failing. What is the likely cause of this issue?

- **a.** The wrong version of Directory Connector is being used.
- **b.** The Directory Connector should not be used in this deployment.
- **c.** The administrator configured the settings wrong on the Directory Connector.
- **d.** Directory Synchronization was not enabled in Webex Control Hub.
- **e.** There are no users in Azure AD to import yet.

5. Which tool is used to configure SSO?

- **a.** Control Hub
- **b.** Directory Connector
- **c.** Directory Connector Management Interface
- **d.** Directory Synchronization Service

6. Where would an engineer go to troubleshoot issues with synchronization when using the Directory Connector?

- **a.** **Monitoring > Troubleshooting** in Webex Control Hub
- **b.** **Monitoring > Reports** in Webex Control Hub
- **c.** Check that the **Directory Synchronization Service** is active
- **d.** **Launch Event Viewer** in Directory Connector Management Interface

7. Which phone model cannot register to the Cisco Unified Communications Manager?

- **a.** 6841
- **b.** 7841
- **c.** 8841
- **d.** Wireless Phone 840
- **e.** Webex Room Phone

8. Which of the following phones require migration before registering to Webex Control Hub?

- **a.** 6841
- **b.** 7841 running MMP Software
- **c.** 8841 running Enterprise Software
- **d.** Webex Desk Pro running CE software

9. What software runs on a Cisco Room Kit Pro when it is registered to the Webex Control Hub?

- **a.** MMP
- **b.** Enterprise

- **c.** RoomOS
- **d.** CE

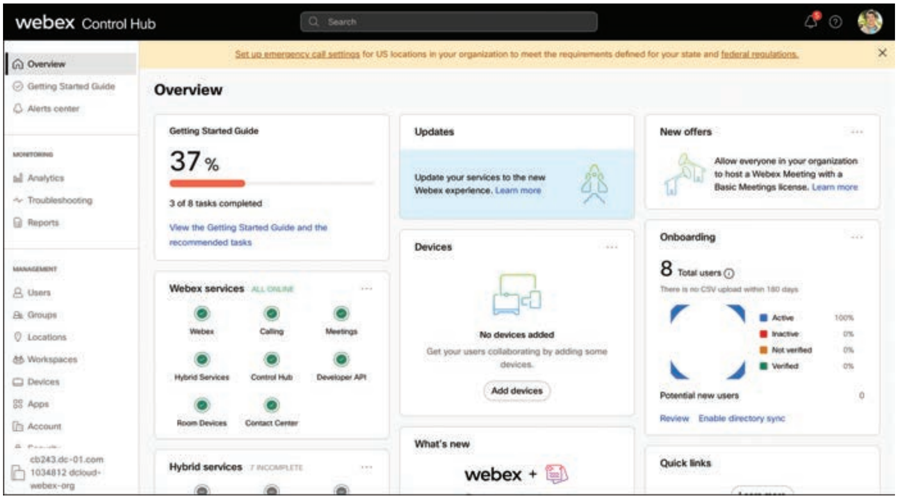
10. Which of the following Telepresence endpoints supports the full Webex Calling feature set when registered to Webex Control Hub?

- **a.** DX80
- **b.** MX800
- **c.** Webex Share
- **d.** Webex Room Phone
- **e.** Webex Board 55

Foundation Topics

Webex Control Hub Overview

When an administrator first logs in to the Webex Control Hub, the home screen is an Overview page showing a summary of their Webex environment. The left column on the page is the main menu for navigating throughout the Webex Control Hub. These menus are always available no matter what menu you decide to navigate to, and they are divided up into three sections: Monitoring, Management, and Services. I will go into each of these sections momentarily. The top three menus are not in a section, per se. They are Overview, Getting Started Guide, and Alert Center. The **Overview** screen makes up the main section of this page. It shows a summary of current activity and license information relating to your Webex account. You will also see information about the overall availability of the Webex environment, onboarding status, available updates, devices, and so on. Figure 23-1 shows the Overview screen on the Webex Control Hub.



Set up emergency call settings for US locations in your organization to meet the requirements defined for your state and federal regulations.

3 of 8 tasks completed

Update your services to the new Webex experience. Learn more

Allow everyone in your organization to host a Webex Meeting with a Basic Meetings license. Learn more

No devices added

Get your users collaborating by adding some devices.

There is no CSV upload within 180 days

Figure 23-1 *Webex Control Hub Overview Screen*

Getting Started Guide is the second menu option after Overview. This page offers a list of onboarding task to set up your Webex environment. They are divided into three categories: Foundational Setup, Advanced Setup, and Adoption. If you click a step, a flyout window appears on the right side of the screen that provides you with a description of the item, the impact it has on your environment, prerequisites before configuring it, if any exist, and a hyperlink to resources about the configuration or service. You get a green confirmation checkmark once the configuration is complete. The following list outlines each category and the recommended configurations within each:

Key Topic

- Foundational Setup
  - **Configure your network:** Check your network configurations to onboard Webex.
  - **Verify your domains**: Prove domain ownership.
  - **Set up auto-license templates:** Streamline user onboarding.
  - **Claim your users:** Manage all users and services under Control Hub.
  - **Claim your domains:** Prevent miscellaneous corporate accounts.
  - **Add users:** Invite users manually or via CSV or Directory Connector.
- Advanced Setup
  - **Set up Active Directory (AD):** Maintain a single source of truth for user management by integrating Active Directory.
  - **Set up Single Sign-On (SSO):** Increase security and enable the easiest sign-in experience for your users.
  - **Configure Hybrid Calendar:** Integrate Microsoft Exchange, Office 365, and Google Calendar with Cisco Webex.
- Adoption
  - **Build your adoption plan:** Establish a smooth rollout for your future Webex users.
  - **Join the Webex community:** Build your knowledge and network.

Alerts Center is the third menu option just below Getting Started Guide. This is a central place to manage alerts for your Webex deployment. Administrators can configure alerts to be delivered through email, webhooks, or in a Webex app space. Regardless of the delivery channel configured, all alerts will always appear in Control Hub.

Each administrator has their own set of alerts and rules that they can create and view in **My alerts** and **My rules** tabs, and they can view all alerts and rules from other administrators in the organization in the **All alerts** and **All rules** tabs. Administrators can also view announcements, such as software updates from Cisco, in the Alerts Center. Alerts for the last 14 days will appear in the **Alerts** section. You can export historical alerts for the last 30 days in a CSV format by clicking the **export** button.

There are two categories of alerts:

- **Threshold-based alerts:** With Threshold-based alerts, administrators can create a rule to monitor for specific events by specifying specific thresholds, such as participants who reach more than 300ms of latency or a packet loss of more than 8%. These alerts are only triggered if the administrators configure them by creating a rule. Administrators can further configure how these alerts are delivered by choosing the delivery channel for them.

- **Service-generated alerts:** These alerts are created automatically by Webex services. Most of these alerts are critical in nature, and the administrator should pay attention to them. Administrators can manage how these alerts are delivered by choosing the delivery channel for them.

Figure 23-2 illustrates the Alerts screen on the Webex Control Hub.

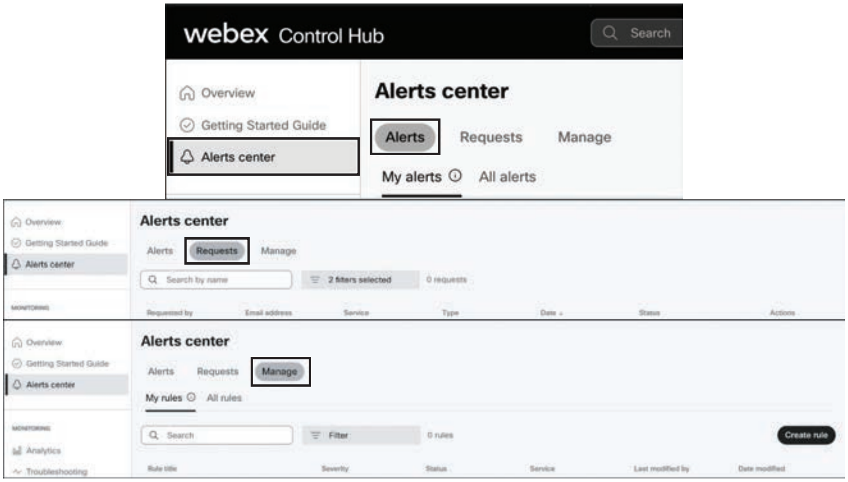


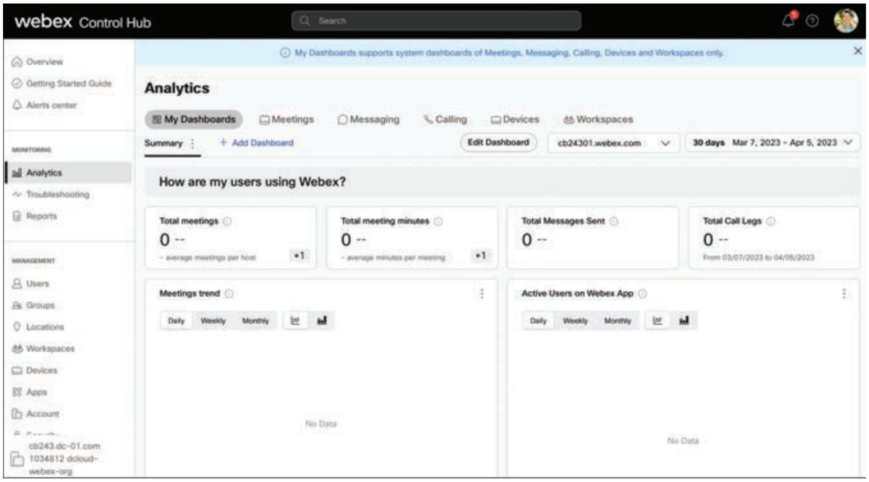
Figure 23-2 *Webex Control Hub Alerts Screen*

Webex Control Hub Monitoring

The Monitoring section of Webex Control Hub is exactly what you might think it is. This section offers a selection of tools to aid in analyzing the efficiency of your Webex environment and troubleshooting issues as they arise. The three available menu options in the Monitoring section are Analytics, Troubleshooting, and Reports.

The **Analytics** section in Control Hub gives administrators access to interactive data visualizations that show important information, such as usage and adoption trends. You can explore data as it automatically adapts to parameters you specify in real time. You have access to various charts in Control Hub, depending on your deployment. You can use this information to evaluate how Webex services and devices are being used in your organization and how often. For example, you can use analytics to track and measure services in your cloud collaboration portfolio. Keep in mind that this analytical data is for general use and should not be used for billing. Historical charts are standard in Control Hub. Most charts are available in daily, weekly, and monthly format. The amount of data you have access to depends on the type of customer you are. If you're a standard customer, you have access to 3 months of data. If you're a Pro Pack customer, you have access to 13 months of data. Analytics data, except for Meetings, is batch-processed each day. Data is made available within 24 hours, and metrics are available by 1:00PM GMT the next day. Meetings data is updated every 10 minutes. Figure 23-3 illustrates the Analytics screen on the Webex Control Hub.

The **Troubleshooting** menu offers media quality data about Webex Meetings and calls using Cisco Webex Calling and Call on Webex, which you can use to pinpoint which users are having meeting and call issues. To clarify, Cisco Webex Calling is a service in Webex that allows users to call out across the PSTN using the Webex app or a unified IP phone. Call on Webex is simply the ability for users to call using SIP over IP. This can be achieved through the Webex app, unified IP phones, or Webex endpoints without a Webex Calling subscription.



My Dashboards supports system dashboards of Meetings, Messaging, Calling, Devices and Workspaces only.

Figure 23-3 *Webex Control Hub Analytics Screen*

You can drill down into meetings or call on Webex on a per-participant basis and see detailed information about their audio, video, and sharing quality. Data is updated every minute for Webex Meetings and Call on Webex, so you can diagnose problems as they arise. Data for Webex Calling is updated at the end of each call. There is a powerful **Diagnostics** section as well, where you can drill down even further into specific meetings or calls that are in progress or that have occurred within the past 21 days. You can search for meetings by meeting number, the email address of the host or participants, conference ID, or the name of cloud-registered devices. You can search for calls with the caller or callee's email address, MAC address, and phone number. You can then drill down into participant details, hop details, video quality, audio quality, and more. Meetings in progress appear at the top of list with an **In Progress** status. Calls appear only after they've ended. Figure 23-4 illustrates the Troubleshooting screen on the Webex Control Hub.

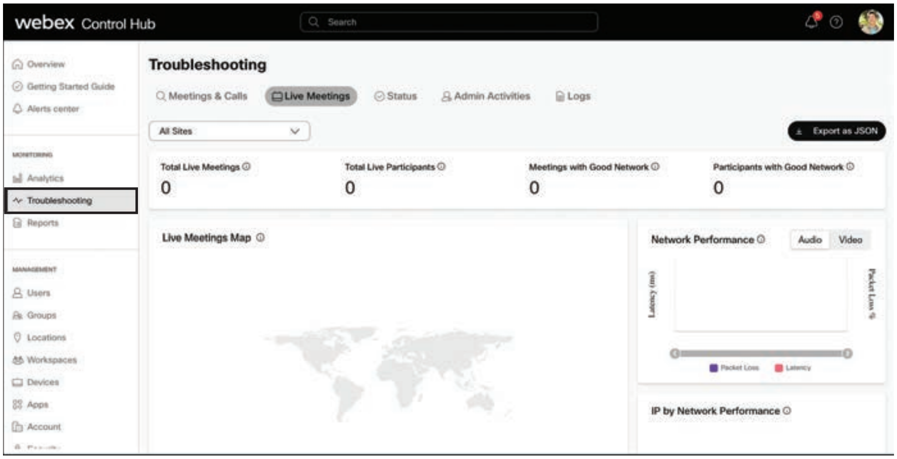


Figure 23-4 *Webex Control Hub Troubleshooting Screen*

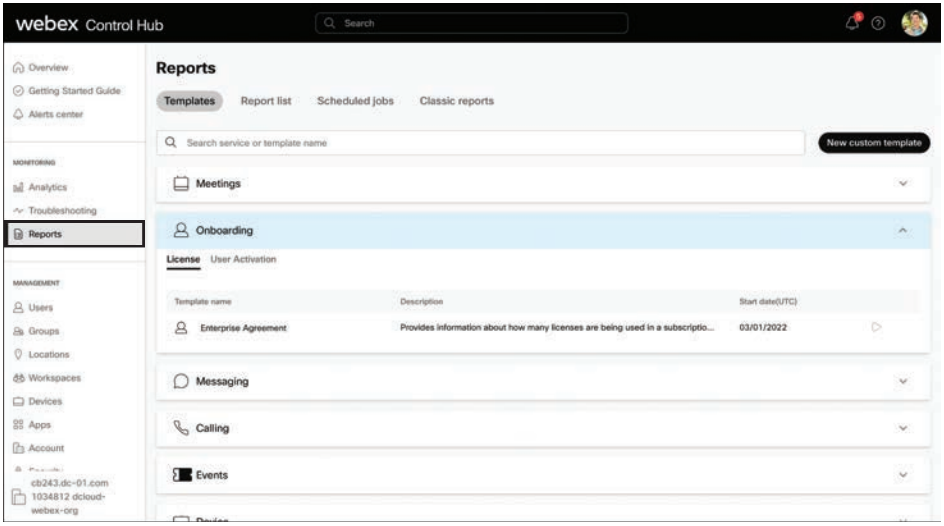
The **Reports** section helps you track and analyze the performance of Webex services in your organization. You can use reports to see details for each meeting, how often users are messaging each other, details for Webex Calling calls and call queues, how often Webex devices are used, onboarding information, and more.

The **Templates** tab allows you to generate a CSV-formatted report immediately or to schedule reports to run automatically in a daily, weekly, or monthly format. When you download a report, it uses the following naming format for the file:

- **Default report template:** *Default Template Name_alphanumeric characters_Download Date*
- **Custom report template:** *Custom Template Name_alphanumeric characters_Download Date*

The **Report list** tab shows a list of reports that are ready for you to download. If you choose to subscribe to a report when scheduling one, you'll also get an email that notifies you when the report is ready for you to download. When the report is generating, the status column changes to "In Progress." When the report is ready to download, the status column changes to "Complete." Your report might take up to 24 hours to generate, depending on the size of the report and how many reports are queued. Generated reports will show up in the **Report list** tab.

The **Scheduled jobs** tab shows a list of reports that are set up to run recurringly. You can see the recurring details for each report and when they were last generated. Figure 23-5 illustrates the Reports screen on the Webex Control Hub.



Template name	Description	Start date(UTC)
Enterprise Agreement	Provides information about how many licenses are being used in a subscriptio...	03/01/2022

Figure 23-5 *Webex Control Hub Reports Screen*

Webex Control Hub Management

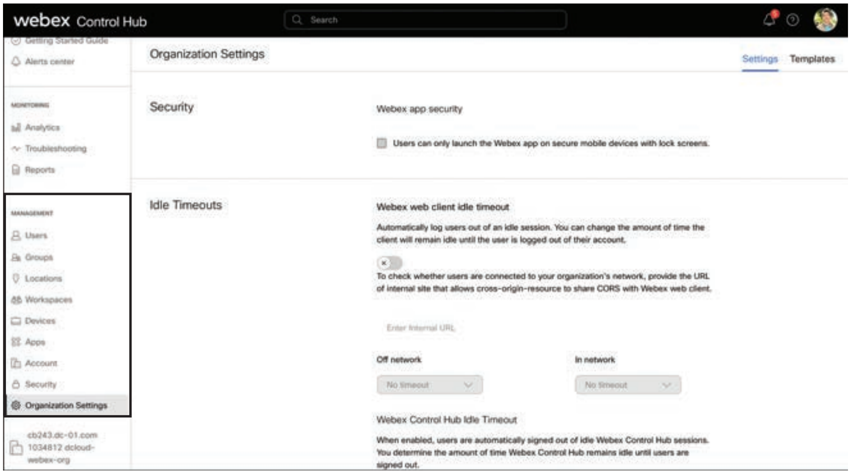
The **Management** section is used for general management of a customer site or sites. From here you can add users, groups, locations, workspaces, and devices. You can manage how users within the organization can utilize the Webex application, and you can manage the overall settings and security for your organization.

The **Users** menu is a high usage area within Webex Control Hub. Users are a core element of Webex. The Webex app, meetings, phones, Webex devices, and most other functions are tied to user accounts. The **Groups** menu allows administrators to organize and bulk-manage users based on common attributes, such as licenses, settings templates, and resources. Workspaces are the physical collaboration meeting rooms within your business site. The details found in the **Workspaces** menu give you an at-a-glance overview of the usage, settings, and environmental status of the physical location. This helps you understand the workspace conditions to make decisions that enhance the end-user experience. The **Devices** menu allows administrators to add Webex devices to your organization. After you add the device, you can configure and manage it here as well. Devices added here could be any type of device from a personal unified IP phone or Webex Desk endpoint, up to large video systems or Webex Boards. The **Apps** menu uses an advanced configuration area that allows functions such as embedded apps within Webex spaces and meetings, shortcuts in various locations, and integrations to various applications. The **Account** menu provides information, such as the organization name, data storage locations, licensing, and subscription information. **Security** is a new menu in Webex Control Hub that used to be a section under Organization Settings (discussed shortly). If you want to secure your users logging in even more, you can enable Single Sign-On (SSO). This Security menu is where SSO can now be enabled.

This brings us to the **Organization Settings** menu. Many items related to all aspects of Webex at the organization level are accessed in this screen. Parameters such as timeouts, internal/external communication, face recognition, and many more are configured here. There are too many to go into at this time, but the following list identifies all the sections under Organization Settings that can be customized or configured to your preferences. Figure 23-6 illustrates the Organization Settings menu options on the Webex Control Hub:

- Security
- Idle Timeouts
- Authenticated Sign in
- Allow to bring your own device (BYOD)
- Internal Communication
- External Communication
- Face Recognition
- Privacy
- Domains
- Self-Registration
- SIP Address for Cisco Webex Calling
- Calling Behavior
- UC Management Profiles
- Directory Synchronization
- Webex User Profile
- People Insights Profiles

- Recommended Messages
- Personal insights
- Authentication
- ThousandEyes
- User sign-in data
- Alerts
- Email
- Branding
- Customize support information
- Retention
- Discover devices for Webex app
- Scheduling in the Webex app
- Apps
- Simultaneous interpretation
- Virtual Background
- Virtual Camera
- VDI for Webex app
- Software updates for Webex app
- Default Landing Screen for Webex App
- Migrate Content
- Network location



Organization Settings

Security

Webex app security

□ Users can only launch the Webex app on secure mobile devices with lock screens.

Idle Timeouts

Webex web client idle timeout

Automatically log users out of an idle session. You can change the amount of time the client will remain idle until the user is logged out of their account.

To check whether users are connected to your organization's network, provide the URL of internal site that allows cross-origin-resource to share CORS with Webex web client.

Enter Internal URL

Off network: No timeout

In network: No timeout

Webex Control Hub Idle Timeout

When enabled, users are automatically signed out of idle Webex Control Hub sessions. You determine the amount of time Webex Control Hub remains idle until users are signed out.

Figure 23-6 *Webex Control Hub Organization Settings*

Webex Control Hub Services

The final section of Webex Control Hub is the Services area. Services deal mostly with how Webex Control Hub interacts with services hosted on other servers, whether they be Cisco servers like Cisco Unified Communications Manager or a third-party server like Microsoft Exchange.

The **Updates and Migrations** menu contains cards to help speed up the process of moving users and devices from Cisco Unified Communications Manager to Webex Control Hub. Many of the cards available under this menu require **Connected UC** to be configured before they can be utilized. The following list outlines each card with a short description. Figure 23-7 illustrates the Updates and Migrations cards available on the Webex Control Hub.

Key Topic

- **Migrate Jabber to the new Webex app:** This card is used to ensure user email addresses, calling, messaging and meetings are all aligned between users located on the Cisco Unified Communications Manager using Jabber and users on the Webex Control Hub. So-called "Common Identity" is achieved when a users' name, email address, and the other aforementioned information that exists in the Cisco Unified Communications Manager aligns with the user information that exists in Webex Control Hub. Migration cannot occur until Common Identity is achieved. The actual steps of migrating from the Jabber client to the Webex app takes place from the Cisco Unified Communications Manager. Once this is complete, the Webex app will register to the Webex Control Hub for IM and presence, but it will register to the Cisco Unified Communications Manager for calling. If you want calling to go through the Webex Control Hub as well, then you can run the wizard on the **Migrate Jabber to the new Webex app** card. Once migration is complete, Webex will use the Webex Control Hub for calling instead of the Cisco Unified Communications Manager. Deployment Insights must be enabled from **Connected UC** before this card can be used.

- **Migrate Enterprise phones to Multiplatform (MPP) firmware:** This card is used to migrate the firmware on phones from Enterprise to Multi-Platform Phone (MPP) so that they can register to Webex Control Hub. All Cisco Unified IP Phones that register to the Cisco Unified Communications Manager must be running Enterprise phone firmware. All Cisco Unified IP Phones registering to the Webex Control Hub must be running MPP firmware. Therefore, if an organization has phones registered to the Cisco Unified Communications Manager that they want to register to the Webex Control Hub instead, they will need to migrate the firmware first. There are several ways to do this, and each method requires a migration license be installed on the phone before the migration can occur. The exception to this rule is this card. You can use this card to launch a wizard that will help you migrate the firmware on your phones. Deployment Insights must be enabled from **Connected UC** before this card can be used.

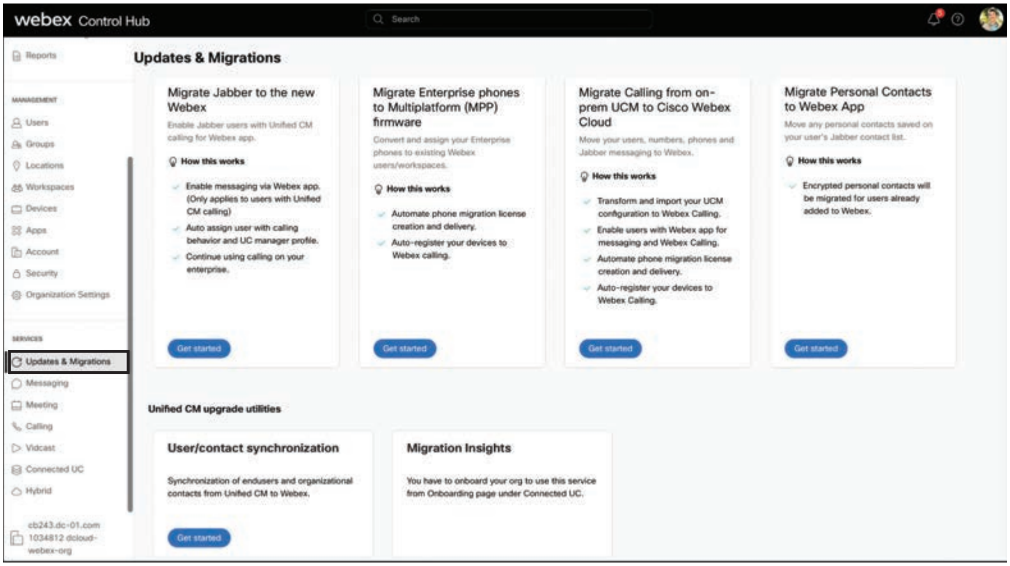
- **Migrate calling from On-Prem to Webex Cloud:** This card works similarly to the previous card. Perform the new and automated device firmware migration from Control Hub so that you can migrate your enterprise devices to cloud. You can migrate the required Enterprise firmware phones to MPP firmware from Control Hub. MPP phones are powered by Webex Calling solutions. MPP firmware can run on certain models of the Cisco IP Phone 6800, 7800, and 8800 series. However, only the Cisco IP Phone 7800 and 8800 series that are the right version have the capability to run either MPP firmware or Enterprise firmware. If you have the appropriate license, you can migrate between the MPP and Enterprise firmware on the Cisco IP Phone 7800 and 8800 series. Use the migration wizard on Control Hub to prepare your devices for migration. The migration wizard automates the device license generation and checks the device eligibility before you start the migration. This tool helps you to migrate your devices and assign them to the existing Webex users or workspaces.

- **Migrate personal contacts to Webex app:** Use Control Hub to migrate your end users' Jabber custom contacts or any third-party custom contact source to Webex personal contacts. Contact migration to cloud is a one-time import that enables you to search, look up, call, message, or invite your contacts similar to Jabber. End users define Webex Personal Contacts in the Webex app. Jabber Custom Contacts refer to non-directory contacts who are outside of your organization and contacts who are stored in the database of Cisco Unified Communications Manager – IM & Presence Service. Third-party contacts refer to contacts who are outside your organization that may be exported and later imported into Webex.

- **User/Contact Synchronization:** Perform the new user synchronization from Control Hub to migrate your users in Cisco Unified Communications Manager. Use this migration tool when you are not using the existing Webex methods to provision users such as Cisco Directory Connector, adding users manually, or using bulk import in Control Hub. There are many benefits to user synchronization. It provides a seamless user search experience. By synchronizing users and contacts to cloud, this feature helps Webex app to provide search functionality similar to Jabber. It also automates the task of synchronizing users from the Cisco Unified Communications Manager database into Webex. This feature facilitates synchronization and simplifies migration tasks, whereas a user sync done manually is error prone and time consuming. User/Contact Synchronization does not require **Connected UC** to be configured prior to setup, but the process of using this tool is much easier if utilized after **Connected UC** is enabled and Deployment Insights is set up. Contacts cannot be synched if used before **Connected UC** is set up, but they will work after Deployment Insights is active.

- **Migration Insights:** Migration Insights is a tool designed to help you to plan your Jabber migration from an on-premises deployment to cloud deployment. It allows you to gather the required information about the user's existing on-premises deployment services, such as third-party integration, endpoint types and configurations, and the type of services used by the end users. You can also view the list of Instant Messaging and Presence and Jabber features that might not be available or might be partially available after migration. These insights will help you to plan and build a timeline for a move to cloud effectively.

The Messaging, Meeting, and Calling menus are advanced settings for the three primary functions of Webex. **Messaging** allows you to configure additional setting to control information exchanges, instant messaging, content management, malware scanning, and more. **Meeting** allows you to control the functions of your meeting domains. You can access settings, manage meetings and webinars, and configure meeting templates. **Calling** allows you to configure which type of calling solution is used for each site within your organization, manage numbers, and configure global calling features such as Auto Attendant. We will delve much deeper into the Calling menus throughout Chapter 24, "Webex Calling Options," Chapter 25, "Webex Calling Features," and Chapter 26, "Webex Calling Using a Local Gateway."



Updates & Migrations

Migrate Jabber to the new Webex

Enable Jabber users with Unified CM calling for Webex app.

How this works

- Enable messaging via Webex app. (Only applies to users with Unified CM calling)
- Auto assign user with calling behavior and UC manager profile.
- Continue using calling on your enterprise.

Migrate Enterprise phones to Multiplatform (MPP) firmware

Convert and assign your Enterprise phones to existing Webex users/workspaces.

How this works

- Automate phone migration license creation and delivery.
- Auto-register your devices to Webex calling.

Migrate Calling from on-prem UCM to Cisco Webex Cloud

Move your users, numbers, phones and Jabber messaging to Webex.

How this works

- Transform and import your UCM configuration to Webex Calling.
- Enable users with Webex app for messaging and Webex Calling.
- Automate phone migration license creation and delivery.
- Auto-register your devices to Webex Calling.

Migrate Personal Contacts to Webex App

Move any personal contacts saved on your user's Jabber contact list.

How this works

- Encrypted personal contacts will be migrated for users already added to Webex.

Unified CM upgrade utilities

User/contact synchronization

Synchronization of endusers and organizational contacts from Unified CM to Webex.

Migration Insights

You have to onboard your org to use this service from Onboarding page under Connected UC.

Figure 23-7 *Webex Control Hub Updates and Migrations Cards*

Webex leap is a new accelerator program that gives small in-house teams the ability to brainstorm, experiment, iterate, and bring to market next-generation collaboration products. Vidcast is a video messaging tool that makes it easy to record videos, share them with teammates or customers, and quickly get feedback on the content helping distributed teams collaborate more effectively. The **Vidcast** menu allows administrators to set templates, manage recordings, and configure settings of Vidcasts.

Webex Cloud-Connected Unified Communications (CCUC) is a set of services in the Webex cloud that provides enhanced business and operational insights with the aim of improving administrative workflow productivity. It allows customers to leverage the benefits of the Webex cloud while keeping their critical calling workload on-premises. Customers log in to Webex Control Hub to get a single global view, where they can manage the entire on-premises Unified Communications (UC) network from a single operations control panel that supports their Cisco cloud or hybrid services. CCUC achieves this with plugins that are installed on the individual Cisco Unified Communications Manager application that send telemetry data to the Webex cloud. Plugins register with the Webex cloud during onboarding and are authenticated to the cloud using the Webex Common Identity framework. After initial onboarding and installation, subsequent updates to these plugins are automatically managed through the cloud. The Webex CCUC services suite provides a cost-effective, cloud-managed admin experience, with multi-cluster visibility. It provides business metrics essential for capacity planning and optimizing resources. It helps system administrators maintain and communicate service-related key performance indicators (KPIs). It provides automated workflows for end-to-end troubleshooting and change management tasks, such as upgrades and certificate management.

The **Connected UC** menu is used to enable Cisco Webex CCUC and connect your on-premises UC applications, such as Cisco Unified Communications Manager and IM & Presence to Control Hub. Many of the migration tasks discussed under the **Updates and**

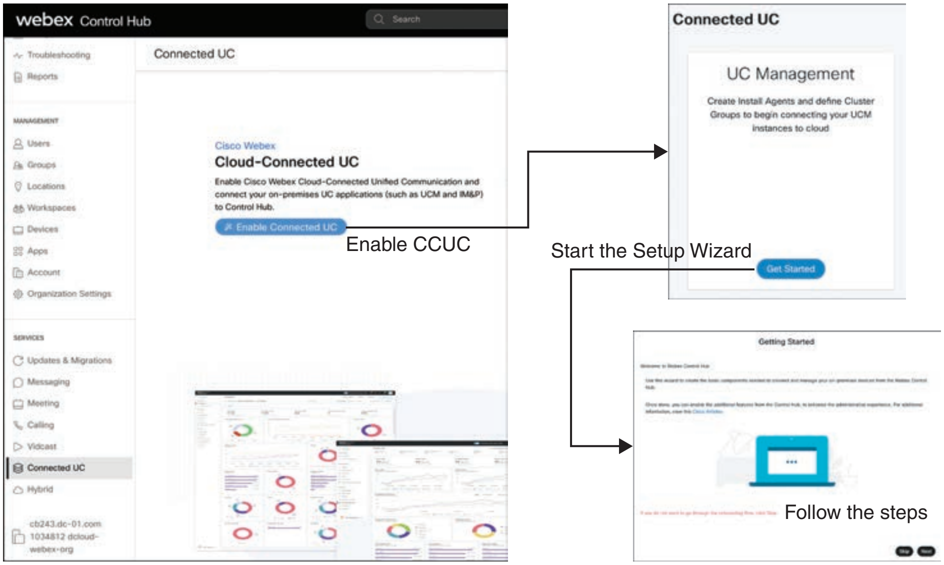
Migrations menu are dependent on services being enabled under **Connected UC**. The steps required to enable CCUC are as follows:

Key Topic

Step 1. Enable Cloud Connected Unified Communications. When you enable Connected UC for the first time, you can start a setup wizard that will walk you through the tasks to set everything up. You can skip the wizard if you'd rather perform the tasks manually on your own. Also, the wizard will only run the first time through. There is no way to restart the wizard if you skip it, or after you've used it the first time through. There are two tasks you will perform during the setup wizard:

a. First, you need to create an Agent Install file. This will need to be installed on Cisco Unified Communications Manager and IM & Presence servers so that Webex Control Hub can communicate with them, pull important files and logs, and manage them overall. All Cisco UC servers running version 12.5 SU4 or later already have the agent .cop file installed.

b. Next, you'll need to create a cluster group. Connected UC on-premises servers are organized in Control Hub using cluster groups. Once an agent install file is installed on UC appliance and verified, the cluster must be assigned to a cluster group. You can create multiple cluster groups if needed. Cluster groups can represent geolocations, release environments, and so on. Figure 23-8 illustrates how to initiate the setup wizard for Connected UC.



Cisco Webex

Cloud-Connected UC

Enable Cisco Webex Cloud-Connected Unified Communication and connect your on-premises UC applications (such as UCM and IM&P) to Control Hub.

UC Management

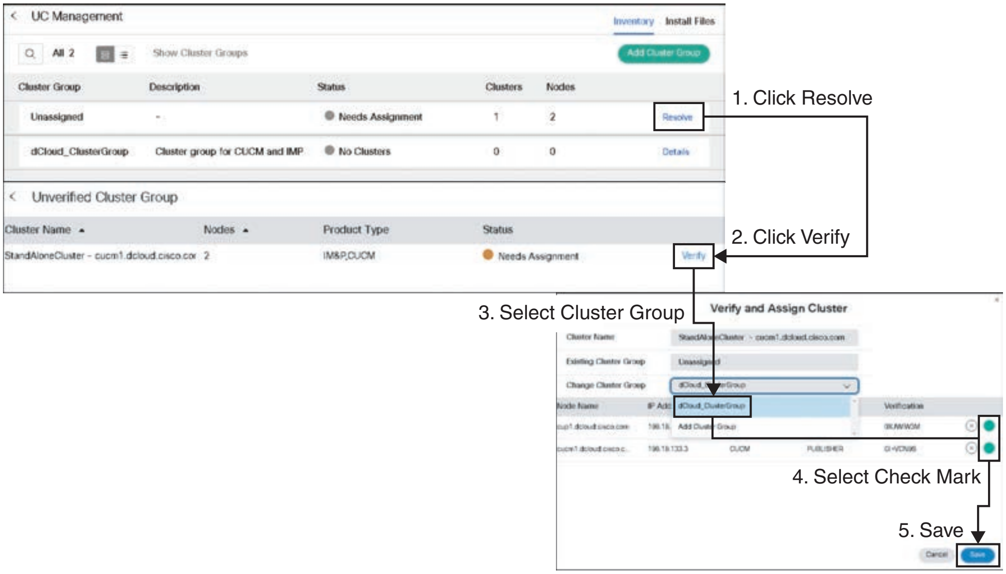
Create Install Agents and define Cluster Groups to begin connecting your UCM instances to cloud

Figure 23-8 *Connected UC Setup Wizard*

Step 2. Install and sync Agent Files. On the Cisco Unified Communications Manager admin CLI prompt, type **utils ucmgmt organization organization_id**. To find out your organization ID, from the customer view in Control Hub, go to **Management > Account**. In the **Company Information** section, you can see the organization ID. For example, organization_id could be

43e67ab7-8f31-4566-abfc-16b3de8362ac. Type **utils ucmgmt agent enable.** After a few minutes, the node is onboarded. Repeat the preceding steps on all the nodes in the cluster, including IM & Presence, Cisco Unity Connections, and Emergency Responder.

Step 3. Verify and assign clusters. From the customer view in Control Hub, go to **Services > Connected UC**. On the **UC Management** card, click **Inventory**. The **UC Management** page appears showing the list of cluster groups. If any of the cluster groups shows the **Needs Verification** status, click **Resolve** next to the cluster group. Click **Verify** next to a cluster. From the **Cluster Group** drop-down list, choose the cluster group to which you want to assign a cluster. After you assign a cluster to the cluster group, all the nodes belonging to that cluster get assigned to the selected cluster group. Click check mark next to the node that you want to assign to the cluster group, or click **X** to remove the node. Finally, click **Save**. Figure 23-9 illustrates how to verify and assign clusters in Connected UC.



Cluster Group	Description	Status	Clusters	Nodes	
Unassigned	-	● Needs Assignment	1	2	Resolve
dCloud_ClusterGroup	Cluster group for CUCM and IMP	● No Clusters	0	0	Details

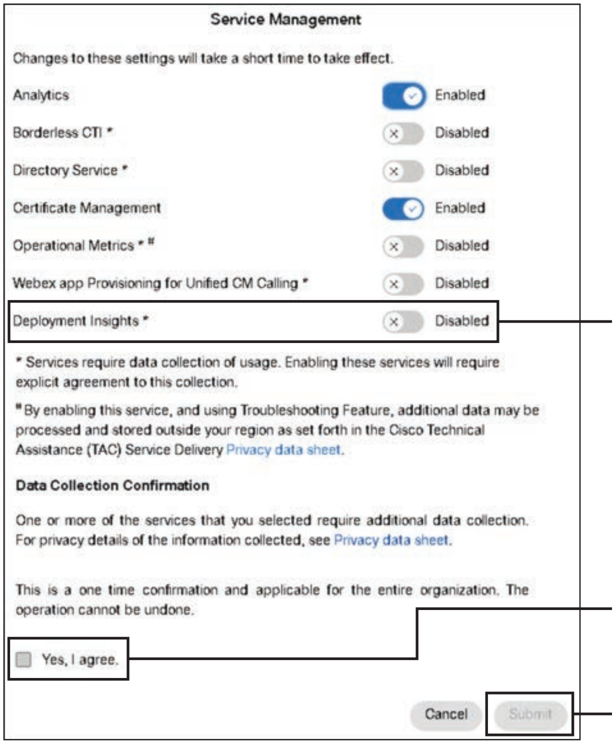
Cluster Name ▲	Nodes ▲	Product Type	Status	
StandAloneCluster - cucm1.dcloud.cisco.com	2	IM&P,CUCM	● Needs Assignment	Verify

Cluster Name: StandAloneCluster - cucm1.dcloud.cisco.com
Existing Cluster Group: Unassigned
Change Cluster Group: dCloud_ClusterGroup

Node Name	IP Add			Verification	
cup1.dcloud.cisco.com	198.18.			[illegible]	⊗ ●
cucm1.dcloud.cisco.c...	198.18.133.3	CUCM	PUBLISHER	[illegible]	⊗ ●

Figure 23-9 *Verify and Assign Clusters*

Step 4. Ensure Deployment Insight Service is enabled. There are several services that can be enabled once all nodes of a cluster have been added. Deployment Insights (DI) is one of the most critical. DI uses telemetry modules through microservices to collect user and device information from the Cisco Unified Communications Manager. Because DI is capable of collecting user information, you must agree to the terms of service before saving these changes. Figure 23-10 illustrates the services related to CCUC that can be enabled once the cluster nodes have been activated.



Service Management

Changes to these settings will take a short time to take effect.

Analytics	Enabled
Borderless CTI *	Disabled
Directory Service *	Disabled
Certificate Management	Enabled
Operational Metrics * #	Disabled
Webex app Provisioning for Unified CM Calling *	Disabled
Deployment Insights *	Disabled

* Services require data collection of usage. Enabling these services will require explicit agreement to this collection.

By enabling this service, and using Troubleshooting Feature, additional data may be processed and stored outside your region as set forth in the Cisco Technical Assistance (TAC) Service Delivery Privacy data sheet.

Data Collection Confirmation

One or more of the services that you selected require additional data collection. For privacy details of the information collected, see Privacy data sheet.

This is a one time confirmation and applicable for the entire organization. The operation cannot be undone.

□ Yes, I agree.

1. Enable Deployment Insights and any other service you need.

2. Click **Yes, I agree** to the Data Collection agreement.

3. Click **Submit** and wait up to eight hours for this service to enable.

Figure 23-10 *Cloud Connected UC Services*

The **Hybrid** menu identifies all the different hybrid integrations that can be incorporated into the Webex solution. Each integration is represented with a card that offers a description and a link to begin setting up the integration. Following is a list of all the different hybrid integrations available, along with a short description. Figure 23-11 illustrates the Hybrid cards available.

Key Topic

- **Hybrid Calendar:** You can use three different Hybrid Calendar integrations within the Webex environment. Hybrid Calendar allows you to use your calendar environment to schedule Webex meetings and add participants. You can simply use *@webex* or *@meet* in a meeting location to insert join details, show upcoming meetings in the Webex app, and provide One Button to Push (OBTP) to join. The three Hybrid Calendar deployment option are as follows:
  - Exchange
  - Office 365
  - Google Calendar
- **Groups Integration:** Connect Webex to Microsoft Office 365 and create teams for your Microsoft 365 groups.
- **Hybrid Calling for Webex Devices:** Hybrid Calling provides Cisco Unified Communications Manager on-premises calling capabilities to Webex cloud-registered devices.

- **Hybrid Message:** Connect Webex to Cisco Unified Communications Manager IM and Presence Service so that Cisco Webex users and Cisco Jabber users can direct message each other.

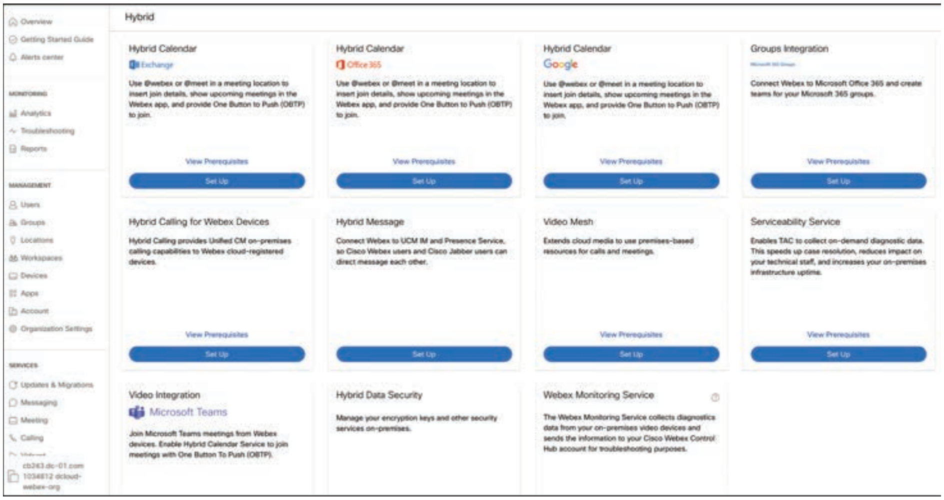
- **Video Mesh:** Extends cloud media to use on-premises-based resources for calls and meetings.

- **Serviceability Service:** Enables TAC to collect on-demand diagnostic data. This speeds up case resolution, reduces impact on your technical staff, and increases your on-premises infrastructure uptime.

- **Video Integration:** Join Microsoft Teams meetings from Webex devices. Enable Hybrid Calendar Service to join meetings with One Button To Push (OBTP).

- **Hybrid Data Security:** Manage your encryption keys and other security services on-premises.

- **Webex Monitoring Service:** The Webex Monitoring Service collects diagnostics data from your on-premises video devices and sends the information to your Cisco Webex Control Hub account for troubleshooting purposes.



Hybrid Calendar
Exchange
Use @webex or @meet in a meeting location to insert join details, show upcoming meetings in the Webex app, and provide One Button to Push (OBTP) to join.

Hybrid Calendar
Office 365
Use @webex or @meet in a meeting location to insert join details, show upcoming meetings in the Webex app, and provide One Button to Push (OBTP) to join.

Hybrid Calendar
Google
Use @webex or @meet in a meeting location to insert join details, show upcoming meetings in the Webex app, and provide One Button to Push (OBTP) to join.

Groups Integration
Microsoft 365 Groups
Connect Webex to Microsoft Office 365 and create teams for your Microsoft 365 groups.

Hybrid Calling for Webex Devices
Hybrid Calling provides Unified CM on-premises calling capabilities to Webex cloud-registered devices.

Hybrid Message
Connect Webex to UCM IM and Presence Service, so Cisco Webex users and Cisco Jabber users can direct message each other.

Video Mesh
Extends cloud media to use premises-based resources for calls and meetings.

Serviceability Service
Enables TAC to collect on-demand diagnostic data. This speeds up case resolution, reduces impact on your technical staff, and increases your on-premises infrastructure uptime.

Video Integration
Microsoft Teams
Join Microsoft Teams meetings from Webex devices. Enable Hybrid Calendar Service to join meetings with One Button To Push (OBTP).

Hybrid Data Security
Manage your encryption keys and other security services on-premises.

Webex Monitoring Service
The Webex Monitoring Service collects diagnostics data from your on-premises video devices and sends the information to your Cisco Webex Control Hub account for troubleshooting purposes.

Figure 23-11 *Webex Hybrid Integration Cards*

Methods of Adding Users to Webex Control Hub

Several options are available for creating Webex accounts or transitioning user accounts from Cisco Unified Communications Manager. It is important to define users within the Webex environments. The most common definition of "user" is a person who has a phone or soft client associated with the user account. Other "users" in Webex are not associated with a person, but they are still technically called "users." *Workspaces* such as conference rooms, lobby phones, and areas with a device or machine account from the calling environment are another type of user. *Service numbers* that are machine accounts for a feature such as a hunt group, paging, or conference device are a third type of user in Webex. *Personal contacts* are the fourth type user. These are directory entries that can be saved on any phone or device for faster calling and can therefore include any of the previously mentioned user types.

Multiple Webex Control Hub options exist for migrating users from the Cisco Unified Communications Manager to Webex or when adding new users into the Webex environment:

Key Topic

- Add users manually, one at a time.
- Add users or change user information by importing a CSV file. Import up to 25 lines to add or change 25 users.
- **Claim existing Webex users** that may have been created as individual Webex accounts.
- **Directory Management** will integrate Webex with an existing Active Directory environment and requires more effort than other options, possibly requiring a connector between environments.
- Synchronize user and contact information with the **User/contact synchronization** tool.

Add Users Manually

You can manually add up to 25 users at a time to your organization by entering their email addresses. You can also manage external users who are in different organizations already by assigning a Webex Meetings license to them. If you get an error when trying to add a user who used their email address to create a trial account, have the user delete their old organization first before adding them to your organization. The wizard used to add users manually is easy to follow. You can add users manually by following these steps:

Key Topic

Step 1. Sign in to Control Hub at **https://admin.webex.com**.

Step 2. Click **Users > Manage users > Manually add users**. You may see a notice that users will automatically receive a welcome email. If you don't want this, do the following:

a. Back out from adding users.

b. Click **Organization Settings > Email**.

c. Toggle off **Automatic activation emails.**

d. Return to **Users > Manage users > Manually add users**.

Step 3. Choose one of the following:

- **Email address**
- **Names and Email address**

Step 4. Create a list. Create a list of users you want to add or modify and then click **Next**. If you're just using email addresses, you can separate them with commas. If you're adding names as well, click + after each entry to add it to the list. You cannot add users who are eligible to be claimed to your organization. You cannot add existing users in your organization or users who already have a Webex account.

Step 5. Assign licenses. If you are using automatic license assignment, you can see which services those users are getting. If you want to override the automatic license assignment for these users, click **Assign license manually** and select the services to assign. If you're not using automatic license assignment, select the services to assign to the users in your list. If you have multiple subscriptions, choose which subscription supplies the licenses. If you added Webex Calling to the user, you can assign a location, phone number, and extension.

Step 6. Assign tracking codes. If you gave your new users Meeting licenses, and if their Meeting sites require tracking codes, add those tracking codes to the users on the next screen of the wizard. If you're not using tracking codes, you can skip this step.

Step 7. Assign content management. If **global access** is selected for your enterprise content management, then content management is automatically assigned to users, and you won't see this screen. Therefore, you can skip this step as well. Otherwise, choose a content management option for each user.

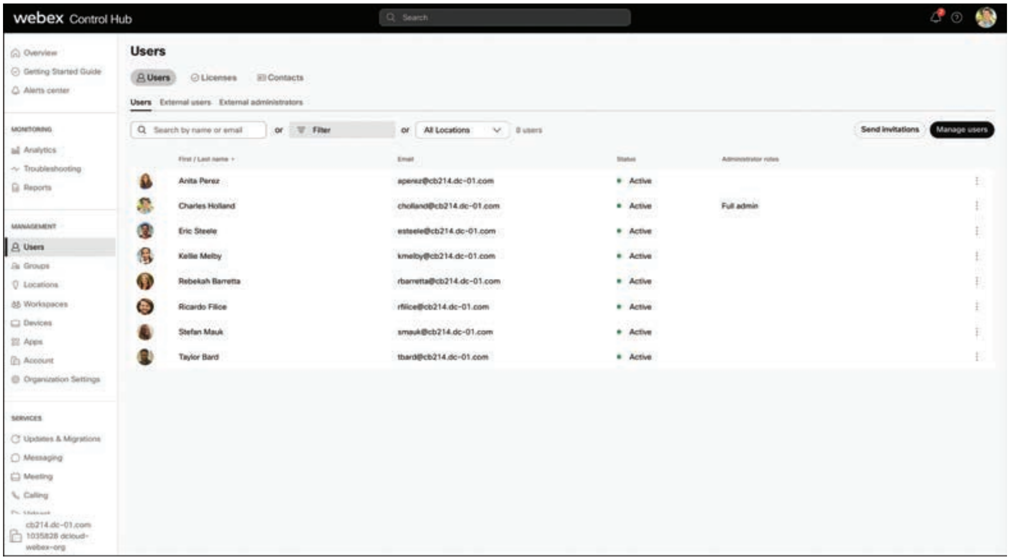
Step 8. Review the list of users and services when you see the **Review** screen.

Step 9. Click **Add Users**.

Webex processes your list of users and licenses and shows you a summary of the results. If you are using automated welcome emails, Webex sends those emails to the new users from your list. The new users are in Control Hub, showing as Pending until they sign in for the first time. Each license you granted is taken from your subscription when the user first signs in to Webex.

Step 10. Review the summary page of records processed and click **Finish** to exit the wizard.

You might get an error when trying to access Calling settings for a newly added user. Cisco recommends that you remove the Webex Calling license and then reassign the calling license to the user. Figure 23-12 illustrates the Users page in Webex Control Hub.



First / Last name	Email	Status	Administrator roles
Anita Perez	aperez@cb214.dc-01.com	Active	
Charles Holland	cholland@cb214.dc-01.com	Active	Full admin
Eric Steele	esteele@cb214.dc-01.com	Active	
Kellie Melby	kmelby@cb214.dc-01.com	Active	
Rebekah Barretta	rbarretta@cb214.dc-01.com	Active	
Ricardo Filice	rfilice@cb214.dc-01.com	Active	
Stefan Mauk	smauk@cb214.dc-01.com	Active	
Taylor Bard	tbard@cb214.dc-01.com	Active	

Figure 23-12 *Webex Control Hub Users Page*

Add Users with a CSV File

You can use the comma-separated value (CSV) template to add up to 20,000 users to your organization and assign services at the same time. If you have more than one CSV file for your organization, then upload one file, and once that task has completed, you can upload the next file. Some spreadsheet editors remove the + sign from cells when the CSV is opened. We suggest you use a text editor to make CSV updates. If you use a spreadsheet editor, make sure to set the cell format to text and then add back any + signs that were removed. To add users to Webex Control Hub using a CSV file, follow these steps:

Key Topic

Step 1. From the customer view in https://admin.webex.com, go to **Users**, click **Manage Users** and choose **CSV Add or Modify Users**.

Step 2. Click **Export** to download the file. You can enter user information on a new line in the CSV file.

- To assign a service, add **TRUE** in that service's column, and to exclude a service, add **FALSE**. The **User ID/Email (Required)** column is the only required field. If you have specific directory and external numbers for each new user, then include the leading + for external numbers without other characters,

- If you have an active license template, leave all the service columns blank, and the template is automatically assigned for the new user in that row.

- To assign a location, enter the name in the **Location** column. If you leave this field blank, the user is assigned to the default location.

- You can't assign enterprise content management permissions to users using the license template.

- If you're adding users as supervisors for Cisco Webex Contact Center, you must add users manually. You can only assign **Standard** and **Premium** roles with a CSV file.

- When entering a user's name, make sure to include their last name; otherwise, you may run into issues.

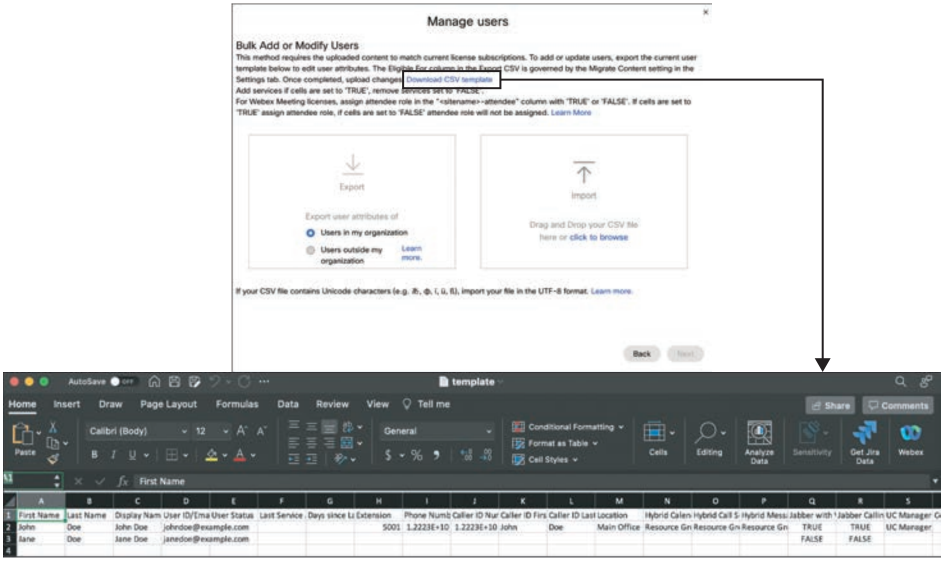
Step 3. Once you have completed filling out the CSV file with all user information, return to the Webex Control Hub, click **Import**, select your file, and click **Open**.

Step 4. Choose either **Add services only** or **Add and remove services**.

Step 5. If you have an active license template, choose **Add services only**.

Step 6. Click **Submit**.

The CSV file is uploaded, and your task is created. You can close the browser or this window, and your task continues to run. Figure 23-13 illustrates the Manger Users page in Webex Control Hub where CSV files can be exported and imported. It also shows what some of the fields in the CSV file look like.



Manage users

Bulk Add or Modify Users

This method requires the uploaded content to match current license subscriptions. To add or update users, export the current user template below to edit user attributes. The Eligible For column in the Export CSV is governed by the Migrate Content setting in the Settings tab. Once completed, upload changes. Download CSV template

Add services if cells are set to 'TRUE', remove services set to 'FALSE'.

For Webex Meeting licenses, assign attendee role in the "<sitename>-attendee" column with 'TRUE' or 'FALSE'. If cells are set to 'TRUE' assign attendee role, if cells are set to 'FALSE' attendee role will not be assigned. Learn More

Export

Export user attributes of

● Users in my organization

○ Users outside my organization Learn more.

Import

Drag and Drop your CSV file here or click to browse

If your CSV file contains Unicode characters (e.g. 赤, ф, ï, ü, ß), import your file in the UTF-8 format. Learn more

Back Next

A1 fx First Name

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	First Name	Last Name	Display Nam	User ID/Ema	User Status	Last Service	Days since La	Extension	Phone Numb	Caller ID Nur	Caller ID Firs	Caller ID Last	Location	Hybrid Calen	Hybrid Call S	Hybrid Messi	Jabber with	Jabber Callin	UC Manager
2	John	Doe	John Doe	johndoe@example.com				5001	1.2223E+10	1.2223E+10	John	Doe	Main Office	Resource Gn	Resource Gn	Resource Gn	TRUE	TRUE	UC Manager
3	Jane	Doe	Jane Doe	janedoe@example.com													FALSE	FALSE	
4																			

Figure 23-13 *Webex Control Hub CSV Files*

Claim Existing Users

Anyone can sign up for a free Webex Account. There are a great number of services you can utilize once your account is active, but this list of services is understandably limited. With a subscription to Webex, the value of these previously utilized services increases exponentially; plus, you gain access to so many more useful tools. What often happens within businesses is that users will sign up for the free Webex account using their work email address before their company purchases a subscription. Should that organization purchase a Webex subscription and activate the account, this does not mean users who already have the free Webex account automatically gain access to those added benefits behind a subscription. They still need to be added to the Webex Control Hub of that organization before the benefits of the subscription can be consumed.

As an administrator, you can claim the accounts of your users who registered on their own for a Webex account. After you do so, they can use features included in the subscription for your organization. You can also check and update the license assignments for these users during the user claim review. There is a tool that allows user content (such as spaces, chat messages, shared files, and so on) to migrate with their app when the user's personal Webex account is claimed. This migrate content feature applies only to personal Webex accounts, however. You can migrate a user from one enterprise organization to another, but you can't transfer their Webex conversations in this case. This helps ensure corporate secrets are not shared outside an organization. Deleting your original organization permanently deletes all information associated with your organization, including data for all users. You'll lose data like Webex app messages and files as well as all Webex Meetings data, including Webex Meetings URLs and meeting recordings. When a user is claimed, all their content in their previous organization will be permanently deleted.

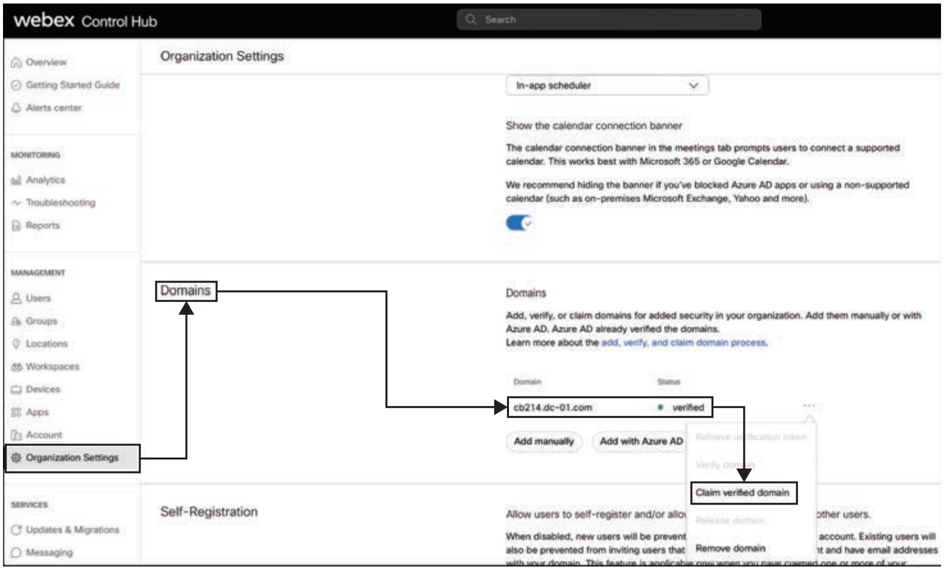
Key Topic

Some Control Hub features require proof of domain ownership. Others use domains to ensure the security and integrity of your organization. You can use domains to help with user management. Verify your domains to prove to Webex that you own them. Verifying domains allows you to claim users into your organization if they signed up into a different organization. You do not have to claim a domain before claiming users, but you must verify your domains before you can claim them. To verify domains, Webex provides a token to add to your domain host's DNS TXT record. To confirm that you own the domain, Webex will check for this token on the DNS server.

Key Topic

You can claim a domain to associate that domain to automatically be created within your organization. Users who sign themselves up for Webex are also associated with this domain. Otherwise, users who sign themselves up are created in a general organization with all the other "free" users. You cannot manage their services until you claim the users into your organization. Again, keep in mind that you don't have to claim a domain to claim a user into your organization.

Users who exist in the free consumer organization are not automatically converted to your organization. You must convert these users. Cisco recommends that you convert consumer users to your organization before claiming the domain. Two different domains can't be claimed for one organization. The purpose of the domain claim is to prevent other organizations from using the domain. You can release a domain if you want to claim it in a different organization, so long as you own the domain and manage both organizations. Figure 23-14 illustrates the menu in Webex Control Hub where a domain can be verified and claimed.



Organization Settings

In-app scheduler

Show the calendar connection banner

The calendar connection banner in the meetings tab prompts users to connect a supported calendar. This works best with Microsoft 365 or Google Calendar.

We recommend hiding the banner if you've blocked Azure AD apps or using a non-supported calendar (such as on-premises Microsoft Exchange, Yahoo and more).

Domains

Add, verify, or claim domains for added security in your organization. Add them manually or with Azure AD. Azure AD already verified the domains.
Learn more about the add, verify, and claim domain process.

Domain	Status
cb214.dc-01.com	● verified

Self-Registration

Allow users to self-register and/or allo other users.

When disabled, new users will be prevent account. Existing users will also be prevented from inviting users that it and have email addresses with your domain. This feature is applicable only when you have claimed one or more of your

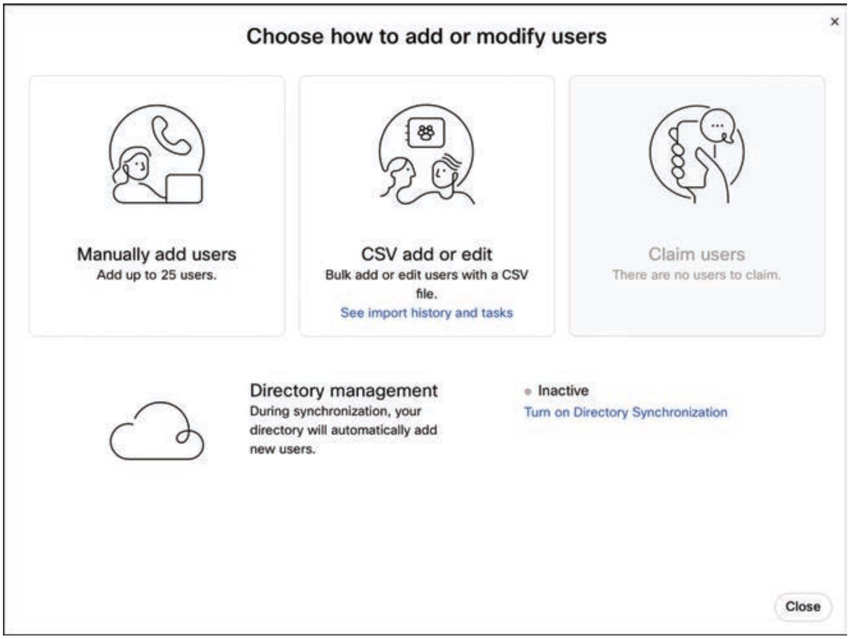
Figure 23-14 *Webex Control Hub Verify and Claim Domain*

The three methods for claiming users in Webex Control Hub are as follows:

- **Method 1: Claim Users:** This method shows you a list of up to 250 users you can claim outside your organization. If there are more than 250 users to claim and you want to make changes to the list, you must export the CSV file and follow the steps in **Method 2: CSV Add or Edit** to continue with the claiming process.

- **Method 2: CSV Add or Edit:** This method exports a CSV file of all users outside your organization that you can claim. You can edit the CSV file to choose who you want to claim.

- **Method 3: Manually Add Users:** As previously described, this method allow you to individually add up to 25 email addresses or names of the users you want to claim. Figure 23-15 illustrates the **Users** menu that allows you to select which method you want to use.



Choose how to add or modify users

×

Manually add users
Add up to 25 users.

CSV add or edit
Bulk add or edit users with a CSV file.
See import history and tasks

Claim users
There are no users to claim.

Directory management
During synchronization, your directory will automatically add new users.

● Inactive
Turn on Directory Synchronization

Close

Figure 23-15 *Webex Control Hub Claim Users Menu*

Key Topic

To use the **Claim users** card, follow these steps:

Step 1. Sign in to Control Hub at **https://admin.webex.com**.

Step 2. Go to **Users**, click **Manage users**, and select **Claim Users**.

Step 3. Select the users you want to claim and then click **Next**.

Step 4. Follow the wizard to add services for the users. If you use automatic license assignment, Webex assigns licenses to the new users.

Step 5. Check the **I understand that claiming these users is permanent and agree to proceed** check box.

Step 6. Click **Add Users**.

Directory Management

There are three methods for adding users to the Webex Control Hub using directory services. You can use only one of these services at a time. If you deploy a second of these services after one of them has already been deployed, the setup will fail. You must disable the first service before deploying the second. Any remnant user data will be deleted after completing the second directory synchronization.

Key Topic

You can synchronize users from an on-premises Microsoft Active Directory (AD), or you can synchronize users from a cloud-based directory service provider. Two cloud-based directory services are approved to interoperate with Webex, Microsoft Azure Active Directory (Azure AD), and Okta.

If your company uses an on-premises AD, you can add users and synchronize them from your AD with Webex Directory Connector. The Directory Connector is an essential tool for synchronizing your AD with the backend Webex cloud directory and allows your users to use cloud services such as Webex Meeting and Webex app services. After adding users through this method, use any of the following options to assign services to your users:

- After the sync status screen, you can select services to add them to all users at once. You can make individual modifications later.
- At any time after you synchronize your users into Webex, you can entitle specific user through an exported CSV template.

If you're using Okta or Azure AD for user management, you can add Webex as an application and then synchronize users from the directories into your organization managed in Control Hub. No on-premises infrastructure or connectors are required. This integration keeps your user list in sync whenever a user is created, updated, or removed from the application in Okta or Azure AD.

You can add Webex to Azure AD and then synchronize users from the directory into your organization managed in Control Hub. The synchronization requires no on-premises infrastructure or connectors. This integration keeps your user list in sync whenever a user is created, updated, or removed from the application in Azure AD. The integration between users in the directory and Control Hub uses the System for Cross-domain Identity Management (SCIM) API. SCIM is an open standard for automating the exchange of user identity information between identity domains or IT systems. SCIM is designed to make it easier to manage user identities in cloud-based applications and services. SCIM uses a standardized API through REST. Use the Azure AD Wizard app in Control Hub to simplify the synchronization of users and groups with Webex. The Wizard app allows you to easily configure which attributes, users, and groups to synchronize as well as to decide whether to synchronize users' avatars to Webex.

You can add Webex to the Okta Integration Network and then synchronize users from the directory into your organization managed in Control Hub. No on-premises infrastructure or connectors are required. This integration keeps your user list in sync whenever a user is created, updated, or removed from the application in Okta. The integration between users in the Okta directory and Control Hub also uses the SCIM API. The Okta integration supports only the following attributes:

- *userName*
- *displayName*
- *name.familyName*
- *name.givenName*
- *externalId*
- *title*

Multivalued attributes, **PhoneNumber** for **mobile** and **work**, as well as **Address** aren't supported by Okta because the operation for **PATCH**, **PUT**, or **DELETE** isn't passed by the Okta application to Webex. If you use Okta for directory synchronization, you'll need to remove these attributes from the Okta mapping or remove the update from the sync configuration. The Okta integration does support the following user synchronization features:

- **Create Users:** Creates or links a user in the Webex app when you assign the app to a user in Okta.
- **Update User Attributes:** Okta updates a user's attributes in Webex when the account is assigned. Future attribute changes made to the Okta user profile automatically overwrite the corresponding attribute value in the Webex cloud.
- **Deactivate Users:** Deactivates a user's Webex account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if you reassign the account to a user in Okta.

User Contact Synchronization

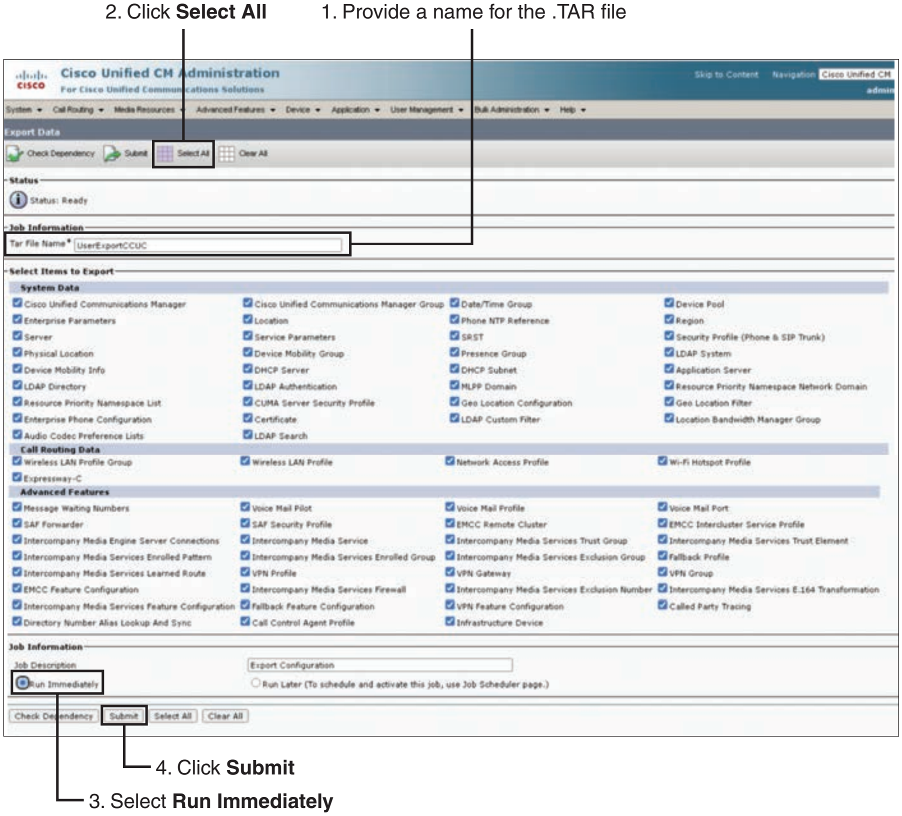
If you have users in the Cisco Unified Communications Manager that you also want to incorporate in Webex Control Hub for enabling CCUC, then it is important that you establish Common Identity. As mentioned previously, Common Identity is established by ensuring the user's email address is the same in Cisco Unified Communications Manager as it is in Webex Control Hub. The best tool for this job is the user synchronization tool found in the Webex Control Hub. This tool differs slightly depending on whether Connected UC has been enabled.

When using the User Synchronization tool prior to enabling Connected UC, the administrator must manually download all the user information from the Cisco Unified Communications Manager prior to importing this information to the Webex Control Hub. This makes sense because without Connected UC enabled, Webex Control Hub is unaware of how to reach Cisco Unified Communications Manager. The basic steps used to synchronize users from Cisco Unified Communications Manager to Webex Control Hub using the User Synchronization tool are as follow:

Key Topic

Step 1. From the Cisco Unified Communications Manager's **Cisco Unified CM Administration** screen, navigate to **Bulk Administration > Import/Export > Export**. Enter a **Tar File Name**, click **Select All**, select the radio button for **Run Immediately**, and click **Submit**. After the file is ready for download, go to **Bulk Administration > Upload/Download Files**, select your file, and download it to your computer. Figure 23-16 illustrates how to export user data from Cisco Unified Communications Manager.

Step 2. From the Webex Control Hub, go to **Services > Updates and Migrations**. Locate the **User/Contact Synchronization** card and click **Get Started**. Ensure all prerequisites are met and then upload the file to the Webex Control Hub you downloaded from the Cisco Unified Communications Manager. This will start the user synchronization process. Follow the steps through the wizard until all users are added. Figure 23-17 illustrates how to import user data to Webex Control Hub for user synchronization.


2. Click **Select All**

1. Provide a name for the .TAR file

Status

Status: Ready

Job Information

Tar File Name* UserExportCCUC

Select Items to Export

System Data

☑ Cisco Unified Communications Manager
☑ Enterprise Parameters
☑ Server
☑ Physical Location
☑ Device Mobility Info
☑ LDAP Directory
☑ Resource Priority Namespace List
☑ Enterprise Phone Configuration
☑ Audio Codec Preference Lists

☑ Cisco Unified Communications Manager Group
☑ Location
☑ Service Parameters
☑ Device Mobility Group
☑ DHCP Server
☑ LDAP Authentication
☑ CUMA Server Security Profile
☑ Certificate
☑ LDAP Search

☑ Date/Time Group
☑ Phone NTP Reference
☑ SRST
☑ Presence Group
☑ DHCP Subnet
☑ MLPP Domain
☑ Geo Location Configuration
☑ LDAP Custom Filter

☑ Device Pool
☑ Region
☑ Security Profile (Phone & SIP Trunk)
☑ LDAP System
☑ Application Server
☑ Resource Priority Namespace Network Domain
☑ Geo Location Filter
☑ Location Bandwidth Manager Group

Call Routing Data

☑ Wireless LAN Profile Group
☑ Expressway-C

☑ Wireless LAN Profile

☑ Network Access Profile

☑ Wi-Fi Hotspot Profile

Advanced Features

☑ Message Waiting Numbers
☑ SAF Forwarder
☑ Intercompany Media Engine Server Connections
☑ Intercompany Media Services Enrolled Pattern
☑ Intercompany Media Services Learned Route
☑ EMCC Feature Configuration
☑ Intercompany Media Services Feature Configuration
☑ Directory Number Alias Lookup And Sync

☑ Voice Mail Pilot
☑ SAF Security Profile
☑ Intercompany Media Service
☑ Intercompany Media Services Enrolled Group
☑ VPN Profile
☑ Intercompany Media Services Firewall
☑ Fallback Feature Configuration
☑ Call Control Agent Profile

☑ Voice Mail Profile
☑ EMCC Remote Cluster
☑ Intercompany Media Services Trust Group
☑ Intercompany Media Services Exclusion Group
☑ VPN Gateway
☑ Intercompany Media Services Exclusion Number
☑ VPN Feature Configuration
☑ Infrastructure Device

☑ Voice Mail Port
☑ EMCC Intercluster Service Profile
☑ Intercompany Media Services Trust Element
☑ Fallback Profile
☑ VPN Group
☑ Intercompany Media Services E.164 Transformation
☑ Called Party Tracing

Job Information

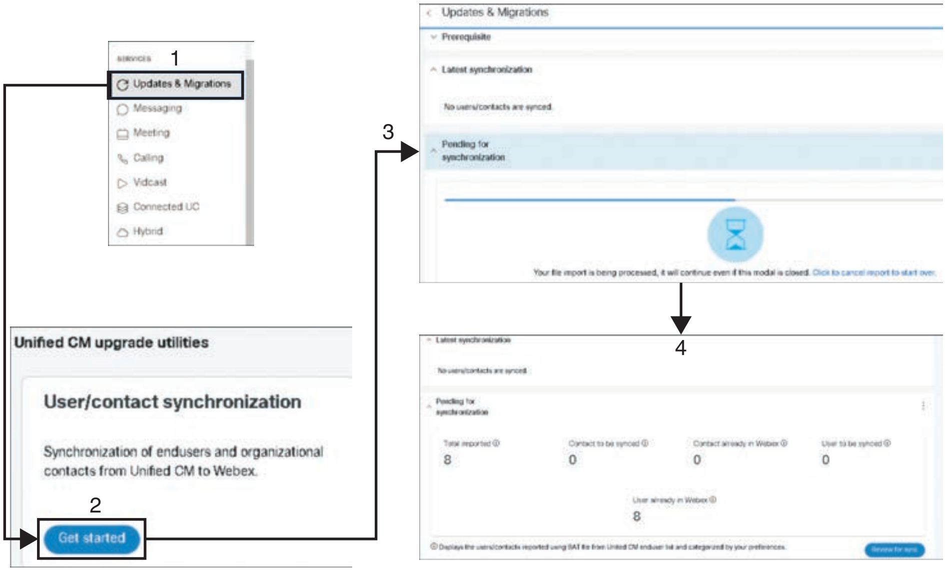
Job Description Export Configuration

● Run Immediately ○ Run Later (To schedule and activate this job, use Job Scheduler page.)

4. Click **Submit**

3. Select **Run Immediately**

Figure 23-16 *User Data Export from Cisco Unified Communications Manager*



Unified CM upgrade utilities

User/contact synchronization

Synchronization of endusers and organizational contacts from Unified CM to Webex.

No users/contacts are synced.

Your file import is being processed, it will continue even if this modal is closed. Click to cancel import to start over.

No users/contacts are synced.

Total imported	Contact to be synced	Contact already in Webex	User to be synced
8	0	0	0

User already in Webex
8

Displays the users/contacts imported using BAT file from Unified CM enduser list and categorized by your preferences.

Figure 23-17 *User Data Export from Cisco Unified Communications Manager*

Setting up user synchronization after Connected UC has been set up is much easier and can save you some time. Since Webex Control Hub is aware of how to communicate with Cisco Unified Communications Manager, there is no need to take that extra step of downloading user information from Bulk Administration on Cisco Unified Communications Manager. You are also presented with choices for user synchronization: you can sync with the Cisco Unified Communications Manager, you can sync with LDAP, or you can use both. This LDAP sync is not the same thing as Directory Connector user import. If you choose to sync with Cisco Unified Communications Manager, you cannot reverse this action, so be sure this is what you want to do before proceeding.

There are some other differences between using user synchronization before and after Connected UC is enabled. If user synchronization is used before Connected UC is enabled, then only users are synched, not contacts. However, after Connected UC is enabled, users and contacts to be synched. Also, if user synchronization is used before Connected UC is enabled, this is a one-time push of user data. If users are added to or deleted from the Cisco Unified Communications Manager after the user synchronization, that data is not replicated to Webex Control Hub. However, setting up user synchronization after Connected UC is enabled allows periodic synchronizations to be scheduled from Webex Control Hub.

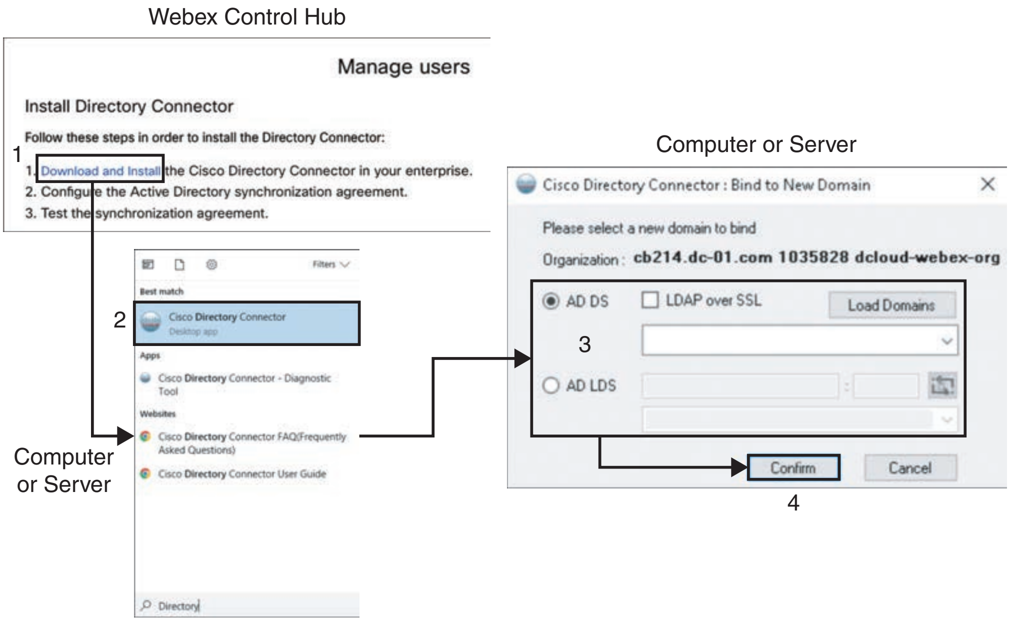
As you can clearly see, Cisco has provided many different avenues that allow organizations to add users to Webex Control Hub based on their needs and the solutions they are deploying. Above all these options, however, there is one method Cisco recommends using—importing users through the Directory Connector.

Directory Connector Configuration

Directory Connector is an on-premises application for identity synchronization into the cloud. You download the Directory Connector software from Control Hub and install it on your local machine. With Directory Connector, you can maintain your user accounts and data in the on-premises AD, so AD becomes the single source of truth. When you make a change on-premises, it is replicated to the cloud. Using directory synchronization through Directory Connector requires communication in three areas:

- **Control Hub** is the single interface that lets you manage all aspects of your Webex organization: view users, assign licenses, download Directory Connector, and configure single sign-on (SSO) if you want your users to authenticate through their enterprise identity provider and you don't want to send email invitations for the Webex app.
- **Directory Connector management interface** is the software that you download from Control Hub and install on a trusted Windows server. For multiple AD domains, you can install one instance of the software for each domain you want to synchronize. Using the software, you can run a synchronization to bring your Active Directory user accounts into Webex, view and monitor synchronization status, and configure Directory Connector services.
- **Directory synchronization service** queries your AD to retrieve users and groups to synchronize to the connector service and Directory Connector.

To use directory synchronization, you need to download and install the Directory Connector from Webex Control Hub. The Directory Connector can be installed on the same server where AD is located or on any other trusted member of the Windows domain. Figure 23-18 illustrates how to download Directory Connector from Webex Control Hub. Here are the steps to follow:


Webex Control Hub
Manage users
Install Directory Connector
1
2
Best match
Cisco Directory Connector
Desktop app
Apps
Cisco Directory Connector - Diagnostic Tool
Websites
Cisco Directory Connector FAQ(Frequently Asked Questions)
Cisco Directory Connector User Guide
Directory
Computer or Server
Computer or Server
Cisco Directory Connector : Bind to New Domain
● AD DS
□ LDAP over SSL
Load Domains
3
○ AD LDS
Confirm
Cancel
4

Follow these steps in order to install the Directory Connector:

1. Download and Install the Cisco Directory Connector in your enterprise.
2. Configure the Active Directory synchronization agreement.
3. Test the synchronization agreement.

Please select a new domain to bind

Organization: cb214.dc-01.com 1035828 dcloud-webex-org

Figure 23-18 *Download Directory Connector from Webex Control Hub*

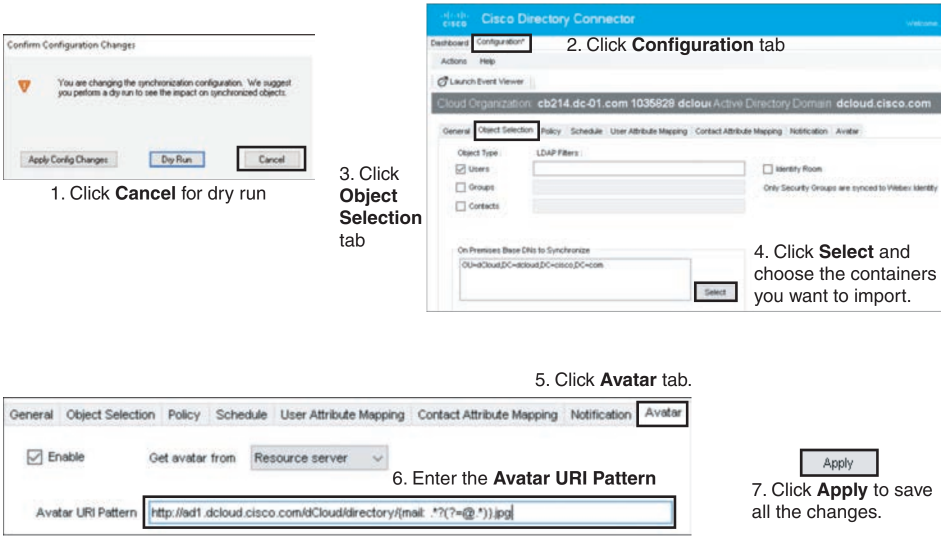
Key Topic

Step 1. Figure out which server or workstation you want the Directory Connector to work from and open a web browser. Navigate to admin.webex.com and log in with an administrator's username and password. Go to **Users > Manage Users > Turn on Directory Synchronization**. On the window that opens, click **Next**, and on the next screen, click the **Download and Install** link. You can cancel the window that's open once you download the app because it will enable itself in Webex Control Hub once the Directory Connector is set up.

Step 2. Once the Directory Connector application has been downloaded and installed, you can search for **Cisco Directory Connector** on your computer or server. When you find it, click the application icon to open it and then sign in with administrator credentials.

Step 3. Select the radio button for the type of AD service you're using, such as **AD DS**, and then click **Confirm**.

Now that the Directory Connector is open, you can configure it to synchronize the users along with their pictures (avatars). You'll want to click **Not Now** to defer the dry run until later. It's best to wait until everything is set up the way you want it before doing a dry run. Figure 23-19 illustrates how to configure the Directory Connector for user import.



You are changing the synchronization configuration. We suggest you perform a dry run to see the impact on synchronized objects.

Cloud Organization: cb214.dc-01.com 1035828 dclou Active Directory Domain: dcloud.cisco.com

Only Security Groups are synced to Webex Identity

OU=dCloud,DC=dcloud,DC=cisco,DC=com

☑ Enable Get avatar from: Resource server

Avatar URI Pattern: http://ad1.dcloud.cisco.com/dCloud/directory/{mail: .*?(?=@.*)}.jpg

1. Click **Cancel** for dry run

2. Click **Configuration** tab

3. Click **Object Selection** tab

4. Click **Select** and choose the containers you want to import.

5. Click **Avatar** tab.

6. Enter the **Avatar URI Pattern**

7. Click **Apply** to save all the changes.

Figure 23-19 *Configure Directory Connector*

Step 4. Click the **Configuration** tab at the top. Click the **Object Selection** tab so you can specify the users to synchronize. The Object Selection page gives you the ability to choose specific users to synchronize. The connector synchronizes the entire domain's users and groups by default. Once you've chosen the containers you want to import, click **Select**.

Step 5. If you want to import avatars for your users as well, then click the **Avatar** tab and check the box next to **Enabled**. In the **Avatar URI Pattern** box, enter the URI path where the avatars are located. This URI path might look something like this:

http://ad1.dcloud.cisco.com/dCloud/directory/{mail: .*?(?=@.*)}.jpg

Click **Apply** at the bottom of the screen when finished. On the popup, click **Apply Config Changes**.

Now is the time you should complete a Sync Dry Run to verify the correct users synchronize. Figure 23-20 illustrates how to perform a dry run.

Step 6. Click the **Dashboard** tab at the top, click the **Sync Dry Run** button, and then click **OK**. If synchronization was successful, you will see a popup confirmation appear with how many objects are added. Click **Done** when finished.

Now you are ready to enable the synchronization.

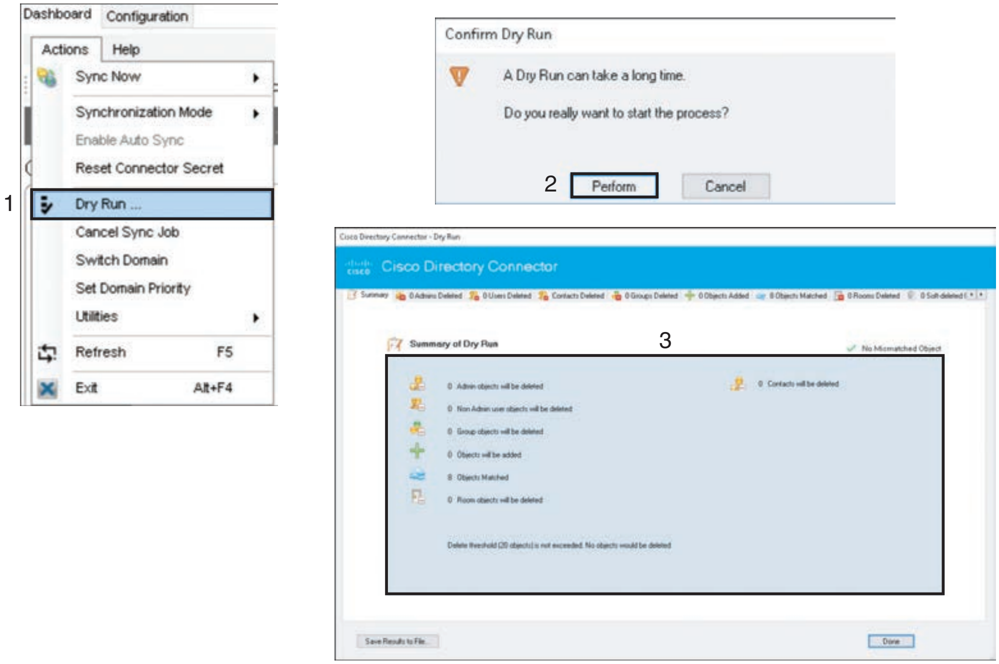
Step 7. Click the **Actions** menu and choose **Synchronization Mode > Enable Synchronization.**

Step 8. Click **No** on the popup asking to perform a dry run since you already performed it.

Step 9. Click **Enable Now** on the popup to enable synchronization.

Once synchronization is enabled, you can complete a full sync.

Step 10. Click the **Actions** menu and choose **Sync Now** > **Full.**



A Dry Run can take a long time.

Do you really want to start the process?

0 Admin objects will be deleted

0 Non Admin user objects will be deleted

0 Group objects will be deleted

0 Objects will be added

8 Objects Matched

0 Room objects will be deleted

0 Contacts will be deleted

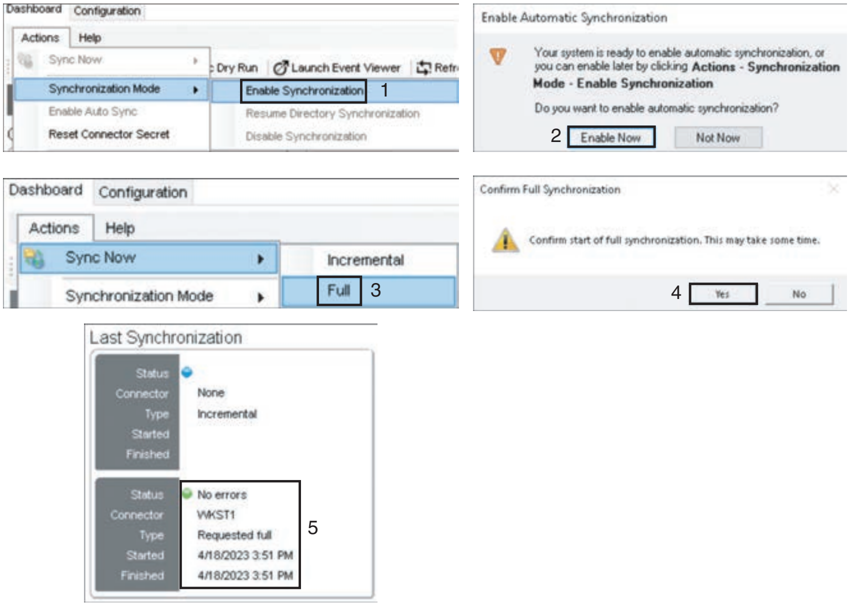
Delete threshold (20 objects) is not exceeded. No objects would be deleted

Figure 23-20 *Perform a Dry Run on Directory Connector*

Step 11. Click **Yes** on the popup.

In the **Current Synchronization** section, you can see the progress of user creation and avatar uploads. After the sync completes, in the **Last Synchronization** section, you should see a status showing no errors. If you do receive any Sync errors or warnings, try completing another full sync. It is worth mentioning here that the Directory Connector does seem to be sensitive to network connectivity issues. Sometimes when you get synchronization errors, simply trying to run it again will resolve the issue. You can also view the errors or warnings in the event view by clicking the **Launch Event Viewer** button in the Directory Connector. Then navigate to **Applications and Services Logs > Cisco Directory Connector** to view all the events. Figure 23-21 illustrates how to enable synchronization and perform a full user synchronization using the Directory Connector.

Step 12. Verify the users have synchronized by returning to the Webex Control Hub and going to **Management > Users**. You should see a list of users imported along with their avatars, if you set that part up, and user information such as email address and name. Figure 23-22 illustrates how a successful user synchronization using the Directory Connector would appear in Webex Control Hub.



Your system is ready to enable automatic synchronization, or you can enable later by clicking **Actions - Synchronization Mode - Enable Synchronization**

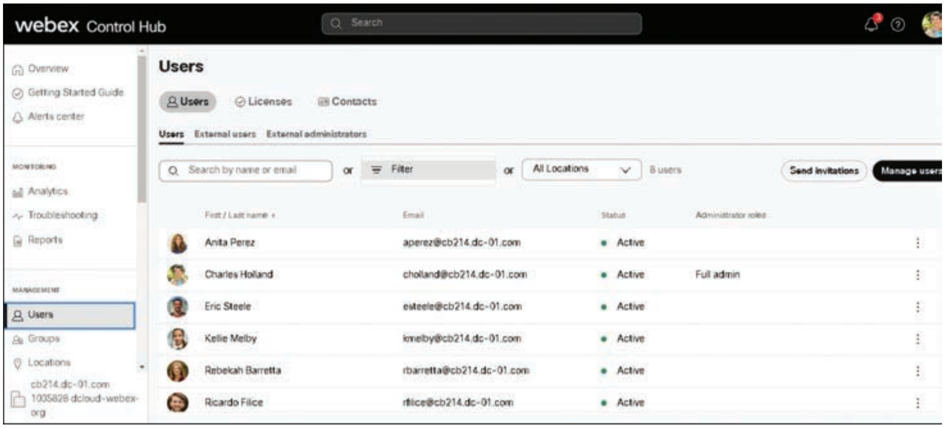
Do you want to enable automatic synchronization?

Confirm start of full synchronization. This may take some time.

Status	
Connector	None
Type	Incremental
Started	
Finished	

Status	No errors
Connector	WKST1
Type	Requested full
Started	4/18/2023 3:51 PM
Finished	4/18/2023 3:51 PM

Figure 23-21 *Perform a Full Synchronization with Directory Connector*



First / Last name	Email	Status	Administrator roles
Anita Perez	aperez@cb214.dc-01.com	Active	
Charles Holland	cholland@cb214.dc-01.com	Active	Full admin
Eric Steele	esteele@cb214.dc-01.com	Active	
Kellie Melby	kmelby@cb214.dc-01.com	Active	
Rebekah Barretta	rbarretta@cb214.dc-01.com	Active	
Ricardo Filice	rfilice@cb214.dc-01.com	Active	

Figure 23-22 *Verify User Synchronization in Webex Control Hub*

Once you have verified your import was successful, you can close the Directory Connector. You have now successfully synchronized the customer's on-premises Active Directory and configured users to their Cisco Webex Control Hub Organization.

Add Unified IP Phones to Webex Control Hub

Registering Cisco Unified IP Phones to the Webex Control Hub is different from registering a Cisco Webex Telepresence endpoint to the Webex Control Hub. Cisco Unified IP Phones use different software than Telepresence endpoints, and Unified IP Phones use different software to register to Cisco Unified Communications Manager than they use to register to Webex Control Hub. You should also be aware that not all Cisco Unified IP Phones can register to Webex Control Hub and Cisco Unified Communications Manager.

Let's begin by examining the phones that can and cannot register to the Webex Control Hub. When Cisco updated the software on Cisco Unified Communications Manager to 12.x, the company required all phones to support TLS 1.2. Cisco chose not to update the software on older phones, so the only phones in the Cisco portfolio at that time that would support TLS1.2 were the 7800 and 8800 series phones. All other models were deprecated. Shortly after that time, Cisco changed Spark to Webex and would only allow currently supported phone models to register to Webex Control Hub. Since then, Cisco has added additional phone models to the lineup, which can all register to Cisco Unified Communications Manager and Webex Control Hub. The exceptions to this rule are the phones in the 6800 series, which will only register to the Webex Control Hub. Table 23-2 identifies all the current Cisco Unified IP Phone models supported and where each phone can register. Note that the 8821, 7831 and 8831 series have all been announced to go end of sale at the time of writing this book, so they are not included in the list.

Table 23-2 Cisco Unified IP Phones Supported in Webex Control Hub

Phone Model	Phone Type	Cisco Unified Communications Manager Registration	Webex Control Hub Registration
6821, 6825, 6841, 6851, 6861, 6871	VoIP Phones	No	Yes
7811, 7821, 7841, 7861	VoIP Phones	Yes	Yes
8811, 8841, 8861	VoIP Phones	Yes	Yes
8845, 8865, 8865NR, 8875	Video Phones	Yes	Yes
7832, 8832, Webex Room Phone	Conference Phones	Yes	Yes
8821-EX, Cisco Wireless Phone 840, Cisco Wireless Phone 860	Wireless Phones	Yes	Yes

Another consideration before registering phones to Webex Control Hub is the software running on them. This was discussed in Chapter 6, "Cisco Solution for Converged Collaboration." However, we will review that information here as well. The Webex Calling feature requires phones that register to Webex Control Hub to be running the Multi-Party Phone (MPP) software. Phones that register to Cisco Unified Communications Manager are required to run Enterprise software. Methods are available to migrate software on phones, depending on where you want to register them. You can also purchase phones with specific software already installed. Migrating phone software does require an upgrade license in most situations, which is included in the Flex licensing plan. That migration license is good for a one-way migration, and it is locked to the MAC address on the phone. The one exception to needing a license is when CCUC is used to migrate phone software from Enterprise to MPP. Also, Key Expansion Modules (KEMs) do not require a migration license. Be aware that some data loss, such as call history and local contacts, can occur during phone software migration.

You have multiple ways to provision a phone to register with Webex Control Hub. You can register one phone at a time on behalf of a user, or you can bulk-provision multiple phones at the same time using a CSV template. Phones can register to Webex Control Hub using their MAC address or an activation code. The activation code can be entered manually, or phones with cameras can use a QR code. You can enter the activation code, or it can be sent to the user the phone is assigned to so that they can activate their own phone.

You must take several steps to provision a phone on behalf of a user. Bear in mind that to compete these steps, the phone must already be running MPP software. A basic overview of these steps follows:

Key Topic

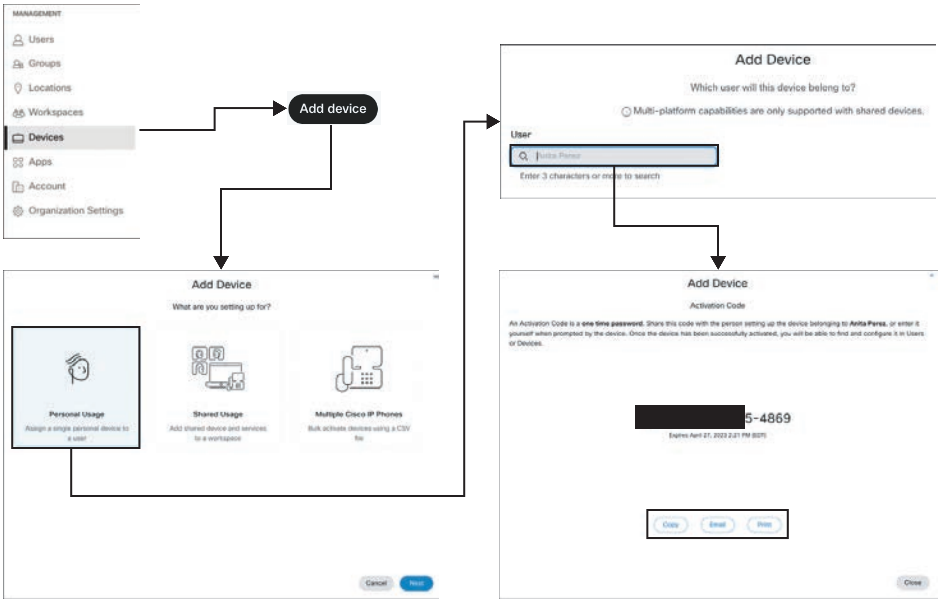
Step 1. In Webex Control Hub, go to **Management > Devices**.

Step 2. Click **Add Device**, choose the **Personal Usage** card, and click **Next**. Other cards include **Shared Usage** and **Multiple Cisco IP Phones**. Shared Usage is used for common area phones, such as lobby phones and conference room phones. The Multiple Cisco IP Phones card is used for bulk-adding phones. This subject will be discussed momentarily.

Step 3. Search for the user you want to provision a phone for, select them from the list, and then click **Next**.

Step 4. This will generate an activation code. You can choose if you want to **Copy**, **Email**, or **Print** the code. Click **Close** when finished.

Step 5. Either you or the user will then need to enter the code into the phone needing to be registered. After a few minutes, the phone should reboot and register. It may take a few minutes until the device is listed on the devices page in Control Hub after the registration is complete. Figure 23-23 illustrates the steps to register a single phone manually to Webex Control Hub.



Add Device

What are you setting up for?

Personal Usage: Assign a single personal device to a user

Shared Usage: Add shared device and services to a workspace

Multiple Cisco IP Phones: Bulk activate devices using a CSV file

Add Device

Which user will this device belong to?

Multi-platform capabilities are only supported with shared devices.

User

Anita Perez

Enter 3 characters or more to search

Add Device

Activation Code

An Activation Code is a **one time password**. Share this code with the person setting up the device belonging to **Anita Perez**, or enter it yourself when prompted by the device. Once the device has been successfully activated, you will be able to find and configure it in Users or Devices.

[redacted]5-4869

Expires April 27, 2023 2:21 PM (EDT)

Figure 23-23 *Register a Single Phone to Webex Control Hub*

Another method of registering phones to Webex Control Hub is to do a bulk phone import. This method will also require administrative access to Webex Control Hub, and it includes several benefits. This method reduces the onboarding time from hours to minutes. The activation code method of registering can still be leveraged with bulk-adding phones. Up to 250 phones can be added or modified in Webex Control Hub using the CSV file via this method. Here are the steps to follow:

Key Topic

Step 1. In Webex Control Hub, go to **Management > Devices.**

Step 2. Click **Add Device**, choose the **Multiple Cisco IP Phones** card, and click **Next.**

Step 3. In the **Download user attributes and sample template** section, use the drop-down menu to select **Add device sample template.**

Step 4. Click the **Download** button to download the **add_device_templateCSV** file. You can also select **User in my organization** from the drop-down menu to download the **exported_usersCSV** file. This will provide you with a list of users in Webex Control Hub that you can associate with phones. Once the CSV file finishes downloading, open it in Excel.

The downloaded template will have sample data that needs to be deleted before you enter the info for your users. The following fields are available, and some will need to be filled out:

- **Username:** This is a required field and should contain the email address of the user you are assigning the phone to. If you are adding a phone to a workspace, you can just put the name of the workspace in this field.
- **Type:** This is a required field, and it is the type of device you are adding. Device types were discussed in the "Methods of Adding Users to Webex Control Hub" section, and they can be defined as **Users**, **Workspaces, Service Numbers**, or **Personal Contacts.** Since service numbers and personal contacts are never associated with a physical device, they are not used in this context. Simply define each entry here as **USER** or **WORKSPACE.**
- **Extension:** This is an optional field but it would typically would be filled out. Users would need an extension for other people to call them, but a workspace, such as a lobby phone, does not necessarily need to allow incoming calls.
- **Phone Number:** This, too, is an optional field that would typically be filled out. Some companies only have a single line coming in, and they use a private branch exchange (PBX) to route calls to different extensions. You only need to add a phone number if the associated phone needs a direct line out to the public switched telephone network (PSTN).
- **Device Type:** This is a required field. For a Cisco Unified IP Phone, you should enter **IP.** For a Webex Telepresence endpoint, you can enter **WEBEX.** If the device is Webex Go, and it will be supporting a direct connection out the PSTN, you should enter **WEBEX_CALLING.**
- **Model:** This field is only required for Cisco Unified IP Phones and Webex Go. Enter the model number here for these types of devices. Leave it blank for Webex Telepresence endpoints.
- **MAC Address:** This is an optional field. If you enter the MAC address for a phone or Webex Telepresence endpoint, then the phone will register

automatically, provided it is not registered to another call control server. If you leave this field blank, an activation code will automatically be generated for that device. The device will not be able to register until the activation code has been entered.

- **Location:** This is an optional field that pertains to Webex Calling when multiple locations are setup for an organization. If you enter a location and are using Webex Calling, this will determine which Local Gateway calls will go out from for calls made across the PSTN.

Step 5. Edit the CSV file as needed for your environment and then save it.

Step 6. Now you need to upload the CSV file you just created. Either drag and drop your CSV file to the **Upload CSV data** section or click the **Choose a file** button to select the file. Once you upload a file, two options will appear for selection if any devices need an activation code.

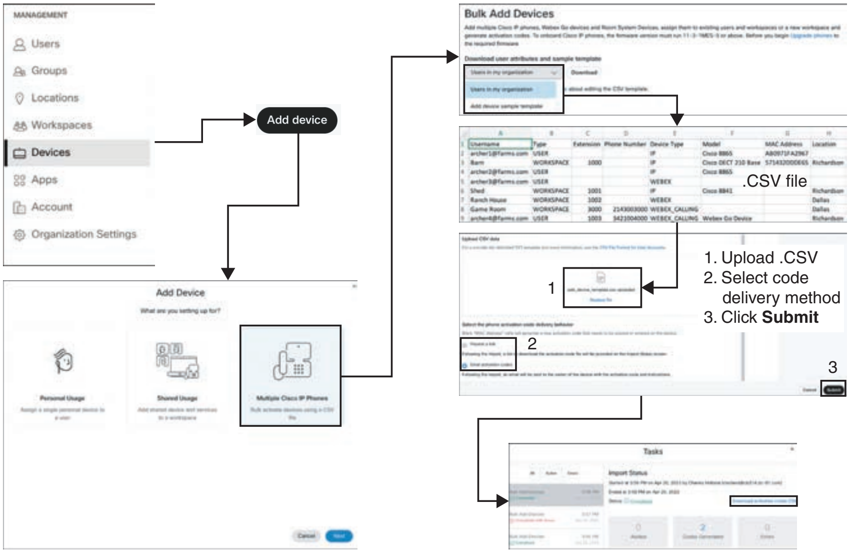
- **Provide a link:** The activation code gets added to a CSV file that you can then download.

- **Email activation code:** If the device is for a place, the activation code gets sent to you, as the administrator. If the device is for a user, the activation code is emailed to the user automatically.

Step 7. Once you've made your selection click **Submit**.

Step 8. If you chose **Provide a link**, you can download the CSV file that contains the generated activation codes. Click the **Download activation codes CSV** link.

Step 9. After you enter the code on the MPP phone, the device will reboot and register. Figure 23-24 illustrates the steps to bulk register devices to Webex Control Hub using a CSV file.



	A	B	C	D	E	F	G	H
1	Username	Type	Extension	Phone Number	Device Type	Model	MAC Address	Location
2	archer1@farms.com	USER			IP	Cisco 8865	A80971FA2967	
3	Barn	WORKSPACE	1000		IP	Cisco DECT 210 Base	571432000E65	Richardson
4	archer2@farms.com	USER			IP	Cisco 8865		
5	archer3@farms.com	USER			WEBEX			
6	Shed	WORKSPACE	1001		IP	Cisco 8841		Richardson
7	Ranch House	WORKSPACE	1002		WEBEX			Dallas
8	Game Room	WORKSPACE	3000	2143003000	WEBEX_CALLING			Dallas
9	archer4@farms.com	USER	1003	3421004000	WEBEX_CALLING	Webex Go Device		Richardson

1. Upload .CSV
2. Select code delivery method
3. Click **Submit**

Figure 23-24 *Register Multiple Phones to Webex Control Hub*

Add Webex Endpoints to Webex Control Hub

Webex Telepresence endpoints can be added to Webex Control Hub using the same methods as Cisco Unified IP Phones plus one additional method. However, there are some differences worth noting. As mentioned previously, Webex Telepresence Endpoints do not have to run MPP software. You do not have to switch the software running on these endpoints at all before registering to Webex Control Hub or Cisco Unified Communications Manager. The software will change to RoomOS as the endpoint registers to Webex Control Hub automatically. If you want to register the endpoint to Cisco Unified Communications Manager again, you can factory-reset the endpoint, and the software will revert to CE once again. This is because Cisco Telepresence endpoints can store two software versions at a time. One of them is active and the other is disabled. A factory default will always revert to the CE software.

As far as which Webex Telepresence endpoint models will register to Webex Control Hub, that part is easy. Every current Telepresence endpoint in Cisco's product portfolio will register. Another way of looking at it is every endpoint that begins with the word "Webex" will register. There are some version restrictions you will need to pay attention to as well. Check what the latest version of software is required for registration and ensure your endpoint supports that version. As of the writing of this chapter, the latest supported version needed is CE8.3.4. I have a DX80 on my desktop that is registered to Webex Control Hub. This is an end-of-sale endpoint with Cisco, but it is still supported. I have no issues registering this endpoint, and it still gets frequent updates as Webex pushes them out.

Cisco Telepresence endpoints used to not support Webex Calling at all. Today all Cisco endpoints that can register to Webex support Webex Calling; however, not all Webex Calling features are supported on all Cisco Telepresence endpoints. All Webex Room, Webex Desk, and Webex Board devices are supported on the Webex Calling Platform with native SIP registration. These devices that support native SIP registration also support the full Webex Calling feature set. Endpoints that can register to Webex but may not have the full feature support include DX70, DX80, Webex Room Phone, SX10, SX20, SX80, MX200G2, MX300G2, MX700, MX800, and the Webex Share.

Webex Telepresence endpoints can register to Webex Control Hub using the same methods outlined in the previous section, "Add Unified IP Phones to Webex Control Hub." Refer to that section for steps how to register them. The simplest way a user can provision a Telepresence endpoint to register to Webex Control Hub is to use the Self Care Portal. The following steps will describe how users can provision these devices themselves.

If a user wants to provision their own Cisco Telepresence endpoint without administrator interaction, they will need to use the following steps. This option is only available to Telepresence endpoints. IP phones require administrator involvement.

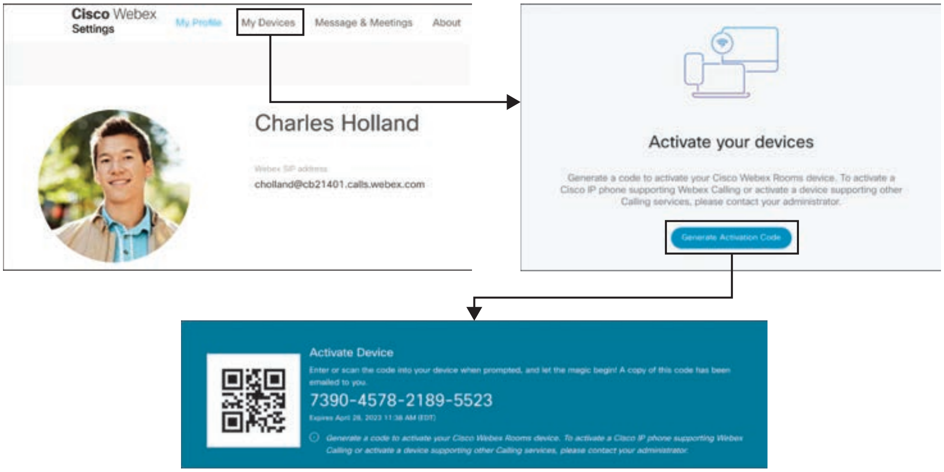
Key Topic

Step 1. From a web browser, go to **settings.webex.com** and log in with your Webex username and password. If your company is using SSO, this will be the same corporate credentials you use for everything.

Step 2. Once logged in, use the menus across the top of the page to select **My Devices**.

Step 3. On the next page that appears, click the **Generate Activation Code** button. An activation code will appear at the bottom of the screen.

Step 4. You can either enter the code manually on your Cisco Telepresence endpoint or scan the QR code using the camera on the endpoint. Once the code has been entered, the endpoint will reboot and register to Webex Control Hub. Figure 23-25 illustrates the steps to self-provision an endpoint to register to Webex Control Hub.



Generate a code to activate your Cisco Webex Rooms device. To activate a Cisco IP phone supporting Webex Calling or activate a device supporting other Calling services, please contact your administrator.

Enter or scan the code into your device when prompted, and let the magic begin! A copy of this code has been emailed to you.

7390-4578-2189-5523

Expires April 28, 2023 11:38 AM (EDT)

Generate a code to activate your Cisco Webex Rooms device. To activate a Cisco IP phone supporting Webex Calling or activate a device supporting other Calling services, please contact your administrator.

Figure 23-25 *Self-Provision a Telepresence Endpoint to Webex Control Hub*

Another method that can be used to register devices to Webex Control Hub that has not been discussed yet is to use the **Shared Usage** card. This method can be used for either Cisco Unified IP Phones or Cisco Telepresence endpoints, although it is more commonly used with Telepresence endpoints for meeting rooms. Use the following steps to add a device and services to a workspace.

Key Topic

Step 1. In Webex Control Hub, go to **Management > Devices**.

Step 2. Click **Add Device**, choose the **Shared Usage** card, and click **Next**.

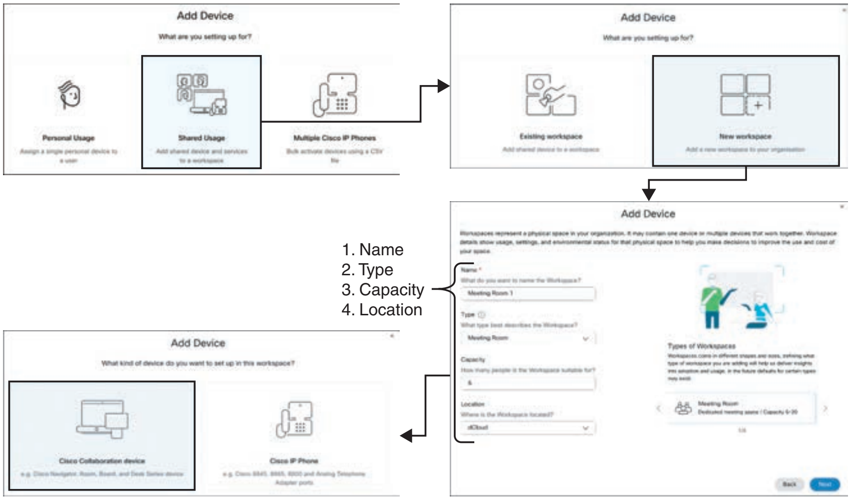
Step 3. On the next page, choose either **New workspace** or **Existing Workspace**, depending on your needs.

Step 4. If you chose **New workspace**, then on the next page enter the workspace information for the new device. This information needs to include the following:

- **Name:** This is the only required field. What do you want to name your workspace?
- **Type:** The **Types of workspaces available** section on the right side of this page provides a brief description of each type. The choices available include:
  - **Desk:** Individual | Capacity 1
  - **Focus:** High concentration | Capacity 1-2
  - **Huddle:** Brainstorm/collaboration | Capacity 2–5
  - **Meeting Room:** Dedicated meeting space | Capacity 6–20
  - **Open Space:** Unstructured agile | Capacity 2–100
  - **Other:** Unspecified

- **Capacity:** How many people is the workspace suitable for?
- **Location:** Where is the workspace located? Location is used for Webex Calling specifically.

Step 5. Click **Next** and then choose the device type. This can be a **Cisco Collaboration device** or **Cisco IP Phone.** Click **Next** once you've made your selection. Figure 23-26 illustrates the steps to initially set up a shared usage device.


Add Device
What are you setting up for?
Personal Usage
Assign a single personal device to a user
Shared Usage
Add shared device and services to a workspace
Multiple Cisco IP Phones
Bulk activate devices using a CSV file
Add Device
What are you setting up for?
Existing workspace
Add shared device to a workspace
New workspace
Add a new workspace to your organization
Add Device
Types of Workspaces
Meeting Room
Dedicated meeting space / Capacity 6-20
Back
Next
Add Device
What kind of device do you want to set up in this workspace?
Cisco Collaboration device
e.g. Cisco Navigator, Room, Board, and Desk Series device
Cisco IP Phone
e.g. Cisco 8845, 8865, 8800 and Analog Telephone Adapter ports

Workspaces represent a physical space in your organization. It may contain one device or multiple devices that work together. Workspace details show usage, settings, and environmental status for that physical space to help you make decisions to improve the use and cost of your space.

Name *
What do you want to name the Workspace?
Meeting Room 1

Type
What type best describes the Workspace?
Meeting Room

Capacity
How many people is the Workspace suitable for?
6

Location
Where is the Workspace located?
dCloud

Workspaces come in different shapes and sizes, defining what type of workspace you are adding will help us deliver insights into adoption and usage, in the future defaults for certain types may exist.

1. Name
2. Type
3. Capacity
4. Location

Figure 23-26 *Initial Steps to Set Up a Shared Usage Device*

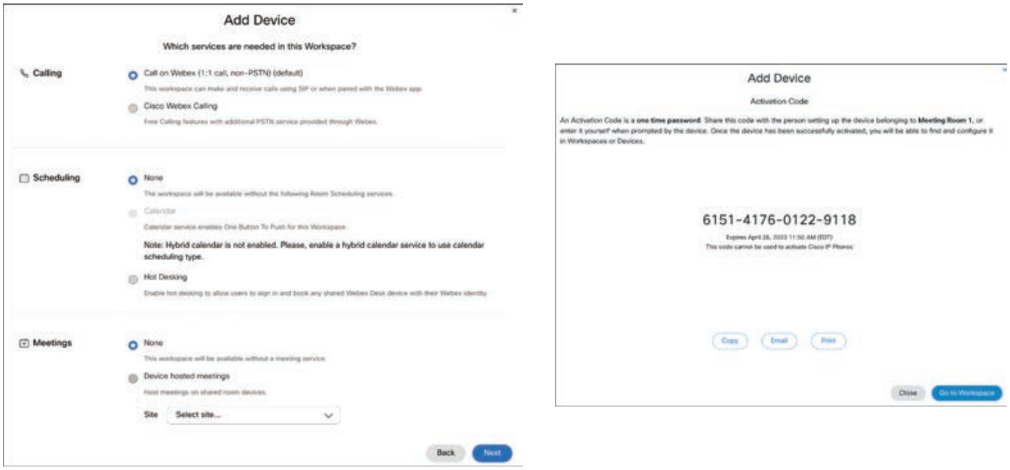
The last page of configuration has to do with the services you want to use with this shared usage device. The settings you choose might differ depending on the function of the device. For example, an open space might contain 25 IP Phones in cubicles that anyone can use on a first-come-first-serve basis. So for the **Scheduling** service you might want to choose **Hot Desking** instead of **Calendar.**

Step 6. Choose which services you want to use for this Workspace device and click **Next.** The categories and choices are as follows:

- **Calling**
  - **Call on Webex (1:1 call, non-PSTN) (default):** This workstation can make and receive calls using SIP or when paired with the Webex app.
  - **Cisco Webex Calling:** Free Calling features with additional PSTN service provided through Webex.
- **Scheduling**
  - **None:** This workspace will be available without the following Room Scheduling services.
  - **Calendar:** Calendar service enables One Button To Push for this workspace.
  - **Hot Desking:** Enable hot desking to allow users to sign in and book any shared Webex Desk device with their Webex identity.

- **Meeting**
  - **None:** This workspace will be available without a meeting service.
  - **Device hosted meetings:** Host meetings on shared room devices. A **Site** drop-down is available to choose the domain space meetings will operate in using this device.

Step 7. The last page will display the activation code. Enter this code in the device, and after a reboot the device will register. Click the **Go to Workspace** button to see a list of all your workspaces. From here you can monitor and manage each workspace. Figure 23-27 illustrates the steps to finish the setup of a shared usage device.



Add Device

Which services are needed in this Workspace?

Calling
● Call on Webex (1:1 call, non-PSTN) (default)
This workspace can make and receive calls using SIP or when paired with the Webex app.
○ Cisco Webex Calling
Free Calling features with additional PSTN service provided through Webex.

Scheduling
● None
The workspace will be available without the following Room Scheduling services.
○ Calendar
Calendar service enables One Button To Push for this Workspace.
Note: Hybrid calendar is not enabled. Please, enable a hybrid calendar service to use calendar scheduling type.
○ Hot Desking
Enable hot desking to allow users to sign in and book any shared Webex Desk device with their Webex identity.

Meetings
● None
This workspace will be available without a meeting service.
○ Device hosted meetings
Host meetings on shared room devices.
Site: Select site...

Add Device

Activation Code

An Activation Code is a **one time password**. Share this code with the person setting up the device belonging to **Meeting Room 1**, or enter it yourself when prompted by the device. Once the device has been successfully activated, you will be able to find and configure it in Workspaces or Devices.

6151-4176-0122-9118

Expires April 28, 2023 11:56 AM (EDT)
This code cannot be used to activate Cisco IP Phones

Figure 23-27 *Final Steps to Set Up a Shared Usage Device*

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 23-3 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 23-3 Key Topics for Chapter 23

Key Topic Element	Description	Page Number
List	Getting Started tasks to complete	544
List	Updates and Migrations cards	550
Steps	Steps required to enable CCUC	553

Key Topic Element	Description	Page Number
List	Hybrid integrations with Webex	555
List	Methods of adding users to Webex	557
Steps	Steps to add users to Webex manually	557
Steps	Steps to add users to Webex using CSV file	559
Paragraph	Verify Domain in Webex	560
Paragraph	Claim Domain in Webex	561
Steps	Claim users in Webex	562
Paragraph	Three Directory Management Services	563
Steps	Steps to use the User Synchronization tool	564
Steps	Download and configure Directory Connector	567
Table 23-2	Cisco Unified IP Phones Supported in Webex Control Hub	571
Paragraph	IP phone software used for registration	571
Steps	Steps to register one phone for a user	572
Steps	Steps to register multiple phones using CSV	573
Steps	Steps to self-provision an endpoint	575
Steps	Steps to register a Shared Usage device	576

Define Key Terms

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

Cisco Webex Calling, Call on Webex, Common Identity, DI, Enterprise Firmware, MPP, Migration Insights, CCUC, Agent Install File, Cluster Group, User (in Webex), Workspaces, Service Numbers, Personal Contacts, CSV, Verify Domain, Claim Domain, Claim Users, Directory Connector, SCIM

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the four main steps to set up Cloud Connected Unified Communications through the Webex Control Hub.
2. List the three directory management options available for user import to the Webex Control Hub.
3. Identify the three areas of communication when using directory synchronization through the Directory Connector.
4. List the five types of workspaces available when registering a Shared Usage device, along with their explanations.

CHAPTER 24

Webex Calling Options

This chapter covers the following topics:

PSTN Options for Webex Calling: This topic will identify the PSTN options available for the Webex Calling solution.

Routers Supporting Local Gateway: This topic will review the different routers that can be used to support the Local Gateway functions for Webex Calling.

Deployment Scenarios for the Local Gateway: This topic will overview the various deployment scenarios for how a Local Gateway can be deployed both with and without a Cisco Unified Communications Manager.

Up to this point, we have established that Webex is a cloud-based solution designed to support any company, regardless of size. Webex Calling revolves around the ability to call out across the public switched telephone network (PSTN) from IP-based devices registered to Webex Control Hub. The size of the company and the options you choose with your Webex subscription will affect the complexity level required to deploy Webex Calling. For small and medium businesses (SMBs) there is a very affordable and simple Webex Calling option. Larger enterprises will need to deploy the more complex solution using the Local Gateway. Before Webex Calling is deployed, you should understand each of the topics discussed in this chapter:

- PSTN options for Webex Calling
  - Cloud-connected PSTN (CCP)
  - Cisco PSTN
  - Premises-based PSTN
- Routers supporting local gateway
  - Cisco routers
  - Third-party routers
  - Registration- and certificate-based local gateway
- Deployment scenarios for the local gateway

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 3.4 Describe cloud calling hybrid local gateway

“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 24-1 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 24-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
PSTN Options for Webex Calling	1–4
Routers Supporting Local Gateway	5–7
Deployment Scenarios for the Local Gateway	8–10

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 the 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. An administrator is setting up Webex Calling for their organization. They currently use the Cisco Unified Communications Manager for on-premises call control. They plan to use Webex also for hybrid communication. Which of the following PSTN options should the administrator choose?
   a. Hybrid-based PSTN
   b. Cisco PSTN
   c. Cloud Connected PSTN
   d. Premises-based PSTN
2. Which of the following statements is true regarding Webex Calling using Cisco PSTN?
   a. Toll-free numbers are supported with the Cisco Calling Plan.
   b. Existing Webex Calling locations can transition to the Cisco Calling Plan.
   c. The Cisco Calling Plan does support Webex Contact Center.
   d. The Cisco Calling Plan allows you to order up to 100 new phone numbers at a time.
3. Which of the following components must be configured in Webex Control Hub before Webex Calling will work using Premises-based PSTN?
   a. Virtual Lines
   b. Service Settings
   c. Locations
   d. PSTN

4. Which of the following SBC products can function as a Local Gateway with Webex Calling? (Select all that apply.)

- **a.** Catalyst 8000v
- **b.** AP 1100v
- **c.** Mediant 8000B/C Gateway & E-SBC
- **d.** ISR880
- **e.** AP 1100
- **f.** Mediant 4000/B SBC

5. Which of the following Cisco routers can be deployed on Amazon AWS to support 3000 concurrent calls?

- **a.** C1000v – 1vcpu (4GB)
- **b.** C1000v – 4vcpu (8GB)
- **c.** C8000v-M (4GB)
- **d.** C8000v-L (8GB)

The correct answer is **C8000v-M (4GB).**

6. Which of the following devices are considered Edge Platforms? (Select all that apply.)

- **a.** ISR1100
- **b.** C8200
- **c.** ISR 4461
- **d.** CSR1000v
- **e.** C8300
- **f.** C8000v

7. Which of the following connection types for Webex Calling allows the greatest number of concurrent calls?

- **a.** SCCP-based
- **b.** Certificate-based
- **c.** MMP-based
- **d.** Registration-based
- **e.** SIP-based

8. When considering which Local Gateway deployment option to implement, which of the following items should you consider? (Select all that apply.)

- **a.** Ownership of PSTN gateway
- **b.** Desired call throughput of the site PSTN connection
- **c.** TDM vs. IP gateway connections
- **d.** Age of gateways
- **e.** Cisco router type

9. Which of the following is a recommended deployment option for the Local Gateway when deploying Webex Calling using the Premises-based PSTN method?

- **a.** Local Gateway and PSTN Connection Co-located
- **b.** Dedicated Local Gateway and PSTN Connections

c. Cisco Unified Communications Manager with Co-located PSTN Gateway/SBC and Local Gateway

d. Partner Hosted Local Gateways

10. Which of the following is the correct call flow in a Webex Calling deployment using Premises-based PSTN?

a. PSTN Gateway > Local Gateway > Cisco Unified Communications Manager > Webex

b. PSTN Gateway > Webex > Local Gateway > Cisco Unified Communications Manager

c. Cisco Unified Communications Manager > PSTN Gateway > Webex > Local Gateway

d. PSTN Gateway > Cisco Unified Communications Manager > Local Gateway > Webex

Foundation Topics

PSTN Options for Webex Calling

Webex Calling Plans, Trunks, and Route Groups provide you with the ability to configure Webex Calling to manage calls between Webex Calling–hosted users and on-premises IP public branch exchange (PBX) users. This solution lets you configure hosted users to use Cloud PSTN (Cloud Connected PSTN [CCP] or Cisco PSTN) or Premises-based PSTN. Once your location is enabled, you must set up PSTN connectivity for Webex Calling users within that location. The following PSTN options are available:

Key Topic

- **Cisco PSTN:** Choose this option if you'd like a bundled solution that allows you to order new PSTN numbers and port existing numbers to Cisco. The Cisco PSTN option is only available under the following conditions:
  - You have purchased and enabled the Cisco Calling Plan.
  - The location is in a country where Cisco Calling Plan is supported.
- **Cloud Connected PSTN:** Choose this option if you're looking for a cloud solution that doesn't require deployment of local hardware and then select your CCP provider of choice. Cloud PSTN (Cisco PSTN or CCP) can only be used to provide PSTN access for Webex Calling users. Calls originating from on-premises users can't access cloud PSTN.
- **Premises-based PSTN (Local Gateway):** Choose this option if you want to keep your current PSTN provider. Trunks for Premises-based PSTN through Local Gateway can also be used to connect to on-premises PBXs. You can retain existing Local Gateway functionality without making any configuration changes. Locations using Local Gateway are set to Premises-based PSTN and Local Gateways become Trunks.

Configure your selected PSTN connection within Control Hub by selecting **Management > Locations** and clicking the **Calling** tab. In the **Calling Connection** section, click **Manage** and then select your PSTN connection of choice.

Cloud Connected PSTN (CCP)

CCP enables global cloud PSTN calling options for Webex Calling Dedicated Instance (DI). Dedicated Instance leverages existing CCP partner peering with Webex Calling for this feature. To enable this feature for DI, Webex Calling introduces a new call routing construct called Route Lists. Route Lists in Webex Calling are lists of numbers reachable through a Route Group. Each Route List is exclusively assigned to a Location that supplies up to 40,000 unassigned numbers from the hosted pool. Only customers with DI entitlements can see or configure Route Lists in Control Hub. Figure 24-1 illustrates a Webex Calling organization with two Route Lists in their respective locations, each of them pointing to the same Route Group/Trunk, which in turn routes to a single Dedicated Instance cluster.

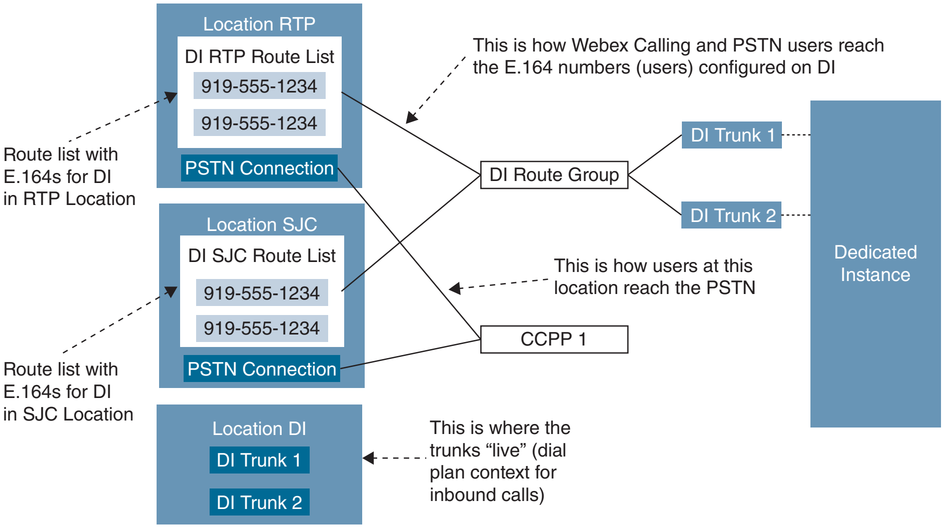

Location RTP
DI RTP Route List
919-555-1234
919-555-1234
PSTN Connection
Route list with E.164s for DI in RTP Location
This is how Webex Calling and PSTN users reach the E.164 numbers (users) configured on DI
DI Route Group
DI Trunk 1
DI Trunk 2
Dedicated Instance
Location SJC
DI SJC Route List
919-555-1234
919-555-1234
PSTN Connection
Route list with E.164s for DI in SJC Location
This is how users at this location reach the PSTN
CCPP 1
Location DI
DI Trunk 1
DI Trunk 2
This is where the trunks "live" (dial plan context for inbound calls)

Figure 24-1 *Route Lists for Cloud Connected PSTN*

For E911 locations, all emergency calls should use the built-in Dedicated Instance E911 capability. E911 calls should not be sent to the Webex Calling Organization.

For non-E911 Dedicated Instance locations that use Cloud Connected PSTN, emergency calls can be sent to the Webex Calling Organization. The calling number of the emergency call must match a PSTN number in a Route List. The Route List will identify the Webex Calling location that the emergency call belongs to and overwrite the calling number with the Emergency Callback Number (ECBN) for that Webex Calling location.

If the calling device on Dedicated Instance does not have valid Direct Inward Dialing (DID), then it should be configured to send the correct ECBN as the calling number for all emergency calls. This will then match the correct Route List in the Webex Calling Organization and send the call appropriately.

Key Topic

Use the following steps to enable CCP for DI:

Step 1. Provision Location(s) in Control Hub.

a. Select **Cloud Connected PSTN** as the connection type for the location and select the corresponding CCP provider.

- **b.** Order PSTN numbers from a CCP provider (integrated or non-integrated). Integrated providers will supply numbers directly to Control Hub, where they will appear automatically. For non-integrated providers, import the PSTN numbers as follows:
    - **i.** Sign in to Control Hub and go to the **Calling > Numbers** menu. Click the **Manage** drop-down menu on the right side of the table and select **Add**.
    - **ii.** Select **Location** from the drop-down menu on the **Selection** page. The PSTN connection associated with the location is listed against the location.
    - **iii.** Add the PSTN numbers purchased in the fields on the **Select Numbers** page. You may add up to 1000 numbers and choose to activate them immediately or later. Click **Save** after all numbers have been added. The confirmation page displays the PSTN numbers that have been added to the location.
- **c.** Perform the following steps for each Location to create a Route List, assign it to an appropriate Route Group, and select which numbers will be assigned to DI:
    - **i.** Navigate to **Calling > Route Lists** and choose an option from the list to view its properties.
    - **ii.** Select a Route Group from the **Routing Choice** menu.
    - **iii.** Click **Add Numbers** and enter the numbers associated with the Route List.
    - **iv.** Select the PSTN numbers in the Route List that are designated for Dedicated Instance (in/out) and then click **Add.** As part of Dedicated Instance service activation, SIP Trunks to Dedicated Instance and the Route Groups are created in Control Hub (the name starts with “WxC-DI”).
- **d.** Configure Dial Plans in Webex Calling with patterns pointing to Dedicated Instance and associate them with a Route Group.

Step 2. Configure Dedicated Instance:

- **a.** Configure the PSTN DIDs and assign them to phones, users, hunt pilot, and so on.
- **b.** Configure the dial plan on Dedicated Instance to route PSTN calls to Webex Calling, using the Route Group, Route List, and SIP Trunks configured during Dedicated Instance service activation.
- **c.** To enable international calling, select the relevant location in the Control Hub **Calling** page. Navigate to **Advanced > Outgoing and Incoming Permissions > Outgoing Calls > International** and select **Allow** from the drop-down menu.

Cisco PSTN

The Cisco Calling Plan offers a bundled solution to simplify your cloud calling experience. As a Webex Calling customer, you can order new PSTN numbers or port existing numbers to Cisco easily and with the full support of Cisco and its partners.

You can select varied connections for multi-site applications. For example, you can select Cisco PSTN for one location, Cloud-Connected PSTN (CCP) for a second location, and Premises-based PSTN for the third location. When choosing the Cisco Calling Plan, the following applies:

- **Requirements:**
  - Your partner must be an authorized Webex Calling partner and have accepted the new Webex Calling addendum through enrollment into the Webex Calling PSTN program.
  - Your partner places an order with Cisco Calling Plan licenses (Outbound Calling Plan and Telephone Numbers) within the Cisco Commerce Workspace (CCW).
- **Limitations:**
  - Cisco Calling Plan service is currently available to specified countries and regions. As this list is constantly changing, you will need to inquire what countries are participating at the time you sign up.
  - Existing Webex Calling locations can't transition to the Cisco Calling Plan.
  - Toll-free numbers aren't currently available. You can't order new toll-free numbers or port existing toll-free numbers to the Cisco Calling Plan.
  - You can order a maximum of 100 new phone numbers at a time. Additional numbers can be placed as a separate order.
  - Cisco Calling Plan is available with the free Webex Calling trial offer. When using the Cisco Calling Plan with a Webex Calling trial, you can create a maximum of 10 new phone numbers.
  - Number porting isn't available with a Webex Calling trial.
  - Cisco Calling Plan isn't supported with Webex Contact Center or other use in which high-concurrent calls or high-volume calls are frequently made.

Use the following steps to enable Webex Calling using Cisco PSTN.

Step 1. From the customer view in https://admin.webex.com, go to **Management > Locations** and select the location you want to update.

Step 2. Select the **Calling** tab and click **Manage** next to **PSTN Connection**.

Step 3. Select **Cisco PSTN** and click **Next**.

Step 4. Enter the contact information and click **Next**. This field is for the contact information of the person who will sign the legal contract with Cisco.

Step 5. Enter the **Emergency Services Address (ESA)** and click **Save**. By default, the ESA entered here is applied to all phone numbers for this location. You can change the ESA for an individual user if needed. For example, you may need to change the ESA if you have a remote employee who works from home.

Step 6. On the summary screen, do one of the following:

- Click **Add numbers.**
- Click **Done.**

You can add numbers to your calling plan later.

Premises-Based PSTN

Premises-based PSTN allows organizations to bring their own carrier by interconnecting any service provider's PSTN with a Premises-based Local Gateway that tightly integrates to Cisco's Webex Calling cloud. This service is provided through existing enterprise routing infrastructure that uses a trunk for the Local Gateway either without an on-premises IP PBX or with an existing Cisco Unified Communications Manager call environment. The PSTN connection can be accessed using Cisco Unified Border Element (UBE) or through an IOS gateway with Primary Rate Interface (PRI) cards. Cisco UBE is the recommended deployment option for Premises-based PSTN and will be the sole focus throughout the rest of Part VI, "Webex Calling."

The Webex Control Hub was discussed extensively in Chapter 23, "Adding Users and Devices in Webex Control Hub." As a review, the Webex Control Hub is a management portal that integrates with Webex Calling to streamline your orders and configuration as well as to centralize your management of the bundled offer: Webex Calling, Webex Messaging, and Webex Meeting. Webex Control Hub is the central point for provisioning all services, devices, and users. You can do first-time setup of your calling service, register MPP phones to the cloud, and configure users by associating devices and adding numbers, services, calling features, and so on. Also, from Control Hub, you can cross-launch to the Calling Admin Portal, which is used to initially configure Webex Calling and to manage it once everything is set up. Important components that need to be configured to enable Webex Calling include Numbers, Locations, Call Routing, and Managed Gateways. These components will be discussed further in Chapter 26, "Webex Calling Using a Local Gateway." Other configuration options include Virtual Lines, Features, PSTN (used for managing cloud PSTN orders), Service Settings, and Client Settings.

The Local Gateway is an enterprise or partner-managed edge device for PSTN interworking and legacy PBX interworking, including Cisco Unified Communications Manager. You can use Webex Control Hub to assign a local gateway to a location, after which Control Hub provides parameters that you can configure on a router. These steps register the Local Gateway with the cloud, and then PSTN service is provided through the gateway to Webex Calling users in a specific location. All communication to and from the cloud is secured using TLS transport for SIP and SRTP for media.

Key Topic

Cisco UBE can be used to connect an enterprise to a telephony service provider over SIP, who will interconnect calls out to the PSTN, and vice versa. If an existing Cisco UBE enterprise deployment is being modified to also utilize the local gateway function for Cisco Webex Calling, Cisco UBE High Availability (HA) can be deployed to ensure call flows and functionalities are not interrupted. Cisco UBE HA Layer 2 box-to-box redundancy uses the Redundancy Group (RG) infrastructure protocol to form an active/standby pair of routers. This pair shares the same virtual IP address (VIP) across their respective interfaces and continually exchange status messages. Cisco UBE session information is check-pointed across the pair of routers, enabling the standby router to take all Cisco UBE call processing responsibilities over immediately if the active router goes out of service, resulting in stateful preservation of signaling and media. As of IOS-XE 16.12.2, Cisco UBE HA can be deployed as a Local Gateway for Cisco Webex Calling Trunk Premises-based PSTN deployments. The purpose of this chapter is to provide an introduction to Webex Calling options, so we will not be diving any deeper into Cisco UBE HA in this book.

Routers Supporting Local Gateway

Webex Local Gateway can be hosted on a variety of Cisco IOS-XE routers and a select group of third-party routers. This topic will cover the platforms, capacities, and software versions required to support Local Gateway functionality on Cisco routes and third-party routers. This chapter will also cover the differences between the registration-based Local Gateway and certificate-based Local Gateway settings.

Cisco Routers

The 1100 and 4000 series of IOS-XE devices are the entry point for Local Gateways and the oldest devices supported to function as Local Gateways. These are the same devices that function today as branch gateways in an on-premises-based VoIP system. This allows the rapid conversion from on-premises to cloud-based or a hybrid calling model without requiring router upgrades.

The smallest supported router for Local Gateway is the ISR 1100 series. These small devices are capable of handling 500 calls with up to five calls per second (CPS). The routers are available with different amounts of memory, WAN, and Ethernet interfaces to suit the needs of small sites. Since telephone ports are not supported with the ISR 1100 series, these routers could only be used as a Cisco UBE using SIP trunks. The ISR 1100 series products went end of sale (EOS) on May 9, 2023 and have an end of support date of May 31, 2028.

The 4000 series of Integrated Services Routers are able to handle the demands of most branch office needs. A wide range of interface choice for WAN, Ethernet, and Telephony allow the user to customize the router to suit their needs. The router can be used as a Cisco UBE for full SIP-based communications but also as a Time Division Multiplexing (TDM) gateway using older circuits such as T1/E1 PRI. The product line supports 500 calls with four CPS on the smallest ISR 4321, up to 10,000 calls and 55 CPS on the largest ISR 4461. This product line eases the process of finding a router with the right mix of interfaces and performance needed for the branch site in your organization. The ISR 4300/4400 line is set to go end of sale (EOS) on November 7, 2023. The product will be supported for several more years, but the latest IOS XE release will be either 17.9 or 17.12, depending on the software train you are utilizing. Table 24-2 identifies all the 1100 and 4000 series routers that support Local Gateway.

Key Topic

Table 24-2 Local Gateway Support on 1100 and 4000 Series Routers

Platform	Cisco UBE SIP-SIP Audio Session (Flow-thru) RTP G.711-RTP G.711	Sustainable CPS IOS-XE 16.1.2+
1100	500 (IOS-XE 16.2+)	5
4321	500	4
4331	1000	10

Platform	Cisco UBE SIP-SIP Audio Session (Flow-thru) RTP G.711-RTP G.711	Sustainable CPS IOS-XE 16.1.2+
4351	2000	13
4431	3000	15
4451	6000	40
4461	10,000 (IOS-XE 17.2.1r+)	55

The replacements for the ISR 1000 and 4000 routers are the Catalyst 8000 Edge Platforms. The Cisco Catalyst 8300 Series Edge Platforms are best-of-breed, 5G-ready, cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud. The C8000 line is broken into two series similar to the 4000 series lineup. The smaller 8200 series provides multi-core processors, up to 32GB of DRAM, up to four Ethernet ports (two support SFP), and one Network Interface Module, which can support various WAN and Telephony interfaces.

The C8300 products contain multicore processors, expandable memory, and up to six Ethernet ports. Two of those ports can support Small Form Factor Pluggable adapters to allow copper or fiber connections. The Edge Platforms also come with dual power supplies for greater redundancy. Numerous WAN and Telephony interface cards allow you to tailor the product to the site's voice and data services, which require support at a branch site.

When the C8000 line is used as a Local Gateway, its performance is upgraded from the ISR 4000 series it replaces. Call throughput ranges from 1500 (middle of the pack for ISR 4000) on the small end to 10,000 on the higher end. Sustainable CPS rates of nine on the C8200L to 55 on the C8300-2N2S-4T2X meet the needs of most branch locations. Table 24-3 identifies all the 1100 and 4000 series routers that support Local Gateway.

Key Topic

Table 24-3 Local Gateway Support on Catalyst 8000 Edge Routers

Platform	Cisco UBE SIP-SIP Audio Session (Flow-thru) RTP G.711-RTP G.711	Sustainable CPS IOS-XE 16.1.2+
C8200L-1N-4T (4GB)	1500 (IOS_XE 17.5.1+)	9
C8200L-1N-4T (8GB)	2500 (IOS_XE 17.4.1a+)	14
C8300L-1N1S-6T (8GB)	7000 (IOS-XE 17.3.2)	40
C8300L-1N2S-6T (8GB)	7500 (IOS-XE 17.3.2)	42
C8300L-1N1S-4T2X (8GB)	8000 (IOS-XE 17.3.2)	45
C8300L-1N2S-4T2X (8GB)	10,000 (IOS-XE 17.3.2)	55

NOTE The following key can be used to help understand the differences between the routers in Table 24-3.

xN = Network Interface Module

xT = 1GB Ethernet Port

xS = Service Modules

xX = 10GB Ethernet Port

A third option for Local Gateways is either the CSR1000v or the C8000v. Both products are virtual machines that can run in a variety of virtual environments. The Cloud Services Router 1000v is a virtual IOS-XE router that can run in VMware ESXi, Citrix XenServer, Microsoft Hyper-V, SuSE KVM, or Red Hat KVM virtual environments. The CSR1000v can also be deployed in Microsoft Azure, Amazon EC2, and Google Cloud Platform. The CSR1000v can support up to IOS-XE version 17.3 software. After that version, the branding and licensing was changed to reflect the new product name of Catalyst 8000v.

The Catalyst 8000v is a continuation of the CSR1000v. The C8000v is a software-based virtual router that combines the functionalities of Cisco Cloud Services Router (Cisco CSR1000V) and Cisco Integrated Services Virtual Router (Cisco ISRv) into a single image that is intended for deployment in cloud and virtual data centers. It is supported in ESXi, KVM, NFVIS hypervisors. Further, you can deploy this router on public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba Cloud.

The router can be deployed as a virtual machine in your virtual environment, and it can be created as a small, medium, or large virtual machine using increasing amounts of vCPU, memory, and other resources. The number of concurrent and sustained CPS also increases. If the C8000v is deployed in a cloud environment such as Microsoft Azure or Amazon AWS, the medium VM is deployed with 3000 concurrent calls and 20 CPS. Table 24-4 identifies the 1000v and 8000v virtual routers that support Local Gateway.

Table 24-4 Local Gateway Support on 1000v and 8000v Virtual Routers

Platform	Cisco UBE SIP-SIP Audio Session (Flow-thru) RTP G.711-RTP G.711	Sustainable CPS IOS-XE 16.1.2+
C8000v-S / C1000v – 1vcpu (4GB)	1000	5
C8000v-M / C1000v – 2vcpu (4GB)	3000	20
Azure / AWS C8000v-M / C1000v – 2vcpu (4GB)	3000	20
C8000v-L / C1000v – 4vcpu (8GB)	6000	30

Third-Party Routers

A relatively new addition to the supported Session Border Controller area are third-party Session Border Controllers (SBCs). The following products running Oracle SBC version 9.0 software are supported as a Local Gateway with Webex Calling:

- AP 1100
- AP3900
- AP 4600
- AP 6300
- AP 6350

- AP 3950 (Starting from SBC 9.0)
- AP 4900 (Starting from SBC 9.0)
- VME
- Oracle SBC on Public Cloud

The following AudioCodes SBCs running software version 7.40A.250.440 or later are supported as Local Gateway with Webex Calling:

- Mediant 500 Gateway and E-SBC
- Mediant 800B/C Gateway and E-SBC
- Mediant 1000B Gateway and E-SBC
- Mediant 2600 E-SBC
- Mediant 4000/B SBC
- Mediant 9000, 9030, 9080 SBC
- Mediant Software SBC (VE/SE/CE)

Finally, the Ribbon line of SBCs has also received approval to function as Local Gateways with Webex Calling. The following Ribbon SBCs running Ribbon Code version 10.1.0 or higher are supported as Local Gateways:

- SBC 5000
- SBC 7000
- SBC SWe

Registration- and Certificate-Based Local Gateway

While it is true that an ISR 4461 can handle 10,000 concurrent calls, that capacity can be restricted to as low as 250 if the connection to the Webex cloud is not chosen correctly. To understand this issue, it is important to understand that there are two ways to connect to the Webex Calling system:

- Registration-based Local Gateway
- Certificate-based Local Gateway

In the registration-based Local Gateway connection, you create the connection in Control Hub and you are provided with the elements needed to allow your Local Gateway to create a TCP connection to the cloud. This is a one-way connection from the Local Gateway to the cloud. One of the big benefits of this connection type is that a technician with limited IOS skills can successfully deploy a Local Gateway behind a NAT/firewall without requiring changes to the NAT or firewall. The connection does not require CA signed certificates, which reduces complexity and cost. However, since the registration consists of a single TCP connection, the link has a lower capacity and is not as durable if there are network issues such as high latency and packet loss. This means that no matter what SBC platform you are using, you are limited to 250 concurrent calls per trunk built on that device. It is possible to build multiple trunks on a single Local Gateway. Careful configuration of outbound interfaces, SIP listening ports, dial-peers, and load balancing for the on-premises Cisco Unified Communications Manager can allow you to exceed the 250-call limit. Figure 24-2 illustrates the connection flow for Webex Calling using registration-based Local Gateway.

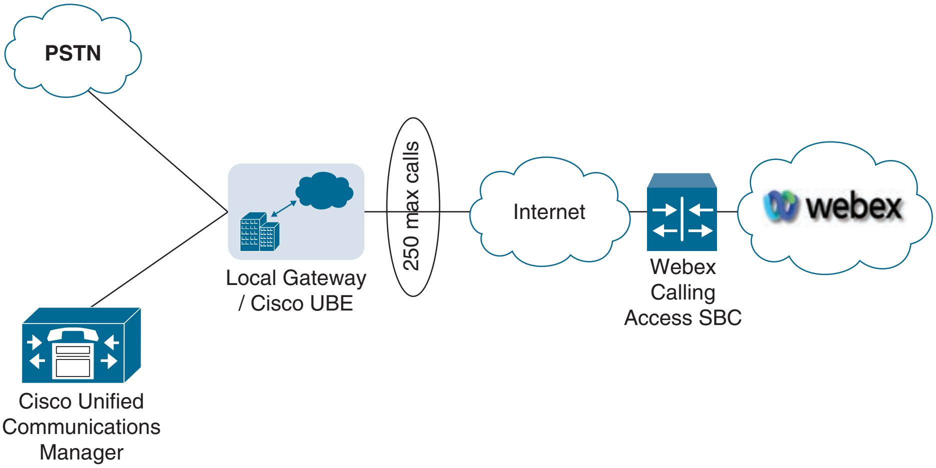

PSTN
Local Gateway / Cisco UBE
250 max calls
Internet
Webex Calling Access SBC
webex
Cisco Unified Communications Manager

Figure 24-2 *Registration-Based Local Gateway*

The certificate-based method of connecting a Local Gateway fixes the capacity issue by using Mutual TLS as the connection type. This method also uses four bi-directional connections rather than a single one-way connection, as with the registration-based connection. This connection type requires CA signed certificates in the Local Gateway. The engineer also needs to add the Webex Calling trust bundle into the Local Gateway so that the SBC trusts the certificates of Webex Calling.

A connection is configured to endure four fully qualified domain names (FQDNs) or a DNS Service Record (SRV) that points to the Access SBCs of Webex Calling. If configured correctly, four bi-directional TLS connections will be created to carry traffic to and from the Local Gateway and Webex Calling. NAT/firewall traversal is possible with the certificate-based connection method using Session Traversal Using NAT (STUN). Figure 24-3 illustrates the connection flow for Webex Calling using certificate-based Local Gateway.

As you can see from these two descriptions, if you are looking for an easy installation and only have a capacity need below 250 concurrent calls over the public Internet, it is recommended that you use the registration-based connection method. If you require up to 2000 concurrent calls over the public Internet, the solution will be certificate-based. It is possible to reach up to 6500 concurrent calls with the certificate-based connection method, but this will require a dedicated Interconnect connection to Webex Edge Connect. If you wish to use any of the newly supported third-party SBCs, you will need to use the certificate-based connection method as well. Table 24-5 identifies sizing parameters for a Local Gateway based on registration type.

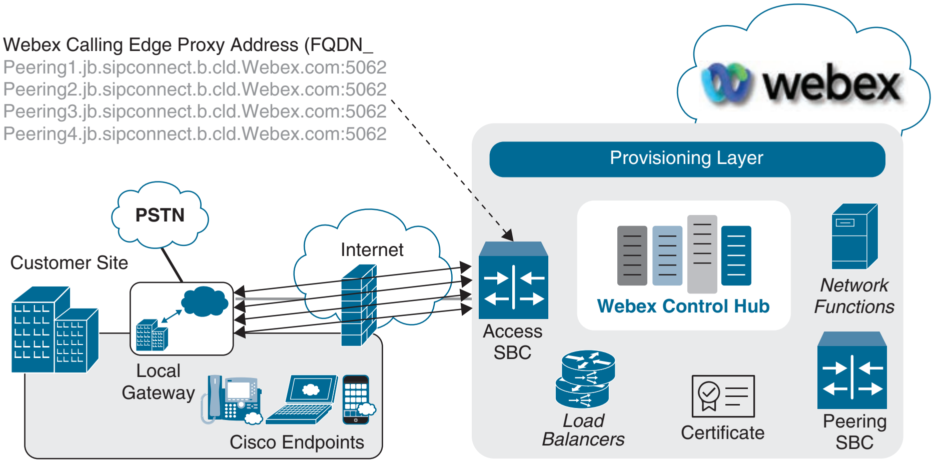

Webex Calling Edge Proxy Address (FQDN_
Peering1.jb.sipconnect.b.cld.Webex.com:5062
Peering2.jb.sipconnect.b.cld.Webex.com:5062
Peering3.jb.sipconnect.b.cld.Webex.com:5062
Peering4.jb.sipconnect.b.cld.Webex.com:5062
webex
Provisioning Layer
PSTN
Customer Site
Internet
Access SBC
Webex Control Hub
Network Functions
Local Gateway
Load Balancers
Certificate
Peering SBC
Cisco Endpoints

Figure 24-3 *Certificate-Based Local Gateway*

Key Topic

Table 24-5 Local Gateway Sizing Parameters Based on Registration Type

Sizing by Concurrent Calls per Local Gateway	Sizing by Number of Users Behind a Local Gateway	Trunk Type Preferred	Minimum Link Quality
~ 2000–6500	65,000	Certificate-based	Interconnect
250–~2000	20,000	Certificate-based	Over the Internet
Up to 250	2500	Registration-based	Over the Internet

Deployment Scenarios for the Local Gateway

Webex Local Gateways can be deployed in different configurations to adapt to the needs of individual customers, depending on several factors. Does the Local Gateway and the PSTN connection share the same physical or virtual hardware? Does the site contain an IP PBX such as Cisco Unified Communications Manager? Is the Local Gateway hosted offsite from the customer through a service provider (SP) or value-added reseller (VAR)? Each of these factors will be address in the following scenarios. The two biggest factors you should you consider when deploying a Local Gateway are who owns the PSTN gateway and what is your desired throughput of the site PSTN connection?

The first scenario to consider is a company that uses all Webex endpoints but wishes to use its local PSTN's circuits. If the customer doesn't already have a device to handle the connection to the PSTN, a single router supporting Local Gateway and PSTN services is a good solution. The router or edge device will supply the Local Gateway functionality as well as the connection to the PSTN. In this scenario, the Webex dial plan routes all non-Webex calls to the trunk pointing to the Local Gateway. The Local Gateway configuration provides the secure connection to the Webex cloud and contains dial-peers, which route calls to the PSTN. Figure 24-4 illustrates a single site deployment for Webex Calling where the PSTN connection and Local Gateway are co-located.

The second scenario separates the Local Gateway function from the PSTN gateway using separate routers. The most common reason for this deployment type is to increase capacity.

The Local Gateway handles all calls to and from the Webex cloud. Any call not destined for Webex is passed to the PSTN gateway. The PSTN gateway uses similar logic to send any calls not designated for the PSTN to the Local Gateway. This simplifies the configuration of each device and allows higher call capacity through each router. Figure 24-5 illustrates a single site deployment for Webex Calling where the PSTN connection and Local Gateway use dedicated routers for each service. This is the recommended deployment option for Webex Calling when an IP PBX is not being used.

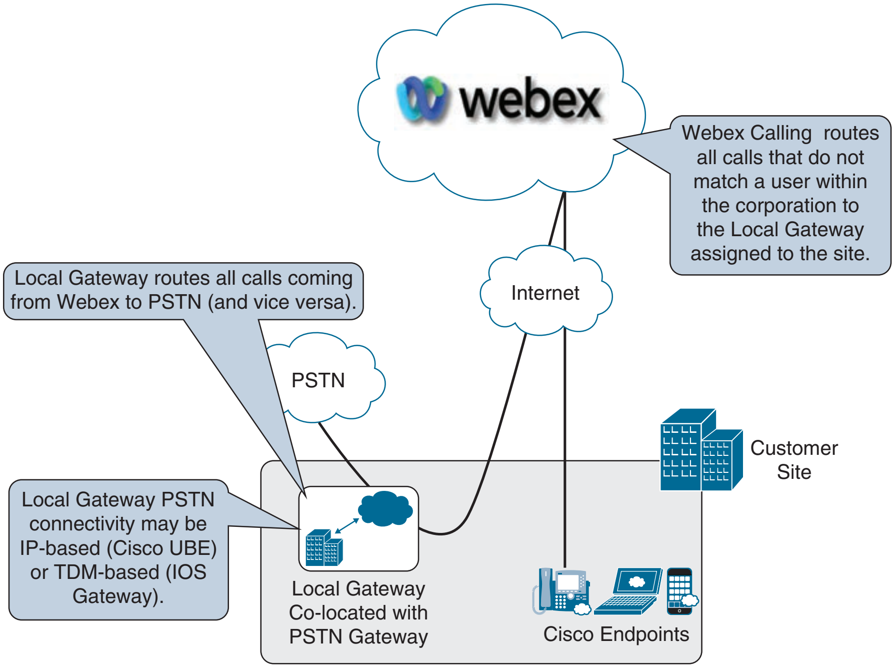

webex
Webex Calling routes all calls that do not match a user within the corporation to the Local Gateway assigned to the site.
Local Gateway routes all calls coming from Webex to PSTN (and vice versa).
Internet
PSTN
Customer Site
Local Gateway PSTN connectivity may be IP-based (Cisco UBE) or TDM-based (IOS Gateway).
Local Gateway Co-located with PSTN Gateway
Cisco Endpoints

Figure 24-4 *Single Site Deployment with Local Gateway and PSTN Connection Co-located*

Another reason to use this deployment model would be if the customer does not control the PSTN device. The customer configures the Local Gateway to hand off all incoming calls from Webex to the PSTN device. Similarly, the PSTN device sends all incoming calls to the Local Gateway.

Adding Cisco Unified Communications Manager to the customer site creates a new scenario because it changes the configuration a bit. In this case, the customer will want the calls from Webex to go to Cisco Unified Communications Manager since there will be an existing dial plan for both on-premises endpoints and the PSTN. Similar to the example of a location with a single router providing both Local Gateway and PSTN functions, the same type of router configuration can be used in this environment. The largest drawback would be the router's capacity to handle sufficient traffic for Cisco Unified Communications Manager, Webex, and PSTN.

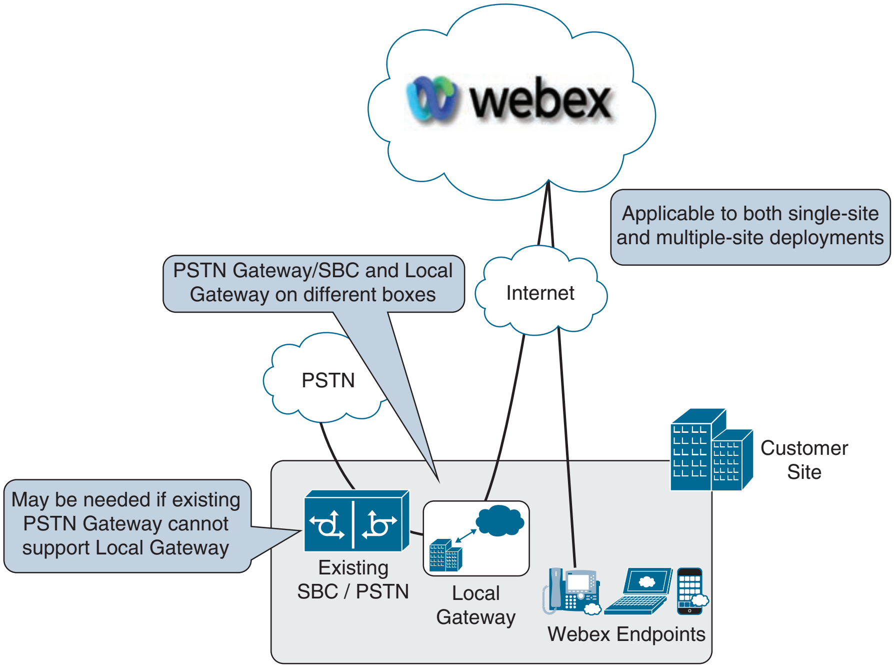

webex
Applicable to both single-site and multiple-site deployments
PSTN Gateway/SBC and Local Gateway on different boxes
Internet
PSTN
Customer Site
May be needed if existing PSTN Gateway cannot support Local Gateway
Existing SBC / PSTN
Local Gateway
Webex Endpoints

Figure 24-5 *Single-Site Deployment with Dedicated Local Gateway and PSTN Connections*

When calls are made from a Webex endpoint, any call not matching the Webex dial plan would be routed to the Local Gateway. The Local Gateway would pass the call to the Cisco Unified Communications Manager. The Cisco Unified Communications Manager dial plan would be leveraged to send calls to either a Cisco Unified Communications Manager–controlled endpoints or routed back the Local Gateway/PSTN device to hand the calls off to the PSTN.

Inbound calls to Webex from the PSTN would route to the PSTN gateway function of the router and onward to the Cisco Unified Communications Manager. The dial plan of the Cisco Unified Communications Manager will be used to determine if the call should be routed to a locally registered device or to a Webex-registered device. When the call is destined for a Webex-registered device, the Cisco Unified Communications Manager will route the call to the Local Gateway function of the router, which forwards the call to the Webex cloud, which will in turn route to the endpoint or phone. Figure 24-6 illustrates a single-site deployment for Webex Calling where the PSTN connection and Local Gateway are co-located on the same router and Cisco Unified Communications Manager is used for on-premises call control.

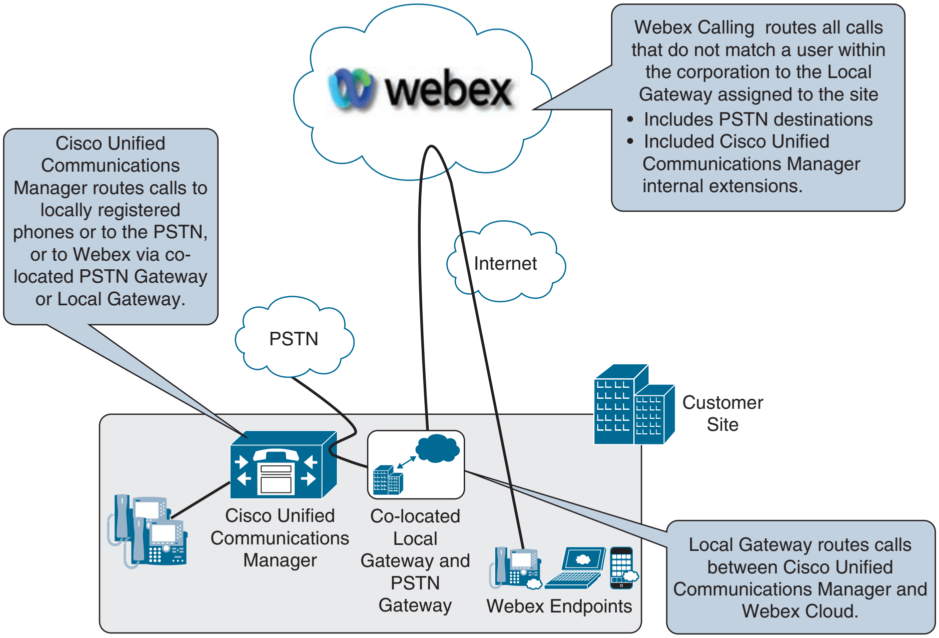

webex
Webex Calling routes all calls that do not match a user within the corporation to the Local Gateway assigned to the site
• Includes PSTN destinations
• Included Cisco Unified Communications Manager internal extensions.
Cisco Unified Communications Manager routes calls to locally registered phones or to the PSTN, or to Webex via co-located PSTN Gateway or Local Gateway.
Internet
PSTN
Customer Site
Cisco Unified Communications Manager
Co-located Local Gateway and PSTN Gateway
Webex Endpoints
Local Gateway routes calls between Cisco Unified Communications Manager and Webex Cloud.

Figure 24-6 *Cisco Unified Communications Manager with Co-located PSTN Gateway/SBC and Local Gateway*

As you might have guessed, the forth scenario deals with using Cisco Unified Communications Manager and a dedicated router for the PSTN gateway function and Local Gateway function. This is the recommended option for Webex Calling using Cisco Unified Communications Manager. You will benefit from increased call capacity and more granule call control. This scenario is best suited for customers that have an existing on-premises call control solution that utilizes high call volume. The call flow for this scenario remains the same as the previously discussed scenario using a Cisco Unified Communications Manager, as shown next. Figure 24-7 illustrates a single-site deployment for Webex Calling where dedicated routers are used for the PSTN connection and Local Gateway, and Cisco Unified Communications Manager is used for on-premises call control.

- Webex > Local Gateway > Cisco Unified Communications Manager > PSTN Gateway
- PSTN Gateway > Cisco Unified Communications Manager > Local Gateway > Webex

Any of the scenarios outlined previously are acceptable deployments. However, when planning for future expansion or growth, it is recommended that you separate the Local Gateway and PSTN gateway functions to gain the highest capacity. In addition, the ownership of the devices (customer vs. PSTN provider) might play a role in the decision.

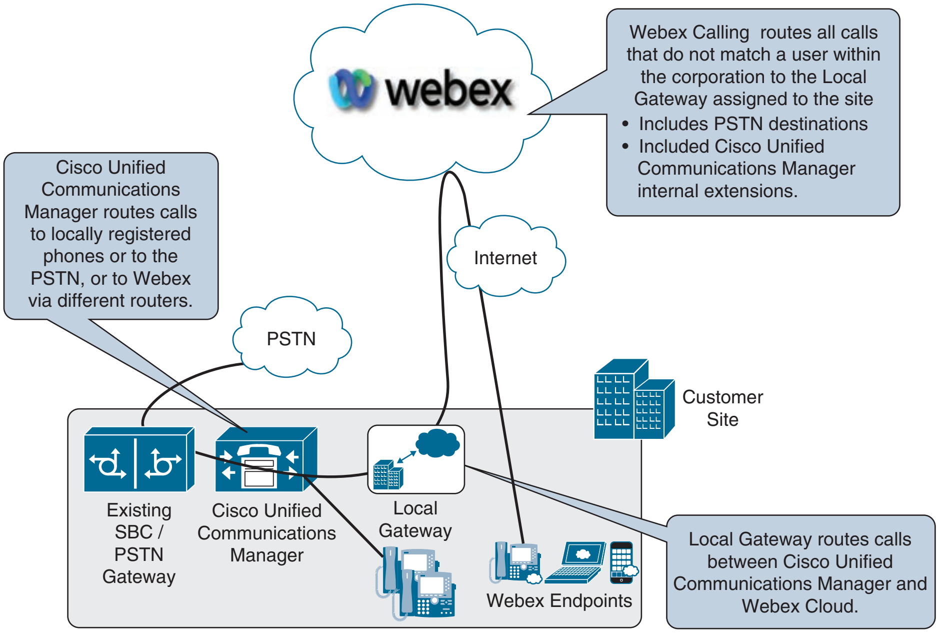

webex
Webex Calling routes all calls that do not match a user within the corporation to the Local Gateway assigned to the site
• Includes PSTN destinations
• Included Cisco Unified Communications Manager internal extensions.
Cisco Unified Communications Manager routes calls to locally registered phones or to the PSTN, or to Webex via different routers.
Internet
PSTN
Customer Site
Existing SBC / PSTN Gateway
Cisco Unified Communications Manager
Local Gateway
Webex Endpoints
Local Gateway routes calls between Cisco Unified Communications Manager and Webex Cloud.

Figure 24-7 *Cisco Unified Communications Manager with dedicated PSTN Gateway/ SBC and Local Gateway*

This brings us to the next scenario. Only one Local Gateway needs to be configured for each organization, but multiple Local Gateways can be configured as well by creating multiple locations in the Webex Control Hub. There are a couple rules that should be followed when creating multiple locations:

Key Topic

- You cannot assign multiple Local Gateways to a single location. Only one Local Gateway can be assigned per locations.
- You can assign a single Local Gateway to multiple locations.

Picture an organization that has three locations configured: Washington, DC, New York, NY, and London, UK. Washington and London have a Local Gateway assigned to them. New York simply uses the same Local Gateway as Washington. If a device registered to New York needs to place a call out the PSTN, the call will traverse from the New York location to Webex, back to Washington, then out the Local Gateway to the PSTN. This is how two or more locations can use the same Local Gateway. However, New York cannot use both the Washington and London local gateways because of the second rule outlined previously. Figure 24-8 illustrates how multiple Local Gateways can be used over multiple locations.

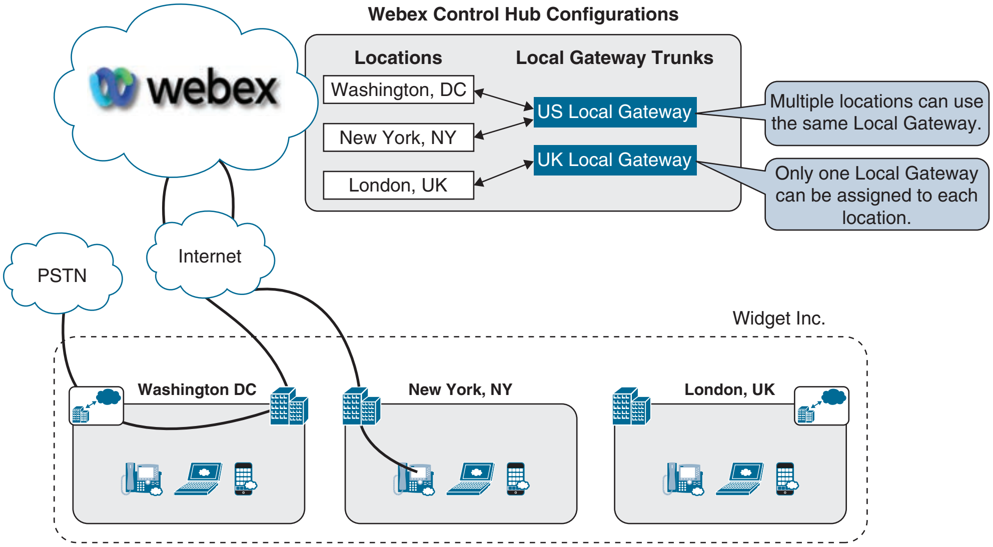


Figure 24-8 *Call Routing Across Multiple Local Gateways*

There is one final scenario you need to understand. Endpoints registered to the Webex Control Hub will communicate directly with Webex in the cloud. They do not have to route calls through the Local Gateway first. That connection is over the Internet, just as you would connect to a website like Cisco.com. In this manner, these endpoints do not have to be co-located with the Local Gateway. Therefore, partners can provide Local Gateway services hosted within their own data centers on behalf of their customers. This could be an official SP or a VAR. In fact, many Cisco VAR partners offer this type of service today. Figure 24-9 illustrates how customers can use the on-premises PSTN Webex Calling option through a hosted Local Gateway within a Cisco Partner environment.

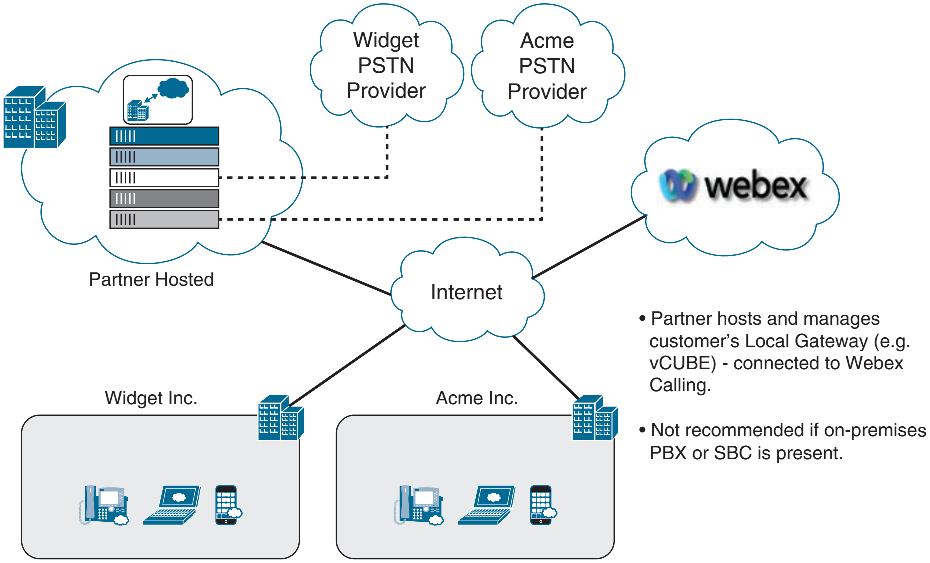

Widget PSTN Provider
Acme PSTN Provider
webex
Partner Hosted
Internet
Widget Inc.
Acme Inc.
• Partner hosts and manages customer's Local Gateway (e.g. vCUBE) - connected to Webex Calling.
• Not recommended if on-premises PBX or SBC is present.

Figure 24-9 *Partner Hosted Local Gateways*

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 24-6 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 24-6 Key Topics for Chapter 24

Key Topic Element	Description	Page Number
List	PSTN options for Webex Calling	583
Steps	Steps to enable Dedicated Instance for CCP	584
List	Cisco PSTN Requirements and Limitations	586
Steps	Enable Webex Calling using Cisco PSTN	586
Paragraph	Cisco UBE High Availability (HA)	587
Table 24-2	Local Gateway Support on 1100 and 4000 Series Routers	588
Table 24-3	Local Gateway Support on Catalyst 8000 Edge Routers	589
Table 24-4	Local Gateway Support on 1000v and 8000v Virtual Routers	590
Sub-Topic	Third-Party Routers	590
Table 24-5	Local Gateway Sizing Parameters Based on Registration Type	593
List	Rules when creating multiple locations	597

Define Key Terms

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

CCP, Cisco PSTN, Premises-based PSTN, Webex Calling DI, Webex Calling Route Lists, Local Gateway, Cisco UBE HA, Branch Gateways, Catalyst 8000 Edge Platforms, CSR1000v, C8000v, Registration-based Local Gateway, Certificate-based Local Gateway

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the three PSTN options for Webex Calling.
2. List the five series of Cisco routers that support the Local Gateway.
3. What are the four companies that offer third-party routers to support the Local Gateway?
4. What are the two rules you must follow when creating multiple locations in the Webex Control Hub for Webex Calling?

CHAPTER 25

Webex Calling Features

This chapter covers the following topics:

Admin-Configurable Features: This topic will describe the Webex Calling features that can only be configured by an administrator to affect the company.

User-Configurable Features: This topic will describe Webex Calling features that can be configured by either an administrator or the user. These features only effect the user who enables them and no one else.

Webex offers calling features that can be used to control how calls are handled within an organization. These features shape to whom calls are routed, how callers are placed on hold or transferred, what happens to callers outside normal business hours, and many other types of call handling. Features can be configured globally to affect everyone within the organization, or they can be configured on a more granular level to only affect a single user. During this chapter we will go through all the current Webex Calling features available at the time this book was written. Keep in mind that new features are being added all the time, so you have a responsibility to keep current on new features as they come out. Topics discussed in this chapter include the following:

- Admin-Configurable Features
- User-Configurable Features

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 4.5 Describe Webex Calling dial plan 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 25-1 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 25-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Admin-Configurable Features	1–6
User-Configurable Features	7–10

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 the 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. How many call park extensions can be added manually per location in Webex Calling?
   - **a.** 10
   - **b.** 100
   - **c.** 1000
   - **d.** 10,000
2. What is the FAC to park a call using Call Park Group?
   - **a.** #58
   - **b.** *58
   - **c.** #68
   - **d.** *68
3. How many agents does Cisco recommend using with call queue in Webex Control Hub?
   - **a.** 25
   - **b.** 50
   - **c.** 100
   - **d.** 250
4. Which feature allows users to answer calls for other members of this feature when they are busy?
   - **a.** Call Park Direct
   - **b.** Call Park Group
   - **c.** Call queue
   - **d.** Call pickup
5. When creating a hunt group in Webex Control Hub, how many agents are supported when you select Weighted call routing?
   - **a.** 10
   - **b.** 50
   - **c.** 100
   - **d.** 1000
6. How many targets can be included in a paging group?
   - **a.** 25
   - **b.** 50
   - **c.** 75
   - **d.** 100
   - **e.** 1000

7. A user enabled Do Not Disturb on their Webex App. Now their desk phone won't ring and the Webex App won't alert them of incoming messages. How can this user prevent phone calls from ringing but still get alerts for messages?

- **a.** The user needs to disable DND on the Webex App and enable DND on the phone.
- **b.** The user needs to modify DND alerts in the Webex user portal.
- **c.** The user needs to modify DND alerts in the Webex admin portal.
- **d.** An administrator needs to modify DND alerts in the Webex admin portal.
- **e.** Alerts for DND cannot be changed.

8. Which feature forwards incoming calls if your Webex Calling primary line is not connected to the network for any reason, such as power outage, failed Internet connection, or wiring problems?

- **a.** Single Number Reach (Office Anywhere)
- **b.** Call Forwarding
- **c.** Call Forwarding (Business Continuity)
- **d.** Selective Forward Calls

9. Which user-configurable feature must be enabled by an administrator before users can use it?

- **a.** Single Number Reach (Office Anywhere)
- **b.** Call Forwarding
- **c.** Call Forwarding (Business Continuity)
- **d.** Selective Forward Calls

10. When a user is configuring sequential ring for their devices, how many additional numbers can they configure?

- **a.** 2
- **b.** 5
- **c.** 10
- **d.** Unlimited

Foundation Topics

Admin-Configurable Features

Many types of features are available to customers using Webex Calling. These features work whether the customer is full cloud or uses Webex in a hybrid environment with an on-premises Cisco Unified Communications Manager. Most Webex Calling features work with the Webex App or MPP Phones registered to the Webex Control Hub. Some of the features are global, meaning they affect the whole organization collectively. These features must be configured by a Webex administrator, which is why they are called "admin-configurable features." Other features available can be configured by an administrator or by a user. These features affect only the user for which they are configured, which is why they are called "user-configurable features." This topic will focus on defining admin-configurable features and how to configure them.

Auto Attendant

The first admin-configurable feature we'll discuss is the Auto Attendant. This feature ensures that calls are answered and that callers' needs are met. You can add greetings, set up menus, and route calls to an answering service, a hunt group, a voicemail box, or a real person. You can create a 24-hour schedule or provide different options when your business is open or closed.

You can use an existing business hours and holiday schedule to configure the time and days your Auto Attendant is operational and nonoperational, or you can create a new schedule when you create an Auto Attendant. Use the following steps to configure your Auto Attendant:

Key Topic

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com, choose **Services > Calling > Features.**

Step 2. Click **Auto Attendant > Create Auto Attendant.**

Step 3. On the **Basics** page, enter the following information and then click **Next:**

- **Location**
- **Auto Attendant Name**
- **Phone Number**
- **Language**

Step 4. On the **Business Hours Schedule** page, select **Assign an existing schedule** and select an option from the drop-down menu, or select **Create a new schedule.** If you create a new schedule you will need to give the schedule a name, set up the office hours of business, and allocate time for lunch breaks. Click **Next** when finished.

Step 5. On the **Holiday Schedule** page, select **Assign an existing schedule** and select an option from the drop-down menu, or select **Create a new schedule.** If you create a new schedule, you will need to click the **Add a new Holiday to the Holiday Schedule** hyperlink and provide the following information. Click **Next** when finished.

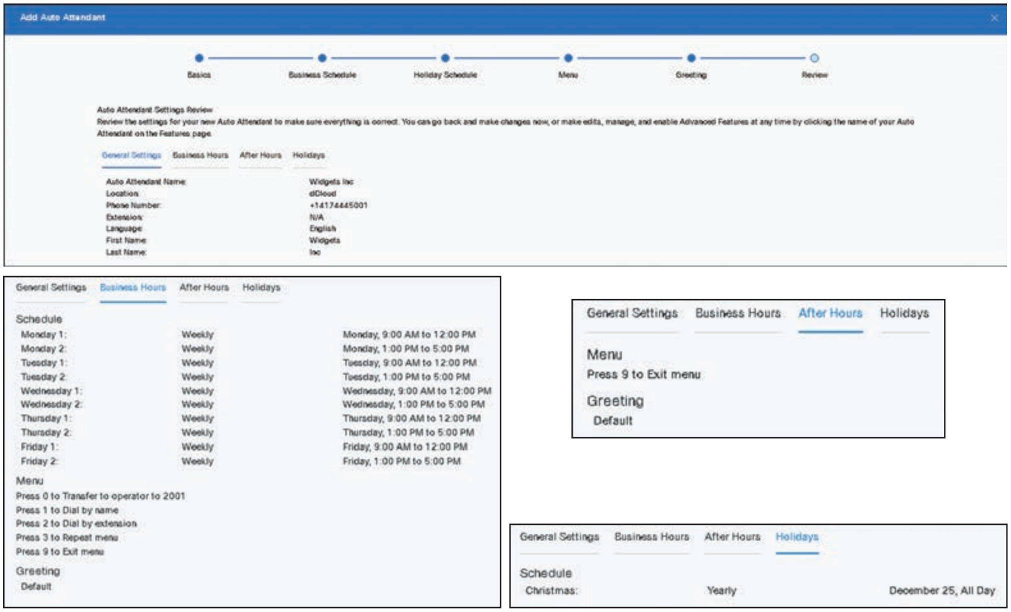
- Holiday name
- Recurrence
- Holiday duration
- Click **Save**
- Select an option from the drop-down menu under **Create a new schedule.**

Step 6. On the **Menu** page, under both the **Business Hours** and **After Hours** tabs, use the drop-down to assign each keypad number to their function. To allow callers to dial an extension without a menu prompt, check the **Enable extension dialing without requiring a menu item** check box. Click **Next.**

Step 7. On the **Greeting** page, under both the **Business Hours** and **After Hours** tabs, choose whether you want to use the **Default greeting** or **Custom greeting.** To record by phone, you will need to set up your voice portal number and passcode for the location this Auto Attendant is associated with. Click **Next.**

Step 8. On the **Review** page, under each tab, review your new Auto Attendant settings to make sure everything is correct. You can click **Back** to make any changes or click **Create** to apply the settings to your new Auto Attendant. Figure 25-1 illustrates the Review page in the Auto Attendant setup wizard.

Step 9. Click **Done** when everything has been completed.



Auto Attendant Settings Review

Review the settings for your new Auto Attendant to make sure everything is correct. You can go back and make changes now, or make edits, manage, and enable Advanced Features at any time by clicking the name of your Auto Attendant on the Features page.

Auto Attendant Name:	Widgets Inc
Location:	dCloud
Phone Number:	+14174445001
Extension:	N/A
Language:	English
First Name:	Widgets
Last Name:	Inc

Schedule

Monday 1:	Weekly	Monday, 9:00 AM to 12:00 PM
Monday 2:	Weekly	Monday, 1:00 PM to 5:00 PM
Tuesday 1:	Weekly	Tuesday, 9:00 AM to 12:00 PM
Tuesday 2:	Weekly	Tuesday, 1:00 PM to 5:00 PM
Wednesday 1:	Weekly	Wednesday, 9:00 AM to 12:00 PM
Wednesday 2:	Weekly	Wednesday, 1:00 PM to 5:00 PM
Thursday 1:	Weekly	Thursday, 9:00 AM to 12:00 PM
Thursday 2:	Weekly	Thursday, 1:00 PM to 5:00 PM
Friday 1:	Weekly	Friday, 9:00 AM to 12:00 PM
Friday 2:	Weekly	Friday, 1:00 PM to 5:00 PM

Menu

Press 0 to Transfer to operator to 2001

Press 1 to Dial by name

Press 2 to Dial by extension

Press 3 to Repeat menu

Press 9 to Exit menu

Greeting

Default

Menu

Press 9 to Exit menu

Greeting

Default

Schedule

Christmas:	Yearly	December 25, All Day

Figure 25-1 *Auto Attendant Setup Wizard Review Page*

Once an Auto Attendant is created, you can create additional Auto Attendants, disable an Auto Attendant, and configure call forwarding for Auto Attendants. There are several settings you can edit as well, such as general settings, phone numbers, dialing options, business hours schedules, business hours menu options, the greeting during business hours, after hours menu options, a greeting for after hours, and holiday schedules. You can also generate Auto Attendant reports.

As demonstrated in the previous steps, every Auto Attendant manually created in Control Hub requires populating a wizard with many parameters. You can also bulk-manage Auto Attendants with bulk inserts or updates using CSV files, which streamlines this process. When exporting data to a CSV file, the number of records may exceed 1000. In such cases, the ZIP file is downloaded, where the ZIP file contains the full set of record(s) in a single CSV file. A separate folder containing all the data is broken down into multiple CSV files with fewer than 1000 records. These files are generated for the administrator to quickly import any updates and upload. If you have a lot of Auto Attendants to add, the bulk-manage Auto Attendant option is very convenient and the CSV support reduces effort for deployment and migration. You will soon be able to support the following functionalities using bulk management for Auto Attendants:

- Deleting an entire Auto Attendant instance
- Creating/modifying/deleting a Call Forwarding rule

- Greeting support for business and holiday hours schedule
- Exposing bulk CSV operations as external APIs
- Creating new schedules

Key Topic

Use the following steps to bulk-manage Auto Attendants:

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com, choose **Services** > **Calling** > **Features**.

Step 2. Click **Auto Attendant > Manage > Bulk Manage**.

Step 3. Select a location from the drop-down list to download data for Auto Attendants on that location or select **All Locations** to download data for all Auto Attendants.

Step 4. Click **Download Data** or **Download .csv template** to verify that your CSV file is properly formatted, making sure to fill in the required information.

Step 5. **Add** or **edit** the first and last name, phone number, and so on within the CSV file and upload the updated CSV file to Webex Control Hub.

Step 6. Click **View import history/tasks** to view the status of your CSV import and indicate whether you've encountered any errors.

Call Park

The Call Park service allows a user to park a call against a user's extension or to a Call Park extension. While the call is parked, the user can make and receive other calls freely and invoke other features without limitation. The Call Park service supports two types of Call Park:

- **Call Park Direct:** Allows users to park a call against a specific user's extension or Call Park extension.
- **Call Park Group:** Allows a defined group of users known as members to automatically park calls against available park destinations configured in a Call Park group. Park destinations can be either members' extensions or Call Park extensions.

Call Park Direct

To park a call to a user or Call Park extension, the parking user puts the active call on hold and initiates a new call to the feature access code (FAC) *68 + (destination user's extension) or (destination Call Park extension). The call remains parked until retrieved or a Call Park recall occurs. To park a call using a Call Park extension being monitored by a user's Cisco phone, the user presses the line key associated with the free Call Park extension.

Key Topic

You can manually add up to 100 Call Park extensions per location using the following steps:

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com/, choose **Services > Calling > Features**.

Step 2. Click **Call Park Extension > Create Call Park Extension**.

Step 3. Select **Manually Add**.

Step 4. Choose the location where you want to add a Call Park extension.

Step 5. Enter a Call Park extension name and extension number.

Step 6. Select **Save**.

You can add multiple Call Park extensions using the following steps:

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com/, choose **Services > Calling > Features**.

Step 2. Click **Call Park Extension > Create Call Park Extension**.

Step 3. Select **Bulk Add in CSV**.

Step 4. Download the CSV template and enter the necessary information. You can add up to 1000 Call Park extensions at a time. Each location can have up to 100 Call Park extensions.

Step 5. Click **Import CSV File**, select the CSV file, and click **Submit**. You can see the CSV import status on the **Tasks** page.

Call Park Group

To park a call to a group, the parking user puts an active call on hold and initiates a new call to the feature access code (FAC) #58. The Call Park Group service automatically hunts for the first available call park destination of the Call Park Group to park the call against. The Call Park Group feature always starts at the first assigned Call Park destination. When a destination is available, and the call is parked against that destination, the caller parking the call receives an announcement with the extension the call is parked against. The parking user may then announce or page that a call has been parked against an extension for retrieval.

Key Topic

Use the following steps to create a Call Park group. Set up or change your Call Park configuration during off-peak hours to avoid any service interruptions.

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com/, choose **Services > Calling > Features**.

Step 2. Click **Call Park Extension** and select a location in the pop-up window.

Step 3. Click **Create Call Park Group** and on the **Location and Name** page, enter a name for the Call Park group. Click **Next**.

Step 4. On the **Members** page, search and add available members by name, phone number, or extension. Here, members define who can park the call. Virtual line numbers can also be added as a member of Call Park group. You can make changes to the existing entries. You can click the trash can icon beside any members you want to remove. Click **Next** when finished.

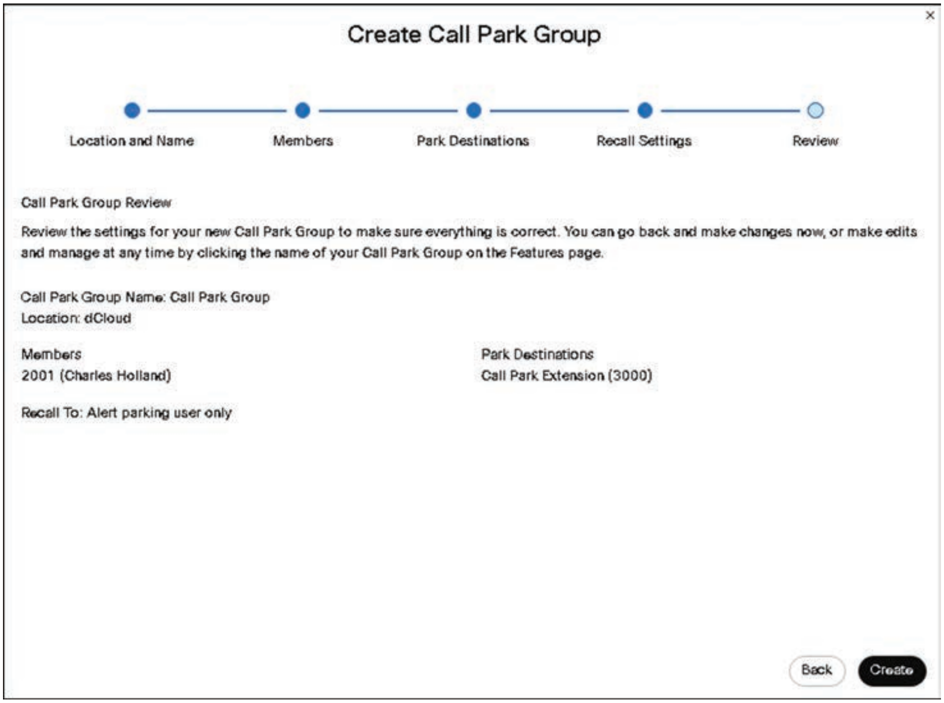
Step 5. On the **Park Destinations** page, the **Use members as park destinations** is disabled by default. This allows you to search for and add Call Park extensions where the group parks the calls. Only Call Park extensions can be added to the destination list. If you want to use participants as destinations, this will disable the use of Call Park extensions. You can click the trash can icon to remove Call Park extensions. Click **Next** when finished.

Step 6. On the **Recall Settings** page, select your preferred **Recall To** option in the drop-down menu. The recall destination is the user or group the call will be directed to if the call is not picked up. The options include following:

- **Alert parking user only:** If a parked call is not picked up, it is reverted to the person who parked the call after the Recall Timer has lapsed. If the parking user does not pick up the reverted call and the Recall Timer lapses again, the parking user is attempted again.
- **Alert parking user first, then hunt group:** If a parked call is not picked up, it is reverted to the person who parked the call after the Recall Timer has lapsed based on the configured recall time. If the parking user does not pick up the reverted call in the set time (Alert Hunt Group Wait Time), the call will be forwarded to the selected hunt group. The call will then follow the hunt group routing and not be reverted.
- **Alert hunt group only:** If a parked call is not picked up the call in the set time (Recall Timer), the call will be forwarded to the selected hunt group. The call will then follow the hunt group routing and not be reverted.

Step 7. Review your settings and then click **Create**. Figure 25-2 illustrates the Review page in the Call Park Group setup wizard.

Step 8. Click **Done** to close the popup window.



Call Park Group Review

Review the settings for your new Call Park Group to make sure everything is correct. You can go back and make changes now, or make edits and manage at any time by clicking the name of your Call Park Group on the Features page.

Call Park Group Name: Call Park Group
Location: dCloud

Members
2001 (Charles Holland)

Park Destinations
Call Park Extension (3000)

Recall To: Alert parking user only

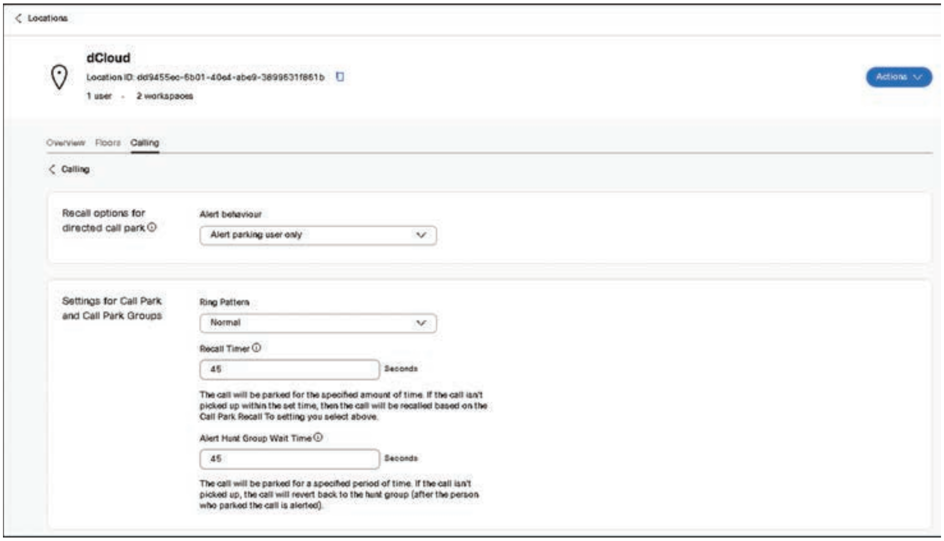
Figure 25-2 *Call Park Group Setup Wizard Review Page*

Call Park Retrieve and Recall User Settings

Once calls are parked, they need to be retrieved by the appropriate user. The following operations apply to both Call Park Direct and Call Park Group. To retrieve the parked call, any user within the organization can dial *88 + (extension of parked call). To retrieve a call from a monitored Call Park extension, the user presses the line key associated with the Call Park extension holding the parked call. If the parked call is not retrieved within the provisioned recall time, the parked call is retrieved and presented to the user who originally parked the call or an alternate recall user.

These settings are at the **Locations** level for Call Park Direct. Go to **Management > Locations**, choose a location and go to **Calling > Calling features settings > Call park settings**. Call Park Group settings are at the **Call Park Group** level and are under **Calling > Features > Call Park Group**. Choose a Call Park Group to edit the settings in a flyout window.

If the parking user's line appears on other phones as shared or monitored, these phones also will be notified of the reverted calls, as shown in the Receptionist Client. The Ring Pattern, Recall Timer, and Alert Hunt Group Wait Time values apply to both Call Park Direct and Call Park Group. These settings are at the **Locations** level and are under **Locations > Calling > Calling features settings > Call park settings**. Figure 25-3 illustrates the Call Park settings under Locations in Webex Control Hub.



Location ID: dd9455ec-6b01-40e4-abe9-3899631f861b

1 user · 2 workspaces

Recall options for directed call park

Alert behaviour: Alert parking user only

Settings for Call Park and Call Park Groups

Ring Pattern: Normal

Recall Timer: 45 Seconds

The call will be parked for the specified amount of time. If the call isn't picked up within the set time, then the call will be recalled based on the Call Park Recall To setting you select above.

Alert Hunt Group Wait Time: 45 Seconds

The call will be parked for a specified period of time. If the call isn't picked up, the call will revert back to the hunt group (after the person who parked the call is alerted).

Figure 25-3 *Call Park Settings in Locations Menu*

Call Queue

You can set up a call queue so that when customers' calls can't be answered, they're provided with an automated answer, comfort messages, and music on hold until someone can answer their call. Group call management is an advanced call queue capability that makes it easy and affordable to support high call volume and team call handling services as a core part of Webex Calling. It adds key features that provide supervisor capabilities, enhance queue policies to determine call routing based on business hours, provide skill-based routing, provide callback capabilities for customers, and provide reports and analytics for administrators. Group call management is an out-of-box feature set within Webex Calling.

Group Call Management refers to a collection of features designed to work together in support of managing high-call-volume sales and support teams for calls directed to a call queue. The features offered by Group Call Management include the following:

- Call queuing
- Skills-based routing
- Request customer callback (for callers in queue)
- Enhanced queue policies for night service, holiday service, force forwarding, and stranded calls
- Additional IVR functions for call whisper message and comfort message bypass
- Agent login/logout of call queues
- Agent status management
- Assign call queue staff to call queues
- Assign supervisors to agents
- Monitor/coach/barge/call takeover (Supervisor functions)
- Call queue reporting and analytics dashboards

Group Call Management is recommended for call queues up to 50 agents. For anything beyond 50 agents, Cisco recommends Webex Contact Center. Webex Contact Center delivers to customers tools that provide more sophisticated customer engagement capabilities, omni-channel routing, and large-scale, high-call-volume deployments.

Use the following steps to create and manage call queues:

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com, choose **Services > Calling > Features**.

Step 2. Click **Call Queue > Create Call Queue**.

Step 3. On the **Basics** page, enter the following information and then click **Next**:

- **Location:** Select a location from the drop-down menu.
- **Call Queue Name:** Enter a name for the call queue.
- **Phone Number:** Assign a primary phone number and/or an extension to the call queue.
- **Allow queue phone number for outgoing calls:** Enable the toggle to allow the queue phone number for outgoing calls.
- **Number of Calls in Queue:** Assign the maximum number of calls for this call queue. Once this number is reached, the overflow settings are triggered. Do not set Number of Calls in Queue to 0. Incoming calls are not allowed if Number of Calls in Queue is set to 0.
- **Caller ID:** Assign the caller ID for the call queue. The caller ID assigned here, along with the calling party's caller ID name and number, will show

when the call queue agents are receiving an incoming call from the queue. The caller ID is also used for calls that are forwarded outside of this call queue. This field is mandatory to navigate to the next screen.

- **Direct Line:** The primary phone number and extension from this queue. Direct line option does not appear if you do not specify a phone number.
- **Assigned Number from the Call Queue's Location:** Select a number from the location.
- **Language:** Select the call queue language from the drop-down menu.

Step 4. On the **Call Routing** page, choose one of the following options and click **Next**:

- **Priority Based**
  - **Circular:** Cycles through all agents after the last agent that took a call. It sends calls to the next available call queue agent.
  - **Top Down:** Sends calls through the queue of agents in order, starting from the top each time.
  - **Longest Idle:** Sends calls to the agent that has been idle the longest. If they don't answer, the call proceeds to the next agent who has been idle second longest, and so on, until the call is answered.
  - **Weighted:** Sends calls to agents based on percentages you assign to each agent in the call queue profile (up to 100%).
  - **Simultaneous:** Sends calls to all agents in a call queue at once.
- **Skill Based:** When you select skill-based call routing, by default routing will happen only based on the skill level. If there is more than one agent with the same skill level, the selected routing pattern is followed to resolve the contention to choose the next agent for call routing.
  - **Circular:** Cycles through all agents after the last agent that took a call. It sends calls to the next available call queue agent.
  - **Top Down:** Sends calls through the queue of agents in order, starting from the top each time.
  - **Longest Idle:** Sends calls to the agent that has been idle the longest. If they don't answer, it proceeds to the next agent who has been idle second longest, and so on, until the call is answered.

Step 5. On the **Overflow Settings** page, determine how overflow calls are handled. Choose one of the following options from the drop-down menu and then click **Next**:

- **Perform busy treatment:** The caller hears a fast busy tone.
- **Play ringing until caller hangs up:** The caller hears ringing until they disconnect.
- **Transfer to phone number:** Enter the number where you want to transfer overflow calls.

You can also enable the following overflow settings. Both options require an additional field to be configured accordingly:

- **Enable overflow after calls wait x seconds:** With this option, you can enter a wait time (in seconds) for callers. Once this wait time is reached by the caller, the overflow treatment is triggered.
- **Play announcement before overflow processing:** If this option is disabled, callers will only hear hold music until the call is answered by a user.

Step 6. On the Announcements page, you can determine the messages and music that callers hear while waiting in the queue. You can enable any of the following options. Once you are finished, click **Next**:

- **Welcome Message:** Play a message when callers first reach the queue. For example, "Thank you for calling. An agent will be with you shortly." This can be set as mandatory. If the mandatory option is not selected and a caller reaches the call queue while there is an available agent, the caller will not hear this announcement and is transferred to an agent.
- **Estimated wait message for Queued Calls:** Notify the caller with either their estimated wait time or position in the queue. If this option is enabled, it plays after the welcome message and before the comfort message.
- **Comfort Message:** Play a message after the welcome message and before hold music. This is typically a custom announcement that plays information, such as current promotions or information about products and services.
- **Comfort Message Bypass:** Play a shorter comfort message instead of the usual Comfort or Music on Hold announcement to all the calls that should be answered quickly. This feature prevents a caller from hearing a short portion of the standard comfort message that abruptly ends when they are connected to an agent.
- **Hold Music:** Play music after the comfort message in a repetitive loop.
- **Call Whisper Message:** Play a message to the agent immediately before the incoming call is connected. The message typically announces the identity of the call queue from which the call is coming.

Step 7. On the **Select Agents** page, click **Add User**, **Workspace**, or **Virtual Line** from the drop-down, then search for or select the users, workspaces, or virtual lines to add to the call queue.

Step 8. Assign a skill level (1 being the highest skill level and 20 being the lowest skill level) to each user or workspaces added to the call queue.

- You can assign a skill level only when you select a skill-based routing type; otherwise, you will not have the option to set the skill level.
- By default, agents with skill level 1 (the highest skill level) are added.

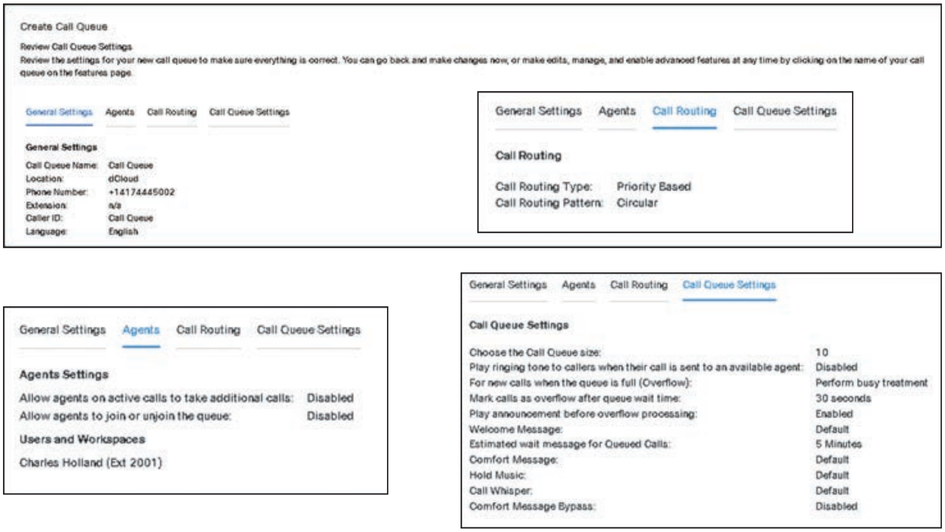
Step 9. (Optional) Select the check box if you want to allow agents on active calls to take additional calls.

Step 10. (Optional) Select the check box if you want to allow agents to join or unjoin the queue.

Step 11. Depending on which call routing option you chose previously, you may need to add extra information, such as adding a percentage weighting to users or workspaces, or in the case of circular or top-down call routing, dragging and dropping users and workspaces in the order of their queue position. Click **Next**.

Step 12. On the **Review** page, review your call queue settings to make sure you've entered the correct details. Figure 25-4 illustrates the review screen for the call queue setup wizard.

Step 13. Click **Create** and **Done** to confirm your call queue settings. Once a queue is created, you can enable or disable the queue using the toggle beside **Enable Call Queue** in the side panel.



Create Call Queue

Review Call Queue Settings

Review the settings for your new call queue to make sure everything is correct. You can go back and make changes now, or make edits, manage, and enable advanced features at any time by clicking on the name of your call queue on the features page

General Settings

Call Queue Name: Call Queue
Location: dCloud
Phone Number: +14174445002
Extension: n/a
Caller ID: Call Queue
Language: English

Call Routing

Call Routing Type: Priority Based
Call Routing Pattern: Circular

Agents Settings

Allow agents on active calls to take additional calls: Disabled
Allow agents to join or unjoin the queue: Disabled

Users and Workspaces

Charles Holland (Ext 2001)

Call Queue Settings

Choose the Call Queue size: 10
Play ringing tone to callers when their call is sent to an available agent: Disabled
For new calls when the queue is full (Overflow): Perform busy treatment
Mark calls as overflow after queue wait time: 30 seconds
Play announcement before overflow processing: Enabled
Welcome Message: Default
Estimated wait message for Queued Calls: 5 Minutes
Comfort Message: Default
Hold Music: Default
Call Whisper: Default
Comfort Message Bypass: Disabled

Figure 25-4 *Call Queue Setup Wizard Review Page*

Once your call queue is created, you can manage it. Different settings you can manage include calls within the queue, policies, announcements, agents, and supervisors. You can also view call queue analytics or reports.

Call Pickup

You can enhance teamwork and collaboration by creating call pickups. Users who are added to a call pickup can answer calls when another member of the call pickup is busy. Group Call Pickup enables a user to answer any ringing line within their pickup group. A pickup group is an administrator-defined set of users within a site to which the Call Pickup feature applies. The Group Call Pickup feature requires call pickup groups to be added, modified, and removed as well as specific users to be assigned to the pickup group. Call pickups must meet the following conditions:

- A user can only be assigned to one call pickup.
- A call pickup can only have users from the same location.
- A location may have multiple call pickups.
- Call pickup names must be unique.

Use the following steps to create a call pickup:

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com, choose **Services > Calling > Features.**

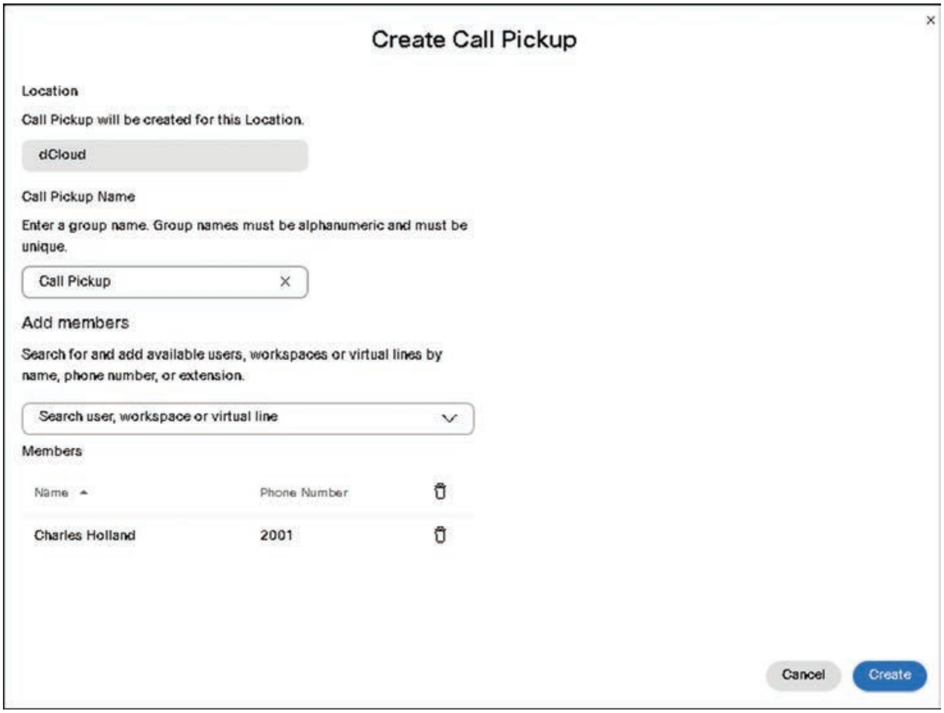
Step 2. Click **Call Pickup** and then click **Create Call Pickup.** You may be asked to select a location in a popup window if this is the first call pickup you've created.

Step 3. Select a location from the **Location** drop-down menu. If you have previously selected a location, ensure the correct one is selected.

Step 4. Enter a unique name for the call pickup.

Step 5. Search for and add available users, workspaces, or virtual lines by name, phone number, or extension to the call pickup.

Step 6. Click **Create** and then click **Done.** Figure 25-5 illustrates the fields that need to be configured for call pickup.



Create Call Pickup

Location

Call Pickup will be created for this Location.

dCloud

Call Pickup Name

Enter a group name. Group names must be alphanumeric and must be unique.

Call Pickup

Add members

Search for and add available users, workspaces or virtual lines by name, phone number, or extension.

Search user, workspace or virtual line

Members

Name	Phone Number
Charles Holland	2001

Figure 25-5 *Call Pickup Configuration Fields*

You can also add and manage call pickup groups in bulk using a call pickup CSV. Once the call pickup has been created, you can edit settings using the following steps:

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com, choose **Services > Calling > Features**.

Step 2. Click **Call Pickup** and select the call pickup you want to edit.

Step 3. Make any changes to the call pickup and then click **Save**.

Hunt Groups

Hunt groups route incoming calls to a group of users or workspaces. You can even configure a pattern to route to a whole group. You can use hunt groups to ensure that all your incoming calls are answered by the right people or routed to voicemail for later response. Hunt groups route incoming calls to specific employees in a predetermined pattern. This is done by assigning a phone number to a group of employees and then setting rules that define how the call is answered, how long the call remains on hold, and to whom to forward the call.

A sales team could use hunt groups to create a sequential routing pattern between them. An incoming call rings one phone, but if there's no answer, the call goes to the next hunt group member in the list and so on. The next call that comes in starts in the list where the last call left off so all sales staff will receive calls eventually. A support team could also use hunt groups to create a pattern of having all phones ring at the same time so that the first available member can take the call. What other scenarios can you imagine where hunt groups would be useful?

Key Topic

The following steps can be used to configure hunt groups in the Webex Control Hub.

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com, go to **Services > Calling > Features**.

Step 2. Click **Hunt Group > Create Hunt Group**.

Step 3. In the **Basics** tab, enter the following information and then click **Next**:

- **Location:** Select a location from the drop-down. A location is a container with location-specific calling configuration.
- **Hunt Group Name:** Enter a name for the hunt group.
- **Phone Number:** Assign a primary phone number and/or an extension to the hunt group.
- **Caller ID:** Assign the caller ID for the hunt group. Caller ID is used for calls that are forwarded outside of this hunt group.
- **Language:** Select the hunt group language in the drop-down menu.

Step 4. In the **Call Routing** tab, choose one of the following options:

- **Circular (Max 1,000 agents):** This option cycles through all members after the last member that took a call. It sends calls to the next available hunt group member.

- **Top Down (Max 1,000 agents):** Send the call through the queue of members in order, starting from the top each time.
- **Longest Idle (Max 1,000 agents):** Sends calls to the member who has been idle the longest. If they don't answer, proceed to the next member who has been idle second longest, and so on, until the call is answered.
- **Weighted (Max 100 agents):** Sends call to idle members based on percentages you assign to each member of the hunt group (up to 100%).
- **Simultaneous (Max 50 agents):** Sends calls to all members in a call queue at once.

Step 5. You can check the **Advance after a set number of rings** check box and use the drop-down to select the number of rings to apply to your call routing choice, if required. Click **Next** when finished.

Step 6. On the **Routing Settings** tab, you can enable one or more of the following options, if required, and then click **Next:**

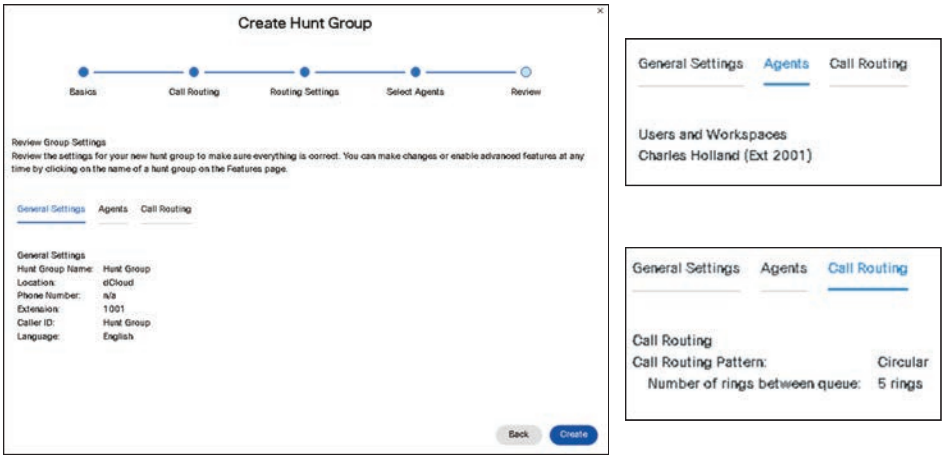
- **Advance when busy:** The hunt group won't ring members when they are on another call and advances to the next member in the hunt group. If the member has Call Waiting enabled and the call is advanced to them, the call waits until the member becomes idle again.
- **Forward after a set number of rings:** Unanswered calls after a defined number of rings forwards to a designated number.
- **Divert calls when unreachable:** Unanswered calls divert to a defined phone number. This could apply to phone calls that aren't answered due to a network outage, or all members of the hunt group are busy and the Advance When Busy option is also enabled. For users only using a mobile device, calls won't be diverted if there is a network outage.

Step 7. In the **Select Agents** tab, search and add users, workspaces, or virtual lines to the call list. Depending on which Call Routing option you chose previously, you need to add extra information such as adding a percentage weighting to users, workspaces, or virtual lines, or in the case of circular call routing, drag and drop users, workspaces, or virtual lines in the order of their queue position. Click **Next** when finished.

Step 8. In the **Review** tab, you get a chance to review your hunt group settings to make sure you've entered the correct details. Figure 25-6 illustrates the review page in the hunt group wizard.

Step 9. Click **Next** and **Done** to confirm your Hunt Group settings.

There are other advanced tasks you can use once your hunt group has been configured. Simply select the hunt group you want to edit and use the menus in the flyout window to make the necessary changes. You can also add and manage hunt groups in bulk using a hunt group CSV.



Review Group Settings

Review the settings for your new hunt group to make sure everything is correct. You can make changes or enable advanced features at any time by clicking on the name of a hunt group on the Features page.

General Settings

Hunt Group Name:	Hunt Group
Location:	dCloud
Phone Number:	n/a
Extension:	1001
Caller ID:	Hunt Group
Language:	English

Users and Workspaces

Charles Holland (Ext 2001)

Call Routing

Call Routing Pattern:	Circular
Number of rings between queue:	5 rings

Figure 25-6 *Hunt Group Setup Wizard Review Page*

Paging Group

Group Paging allows a user to place a one-way call or group page to up to 75 target users and workspaces by dialing a number or extension assigned to a specific paging group. You can create a paging group so that users can send an audio message to a person, department, or team. The Group Paging service makes a simultaneous call to all the assigned targets and announces to the originator that the system is ready for paging. After speaking, the originator ends the page by hanging up the call.

There are a few things to note before setting up this feature. You can assign a user as both a paging target and paging originator in a paging group. Locations can have multiple Group Paging services configured because you can define a paging originator and/or a paging target in multiple paging groups. If a user is not on the phone, the call from a group page is automatically answered and the target hears a paging announcement to alert them they are receiving a page. If a paging target is on a call, the page is not automatically answered. If a paging target chooses not to answer the page, the group paging call won't forward to the paging target's voicemail. If a paging target has Do Not Disturb enabled on their phone, they won't be paged. If a paging target has Single Number Reach (Office Anywhere), Call Forwarding, or Simultaneous Ring enabled, the configured destination service won't be called. When the page is set up to the paging targets, the originator receives a "Paging System Ready" announcement, alerting them to begin speaking. The group page is a one-way audio service. The paging originator has a one-way talk path to the paging targets. The paging targets do not have a talk path to each other or to the paging originator for the duration of the page.

Before you configure a paging group in Webex Control Hub, you should check that the extensions you plan to assign to a paging group are available and unassigned. Also, paging groups must have more than one member, and each member must have at least one registered device. If someone pages a group with no registered devices, they'll hear a busy signal. Finally, paging groups only work with the Cisco IP Phone 6800, 7800, or 8800 series as well as Analog Telephone Adapters (ATAs) 191 and 192. Paging cannot be used in conjunction with the Webex App. For customers in the Asia-Pacific region, the Calling Line field is autopopulated with the username. You cannot modify the Calling Line field. Use the following steps to configure a paging group:

Key Topic

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com, go to **Services > Calling > Features.**

Step 2. Select **Paging Group > Create Paging Group.**

Step 3. In **Settings**, select the **Location**, **Paging Group Name**, and then a **Phone Number** or **Extension**, or both.

Step 4. Select the group paging language in the **Language** drop-down menu.

Step 5. For **Calling Line ID**, enter the **Calling ID First Name** and **Calling ID Last Name** that displays on target users' phones when a group page is performed.

Step 6. Select the **Calling ID Label** to determine what is shown on target users' caller ID when a group page is performed. Click **Next.**

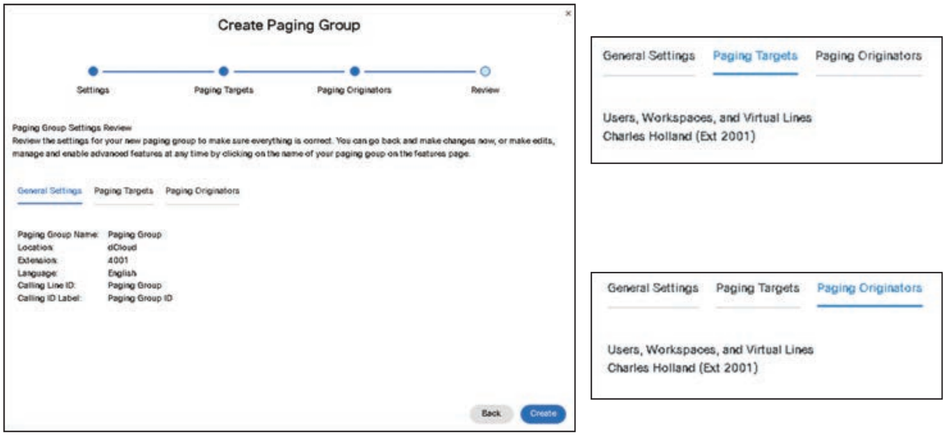
- **Paging Group ID:** Displays the calling line ID name.
- **Page Originator:** Displays the calling line ID name and number of the user who originates the page.

Step 7. In the **Paging Targets** section, search for and add up to 75 users, workspaces, or virtual lines in the organization that can **receive** paging announcements.

Step 8. Select the **Copy my paging targets to my paging originators** check box to copy added users for paging originators in the next section. Click **Next.**

Step 9. In the **Paging Originators** section, search for and add users, workspaces, or virtual lines in the organization that can initiate paging announcements. Click **Next.**

Step 10. In the **Paging Group Settings Review** section, review your settings under each tab. Click **Create** and **Done.** Figure 25-7 illustrates the review page in the paging group wizard.



Paging Group Settings Review

Review the settings for your new paging group to make sure everything is correct. You can go back and make changes now, or make edits, manage and enable advanced features at any time by clicking on the name of your paging goup on the features page.

Paging Group Name: Paging Group
Location: dCloud
Extension: 4001
Language: English
Calling Line ID: Paging Group
Calling ID Label: Paging Group ID

Users, Workspaces, and Virtual Lines
Charles Holland (Ext 2001)

Users, Workspaces, and Virtual Lines
Charles Holland (Ext 2001)

Figure 25-7 *Paging Group Setup Wizard Review Page*

Once a paging group has been created, you can use the following steps to make changes if needed:

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com, go to **Services > Calling > Features.**

Step 2. Select **Paging Group** and select a paging group that you want to edit from the list.

Step 3. You can edit the following settings:

- **General Settings:** Edit the location, calling line ID, and calling ID label for the paging group.
- **Phone Number:** Edit the phone number or extension for the paging group.
- **Paging Targets:** Edit, add, or delete the list of users, workspaces, or virtual lines that can receive the paging announcement.
- **Paging Originators:** Edit the list of users, workspaces, or virtual lines that can initiate the paging announcements.

Step 4. Click **Save** after making any changes to the paging group.

Other Admin Configurable Features

Many other admin-configurable features are available, although these are less commonly used. Therefore, instead of going into detail about each of these features, we'll look at brief explanation of each. For more information about these features, and how to configure them in Webex Control Hub, you can go to https://help.webex.com and search for them within this database.

Cisco Digital Enhanced Cordless Telecommunications (DECT) phone systems are cordless phones that can all operate from a single base station within their range of communication. This is a great solution for warehouses, construction sites, lumber yards, and so on. Webex Calling provides multicell support for the Cisco IP DECT DBS-210, allowing the provisioning of up to 1000 lines across up to 254 bases. Administrators can build and manage Cisco DECT network settings within Cisco Webex Control Hub. The Cisco IP DECT Series consist of these Cisco devices:

Key Topic

- Cisco IP DECT DBS 110 Single-Cell Base Station
- Cisco IP DECT DBS 210 Multi-Cell Base Station (up to 254 bases)
- Cisco DECT Handsets (6823 and 6825)

The Single Number Reach feature allows users to make, receive, and move calls to or from any designated device. For example, when a user is on a call using their desktop phone, they can push or pull that call to or from their mobile phone. When users place long-distance or international calls from a phone, usage is tracked and reflected on your invoice. The Single Number Reach feature isn't automatically set up when service is provisioned. Before users can start using the Single Number Reach feature, you must first create a Single Number Reach for a location and then assign a phone number to be used as the Single Number Reach portal. This is an administrative duty that must be performed before users can set up Single Number Reach (Office Anywhere) for themselves. More on that in the next topic.

The Receptionist Client is a web-based tool that combines your desk phone with a desktop interface and enables you to process calls to users within your organization. You can screen incoming calls, manage calls and contacts, and monitor calls in a queue. Users, such as receptionists, can access the receptionist feature from the Calling User Portal. A desk phone or Webex App is required to place and/or receive calls. Once you're signed in, the display panes in the dashboard allow you to do the following:

Key Topic

- View global messages, application settings, and information about your user account and call state
- View and change your current settings
- View and manage active calls from the calls console
- Create and manage contacts
- Monitor and manage queued calls from the queued calls pane

The Virtual Extensions feature allows you to assign extensions to external phone numbers that users frequently call to make their lives easier. You might have remote workers on a separate telephony system or a key customer you want to reach easily. First, you can associate an extension with their external phone number. Then, you can contact them using their extension just like you contact anybody else in your organization with an assigned extension. For calls from external phone numbers associated with a virtual extension, the virtual extension and the name assigned to that virtual extension are presented on the called destination within Webex Calling. There are two modes of operation for virtual extensions. The mode you choose applies to your entire organization. Most customers will use the default mode (Standard). You can select the other available mode (Enhanced). With *Enhanced* mode enabled, virtual extensions will not function correctly unless your PSTN provider supports specific network signaling extensions. In *Standard* mode, virtual extensions must be associated with a valid E.164.

The Voicemail Group feature allows you to manage a shared voicemail and inbound fax box for Webex Calling. You can create a shared voicemail box and inbound fax box to assign to users or call routing features like an Auto Attendant, call queue, or hunt group. With the voicemail group feature, you can set up new message notifications, choose where you want the messages stored, and customize the voicemail box greeting. You might use a voicemail group for any of the following scenarios:

- You need a general-purpose voicemail for a department or workgroup.
- You'd like to add a voicemail option to an Auto Attendant or hunt group.
- You'd like to send the overflowed incoming calls from a call queue to a shared voicemail box.
- You have users who only need a voicemail box.

The Announcement Files feature is an announcement repository that helps manage audio files from a common location that are used in various services, such as Auto Attendant announcements, music on hold, and call queue announcements. You can update these announcements once and apply them against all the respective instances. This feature provides a more scalable way to update Auto Attendants and allows administrators to update company-wide announcements, such as a holiday announcement. You can set the announcement repository at the Customer Level Repository and the Location Level Repository. The Announcement Repository option at the customer and location level provides the following capabilities:

- Add, update, and delete the audio files
- Replace existing announcement files
- Filter and Sort capability to view the files
- Display the file information and the feature instance that is attached with an announcement.
- Support for localization of the announcements

User-Configurable Features

As mentioned in the previous topic, user-configurable features are features that can be configured by either an administrator or a user. These features affect only the user for which they are configured, unlike admin-configurable features, which affect everyone within the organization. This topic will focus on defining user-configurable features and how to configure them. Some of these features require only a toggle to be switched on for the feature to be used, while others will require additional configuration. The first three features we will discuss in this topic are those that require only a toggle to be switched to enable the feature.

Anonymous Call Rejection

You can set up Anonymous Call Rejection to reject all incoming calls from unidentified or blocked caller IDs. Use the following steps to configure this feature:

Key Topic

Step 1. Go to https://settings.webex.com and select **Webex Calling**.

Step 2. From the calling user portal, go to **Call Settings**.

Step 3. Toggle on **Anonymous Call Rejection**.

Call Waiting

Call Waiting allows you to place an ongoing call on hold to answer a new incoming call at your discretion. Should you choose to disregard the incoming call, it will be transferred to your voicemail or another predetermined destination. Use the following steps to configure this feature:

Step 1. Go to https://settings.webex.com and select **Webex Calling**.

Step 2. From the calling user portal, go to **Call Settings**.

Step 3. Toggle on **Call Waiting**.

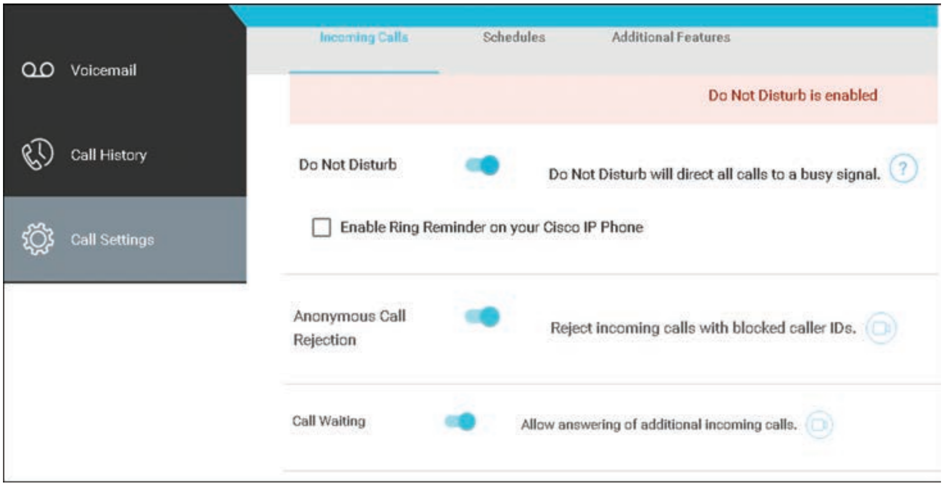
Do Not Disturb

When you need time to focus and do not want any incoming call notifications to disturb you, now you do not have to enable Do Not Disturb (DND) on each of your Webex Calling registered clients separately. When you enable it on the Webex App, the state is automatically synchronized to your desk phone. Similarly, when you enable it on your desk phone, the state is automatically synchronized to your Webex App. When you set DND status on Webex Calling–registered clients, you do not get a notification of the incoming call. The calls go directly to voicemail if the call forward busy setting is configured. The caller hears a busy signal if the voicemail is not configured. Figure 25-8 illustrates how to enable these three features. You can also enable DND from the user portal using the following steps:

Step 1. Go to https://settings.webex.com and select **Webex Calling.**

Step 2. From the calling user portal, go to **Call Settings.**

Step 3. Toggle on **Do Not Disturb (DND).** This will disable other features you have active when it is enabled.



Do Not Disturb is enabled

Do Not Disturb ● Do Not Disturb will direct all calls to a busy signal.

□ Enable Ring Reminder on your Cisco IP Phone

Anonymous Call Rejection ● Reject incoming calls with blocked caller IDs.

Call Waiting ● Allow answering of additional incoming calls.

Figure 25-8 *Enabling Anonymous Call Rejection, Call Waiting, and Do Not Disturb*

When the user enables DND on the desk phone and it is synchronized to the Webex App, it disables both call and message notifications. If some users do not want message notifications to be disabled, the admin can disable DND synchronization. Administrators can use the following steps to disable DND synchronization:

Step 1. From the Webex Control Hub administration portal at https://admin.webex.com, go to **Services > Calling > Client Settings.**

Step 2. In the Do Not Disturb (DND) Status Sync section, toggle to disable **Allow DND to be synchronized.**

Call Forwarding

If you're going to be away from your desk but don't want to miss an important phone call, you can forward your calls to another phone number using Call Forwarding. Use the following steps to configure Call Forwarding:

Step 1. Go to https://settings.webex.com and select **Webex Calling.**

Step 2. From the calling user portal, go to **Call Settings.**

Step 3. Toggle on **Call Forwarding.**

Step 4. Select the Call Forwarding option you would like to use from the following list:

- Always
- When Busy

- **When No Answer.** You will also need to select the number of rings before forwarding with this option.

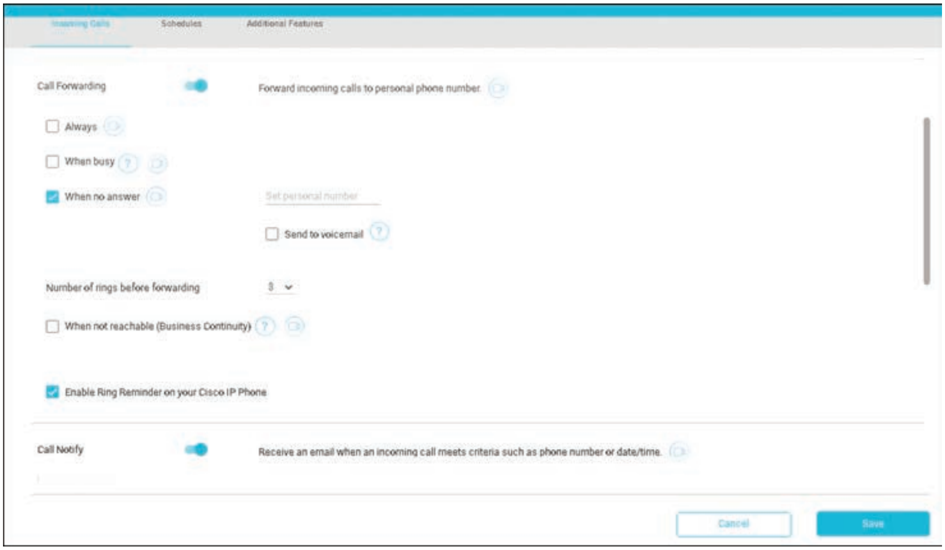
- **When Not Reachable (Business Continuity).** Forwards incoming calls if your Webex Calling primary line is not connected to the network for any reason, such as power outage, failed Internet connection, or wiring problems.

- **Enable Ring Reminder on your Cisco IP Phone.** A notification sound is played.

Step 5. Enter a phone number to forward calls to. Optionally, you can check the box beside **Send to voicemail** to forward the call to voicemail.

Step 6. Optionally, you can enable **Call Notify.** This allows you to receive an email when an incoming call meets certain criteria, such as a phone number or a date and time.

Step 7. Click **Save.** Figure 25-9 illustrates how to enable Call Forwarding.



Call Forwarding ● Forward incoming calls to personal phone number.

☐ Always

☐ When busy

☑ When no answer   Set personal number

☐ Send to voicemail

Number of rings before forwarding 3

☐ When not reachable (Business Continuity)

☑ Enable Ring Reminder on your Cisco IP Phone

Call Notify ● Receive an email when an incoming call meets criteria such as phone number or date/time.

Figure 25-9 *Enabling Call Forwarding*

Selective Calling

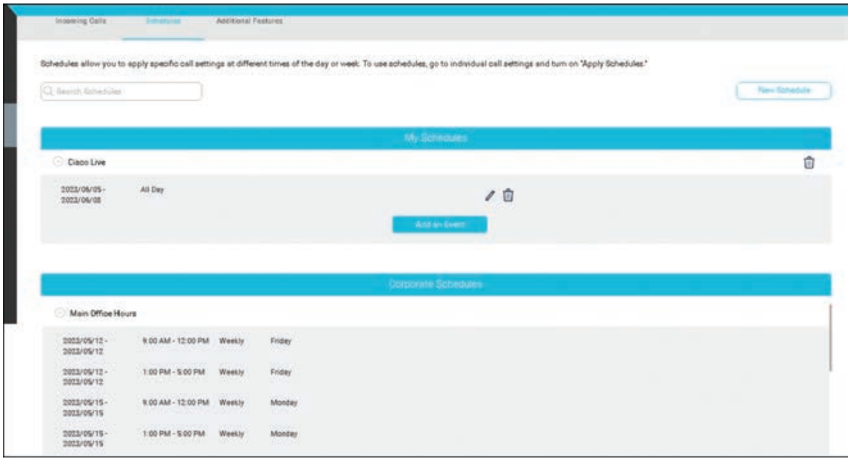
Selective calling allows you to choose which calls you accept, reject, and forward in the calling user portal. You can create different rules to accept, reject, or forward certain calls based on the phone number, who's calling, and/or the time and day of the call. Use the following steps to selectively accept calls:

Step 1. Go to https://settings.webex.com and select **Webex Calling.**

Step 2. From the calling user portal, go to **Call Settings.**

Step 3. Toggle on **Selectively Accept Calls.**

Step 4. Select a predefined schedule from the drop-down menu. If you do not see a schedule you would like to use for this setting, you can add a schedule on the **Schedules** tab. Figure 25-10 illustrates the Schedules tab.



Schedules allow you to apply specific call settings at different times of the day or week. To use schedules, go to individual call settings and turn on "Apply Schedules."

Cisco Live

2023/06/05 - 2023/06/08	All Day		

Main Office Hours

2023/05/12 - 2023/05/12	9:00 AM - 12:00 PM	Weekly	Friday
2023/05/12 - 2023/05/12	1:00 PM - 5:00 PM	Weekly	Friday
2023/05/15 - 2023/05/15	9:00 AM - 12:00 PM	Weekly	Monday
2023/05/15 - 2023/05/15	1:00 PM - 5:00 PM	Weekly	Monday

Figure 25-10 *Schedules Tab for User Configurable Features*

Step 5. Click **Add Schedule** to set the following parameters:

- **When:** Select your predefined schedule from the drop-down menu.
- **And:** Select if you would like to accept calls from any phone number or select phone numbers. If you choose Select Phone Numbers, enter the additional details.
- **Then:** Choose to **Accept** or **Don't accept** the calls that fit within these parameters. Click **Save.**

Selectively Reject Calls

You can reject calls at specific times from specific callers. This setting will take precedence over Selectively Accept Calls. Use the following steps to selectively reject calls:

Step 1. Go to https://settings.webex.com and select **Webex Calling.**

Step 2. From the calling user portal, go to **Call Settings.**

Step 3. Toggle on **Selectively Reject Calls.**

Step 4. Select a predefined schedule from the drop-down menu. If you do not see a schedule you would like to use for this setting, you can add a schedule on the Schedules tab.

Step 5. Click **Add Schedule** to set the following parameters:

- **When:** Select your predefined schedule from the drop-down menu.
- **And:** Select if you would like to reject calls from any phone number or select phone numbers. If you choose **Select Phone Numbers**, enter the additional details.
- **Then:** Choose to **Accept** or **Don't accept** the calls that fit within these parameters.

Step 6. Click **Save.**

Selectively Forward Calls

You can forward calls at specific times from specific callers. This setting takes precedence over call forwarding. Use the following steps to selectively forward calls:

Step 1. Go to https://settings.webex.com and select **Webex Calling**.

Step 2. From the calling user portal, go to **Call Settings**.

Step 3. Toggle on **Selectively Forward Calls**.

Step 4. Enter the phone number to forward calls to. Check the box next to **Send to voicemail** to forward all calls to voicemail.

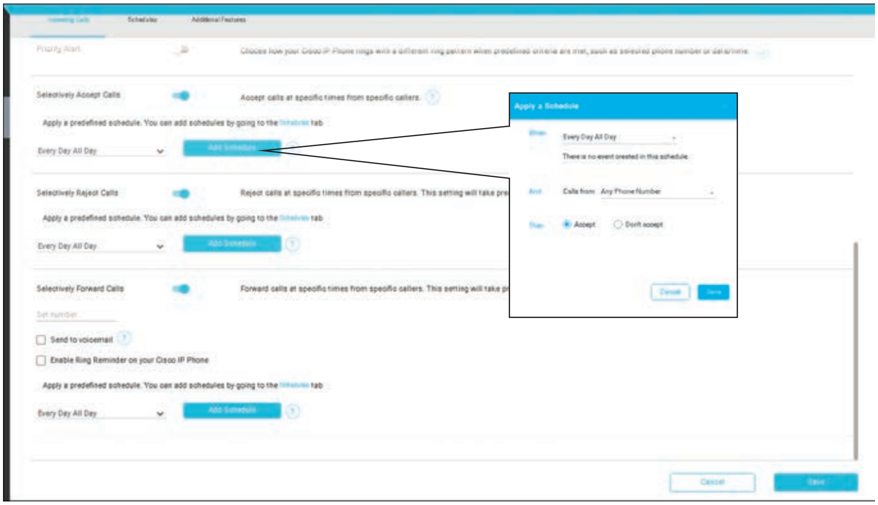
Step 5. Check the box next to **Use ring reminder** to enable a ring reminder for these calls.

Step 6. Select a predefined schedule from the drop-down menu. If you do not see a schedule you would like to use for this setting, you can add a schedule on the **Schedules** tab.

Step 7. Click **Add Schedule** to set the following parameters:

- **Forward to:** Enter the phone number to forward calls to during this schedule or check the **Send to voicemail** box.
- **When:** Select your predefined schedule from the drop-down menu.
- **And:** Select if you would like to accept calls from any phone number or select phone numbers. If you choose **Select Phone Numbers**, enter the additional details.
- **Then:** Choose to **Forward** or **Don't Forward** the calls that fit within these parameters.

Step 8. Click **Save**. Your schedule is added to a **Forward** or **Don't Forward** table. You can edit or delete schedules from the tables, as needed. Figure 25-11 illustrates how to configure the Selective Accept Calls, Selectively Reject Calls, and the Selectively Forward Calls settings.



Priority Alert — Choose how your Cisco IP Phone rings with a different ring pattern when predefined criteria are met, such as selected phone number or date/time.

Selectively Accept Calls — Accept calls at specific times from specific callers.

Apply a predefined schedule. You can add schedules by going to the Schedules tab

Every Day All Day

Selectively Reject Calls — Reject calls at specific times from specific callers. This setting will take pre

Apply a predefined schedule. You can add schedules by going to the Schedules tab

Every Day All Day

Selectively Forward Calls — Forward calls at specific times from specific callers. This setting will take pr

Set number

□ Send to voicemail

□ Enable Ring Reminder on your Cisco IP Phone

Apply a predefined schedule. You can add schedules by going to the Schedules tab

Every Day All Day

When: Every Day All Day

There is no event created in this schedule

And: Calls from: Any Phone Number

Then: ● Accept ○ Don't accept

Figure 25-11 *Configure Selectively Accept, Reject, and Forward Calls*

Call Notify

With the Call Notify feature, you can receive an email notification when a call or voicemail is received. When enabled, this feature treats all calls to your extension as busy. You can also enable a ring reminder to provide a brief ringtone to your desk phone when you receive calls. Use the following steps to configure Call Notify:

Step 1. Go to https://settings.webex.com and select **Webex Calling.**

Step 2. From the calling user portal, go to **Call Settings.**

Step 3. Toggle on **Call Notify.**

Step 4. Enter an email address to send notifications.

Step 5. Select a predefined schedule from the drop-down menu. If you do not see a schedule you would like to use for this setting, you can add a schedule on the **Schedules** tab.

Step 6. Click **Add Schedule** to set the following parameters:

- **When**: Select your predefined schedule from the drop-down menu.
- **And**: Select if you would like to accept calls from any phone number or select phone numbers. If you choose **Select Phone Numbers**, enter the additional details.
- **Then**: Choose either **Notify me** or **Don't notify me** for the calls that fit within these parameters.

Step 7. Click **Save.** Your schedule is added to a **Notify Me** or **Don't Notify Me** table. You can edit or delete schedules from the tables, as needed.

Single Number Reach

In the previous topic, I mentioned Single Number Reach because there are some administrative duties that must be set up before users can use this feature. As a review, with Single Number Reach (Office Anywhere), you can make, receive, and move calls to or from any device, such as a desk phone and mobile phone, without interruption. Once you've added the device's phone number in the calling user portal, all the listed devices ring when you receive a call. Also, if you make outgoing calls from any of your devices, your Webex Calling primary number is used as the caller ID for identity. Users can use the following steps to configure Single Number Reach (Office Anywhere):

Step 1. Go to https://settings.webex.com and select **Webex Calling.**

Step 2. From the calling user portal, go to **Call Settings.**

Step 3. Toggle on **Single Number Reach (Office Anywhere).**

Step 4. Mark the check box if you want to enable contact calling from the Directory tab.

Step 5. Click **Add Personal Number** to add a phone number to be used as your Single Number Reach (Office Anywhere) number.

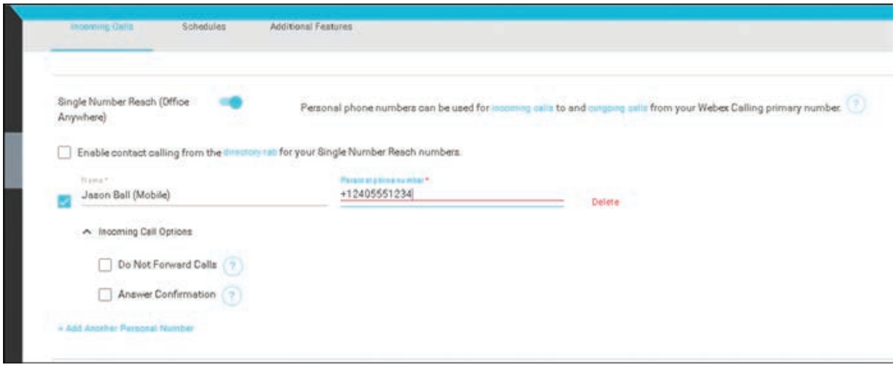
Step 6. Enter the **Name** and **Phone Number.** Once you add a phone number, the number gets activated. To deactivate it, uncheck the box next to the phone number.

Step 7. Click **Incoming Call Options** to expand the following settings that can be selected for this phone number:

- **Do Not Forward Calls:** Your calls aren't forwarded, even if you have call forwarding enabled.
- **Answer Confirmation:** When someone calls you, they're prompted to press a key before being connected. Use this option if you want your callers to know that their call is automatically going to your Single Number Reach (Office Anywhere) number.

Step 8. Optionally, you can add another personal number by clicking **Add Another Personal Number** and then following Steps 6 and 7 again.

Step 9. Click **Save.** Figure 25-12 illustrates how to configure the Single Number Reach (Office Anywhere) settings.



Single Number Reach (Office Anywhere) ●

Personal phone numbers can be used for incoming calls to and outgoing calls from your Webex Calling primary number.

□ Enable contact calling from the directory tab for your Single Number Reach numbers

☑ Name* Jason Ball (Mobile) Personal phone number* +12405551234 Delete

Incoming Call Options

□ Do Not Forward Calls

□ Answer Confirmation

+ Add Another Personal Number

Figure 25-12 *Configure Single Number Reach (Office Anywhere)*

Priority Alert

Priority Alert is a feature that allows you to set up a unique ringtone based on predefined criteria. This is helpful, for example, when you want to be quickly notified that a specific phone number is calling you. Use the following steps to configure Priority Alert:

Step 1. Go to https://settings.webex.com and select **Webex Calling.**

Step 2. From the calling user portal, go to **Call Settings.**

Step 3. Toggle on **Priority Alert.**

Step 4. Select a predefined schedule from the drop-down menu. If you do not see a schedule you would like to use for this setting, you can add a schedule on the **Schedules** tab.

Step 5. Click **Add Schedule** to set the following parameters:

- **When:** Select your predefined schedule from the drop-down menu.
- **And:** Select if you would like to accept calls from any phone number or select phone numbers. If you choose **Select Phone Numbers**, enter the additional details.
- **Then:** Choose to **Alert** or **Don't alert** for the calls that fit within these parameters.

Step 6. Click **Save** to save your Priority Alert parameters. Your schedule is added to an **Alert** or **Don't alert** table. You can edit or delete schedules from the tables, as needed.

Sequential Ringing

Sequential Ring allows you to create a list of up to five additional numbers to ring in a specific order when you receive incoming calls following the schedules you create. When a caller dials a user that has Sequential Ring enabled, they hear an announcement asking them to stay on the line. If the interrupt setting is enabled, the caller also hears a message to press pound to interrupt the search, if applicable. The caller hears ringing after the first announcement. If a call is answered by any of the numbers in the search list, the search is stopped. Every 20 seconds, a comfort message is played asking the caller to stay on the line. If the interrupt button (#) is pressed, the caller is provided with the subscriber's no answer processing. After all numbers were tried and not answered, the ring back or announcement is interrupted, and the caller is provided with the subscriber's no answer processing, which is voicemail in most cases. Use the following steps to configure Sequential Ringing:

Step 1. Go to https://settings.webex.com and select **Webex Calling.**

Step 2. From the calling user portal, go to **Call Settings.**

Step 3. Toggle on **Sequential Ringing.**

Step 4. Enter a list of 10-digit numbers or E.164 International numbers to be rung in order from 1 to 5. With each line you input, you can also set the number of rings for each device.

Step 5. Select the number of rings from the **Number of Rings** dropdown menu and then select **Check Answer Confirmation** for each number if you want the called party to press 1 on the keypad to receive the call.

Step 6. To have a number ring the primary line first, check **Ring Webex Calling Primary Line first.** Then input the number of rings.

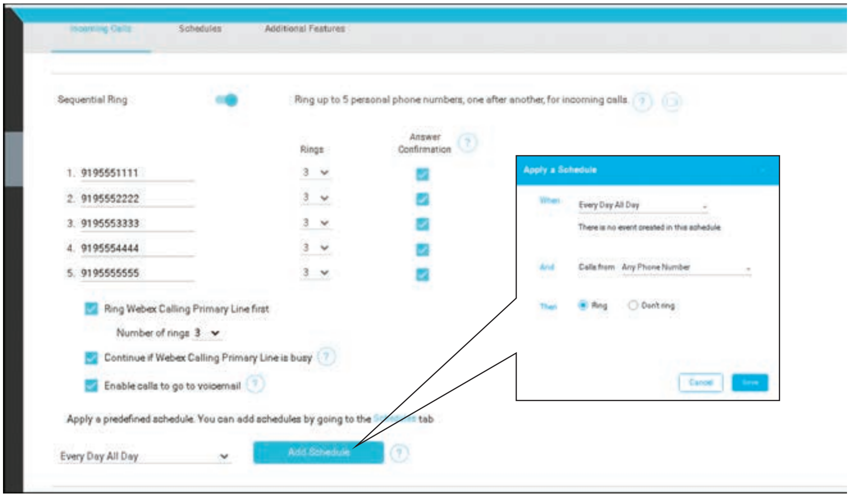
Step 7. To allow callers to go to voicemail, check **Enable calls to go to voicemail**.

Step 8. Select a predefined schedule from the drop-down menu. If you do not see a schedule you would like to use for this setting, you can add a schedule on the **Schedules** tab.

Step 9. Click **Add Schedule** to set the following parameters:

- **When**: Select your predefined schedule from the drop-down menu.
- **And**: Select if you would like to accept calls from any phone number or select phone numbers. If you choose **Select Phone Numbers**, enter the additional details.
- **Then**: Choose **Ring** or **Don't ring** for the calls that fit within these parameters.

Step 10. Click **Save** to save your sequential ringing parameters. Your schedule is added to a **Ring** or **Don't ring** table. You can edit or delete schedules from the tables, as needed. Figure 25-13 illustrates how to configure Sequential Ring.



Sequential Ring ● Ring up to 5 personal phone numbers, one after another, for incoming calls.

	Rings	Answer Confirmation
1. 9195551111	3	☑
2. 9195552222	3	☑
3. 9195553333	3	☑
4. 9195554444	3	☑
5. 9195555555	3	☑

☑ Ring Webex Calling Primary Line first

Number of rings 3

☑ Continue if Webex Calling Primary Line is busy

☑ Enable calls to go to voicemail

Apply a predefined schedule. You can add schedules by going to the Schedules tab

Every Day All Day

Apply a Schedule

When: Every Day All Day

There is no event created in this schedule

And: Calls from Any Phone Number

Then: ● Ring ○ Don't ring

Figure 25-13 *Configure Sequential Ringing*

Simultaneous Ringing

Simultaneous Ringing is a feature that rings your office phone and other phones, of your choice, at the same time. You can also set up schedules to ring these phones during certain times of the day and/or days of the week. Use the following steps to configure Simultaneous Ringing:

Step 1. Go to https://settings.webex.com and select **Webex Calling.**

Step 2. From the calling user portal, go to **Call Settings.**

Step 3. Toggle on **Simultaneous Ringing.**

Step 4. Enter a list of 10 phone numbers to ring simultaneously when your phone receives an incoming call.

Step 5. If you don't want these phone numbers to ring when you are on a call, check the box next to **Do not ring when on a call.**

Step 6. Check the box next to **Answer Confirmation** to prompt the call recipient to press a key before being connected. Use this setting when you want the call recipient to know that the incoming call didn't reach them directly.

Step 7. If you would like to set up when these phone numbers ring, toggle on **Apply Schedules.**

Step 8. Select a predefined schedule from the drop-down menu. If you do not see a schedule you would like to use for this setting, you can add a schedule on the **Schedules** tab.

Step 9. Click **Add Schedule** to set the following parameters:

- **When:** Select your predefined schedule from the drop-down menu.
- **And:** Select if you would like to accept calls from any phone number or select phone numbers. If you choose **Select Phone Numbers**, enter the additional details.
- **Then:** Choose **Ring** or **Don't ring** for the calls that fit within these parameters.

Step 10. Click **Save** to save your sequential ringing parameters. Your schedule is added to a **Ring** or **Don't ring** table. You can edit or delete schedules from the tables, as needed. Figure 25-14 illustrates how to configure Simultaneous Ringing.

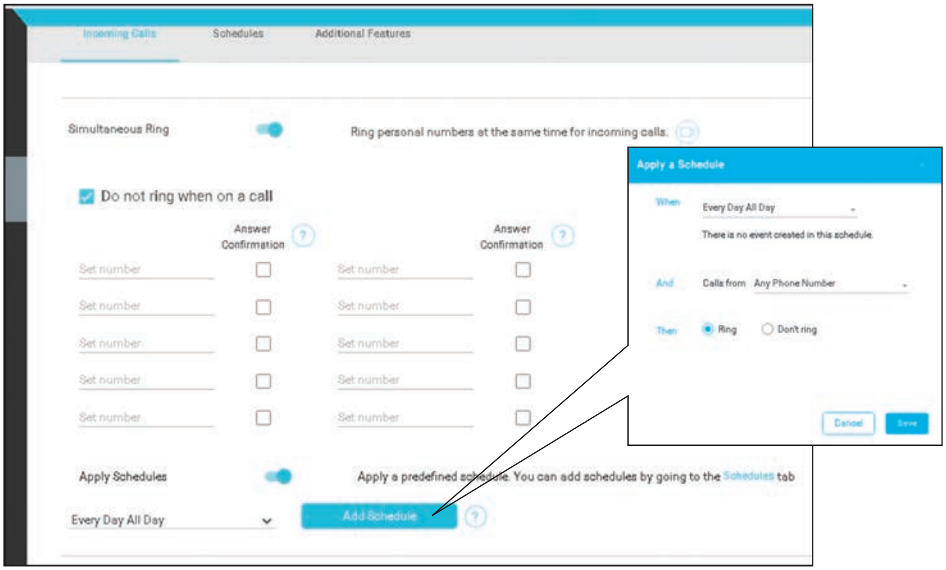


Figure 25-14 *Configure Simultaneous Ringing*

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 25-2 lists a reference of these key topics and the page numbers on which each is found.

Table 25-2 Key Topics for Chapter 25

Key Topic Element	Description	Page Number
Steps	Configure Auto Attendant	603
Steps	Bulk-Manage Auto Attendants	605
Steps	Call Park Direct	605
Steps	Call Park Group	606
List	Group Call Management Features	609
Steps	Create and Manage Call Queues	609
List	Call Pickup Criteria	613
Steps	Configure Call Pickup	613

Key Topic Element	Description	Page Number
Steps	Configure Hunt Group	614
Steps	Configure Paging Group	617
List	Cisco DECT devices	618
List	Receptionist feature display pane functions	619
Steps	Configure Anonymous Call Rejection	620

Define Key Terms

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

Auto Attendant, Call Park Direct, Call Park Group, FAC, Call Queue, Group Call Management, Call Pickup, Group Call Pickup, Hunt Groups, Paging Group, DECT, Receptionist Client, Virtual Extensions, Voicemail Group, Announcement Files, Anonymous Call Rejection, Call Waiting, DND, Call Forwarding, Selective Calling, Call Notify, Single Number Reach (Office Anywhere), Priority Alert, Sequential Ring, Simultaneous Ringing

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the four criteria for call pickup.
2. List the Cisco DECT devices that can register to Webex Control Hub.
3. Where should users go in the user portal to configure their own Webex Calling features?

This page intentionally left blank

CHAPTER 26

Webex Calling Using a Local Gateway

This chapter covers the following topics:

Webex Control Hub Settings: This topic will guide you through the steps required to initiate Webex Calling from the Webex Control Hub. These steps will include configuring Locations, Numbers, Call Routing, and Gateway settings.

Router Configuration Settings: This topic will guide you through the steps required to configure a Cisco router as a Local Gateway and Cisco Unified Border Element (Cisco UBE). These steps will include how to configure security settings on the router critical to Webex Calling, firewall and NAT traversal requirements, and configuration settings for inbound and outbound calling between Cisco UBE and Local Gateway when a Cisco Unified Communications Manager is in use.

Webex Calling is an ever-evolving solution. Over the years it has gone by different names, it has supported different capabilities, and it continuously grows to encompass all the calling needs of an organization. Webex Calling supports three basic deployments. Customers who choose to subscribe to Cisco PSTN or Cloud Connected PSTN (CCP) will find the deployment steps to be quite easy to follow. These deployment methods are more than suitable for small- to medium-sized businesses. For larger organizations there is a third option for deploying Webex Calling through a premises-based public switched telephone network (PSTN) carrier. This deployment method is much more complex and therefore requires a much deeper explanation.

In this chapter, you will learn how to deploy a premises-based Webex Calling solution using a Cisco IOS-XE router running Cisco Unified Border Element (Cisco UBE) and Local Gateway services. Topics discussed during this lesson include the following:

- Webex Control Hub Settings
  - Locations
  - Numbers
  - Call Routing
  - Gateway Settings
- Router Configuration Settings
  - Security Settings
  - Firewall and NAT Traversal

- Inbound Call Settings
- Outbound Call Settings

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.0 (CLCOR 350-801) exam:

- 4.5 Describe Webex Calling dial plan features
  - 4.5.a Locations and numbers
  - 4.5.b Outgoing and incoming permissions

"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 26-1 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 26-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Webex Control Hub Settings	1–5
Router Configuration Settings	6–10

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 the 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. When an engineer begins configuring Webex Calling in the Webex Control Hub, which of the following settings must be configured first?
   - a. Numbers
   - b. Locations
   - c. Call Routing
   - d. Gateway Settings
2. Which of the following is a prerequisite to ordering Cisco PSTN?
   - a. There are no prerequisites to ordering Cisco PSTN. Any company can use it.
   - b. Cisco PSTN can only be ordered by companies with fewer than 300 numbers.
   - c. Cisco PSTN is only available to companies that already have a PSTN carrier and want to switch.
   - d. Your location is in a country where Cisco PSTN is supported.

3. An engineer changed the language preference on a Webex Calling location after it had already been created. One user contacted the engineer saying the change did not take effect on their device. What would create this issue?
   - a. Language changes after a location is created will only apply to new users and devices.
   - b. The engineer didn't change the language correctly.
   - c. The engineer didn't apply the settings after making the change.
   - d. Language settings cannot be changed after the location has been created.
4. A customer who already has a Webex Calling solution deployed using CCP wants to change their carrier. Which of the following is a viable option for this customer?
   - a. They can choose any carrier they want when they set up a premises-based PSTN.
   - b. They can choose another CCP provider or Cisco PSTN.
   - c. They can only choose Cisco PSTN.
   - d. Once they choose a CCP provider, they cannot change to another.
5. Which of the following statements is true when setting up trunks and local gateways for Webex Calling?
   - a. Each location can use multiple trunks, but other locations cannot use the same trunk.
   - b. Each location can only use one trunk, and no other location can use that trunk.
   - c. Each location can only use one trunk, but multiple locations can use the same trunk.
   - d. Each location can use multiple trunks, and multiple locations can use the same trunks.
6. Where in the Cisco IOS-XE router would an engineer provision the SIP digest credentials on the Local Gateway using the information generated from the Webex Control Hub?
   - a. **voice class tenant 100** and **voice class sip-profiles 100**
   - b. **voice class tenant 200** and **voice class sip-profiles 200**
   - c. **voice class tenant 300** and **voice class sip-profiles 300**
   - d. **voice class tenant 200** and **voice class uri 200 sip**
7. Which NAT and firewall traversal protocol is used by the Local Gateway to establish a two-way connection with the Webex Control Hub?
   - a. STUN
   - b. TURN
   - c. ICE
   - d. Assent
   - e. H.460.18/19
8. Which of the following protocols is used by the Local Gateway to connect with the Webex Control Hub?
   - a. SIP TCP
   - b. SIP UDP

- **c.** SIP TLS
- **d.** Basic secure TCP connection

9. Which of the following statements is true when setting up the firewall and NAT traversal for Webex Calling?

- **a.** The firewall needs to allow inbound traffic to specific IP addresses/ports.
- **b.** The firewall needs to allow inbound and outbound traffic to specific IP addresses/ports.
- **c.** The firewall needs to allow inbound and outbound traffic to all ports.
- **d.** The firewall needs to allow outbound traffic to specific IP addresses/ports.

10. An engineer is setting up a router for Webex Calling. The customer will be using Cisco UBE and a Cisco Unified Communications Manager for call routing. Which of the following practices should the engineer use to ensure proper routing of calls?

- **a.** Inbound and outbound calls through the Cisco Unified Communications Manager should use one trunk and routing port.
- **b.** Inbound and outbound calls through the Cisco Unified Communications Manager should use two trunks and routing ports to distinguish between PSTN and Webex destinations.
- **c.** Inbound and outbound calls through the Cisco Unified Communications Manager should use four trunks and routing ports to distinguish calls to and from the PSTN from calls to and from Webex destinations.
- **d.** Inbound and outbound calls through the Cisco Unified Communications Manager should use one trunk and two routing ports to distinguish between PSTN and Webex destinations.

Foundation Topics

Webex Control Hub Settings

When a customer deploys the Webex Calling solution using their own PSTN provider, two sides to the solution need to be configured. The Webex Control Hub must be configured first because there are some settings that must be retrieved from this configuration that are used for the second part of this solution. The second part of the solution involves configuring the Cisco IOS-XE router. The order settings that must be configured for Webex Calling are Locations, Numbers, Call Routing, Local Gateway (on the Cisco IOS-XE router), and then Gateway (on Webex Control Hub). Let's begin by examining how to configure the Webex Control Hub for Webex Calling.

Locations

Locations are settings configured in the Webex Control Hub for Webex Calling that allow you to group together any users and devices using the calling feature that have the same dialing behaviors based on their location. This can be configured based on any location that will have a Local Gateway assigned to it. For example, if you have a headquarters office in Los Angeles, California and a regional office in San Diego, California, you could create a single location called California and use it for calling out of either office. However, if you have an office in Los Angeles, California and an office in New York, New York, and another office in London, England, you might want to create two or three locations. In this scenario, Los Angeles and New York could share a location called USA Location, while London uses another location called UK Location. Alternatively, all three offices could use their own dedicated location named after their respective cities.

Key Topic

Locations used to be configured under the **Services > Calling** menu. However, since locations impact so many other aspects of the Webex environment, Cisco moved **Locations** to the **Management** menus to better serve the whole Webex environment. To configure locations in the Webex Control Hub, use the following steps:

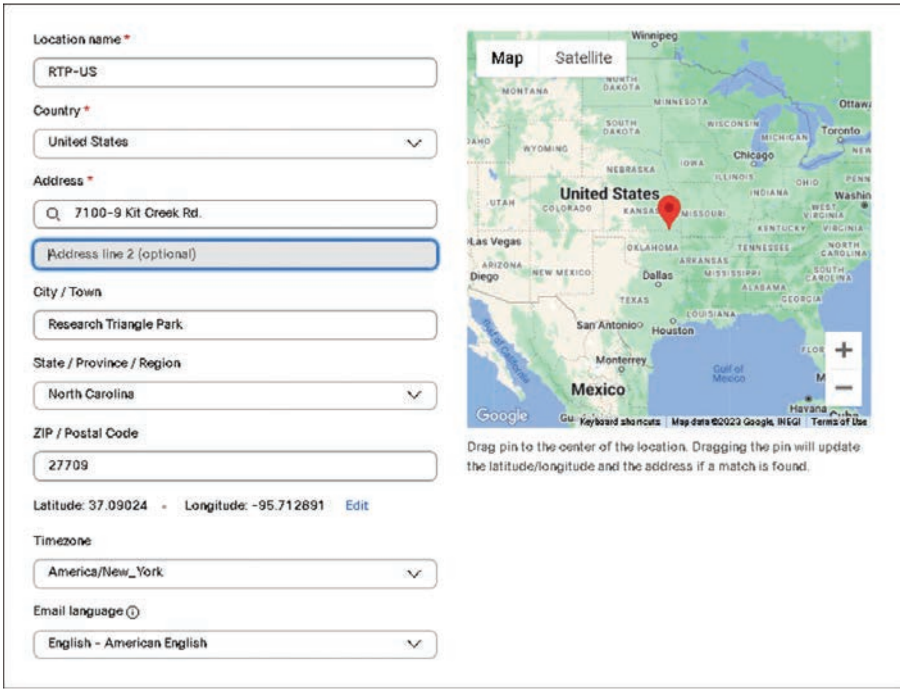
Step 1. Log in to Control Hub (https://admin.webex.com) and go to **Management > Locations.**

Step 2. Click the **Manage location** drop-down in the top-right corner of the screen and select **Create Manually.**

Step 3. Enter the following information and then click **Create:**

- **Location Name:** Enter a unique name to identify the location.
- **Country:** Choose a country to tie the location to. For example, you can create one location (headquarters) in the United States and another (branch) in the United Kingdom. The country you choose determines the address fields that follow. The ones documented here use the U.S. address convention as an example.
- **Location Address:** Enter the location's main mailing address.
- **City/Town:** Enter a city for this location.
- **State/Province/Region:** From the drop-down, choose a state.
- **ZIP/Postal Code:** Enter the ZIP or postal code.
- **Announcement Language:** Choose the language for audio announcements and prompts for new users and features.
- **Email Language:** Choose the language for the email communication with new users.
- **Time Zone:** Choose the time zone for the location.
- **Email Language:** Choose the language you would like to use for automated email communications.

Step 4. On the next page, you will be presented with options to set up PSTN connectivity for this location, assign workspaces to this location, add floors to better track workspaces and devices, or assign users to locations. All this can be performed at a later time, as well. Click **Close.** Figure 26-1 illustrates how to configure locations in Webex Control Hub.



Location name *

RTP-US

Country *

United States

Address *

7100-9 Kit Creek Rd.

Address line 2 (optional)

City / Town

Research Triangle Park

State / Province / Region

North Carolina

ZIP / Postal Code

27709

Latitude: 37.09024 · Longitude: -95.712891 Edit

Timezone

America/New_York

Email language

English - American English

Drag pin to the center of the location. Dragging the pin will update the latitude/longitude and the address if a match is found.

Figure 26-1 *Configure Locations in Webex Control Hub*

Locations can be deleted or updated. Before deleting a location, get a list of the users and workspaces associated with that location. Go to **Services > Calling > Numbers** and from the drop-down menu, select the location to be deleted. You must delete those users and workspaces before you delete the location. Keep in mind that any numbers associated with this location will be released back to your PSTN provider; you'll no longer own those numbers.

Updating an existing location allows you to change your PSTN setup, the name, time zone, and language of a location after it's created. Keep in mind, though, that the new language applies only to new users and devices. Existing users and devices continue to use the old language.

Numbers

Numbers are simply the phone numbers used to contact your organization. They can be assigned to a main number for the company where the caller can access an extension from a directory, or they can be assigned to each user. There are two ways to configure numbers in the Webex Control Hub. Because you have to set up locations before numbers, you can use the **Locations** menu to continue setting up numbers. Alternatively, you can go to **Services > Calling > Numbers** and add numbers from this page. The following instructions will describe how you can configure numbers from the **Locations** menu:

Key Topic

Step 1. From the **Locations** menu, select the location you want to configure numbers for and then click the **Calling** tab.

Step 2. In the **Calling connection** section, click **Manage**.

Step 3. Click the **Set up calling** button in the middle of the page, choose one of the following options, and then click **Next:**

- **Cisco PSTN:** Choose this option if you'd like a Cloud PSTN solution from Cisco. The Cisco Calling Plan is a full PSTN replacement solution that provides emergency calling as well as inbound and outbound domestic and international calling, and it allows you to order new PSTN numbers or port existing numbers to Cisco. The Cisco PSTN option is only visible under the following conditions:

- You have purchased at least one committed Cisco Calling Plan OCP (Outbound Calling Plan).

- Your location is in a country where the Cisco Calling Plan is supported.

- Your location is new. Pre-existing locations that have had other PSTN capabilities assigned aren't eligible for the Cisco Calling Plan at this time. Open a support case for guidance. You are hosted in a Webex Calling data center in a region in which the Cisco Calling Plan is supported.

- **Cloud Connected PSTN:** Choose this option if you're looking for a cloud PSTN solution from one of the many Cisco CCP partners or if the Cisco Calling Plan isn't available in your location. CCP partners offer PSTN replacement solutions, extensive global coverage, and a broad and varied range of features, packaging, and pricing.

- Only partners that support your location's country are displayed. Partners are listed either with a logo or as a brief string of text followed by a region, in parentheses. Examples are (EU), (US), and (CA). Partners listed with a logo always offer Regional Media for CCP. For partners displaying as a string, choose the region closest to the country of your location to ensure Regional Media for CCP. If you see the option **Order numbers now** under a listed provider, we recommend that you choose that option so that you can benefit from integrated CCP. Integrated CCP enables the procuring and provisioning of phone numbers in Control Hub on a single pane of glass. Non-integrated CCP requires you to procure your phone numbers from the CCP partner outside of Control Hub.

- **Premises-based PSTN (formerly Local Gateway):** You can choose this option if you want to keep your current PSTN provider or want to connect non-cloud sites with cloud sites. For the purpose of this chapter, this is the option we will be observing.

The choice of PSTN option is at each location level (each location has only one PSTN option). You can mix and match as many options as you'd like for your deployment, but each location will have one option. Once you've selected and provisioned a PSTN option, you can change it by clicking **Manage** in the location PSTN properties. Some options, such as Cisco PSTN, however, might not be available after another option has been assigned.

Step 4. On the **Connection Type** screen, use the drop-down menu to select **None**. Even though None is already shown, you will still need to select it from the drop-down menu before you can continue. This screen is the routing choice, or trunk, for these numbers. You have not created a trunk yet, which is why you need to select None at this time.

Step 5. Check the box beside the confirm statement and click **Next**.

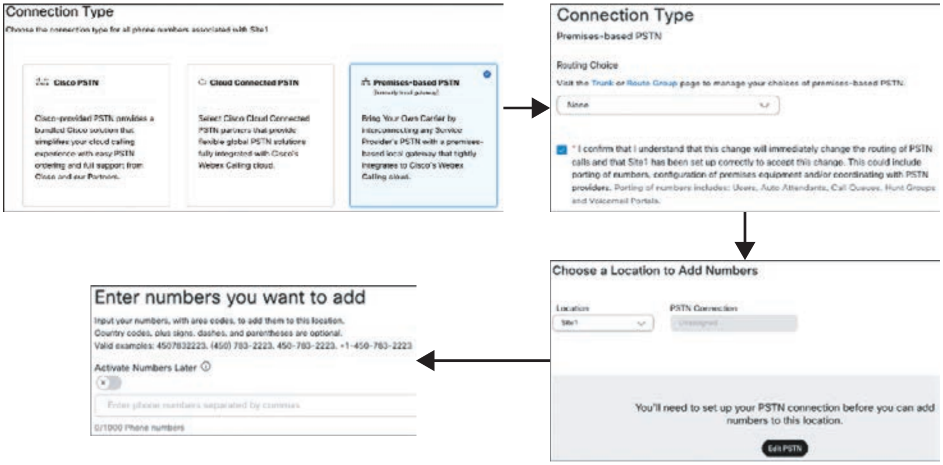
Step 6. On the next screen you'll be presented with the option to add the numbers now or later. Click the **Add Numbers Now** button.

Step 7. The next screen will show the **Location** and **PSTN Connection** type you chose before. Click **Next**.

Step 8. Enter phone numbers as comma-separated values and then click **Save**.

Step 9. On the confirmation screen, verify the numbers are correct and click **Close**.

Numbers are added for the specific location. Valid entries move to the **Validated Numbers** field, and invalid entries remain in the **Add Numbers** field, accompanied by an error message. Depending on the location's country, the numbers are formatted according to local dialing requirements. For example, if a country code is required, you can enter numbers with or without the code, and the code is prepended. After you create a location, you can enable emergency 911 services for that location. Figure 26-2 illustrates how to configure Numbers in Webex Control Hub.



Connection Type

Choose the connection type for all phone numbers associated with Site1

Cisco PSTN

Cisco-provided PSTN provides a bundled Cisco solution that simplifies your cloud calling experience with easy PSTN ordering and full support from Cisco and our Partners.

Cloud Connected PSTN

Select Cisco Cloud Connected PSTN partners that provide flexible global PSTN solutions fully integrated with Cisco's Webex Calling cloud.

Premises-based PSTN

(formerly local gateway)

Bring Your Own Carrier by interconnecting any Service Provider's PSTN with a premises-based local gateway that tightly integrates to Cisco's Webex Calling cloud.

Connection Type

Premises-based PSTN

Routing Choice

Visit the Trunk or Route Group page to manage your choices of premises-based PSTN.

None

☑ * I confirm that I understand that this change will immediately change the routing of PSTN calls and that Site1 has been set up correctly to accept this change. This could include porting of numbers, configuration of premises equipment and/or coordinating with PSTN providers. Porting of numbers includes: Users, Auto Attendants, Call Queues, Hunt Groups and Voicemail Portals.

Choose a Location to Add Numbers

Location: Site1

PSTN Connection: Unassigned

You'll need to set up your PSTN connection before you can add numbers to this location.

Edit PSTN

Enter numbers you want to add

Input your numbers, with area codes, to add them to this location.
Country codes, plus signs, dashes, and parentheses are optional.
Valid examples: 4507832223, (450) 783-2223, 450-783-2223, +1-450-783-2223

Activate Numbers Later ⓘ

Enter phone numbers separated by commas

0/1000 Phone numbers

Figure 26-2 *Configure Numbers in Webex Control Hub*

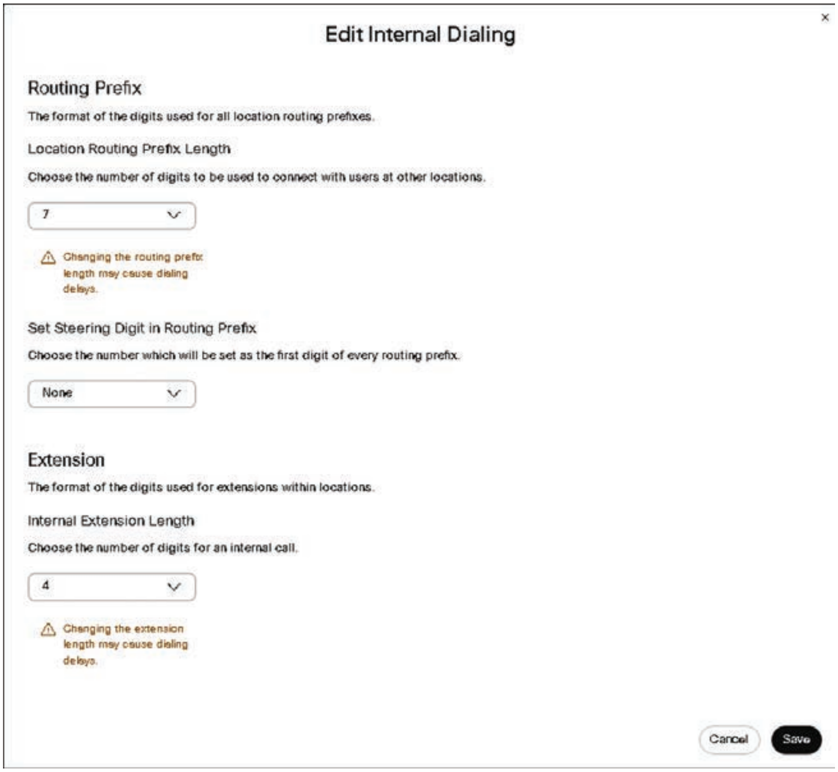
Loosely related to numbers, there are some settings used for internal dialing. As you change your dial plan, the sample numbers in Control Hub update to show these changes. The following steps will allow you to configure outgoing calling permissions for a location:

Key Topic

Step 1. From the Webex Control Hub, go to **Services > Calling > Service Settings** and then scroll to **Internal Dialing**.

Step 2. Configure the following optional dialing preferences, as needed:

- **Location Routing Prefix Length:** Cisco recommends this setting if you have multiple locations. You can enter a length of 2–7 digits. If you have multiple locations with the same extension, users must dial a prefix when calling between locations. For example, if you have multiple stores, all with the extension 1000, you can configure a routing prefix for each store. If one store has a prefix of 888, you'd dial 8881000 to reach that store. If a company had multiple international locations, then the country code could be used as the prefix for IP routing as well.
- **Steering Digit in Routing Prefix:** You can set a value here regardless of whether you use location routing prefixes. A steering digit will be the first digit of every routing prefix.
- **Internal Extension Length:** You can enter 2–6 digits. If you increase your extension length, existing speed dials to internal extensions are not automatically updated. Figure 26-3 illustrates how to configure internal dialing in Webex Control Hub.



Edit Internal Dialing

Routing Prefix

The format of the digits used for all location routing prefixes.

Location Routing Prefix Length

Choose the number of digits to be used to connect with users at other locations.

7

Changing the routing prefix length may cause dialing delays.

Set Steering Digit in Routing Prefix

Choose the number which will be set as the first digit of every routing prefix.

None

Extension

The format of the digits used for extensions within locations.

Internal Extension Length

Choose the number of digits for an internal call.

4

Changing the extension length may cause dialing delays.

Figure 26-3 *Configure Internal Dialing in Webex Control Hub*

Step 3. To specify internal dialing for specific locations, go to **Management > Locations**, select a location, and click the **Calling** tab.

Step 4. In the **Dialing** section, you can choose one of the following options and change the dialing behavior as needed. Click **Save** when finished:

- **Internal Dialing**: Under **Routing Prefix**, select the routing prefix users at other locations need to dial in order to contact someone at this location. The routing prefix of each location must be unique. We recommend that the prefix length match the length set at the organization level, but it must be 2–7 digits long. **Calls to On-Premises Extensions** can also be set to route unknown extensions to the premises as internal calls. This setting might be needed when a Cisco Unified Communications Manager is being used.

- **External Dialing**: Optionally, you can choose an outbound dial digit that users must dial to reach an outside line. The default is None, and you can leave it if you don't require this dialing habit. If you do decide to use this feature, we recommend that you use a different number from your organization's steering digit. Users can include the outbound dial digit when making external calls to mimic how they dialed on legacy systems. However, all users can still make external calls without the outbound dial digit.

When these changes are implemented in a production environment, there is an impact to existing users. Users must restart their phones for changes in dialing preferences to take effect. Also, user extensions should not start with the same number as the location's steering digit.

Call Routing

Key Topic

When you are trying to set up Webex Calling using premises-based PSTN, you need to register a Local Gateway to the Webex Cloud. The first step in configuring a Local Gateway is to create a trunk where the Local Gateway will register. Each location you create in the Webex Control Hub can support only one trunk, but you can build a Local Gateway configuration using Cisco UBE High Availability for a more redundant solution. Also, you can set up multiple locations using the same trunk, or you can configure multiple locations, each using their own trunk.

Locations must exist before you can add a premises-based PSTN. Therefore, prior to creating the trunk, be sure to create any locations and specific settings and numbers that will be used with the trunk, as instructed earlier in this chapter. Be sure you understand the premises-based PSTN (Local Gateway) requirements for Webex Calling. This can be a complex service to set up. Once you are ready to create your trunk, you can do so in three steps:

Key Topic

Step 1. From the Webex Control Hub, go to **Services > Calling > Call Routing** and select **Add Trunk**.

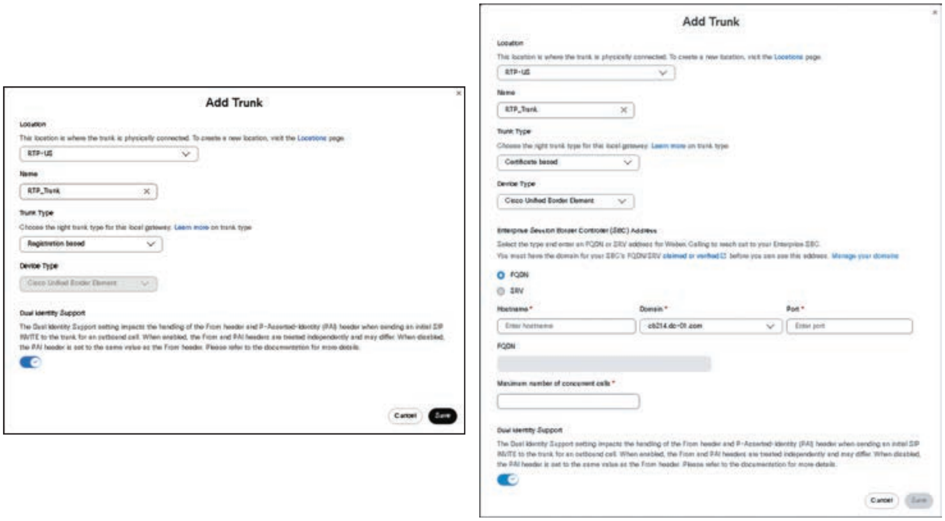
Step 2. Populate the fields that appear in the new window that opens:

- **Location**: Choose a location you created previously.

- **Name**: Enter a name for the trunk. The name can't be longer than 24 characters.

- **Trunk Type:** Choose a trunk type from the drop-down list. The choices are **Registration based** (default) and **Certificate based.** The differences between these choices were described in Chapter 24, “Webex Calling Options.”
- **Device Type:** This field is grayed out if you choose **Registration based** from the previous drop-down option. If you choose **Certificate based**, you’ll need to configure the following options:
- **Select Device:** Choose between Cisco Unified Border Element, Oracle Session Border Controller, AudioCodes Session Border Controller, and Ribbon Session Border Controller.
- **Enterprise Session Border Controller (SBC) Address:** Select **FQDN** or **SRV** and then enter an address for Webex Calling to reach out to your Enterprise SBC. The domain for your SBC’s FQDN/SRV must be claimed or verified before you can use this address.
- **Maximum number of concurrent calls:** Enter the maximum number of concurrent calls you want to support within the locations associated with this trunk.
- **Dual Identity Support:** The Dual Identity Support setting impacts the handling of the From header and P-Asserted-Identity (PAI) header when an initial SIP INVITE is sent to the trunk for an outbound call. When enabled, the From and PAI headers are treated independently and may differ. When disabled, the PAI header is set to the same value as the From header. The default is toggled on.

Step 3. Click **Save.** Figure 26-4 illustrates how to initially configure call routing in Webex Control Hub.



Add Trunk

Location

This location is where the trunk is physically connected. To create a new location, visit the Locations page

RTP-US

Name

RTP_Trunk

Trunk Type

Choose the right trunk type for this local gateway. Learn more on trunk type

Registration based

Device Type

Cisco Unified Border Element

Dual Identity Support

The Dual Identity Support setting impacts the handling of the From header and P-Asserted-Identity (PAI) header when sending an initial SIP INVITE to the trunk for an outbound call. When enabled, the From and PAI headers are treated independently and may differ. When disabled, the PAI header is set to the same value as the From header. Please refer to the documentation for more details.

Add Trunk

Location

This location is where the trunk is physically connected. To create a new location, visit the Locations page

RTP-US

Name

RTP_Trunk

Trunk Type

Choose the right trunk type for this local gateway. Learn more on trunk type

Certificate based

Device Type

Cisco Unified Border Element

Enterprise Session Border Controller (SBC) Address

Select the type and enter an FQDN or SRV address for Webex Calling to reach out to your Enterprise SBC.
You must have the domain for your SBC's FQDN/SRV claimed or verified before you can use this address. Manage your domains

● FQDN
○ SRV

Hostname * Enter hostname

Domain * cb214.dc-01.com

Port * Enter port

FQDN

Maximum number of concurrent calls *

Dual Identity Support

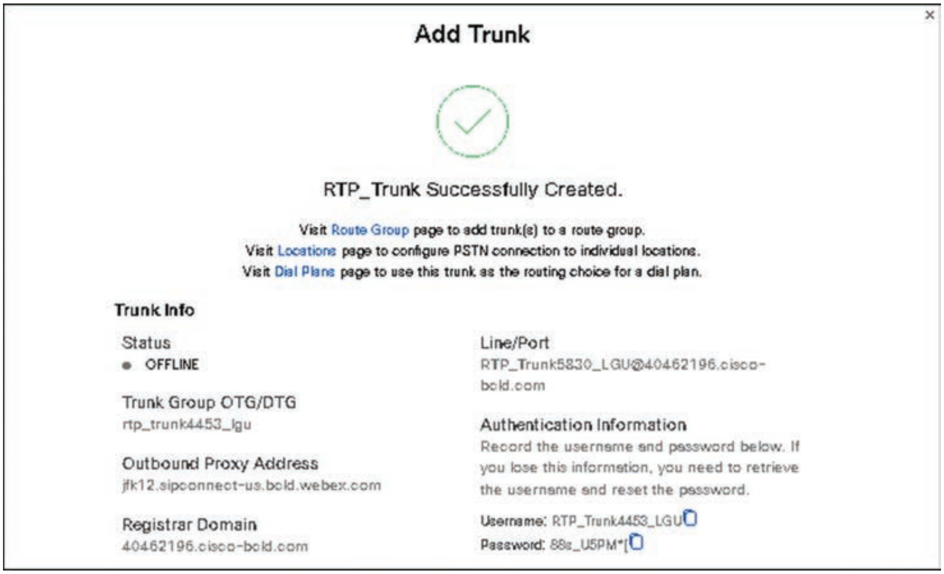
The Dual Identity Support setting impacts the handling of the From header and P-Asserted-Identity (PAI) header when sending an initial SIP INVITE to the trunk for an outbound call. When enabled, the From and PAI headers are treated independently and may differ. When disabled, the PAI header is set to the same value as the From header. Please refer to the documentation for more details.

Figure 26-4 *Configure Call Routing in Webex Control Hub*

After you save the trunk settings, you're presented with the relevant parameters you'll need to configure on the router for the local gateway. You'll also generate a set of SIP digest credentials to secure the PSTN connection. Trunk information appears on the screen as follows:

- Register Domain
- Trunk Group OTG/DTG
- Line/Port
- Outbound Proxy Address

Cisco recommends that you copy this information from Control Hub and paste it into a local text file or document so you can refer to it when you're ready to configure the premises-based PSTN. If you lose the credentials, you must generate them from the trunk information screen in Control Hub. Click **Retrieve Username and Reset Password** to generate a new set of authentication credentials to use on the trunk. Note that if you generate a new password after the trunk has been set up, it will break the connection between the local gateway and the Webex Control Hub. Figure 26-5 illustrates the trunk information generated from Webex Control Hub that will be used to configure the Local Gateway on the Cisco Router.



RTP_Trunk Successfully Created.

Visit Route Group page to add trunk(s) to a route group.
Visit Locations page to configure PSTN connection to individual locations.
Visit Dial Plans page to use this trunk as the routing choice for a dial plan.

Trunk Info

Status
● OFFLINE

Trunk Group OTG/DTG
rtp_trunk4453_lgu

Outbound Proxy Address
jfk12.sipconnect-us.bcld.webex.com

Registrar Domain
40462196.cisco-bcld.com

Line/Port
RTP_Trunk5830_LGU@40462196.cisco-bcld.com

Authentication Information
Record the username and password below. If you lose this information, you need to retrieve the username and reset the password.

Username: RTP_Trunk4453_LGU
Password: 88s_U5PM*[

Figure 26-5 *Trunk Information for Local Gateway Configuration*

Gateway Settings

The next step would be to log in to the router and configure the Cisco UBE and Local Gateway settings. These settings will be covered in the next section. Because we are already talking about what needs to be configured in the Webex Control Hub, this section makes the assumption that all the router configurations have been completed. You need to give the connection about 2–3 minutes to become active before returning to the Webex Control Hub. To finish the configuration, you need to perform a few more steps to associate the Local

Gateway with the location. First, you need to change the connection type from **None**, which you set when configuring numbers, to the trunk you created on the Local Gateway.

Key Topic

Step 1. From the Webex Control Hub, go to **Management > Locations** and select the location you want to change for the trunk.

Step 2. Click the **Calling** tab. In the **Calling connection** section, click **Manage**.

Step 3. On the **Connection Type** page, use the drop-down menu under **Routing Choice** to choose the newly added trunk.

Step 4. Check the box to confirm the effects of the change and then click **Next**. On the next page, click **Done (add numbers later)**.

Now you can check on the status of the trunk. If you still get an **Offline** status, you may not have waited long enough after configuring the Local Gateway on the router. Wait a few more minutes and refresh your screen to check the status again. Use the subsequent steps to check the status.

Step 5. From the Webex Control Hub, go to **Services > Calling > Call Routing**. Alternatively, you can click **Premise-based PSTN** on the **Location > Calling** page and then click the trunk name below to go to **Call Routing**.

Step 6. Select the trunk from the list you want to configure. On the fly-out window beside **Trunk info**, click **Manage**. You should be able to see the **Status** of the trunk from this page. Figure 26-6 illustrates how to verify the Local Gateway is active and Webex Calling setup is complete.

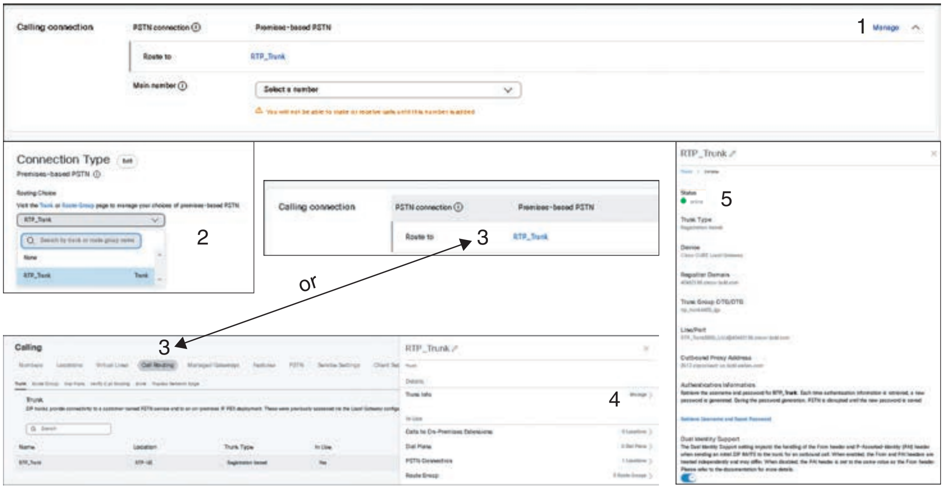
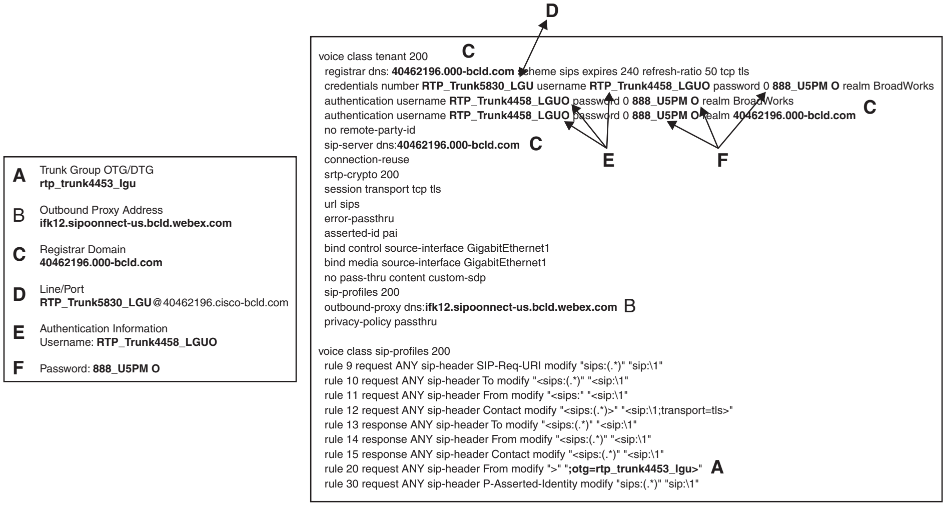


Figure 26-6 *Verify the Local Gateway Is Active in Webex Control Hub*

Router Configuration

When adding a Local Gateway, you must follow some essential steps to set up the security and authentication properly. First, partners need to define the Local Gateway for a customer site generating connection parameters. This part of the process is performed from the Webex

Control Hub as described in the previous section. Key information is generated, which in turn is used to configure the Local Gateway, allowing the Local Gateway to communicate with Webex in the cloud. As mentioned before, retain this information to be used on the Local Gateway. Figure 26-7 illustrates where trunk information generated in Webex Control Hub should be used in the router configurations for Local Gateway.



A Trunk Group OTG/DTG
rtp_trunk4453_lgu

B Outbound Proxy Address
ifk12.sipoonnect-us.bcld.webex.com

C Registrar Domain
40462196.000-bcld.com

D Line/Port
RTP_Trunk5830_LGU@40462196.cisco-bcld.com

E Authentication Information
Username: **RTP_Trunk4458_LGUO**

F Password: **888_U5PM O**

```
voice class tenant 200
  registrar dns: 40462196.000-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls
  credentials number RTP_Trunk5830_LGU username RTP_Trunk4458_LGUO password 0 888_U5PM O realm BroadWorks
  authentication username RTP_Trunk4458_LGUO password 0 888_U5PM O realm BroadWorks
  authentication username RTP_Trunk4458_LGUO password 0 888_U5PM O realm 40462196.000-bcld.com
  no remote-party-id
  sip-server dns:40462196.000-bcld.com
  connection-reuse
  srtp-crypto 200
  session transport tcp tls
  url sips
  error-passthru
  asserted-id pai
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  no pass-thru content custom-sdp
  sip-profiles 200
  outbound-proxy dns:ifk12.sipoonnect-us.bcld.webex.com
  privacy-policy passthru

voice class sip-profiles 200
  rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
  rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
  rule 11 request ANY sip-header From modify "<sips:" "<sip:\1"
  rule 12 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"
  rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
  rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
  rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
  rule 20 request ANY sip-header From modify ">" ";otg=rtp_trunk4453_lgu>"
  rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"
```

Figure 26-7 *Trunk Info Used in Router for Local Gateway*

Security Settings

The Local Gateway needs to register over SIP TLS using connection parameters from the Webex Control Hub. This part of the process requires an administrator to configure the Local Gateway so that it can register to the Webex Control Hub and communicate with Webex in the cloud.

Step 1. You need to create a trust point using TLS version 1.2. Download a signed CA root bundle to that trust point in the router by entering the **crypto pki trustpool import clean url** command.

Step 2. You'll need to provision the SIP digest credentials generated from the Webex Control Hub and configured on the Local Gateway using **voice class tenant 200** and **voice class sip-profiles 200**, as demonstrated in Figure 26-7.

Step 3. At this point, the Local Gateway will use a TLS connection to validate Session Border Controller (SBC) certificates using the CA root bundle.

Webex will then authenticate the Local Gateway registration, and the Local Gateway registers to the Webex Control Hub. Figure 26-8 illustrates the security handshake and registration process that happens between the Local Gateway and Webex Control Hub.

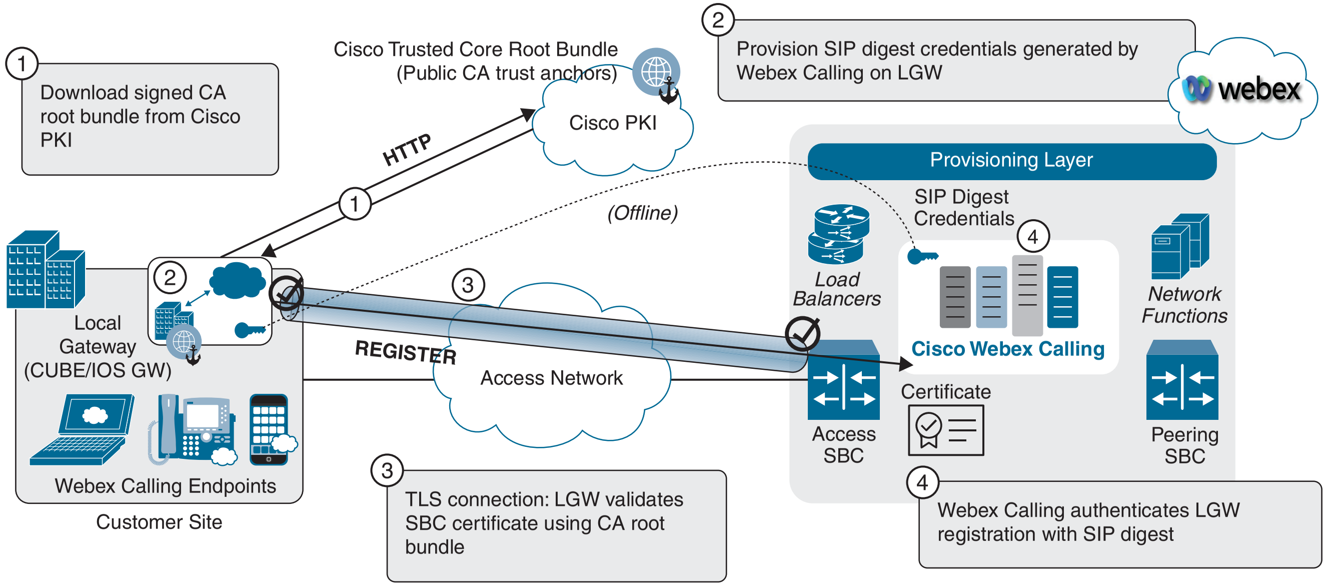

1
Download signed CA root bundle from Cisco PKI
Cisco Trusted Core Root Bundle (Public CA trust anchors)
Cisco PKI
HTTP
1
2
Provision SIP digest credentials generated by Webex Calling on LGW
webex
Provisioning Layer
SIP Digest Credentials
4
Load Balancers
Network Functions
Cisco Webex Calling
Certificate
Access SBC
Peering SBC
(Offline)
2
Local Gateway (CUBE/IOS GW)
3
REGISTER
Access Network
Webex Calling Endpoints
Customer Site
3
TLS connection: LGW validates SBC certificate using CA root bundle
4
Webex Calling authenticates LGW registration with SIP digest

Figure 26-8 *Security Handshake and Local Gateway Registration Process*

Firewall and NAT Traversal

In most cases, the Local Gateway and endpoints can sit on the *internal* customer network using private IP addresses with NAT, and media latching is in the Webex SBC.

The firewall needs to allow *outbound* traffic (SIP, RTP/UDP, HTTP) to specific IP addresses/ports. STUN is used to create pinholes for outbound traffic. Inbound traffic will use the same flow once the STUN connection is established. Table 26-2 identifies the ports, protocols, and IP addresses that will be used for firewall and NAT traversal. Figure 26-9 illustrates how the firewall and NAT traversal work for Webex Calling.

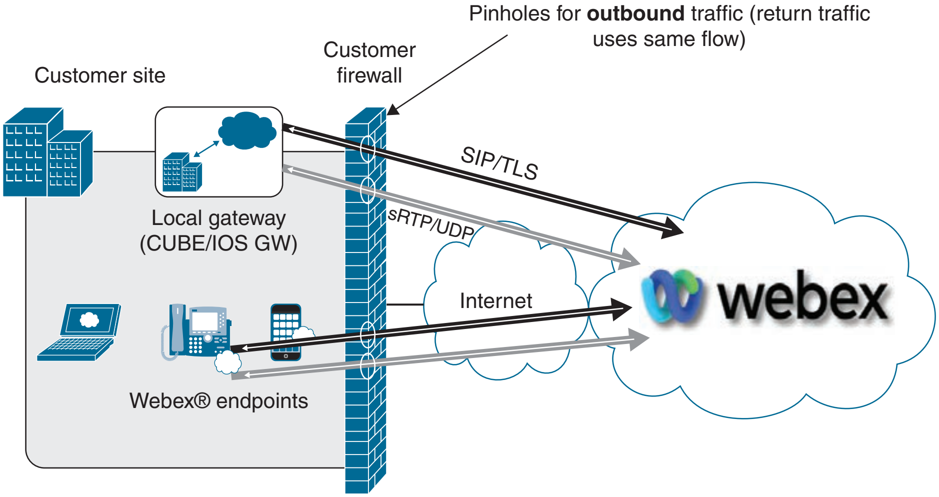

Pinholes for **outbound** traffic (return traffic uses same flow)
Customer firewall
Customer site
SIP/TLS
sRTP/UDP
Local gateway (CUBE/IOS GW)
Internet
webex
Webex® endpoints

Figure 26-9 *Firewall and NAT Traversal Process for Webex Calling*

Key Topic

Table 26-2 Firewall and NAT Traversal Port, IP Addresses, and Protocols

Purpose	Source IP	Source Ports	Protocol	Destination IP	Destination Ports
SIP Signaling	Webex Calling facing interface of Local Gateway	8000–65535	TCP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25	8934
RTP Media	Webex Calling facing interface of Local Gateway	8000–48000	UDP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25	19560–65535

Inbound Call Settings

Registering the Local Gateway to Webex Control Hub does not control when or how calls are routed. These settings must be added to the router as well. If you are not using an IP PBX, such as the Cisco Unified Communications Manager, then you only need to configure Cisco UBE settings to route calls between the ITSP and the router and between the Webex Control Hub and the Local Gateway. If you are using an IP PBX, you also need to configure settings to route calls between Cisco UBE to the Cisco Unified Communications Manager and between Cisco Unified Communications Manager and Webex Control Hub using the Local Gateway. Cisco UBE and the Local Gateway services can run on the same router, or they can run on separate routers as described in Chapter 24. The settings shown in this example assume that Cisco Unified Communications Manager is being used and that Cisco UBE is sharing the same router as the Local Gateway.

First, let's look at call routing from an ITSP to the Cisco Unified Communications Manager using Cisco UBE:

1. Incoming calls to the SBC are matched based on "via URI." Calls inbound to the Cisco Unified Communications Manager are over two trunks to distinguish between PSTN and Webex destinations. The via URI match between Cisco Unified Communications Manager and Cisco UBE is done based on port 5060.
2. The inbound dial peer will point to a dial peer group.
3. The outbound dial peers in the Dial Peer Group (DPG) then use server groups to route to Cisco Unified Communications Manager nodes. In this example, there are up to seven nodes, so they have been divided into two server groups. Example 26-1 identifies the commands needed in Cisco UBE to handle incoming calls from the PSTN.

Key Topic

Example 26-1 *Cisco UBE Commands for Incoming Call Handling from PSTN*

```
voice class uri 100 sip
 host <PSTN IP address>

dial-peer voice 100 voip
 description Inbound dialpeer from PSTN
 incoming uri via 100
 destination dpg 302

voice class dpg 302
  dial-peer 305 preference 1
  dial-peer 307 preference 1

voice class server-group 305
  ipv4 <cucm-node-1>
  ipv4 <cucm-node-5>

voice class server-group 307
 ipv4 <cucm-node-6>
 ipv4 <cucm-node-7>

dial-peer voice 305 voip
 description Outgoing dial-peer to CUCM for inbound from
 PSTN - 1st 5
 destination-pattern .T
 session server-group 305

dial-peer voice 307 voip
 description Outgoing dial-peer to CUCM for inbound from
```

```
PSTN- 2nd 5
destination-pattern .T
session server-group 307
```

The call flow through the Cisco Unified Communications Manager can work in a variety of ways, depending on how you've configured your dial plan. For this scenario, the call flow through the Cisco Unified Communications Manager will work as follows:

1. A call comes to a PSTN DID number.
2. The Cisco UBE translates that number into a four-digit extension and sends it to Cisco Unified Communications Manager.
3. The Cisco Unified Communications Manager translation pattern matches on four of those extensions and prefixes the number with an 8.
4. That translated number matches a route pattern that sends the call to the trunk preconfigured for the Local Gateway. The preconfigured trunk uses a SIP Trunk Security Profile configured for incoming port 5065.

Just as with inbound traffic from the PSTN, inbound calls to the Local Gateway are matched based on via URI. Calls inbound from Cisco Unified Communications Manager are over two trunks to distinguish between PSTN and Webex. The via URI match between Cisco Unified Communications Manager and Local Gateway is done based on port 5065.

1. The via URI uses an inbound dial peer to point to a dial peer group.
2. The outbound dial peers in the DPG then reroutes the call to Webex.
3. Webex will then find the registered phone matching the dialed alias and connect the call. Example 26-2 identifies the commands needed in the Local Gateway to handle incoming calls from Cisco Unified Communications Manager to Webex Control Hub.

Key Topic

Example 26-2 *Local Gateway Commands for Incoming Calls to Webex Control Hub*

```
voice class uri  300 sip
 pattern <cucm-nodes-ip-address and port-regex-for-dcloud>
 ex:  pattern 10\.1\.2\..*:5065 matches 10.1.2.X:5065
 range

dial-peer voice 300 voip
 description Incoming dial-peer from CUCM for dcloud
 incoming uri via 300
 destination dpg 200

voice class dpg 200
 dial-peer 201 preference 1

dial-peer voice 201 voip
 description Outgoing dial-peer to BroadCloud
 destination-pattern .T
 session-target sip-server
```

Outbound Call Settings

Outbound calls from the Local Gateway to the PSTN or to the Cisco Unified Communications Manager follow a similar order:

1. Inbound calls on the Local Gateway from Webex are matched based on "via URI." Because these calls are inbound to the Cisco Unified Communications Manager from the Local Gateway, the via URI match is done based on port 5065.
2. The via URI uses an inbound dial peer to point to a dial peer group.
3. The outbound dial peers in the DPG then use server groups to route to the Cisco Unified Communications Manager nodes. Example 26-3 identifies the commands needed in the Local Gateway to handle outgoing calls to Cisco Unified Communications Manager from Webex Control Hub.

Key Topic

Example 26-3 *Local Gateway Commands for Outgoing Calls from Webex Control Hub*

```
voice class uri 200 sip
  pattern :8934

dial-peer voice 200 voip
  description Incoming dial-peer from Webex
  incoming uri via 200
  destination dpg 300

voice class dpg 300
  dial-peer 301 preference 1
  dial-peer 303 preference 1

voice class server-group 301
  ipv4 <cucm-node-1> port 5065
  ipv4 <cucm-node-5> port 5065

voice class server-group 303
 ipv4 <cucm-node-6> port 5065
 ipv4 <cucm-node-7> port 5065

dial-peer voice 301 voip
 description Outgoing dial-peer to CUCM for inbound from
 Webex - 1st 5
 destination-pattern .T
 session server-group 301

dial-peer voice 303 voip
 description Outgoing dial-peer to CUCM for inbound from
 Webex - 2nd 5
 destination-pattern .T
 session server-group 303
```

The Cisco Unified Communications Manager then routes calls to Cisco UBE over port 5060:

1. Inbound calls to the Cisco UBE are matched based on "via URI." Since calls are inbound from Cisco Unified Communications Manager to Cisco UBE, the via URI match is done based on port 5060.
2. The inbound dial peer will point to a dial peer group.
3. The outbound dial peer in the DPG is then used to route the call out to the ITSP. Example 26-4 identifies the commands needed in the local gateway to handle incoming calls from Cisco Unified Communications Manager to Cisco UBE and out to the ITSP.

Key Topic

Example 26-4 *Cisco UBE Calls Outbound to PSTN*

```
voice class uri 302 sip
 pattern <cucm-nodes-ip-address and port-regex-for-pstn>
 ex:  pattern 10\.1\.2\..*:5060 matches 10.1.2.X:5060
 range

dial-peer voice 302 voip
 description Incoming dial-peer from CUCM for pstn
 incoming uri via 302
 destination dpg 100

voice class dpg 100
 dial-peer 101 preference 1

dial-peer voice 101 voip
 description Outgoing dial-peer to PSTN
 destination-pattern .T
 session target ipv4:<pstn ip address>
```

You can enter the command from the command line **show sip-ua registrar status** to view the status of the trunk. However, even with an active status, the trunk cannot be used until you return to Webex Control Hub and select the appropriate trunk. This is the point where you save the configurations on your router and follow the steps previously discussed in the "Gateway Settings" subsection to select the appropriate trunk and verify the status is **Active**.

You should now have learned the skills to deploy a premises-based Webex Calling solution using a Cisco IOS-XE router running Cisco UBE and Local Gateway services. You should now know how to configure Webex Control Hub settings and perform router configuration to support Webex Calling.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 26-3 lists a reference of these key topics and the page numbers on which each is found.

Table 26-3 Key Topics for Chapter 26

Key Topic Element	Description	Page Number
Steps	Configure Locations in Webex Control Hub	636
Steps	Configure Numbers in Webex Control Hub	637
Steps	Configure Dial Routing	639
Paragraph	Number of local gateways per location	641
Steps	Configure a trunk in Webex Control Hub	641
Steps	Configure Gateway Settings and verify trunk	644
Steps	Register Local Gateway to Webex Control Hub	645
Table 26-2	Firewall and NAT Traversal Port, IP Addresses, and Protocols	647
Example 26-1	Cisco UBE Commands for Incoming Call Handling from PSTN	648
Example 26-2	Local Gateway Commands for Incoming Calls to Webex Control Hub	649
Example 26-3	Local Gateway Commands for Outgoing Calls from Webex Control Hub	650
Example 26-4	Cisco UBE Calls Outbound to PSTN	651

Define Key Terms

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

Locations, Numbers, CCP, Cisco PSTN, Premises-based PSTN, Local Gateway, Cisco UBE, SBC

Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. It might not be necessary to memorize the complete syntax of every command, but you should be able to remember the basic keywords needed.

To test your memory of the commands, cover the right side of Tables 26-4 through 26-8 with a piece of paper, read the description on the left side, and then see how much of the command you can remember.

The CCLOR 350-801 exam focuses on practical, hands-on skills that are used by a networking professional. Therefore, you should be able to identify the commands needed to configure and test IOS XE commands for codec preference lists, dial peers, voice translation rules and profiles, BRI interfaces, PRI interfaces, and **show** commands used for verifying BRI and PRI interfaces.

Table 26-4 Cisco IOS XE Commands for Local Gateway Registration

Task	Command Syntax
This command will download a signed CA root bundle to create a trust point using TLS version 1.2 in the router.	`crypto pki trustpool import clean url`

These commands establish communication with Webex Control Hub for registration of the local gateway.	`voice class Tenant 200`
	`  registrar dns:XXXXXX scheme sips expires 240 refresh-ratio 50 tcp tls`
	`  credentials number XXXXXX username XXXXXX password 0 XXXXXX realm BroadWorks`
	`  authentication username XXXXXX password 0 XXXXXX realm BroadWorks`
	`  authentication username XXXXXX password 0 XXXXXX realm XXXXXX`
	`  no remote-party-id  sip-server dns:XXXXXX  connection-reuse`
	`  srtp-crypto 200  session transport tcp tls  url sips  error-passthru asserted-id pai`
	`  bind control source-interface GigabitEthernet1`
	`  bind media source-interface GigabitEthernet1`
	`  no pass-thru content custom-sdp`
	`sip-profiles 200`
	`  outbound-proxy dns:XXXXXX  privacy-policy passthru`

Configure the following SIP profile required to convert SIPS URIs back to SIP, as Webex Calling does not support SIPS URIs in the request/response messages (but needs them for SRV query; for example, **_sips._tcp.<outbound-proxy>**).
rule 20 modifies the From header to include the **Trunk Group OTG/DTG** parameter from Control Hub to uniquely identify a LGW site within an enterprise. Make sure you replace that with your **Trunk Group OTG/DTG** information.
	`voice class sip profiles 200`
	`rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"`
	`  rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"`
	`  rule 11 request ANY sip-header From modify "<sips:" "<sip:\1"`
	`  rule 12 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"`
	`  rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"`

Task	Command Syntax
	rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1" rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1" rule 20 request ANY sip-header From modify ">" ";otg=XXXXXX>" rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"

Table 26-5 Cisco IOS XE Commands for Inbound Calls from Cisco UBE

Task	Command Syntax
These commands are needed to route calls from Cisco UBE to Cisco Unified Communications Manager destined for Webex Control Hub registered devices.	voice class uri 100 sip host <PSTN IP address> dial-peer voice 100 voip description Inbound dialpeer from PSTN incoming uri via 100 destination dpg 302 voice class dpg 302 dial-peer 305 preference 1 dial-peer 307 preference 1 voice class server-group 305 ipv4 <cucm-node-1> ipv4 <cucm-node-5> voice class server-group 307 ipv4 <cucm-node-6> ipv4 <cucm-node-7> dial-peer voice 305 voip description Outgoing dial-peer to CUCM for inbound from PSTN – 1st 5 destination-pattern .T session server-group 305

Task	Command Syntax
	dial-peer voice 307 voip description Outgoing dial-peer to CUCM for inbound from PSTN- 2nd 5 destination-pattern .T **session server-group 307**

Table 26-6 Cisco IOS XE Commands for Inbound Calls to Local Gateway

Task	Command Syntax
These are the commands Local Gateway will use to route calls from Cisco Unified Communications Manager to Webex Control Hub.	voice class uri 300 sip pattern <cucm-nodes-ip-address and port-regex-for-dcloud> ex: pattern 10\.1\.2\..*:5065 matches 10.1.2.X:5065 range dial-peer voice 300 voip description Incoming dial-peer from CUCM for dcloud incoming uri via 300 destination dpg 200 voice class dpg 200 dial-peer 201 preference 1 dial-peer voice 201 voip description Outgoing dial-peer to BroadCloud destination-pattern .T **session-target sip-server**

Table 26-7 Cisco IOS XE Commands for Outbound Calls from Local Gateway

Task	Command Syntax
These are the commands Local Gateway will use to route calls from Webex Control Hub to Cisco Unified Communications Manager.	voice class uri 200 sip pattern :8934 dial-peer voice 200 voip description Incoming dial-peer from Webex incoming uri via 200 destination dpg 300

Task	Command Syntax
	voice class dpg 300 dial-peer 301 preference 1 dial-peer 303 preference 1 voice class server-group 301 ipv4 <cucm-node-1> port 5065 ipv4 <cucm-node-5> port 5065 voice class server-group 303 ipv4 <cucm-node-6> port 5065 ipv4 <cucm-node-7> port 5065 dial-peer voice 301 voip description Outgoing dial-peer to CUCM for inbound from Webex – 1st 5 destination-pattern .T session server-group 301 dial-peer voice 303 voip description Outgoing dial-peer to CUCM for inbound from Webex – 2nd 5 destination-pattern .T **session server-group 303**

Table 26-8 Cisco IOS XE Commands for Outbound Calls to Cisco UBE

Task	Command Syntax
These commands are used to route calls from Cisco Unified Communications Manager to Cisco UBE destined for the PSTN.	voice class uri 302 sip pattern <cucm-nodes-ip-address and port-regex-for-pstn> ex: pattern 10\.1\.2\..*:5060 matches 10.1.2.X:5060 range

Task	Command Syntax
	dial-peer voice 302 voip description Incoming dial-peer from CUCM for pstn incoming uri via 302 destination dpg 100 voice class dpg 100 dial-peer 101 preference 1 dial-peer voice 101 voip description Outgoing dial-peer to PSTN destination-pattern .T session target ipv4:<pstn ip address>

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. In what order should settings be configured for Webex Calling both in Webex Control Hub and Local Gateway?
2. List the three PSTN options for Webex Calling.
3. What three-step process would the Cisco Unified Communications Manager use to route calls from Cisco UBE to Local Gateway?

This part covers the following topics:

- **Chapter 27, Understanding Cisco Unity Connection:** This chapter will introduce the Cisco Unity Connection application in a Cisco Unified Communications solution. Topics will include integration, system settings, call handlers, call routing, distribution lists, authentication rules, and dial plan.
- **Chapter 28, Cisco Unity Connection End-User and Voice Mailbox:** This chapter will explain how to configure different components within a Cisco Unity Connection application. Topics covered in this chapter will include Cisco Unity Connection end-user templates, Class of Service, password settings and roles, transfer rules and greetings, call actions, message actions and caller input, TUI, and voice mailboxes.
- **Chapter 29, Deploying the Webex Application:** This chapter will provide an overview of the Webex app, the configuration components required to support Webex app registration to the Cisco Unified Communications Manager, and examine the extra configuration components needed to migrate existing Cisco Jabber clients to Webex App

Part VII

Collaboration Applications

CHAPTER 27

Understanding Cisco Unity Connection

This chapter covers the following topics:

Cisco Unity Connection Integration: This topic will describe Cisco Unity Connection in a Cisco Unified Communications solution, and it will describe the Cisco Unity Connection integration with Cisco Unified Communications Manager using SCCP and SIP.

Cisco Unity Connection System Settings: This topic will describe the main system settings of Cisco Unity Connection.

Cisco Unity Connection Call Handlers: This topic will describe the three different call handlers that are available in the Cisco Unity Connection.

Cisco Unity Connection Call Routing: This topic will describe the Cisco Unity Connection direct call-routing and forward call-routing rules.

Cisco Unity Connection Distribution Lists: This topic will describe the Cisco Unity Connection distribution lists future.

Cisco Unity Connection Authentication Rules: This topic will describe the Cisco Unity Connection authentication rules feature.

Cisco Unity Connection Dial Plan: This topic will describe the dial plan in Cisco Unity Connection.

This chapter describes the integration of Cisco Unity Connection with Cisco Unified Communications Manager via different protocols. The main Cisco Unity Connection system-level features are explained, including call handlers and the dial plan. Topics discussed in this chapter include the following:

- Cisco Unity Connection Integration
- Cisco Unity Connection System Settings
- Cisco Unity Connection Call Handlers
- Cisco Unity Connection Call Routing
- Cisco Unity Connection Distribution Lists
- Cisco Unity Connection Authentication Rules
- Cisco Unity Connection Dial Plan

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 6.1 Configure Cisco Unity Connection mailbox and MWI
- 6.2 Configure Cisco Unity Connection SIP integration options to call control
- 6.3 Describe Cisco Unity Connection call handlers

"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 27-1 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 27-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Cisco Unity Connection Integration	1
Cisco Unity Connection System Settings	2
Cisco Unity Connection Call Handlers	3
Cisco Unity Connection Call Routing	4
Cisco Unity Connection Distribution Lists	5
Cisco Unity Connection Authentication Rules	6
Cisco Unity Connection Dial Plan	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. When creating a SIP trunk from the CUCM to CUC, an administrator must configure a SIP trunk security profile. Which setting on the SIP trunk security profile must be checked?

a. Accept out-of-dialog refer

b. Accept unsolicited notifications

c. Accept replaces header

d. All of these answers are correct.

2. How many voicemail users are supported in a Cisco Unity Connection cluster?
   a. 1000
   b. 2000
   c. 10,000
   d. 20,000
3. How many different types of call handlers are supported on the Cisco Unity Connection solution?
   a. 1
   b. 2
   c. 3
   d. 4
4. Which of the following is a call-routing rule condition?
   a. Schedule
   b. Call handler
   c. Conversation
   d. User with mailbox
5. On the Cisco Unity Connection server, what is the maximum number of private distribution lists allowed per user?
   a. 25
   b. 99
   c. 999
   d. 9999
6. When a user fails to sign in to Cisco Unity Connection past the allowable limitation, what is the default lockout duration in minutes?
   a. 1 minute
   b. 5 minutes
   c. 30 minutes
   d. 60 minutes
7. Where does the default partition get its name in the Cisco Unity Connection server?
   a. From the CUC name.
   b. From the search space.
   c. It's named the <none> partition by default.
   d. The administrator is prompted to name the partition before it can be used.

Foundation Topics

Cisco Unity Connection Integration

Cisco Unity Connection (CUC) integrates messaging and voice recognition components to provide global access to calls and voice messages for up to 20,000 users on a single CUC server, and it can scale up to 100,000 users supported in a full CUC cluster. CUC advanced communication services offer voice commands to place calls or listen to messages in hands-free mode. Users can also check messages over the telephone or from a desktop through an email inbox or browser.

CUC has its own integrated message and data store, which runs on a Linux-based platform. CUC can integrate with the Cisco Unified Communications Manager, the Cisco Unified Communications Manager Express, or even to a traditional PBX system. It can also be configured to import a user database from Cisco Unified Communications Manager using the AXL API. This API allows CUC to read the users from the Cisco Unified Communications Manager database using SOAP, HTTP, or HTTPS. CUC provides a telephone user interface (TUI) and a voice user interface (VUI). With an IP phone and Voice View Express, the mailbox can be checked and browsed visually using a graphical user interface (GUI).

CUC can integrate with a Microsoft Exchange Server to bring voice messages to an IMAP desktop email inbox. The WebDAV service allows users to import calendaring information from Microsoft Exchange for personal transfer rules. Microsoft Active Directory (AD) integration is available for synchronizing CUC usernames and passwords to AD using the LDAP interface. Authentication for web-based application access is an optional feature of the AD integration.

CUC also supports simultaneous integrations with multiple telephone systems at the same time. Cisco Unified Communications Manager supports phone system integration through IP protocols SIP or SCCP. Circuit-switched phone system integrations are accomplished through the Cisco PBX IP Media Gateway (PIMG) or Cisco T1 IP Media Gateway (TIMG) and a SIP trunk.

Key Topic

Although the Cisco Unified Communications Manager can integrate with CUC using SCCP, the SIP integration requires fewer configuration elements, making it an easier and preferable solution to deploy. When the Cisco Unified Communications Manager is integrated with SIP, a SIP trunk security profile needs to be created first, which will be used with the SIP trunk pointing to the CUC system. After the SIP trunk is created, a route pattern is used in conjunction with the voicemail profile and voicemail pilot. When a user presses the Messaging button on the IP phone, the configured number in the voicemail pilot is searched within the Cisco Unified Communications Manager. The route pattern will make the match and route the call to the CUC. Unlike SCCP integrations with the CUC, SIP integration does not require the number of ports to be specified in the Cisco Unified Communications Manager. They need to be specified only in the CUC. Another significant difference between SIP and SCCP integration involves how the message waiting indicator (MWI) is handled. With SIP, there are no explicit MWI numbers for MWI on or MWI off. Finally, the SIP integration uses port 5060, which is the standard SIP port. The IP phones also use port 5060 to communicate with the Cisco Unified Communications Manager. The communication between the IP phone and CUC can be secured using port 5061 as well. To configure SIP integration toward the CUC on the Cisco Unified Communications Manager, follow these steps:

Step 1. Configure a SIP trunk security profile:

a. From Cisco Unified CM Administration, navigate to **System > Security > SIP Trunk Security Profile.**

b. Click **Add New** and configure the following settings:

- **Name:** Provide a name such as **Nonsecure CUC SIP Trunk Security Profile.**

- **Device Security Mode:** Non Secure
- **Incoming Transport Type:** TCP + UDP
- **Outgoing Transport Type:** TCP
- **Incoming Port:** 5060

c. Check all of the following boxes:

Key Topic

- **Accept out-of-dialog refer:** This setting allows the Cisco Unified Communications Manager to accept incoming non-INVITE, out-of-dialog REFER requests that come via the SIP trunk. This box must be checked for SIP CUC integrations.
- **Accept unsolicited notifications:** This setting allows Cisco Unified Communications Manager to accept incoming non-INVITE, unsolicited notification messages that come via the SIP trunk. This box must be checked for SIP CUC integrations.
- **Accept replaces header:** This setting allows Cisco Unified Communications Manager to accept new SIP dialogs, which have replaced existing SIP dialogs. This box must be checked for SIP CUC integrations.

d. Click **Save.**

Step 2. Configure a SIP trunk to the CUC:

a. Navigate to **Device > Trunk.**

b. Click **Add New** and select **SIP Trunk** from the first drop-down box.

c. Two more drop-down boxes will appear. Leave them with their default settings and click **Next.**

d. Configure the following settings:

- **Device Name:** Provide a name for the trunk (no spaces allowed).
- **Device Pool:** Choose an appropriate device pool from the drop-down list.
- **Incoming Calls > Calling Search Space:** Choose an appropriate CSS from the drop-down list.
- **Incoming Calls > Redirecting Diversion Header Delivery – Inbound:** Check this box. This setting is required for a SIP trunk to CUC.
- **Outbound Calls > Calling and Connected Party Info Format:** Deliver DN only in connected party.
- **Outbound Calls > Redirecting Diversion Header Delivery – Outbound:** Checking this box will include the redirecting number in the outgoing INVITE message from the Cisco Unified Communications Manager to indicate the original called party number and the redirecting reason of the call when the call is forwarded. Use Redirecting Number for voice-messaging integrations only.

- **SIP Information > Destination > Destination Address:** Enter the IP address of CUC.
- **SIP Information > Destination > Destination Port:** 5060.
- **SIP Information > SIP Trunk Security Profile:** Choose the SIP trunk security profile created previously.
- **SIP Information > Rerouting Calling Search Space:** Choose the appropriate CSS.
- **SIP Information > Out-of Dialog Refer Calling Search Space:** This CSS is used when a Cisco Unified Communications Manager refers a call that is coming into a SIP user to a third party when no involvement of the SIP user exists. In this case, the system uses the Out-of-Dialog Calling Search Space of the SIP user. For example, a call may come in to a user who is not logged in. The call is then immediately rerouted to the user's voice mailbox. Permission for that call redirect would be granted using the
Out-of Dialog Refer CSS.
- **SIP Information > SIP Profile:** SIP Profile for CUC.

e. Click **Save**. A dialog box will pop up. Click **OK**.

f. No SIP trunks, including newly created ones, will take effect until they have been reset. Click **Reset**. A new popup will appear. Click **Reset** and then click **Close**.

Step 3. Configure the voicemail pilot and the voicemail port:

a. Navigate to **Advanced Features > Voice Mail > Voice Mail Pilot.**

b. Click **Add New** and configure the following settings:

- **Voice Mail Pilot Number:** Enter a dialable number for the pilot.
- **Calling Search Space:** Enter an appropriate CSS.
- **Make This the Default Voice Mail Pilot for the System:** Check this box.

c. Click **Save**.

d. Navigate to **Advanced Features > Voice Mail > Voice Mail Pilot.**

e. Click **Add New** and configure the following settings:

- **Voice Mail Profile Name:** Provide an appropriate name.
- **Voice Mail Pilot:** Associate the previously configured voice mail pilot with this profile.
- **Make This the Default Voice Mail Pilot for the System:** Check this box.

f. Click **Save**.

Step 4. Configure a route pattern:

a. Navigate to **Call Routing > Route/Hunt > Route Pattern**.

b. Click **Add New** and configure the following settings:

- **Route Pattern:** The number should match the voice mail pilot.
- **Partition:** Choose the appropriate partition.
- **Gateway/Route List:** Choose the CUC trunk created previously.
- **Provide Outside Dial Tone:** Unchecked.

c. Click **Save**.

Cisco Unity Connection System Settings

In the simplest form, CUC can be deployed as a standalone server in a Unified Communications solution. CUC implementations include a 500-user integration with Cisco Unified Communications Manager Business Edition, which collocates CUC to a CUC server cluster that supports 20,000 voicemail users.

In a single-site deployment, typically only one codec is used: G.711. Therefore, no Call Admission Control or transcoders are necessary because no additional branches are connected via the WAN. WAN connections typically use the G.729 codec, which would require transcoders when routing to the CUC.

The platform overlay determines the capacity, capabilities, and number of users supported. If high availability and redundancy are needed, or if there will be multiple locations or expected growth, another deployment model might better meet the needs of the organization. Traffic patterns need to be evaluated only when CUC is used as a centralized voice-messaging system or in a distributed voice-messaging solution. Imagine that 250 users located in a branch office are using a centralized voice-messaging system. If only 10 percent were to use the voice-messaging system at the same time, then voice-messaging would bring 25 connections (25 calls × 24 kbps on Layer 3 = 600 kbps) to the voice traffic pattern for the CUC application. These 25 calls will also need to be transcoded, which will require additional DSP resources at the headquarters location. Figure 27-1 illustrates the scenario explained here using a centralized deployment of CUC between a headquarters and branch office location.

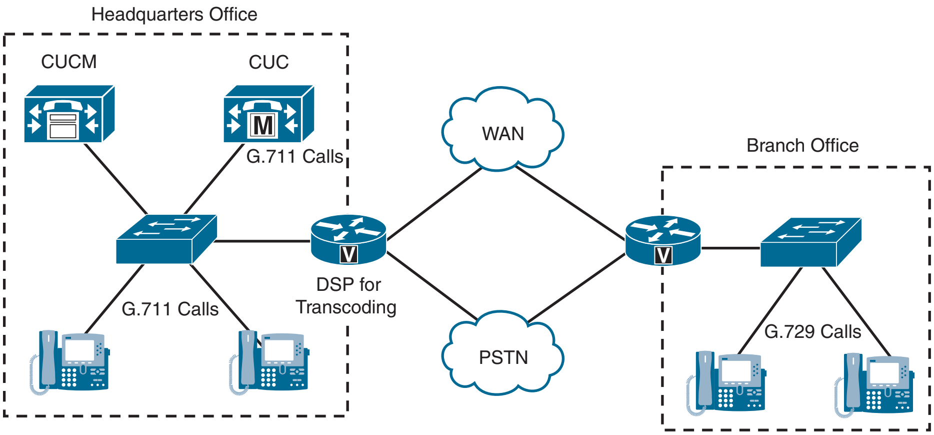


Figure 27-1 *Centralized Deployment of CUC*

CUC system settings are very powerful and offer many configuration options. This book will cover only the settings related to end-user administration and a single-site deployment.

The general settings allow the administrator to modify the default settings. The time zone setting depends on settings configured during the CUC installation. The default system language and the system default TTS language are English (US). The default recording format is G.711 mu-law, and the default maximum greeting length is 90 seconds. The administrator can also define the action in case a recipient cannot be found. The predefined roles can be used to limit the GUI access to certain configuration areas or limit the TUI for different kinds of administrators. The different predefined roles in the CUC are as follows:

- The audio text administrator administers call handlers, directory handlers, and interview handlers.
- The greeting administrator manages call handler–recorded greetings via TUI.
- The help desk administrator resets user passwords, unlocks user accounts, and views user settings.
- The remote administrator manages the database using remote management tools.
- The system administrator is the top-level administrator and can access all CUC administrative functions, reports, and tools for servers and users.
- The technician can access functions that enable management of the system and phone system integration settings, viewing of all system and user settings, and can run all reports and diagnostic tools.
- The user administrator manages users and can access all user administration functions, reports, and user administration tools.

The enterprise parameters and service parameters on the CUC are like the Cisco Unified Communications Manager enterprise parameters and service parameters. These parameters allow restriction of CUC user option pages, QoS settings, and so on. LDAP can be integrated and allows use of the LDAP synchronization and LDAP authentication. With the use of LDAP authentication, a single password login can be offered for user access to many different services. Additional system settings will be covered in greater detail later in this chapter.

Cisco Unity Connection Call Handlers

Call handlers are messaging systems that allow calls to be routed to specific destinations based on the caller's input. Contact centers use call handlers quite often. Think of a time you called into a bank or an airline. A messaging system answers the call and provides menu options that must be selected to route the call to the appropriate agent. In CUC call management, there are three different kinds of call handlers. System call handlers are used for greetings and can offer the caller different call actions depending on the digit that the caller selects. Directory call handlers allow callers to search for users on the CUC system or on connected voice-messaging systems. Interview call handlers allow the system to ask the caller questions and record the answers. The recorded message can be sent to any voicemail user.

There are three preconfigured system call handlers: goodbye, opening greeting, and operator. The opening greeting is the greeting that callers will hear when they call the general voice-messaging system numbers. These callers cannot be subscribers; otherwise, they are subscribers who do not transmit their calling number. If the caller is a subscriber, the system will prompt that user to enter an ID and PIN to log in to a personal mailbox.

A system call handler can manage incoming calls to the main DID number of a company or for all company phone numbers. The system call handler may play a greeting for callers and offer a list of choices that can be selected based on the numeric key pressed on the caller's phone. Figure 27-2 illustrates how a call handler may operate.

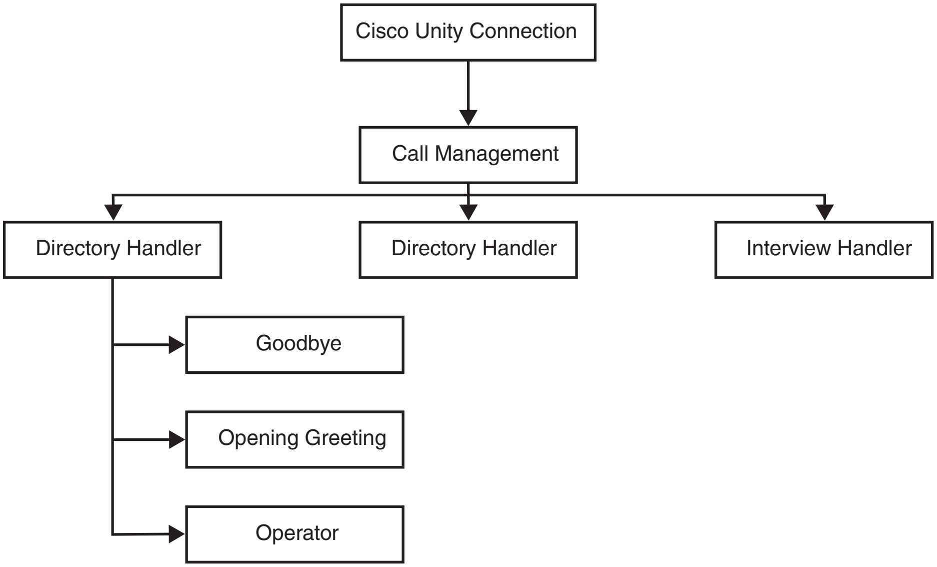


Figure 27-2 *Call Handler Operation*

Based on Figure 27-2, when a caller dials in to the company represented, the system call handler answers the call. If the caller presses 1 on the phone keypad, the caller can search via a directory call handler through the company directory and select an employee with a simple key press, assuming the employee is listed. If the caller presses 2, then another system call handler plays a different greeting, which will then route the caller to an interview call handler. The interview call handler can ask for the name, phone number, email address, and the position for which the caller wants to apply. If the caller presses 4, the caller will automatically be rerouted to the local tech support number. Similarly, when the caller presses zero, the caller is rerouted to the operator. A hidden menu can also be made available, and it can require authentication after it is selected to prevent unwanted calls from connecting.

Cisco Unity Connection Call Routing

Call routing is the method the CUC employs to handle calls from users in the system, as well as undefined callers from outside the organization. Both direct calls into the system and forwarded calls from another system, such as a call forward option on the Cisco Unified

Communications Manager, can be handled differently based on call rules and conditions configured within the system. Direct call-routing rules process calls from users and unidentified callers who dialed directly into CUC. Forwarded-routing rules process calls that are forwarded to CUC. The difference between direct routing and forward routing is the origin of the call: direct call or forwarded call. Call-routing rules can be manually configured in CUC, but some predefined rules are already implemented. The following rules are the predefined *direct* routing rules:

- **Attempt Sign-In:** Calls from users are routed to the user login conversation.
- **Opening Greeting:** Calls forwarded from an extension that is not associated with a user account are routed to the opening greeting.

The predefined *forwarded* routing rules are as follows:

- **Attempt Forward:** All calls forwarded from a user extension are routed to the user greeting.
- **Opening Greeting:** Calls forwarded from an extension that is not associated with a user account are routed to the opening greeting.

Call-routing rules allow a call to be filtered, and an action can be applied to the call, such as all calls that are received from a number that is associated with a "good" customer are directly transferred to an appropriate number. Another example could be that all calls placed to a discontinued number within the company are played a greeting informing the caller that the number has changed, and the caller is then transferred to the company auto-attendant. The call-routing rules can be specified based on the following parameters or conditions:

- Calling number, such as 2001 or 123* (for all four-digit numbers that start with 123)
- Called number
- Voicemail port from 1 to *n* (applies to direct calls only)
- Phone systems, if more than one is used (applies to direct calls only)
- Forwarding station (applies to forwarded calls only)
- Schedule, which can be defined for all hours, weekdays, or customized timeframes

Combined with the call action, the administrator can now define special call treatment based on certain criteria, such as all calls from area code 919 will go to the sales rep assigned to that territory. Another scenario could be that a holiday greeting is played during the last week of December announcing a company closure during that time. Figure 27-3 illustrates the call actions and rule conditions that can be set with call routing on the CUC.

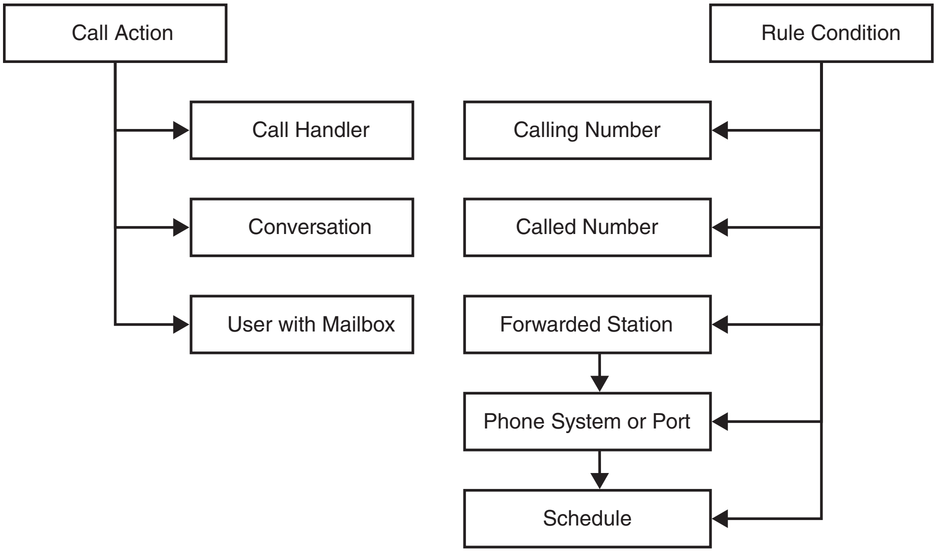


Figure 27-3 *Call-Routing Call Actions and Rule Conditions*

Cisco Unity Connection Distribution Lists

System distribution lists in CUC are used to send voice messages to multiple users. The users who are members of a system distribution list are typically those who need the same information on a regular basis, such as employees within a department or members of a team. The predefined system distribution lists are undeliverable messages, all voicemail users, and all voicemail-enabled contacts.

Voicemail users can configure private distribution lists as well. The administrator can define a maximum number of 99 private distribution lists per user, but the default is 25. Within the private distribution, the number of members can be set to a maximum of 999, although the default is 99.

Cisco Unity Connection Authentication Rules

With CUC authentication rules, the security level used to allow voicemail users to connect to the voice-messaging system can be set and controlled with restrictive parameters that better secure the production networked environment. Although the default values can be changed, the following settings for each authentication rule can be defined, where the values in the parentheses specify the default value:

Key Topic

- Failed Sign-In (3) Attempts or no limit for Failed Sign-Ins
- Reset Failed Sign-In Attempts Every (30) Minutes
- Lockout Duration (30) Minutes or Administrator Must Unlock
- Minimum Duration Between Credential Changes (1440=1 Day) Minutes
- Credentials Expire After (180) Days or Never Expire
- Expiration Warning (0) Days

- Minimum Credential Length (6)
- Stored Number of Previous Credentials (5)
- Check for Trivial Passwords

As mentioned before, all of the settings that are in parentheses are the default values, and they can be modified to suit each unique corporate network respectively. If a company wanted to allow voicemail users to use the PIN 123, the administrator would need to disable the Check for Trivial Passwords setting and change the Minimum Credential Length from the default value of 6 characters to 3 characters.

Cisco Unity Connection Dial Plan

The dial plan in CUC is similar to the Cisco Unified Communications Manager. The CUC dial plan is based on partitions and search spaces. These entities can be compared to the Cisco Unified Communications Manager Partitions and Calling Search Spaces. By default, all users on the CUC are in the same default partition. A search space is made up of a collection of partitions. A directory call handler allows callers to dial users based on the collective partitions of which the search space is made up.

During the installation of CUC, a name must be entered. This CUC name is the default name of the preconfigured partition and search space. Both the partition and search space are preselected within applicable settings of the CUC, such as in the user and call handler templates. Therefore, all new users or call handlers belong to this default partition and have the default search space assigned.

A search space can be used to control where a directory call handler, and therefore a caller, can search for users when the caller selects the options to dial a user or send a message. The search space can limit the caller search to only the current server, all servers, or only in certain partitions. An example could be in a multisite scenario where the administrator creates a directory call handler per location. These site-specific directory call handlers can be set up so that they search for users only in their designated sites, but they will not search the complete company directory. Another example would be to place managers into a manager partition, so the external users cannot dial a manager directly.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 27-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 27-2 Key Topics for Chapter 27

Key Topic Element	Description	Page Number
Paragraph	SIP Integration Between CUCM and CUC	663
List	SIP Trunk Security Profile Check Boxes	664
List	Predefined Administrator Roles in CUC	667
Paragraph	CUC Call Management Call Handler Types	667
List	Predefined Routing Rules	669
List	Authentication Rules and Their Default Values	670

Define Key Terms

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

API, AXL, Call Handlers, Call Routing, CUC, DID, Distribution Lists (CUC), GUI, IMAP, PIMG, SOAP, TIMG, TUI, VUI, WebDAV

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the four main steps to configure SIP integration from CUCM to CUC.
2. List the three call handlers in a CUC system and their function.
3. List the two predefined direct routing rules and the two predefined forwarded routing rules on the CUC.

This page intentionally left blank

CHAPTER 28

Cisco Unity Connection End-User and Voice Mailbox

This chapter covers the following topics:

Cisco Unity Connection End-User Templates Overview: This topic will describe the user templates and how the user templates can be used in different scenarios.

User Templates Basics: This topic will describe the important user template settings.

Default Class of Service: This topic will describe CoS as it pertains to Cisco Unity Connection user configuration.

Password Settings and Roles: This topic will describe the password settings and roles that you can configure for Cisco Unity Connection users.

Transfer Rules and Greetings: This topic will describe the transfer rules and greetings available for Cisco Unity Connection users.

Call Actions: This topic will describe call actions that can be configured in Cisco Unity Connection.

Message Actions and Caller Input: This topic will describe message actions and caller input options that can be configured in Cisco Unity Connection.

TUI Experience: This topic will describe phone menu parameters that you can configure to modify the TUI experience for the user.

Cisco Unity Connection End Users: This topic will describe the main Cisco Unity Connection user parameters and how a user account can be individualized. This topic will also describe how to import users to the Cisco Unity Connection server manually, from the Cisco Unified Communications Manager, through an LDAP integration, and through the Bulk Administration Tool.

Cisco Unity Connection Voice Mailboxes: This topic will describe the voice mailbox parameters of a user, message aging policy, and mailbox quotas.

The preceding chapter provided a brief introduction to the Cisco Unity Connection server and the services available through this application. This chapter will delve deeper into each of the configuration components that revolve around end users and the end-user mailbox. Topics discussed in this chapter include the following:

- Cisco Unity Connection End-User Templates Overview
- User Templates Basics
- Default Class of Service

- Password Settings and Roles
- Transfer Rules and Greetings
- Call Actions
- Message Actions and Caller Input
- TUI Experience
- Cisco Unity Connection End Users
- Cisco Unity Connection Voice Mailboxes

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 6.1 Configure Cisco Unity Connection mailbox and MWI
- 6.2 Configure Cisco Unity Connection SIP integration options to call control
- 6.3 Describe Cisco Unity Connection call handlers

“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 28-1 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 28-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Cisco Unity Connection End-User Templates Overview	1
User Templates Basics	2
Default Class of Service	3
Password Settings and Roles	4
Transfer Rules and Greetings	5
Call Actions	6
Message Actions and Caller Input	7
TUI Experience	8
Cisco Unity Connection End Users	9
Cisco Unity Connection Voice Mailboxes	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. When you are creating an authentication rule on the CUC, which of the following is a criterion for passwords and PINs when the Check for Trivial Passwords box is checked?
   - **a.** The password or PIN is not the same as the primary extension that is assigned to the user.
   - **b.** Passwords must have no fewer than 15 characters.
   - **c.** PINs must have no fewer than eight digits.
   - **d.** Passwords and PINs cannot have more than two repeating letters, characters, or numbers.
2. Which of the following user template basics settings is considered one of the three main components?
   - **a.** Dial Plan
   - **b.** Class of Service
   - **c.** Location
   - **d.** Time Zone
3. What is the default timer length in the CUC server for total message length?
   - **a.** 30 seconds
   - **b.** 60 seconds
   - **c.** 300 seconds
   - **d.** 600 seconds
4. When changing the password settings on a user template, what must an administrator do after the template settings have been saved?
   - **a.** Commit the password settings with the user template.
   - **b.** Create a PIN to use with the template.
   - **c.** Create an authentication rule to use with the password settings.
   - **d.** Nothing more needs to be done.
5. Which of the following is considered a rare greeting on the CUC?
   - **a.** Holiday greeting
   - **b.** Closed greeting
   - **c.** Alternate greeting
   - **d.** Internal
6. Which of the following is a call action on the CUC that could occur after a greeting is played?
   - **a.** Restart greeting
   - **b.** Caller or user system transfer

- **c.** Sign-in
- **d.** Broadcast message administrator

7. What is the default after message action when configuring message action settings on the CUC?

- **a.** Leave a Message
- **b.** Transfer to Operator
- **c.** Replay Message
- **d.** Hang Up

8. When you are configuring TUI settings in the CUC, what is the default timer for entering digits, such as how long to wait for the next digit when entering a name?

- **a.** 3 seconds
- **b.** 5 seconds
- **c.** 7 seconds
- **d.** 10 seconds

9. When user import is set up on the CUC server through an LDAP integration, and the resync interval is enabled, what is the minimum interval that can be set?

- **a.** 1 hour
- **b.** 6 hours
- **c.** 12 hours
- **d.** 24 hours

10. The Mailbox Quota setting on the CUC is used to specify the maximum space per user for message storage in CUC on the system or user level. What is the Warning Quota default value?

- **a.** 6 MB
- **b.** 12 MB
- **c.** 18 MB
- **d.** 24 MB

Foundation Topics

Cisco Unity Connection End-User Templates

User templates can be used to work faster and more effectively on reoccurring tasks. General parameters, which are the same for all users or groups of users, can be predefined. If new users are added to the Cisco Unity Connection (CUC) system, all users will have the same preselected settings, such as language or time zone settings. If the user template is changed at any time, these new settings will affect only users who are created after the user template has been changed. To change parameters for existing users or a group of existing users, you can use the Cisco Unified Communications Manager Bulk Administration Tool, which will be covered later in this chapter.

Key Topic

There are two pre-existing user templates in the CUC. The first user template is for administrators, and the second is for users. An administrator could build different user template models where certain settings are preconfigured for managers, while other settings are preconfigured for employees, and yet other settings are preconfigured for trainees. The managers might have mailboxes with more space for voice messages or accept notifications via their mobile phone when a new message arrives. Employees might have preconfigured message actions, and trainees may be limited to listening to voice messages only. User templates can also be based on the location and can specify the language to use and the time zone for the location so that messages are reported with the correct timestamp. When creating a new user in CUC, you can just select the user template, and the user template settings will be copied to the new user. Figure 28-1 illustrates the user template models available on the CUC.

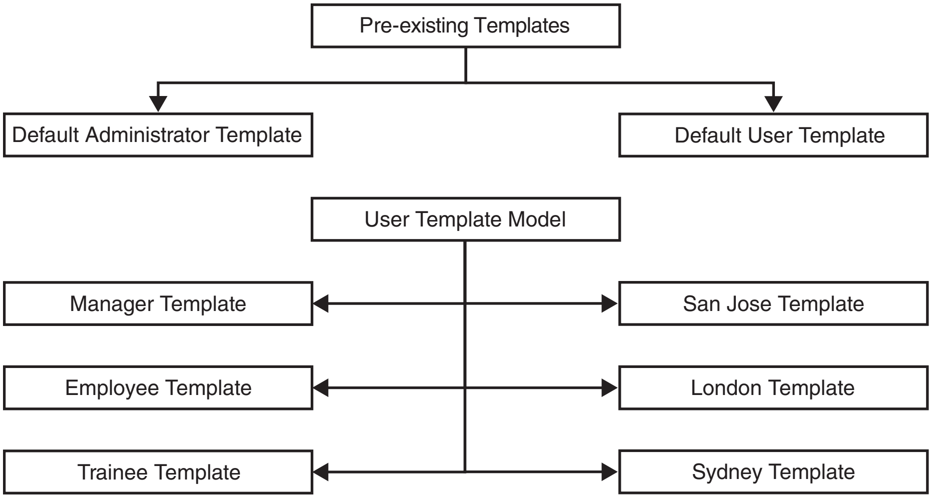


Figure 28-1 *Cisco Unity Connection User Template Model*

User-related parameters can be defined in different places within the CUC administration:

Key Topic

- Enterprise and service parameters on the highest level
- General settings on the system level
- User templates on the mid-level
- User settings on the low level

In a CUC system, user parameters can be set in many places. The Cisco Unified Communications Manager Administration enterprise and service parameters provide one such place where these settings can be set, and these settings will be valid for all entities in the CUC system. These settings will be inherited by the general settings on the CUC. When a change is introduced in the enterprise or service parameters, these changes will affect user settings at all other levels immediately. The next level is general settings, which will be inherited by the user settings. A change on this level will also affect all users immediately. The user templates can override the general settings for new users. A change in the user template will not affect existing devices because the parameters are copied from the user template during the creation of a new user. On the user level, a setting change will override any other setting but only for that one user. If a manager needed additional mailbox space for voice messages, the mailbox quota could be modified on the user level for that manager only.

The CUC user template is divided into the user template basics and additional parameters. The most common parameters include setting the password and PIN, message settings, and actions; modifying the telephone user interface (TUI) experience; and enabling message notifications on different devices. The following steps are required to configure a user template. Any examples provided in these steps are for demonstration purposes only. Settings should be configured in a production environment based on the designed purpose and functions.

Step 1. Create an authentication rule for the user template.

a. In a web browser, navigate to the CUC Administration page by entering the address **https://<*IP_Address*>/cuadmin**.

b. Log in and navigate to **System Settings > Authentication Rules**.

c. Choose **Recommended Voice Mail Authentication Rule** and change the following parameters:

- **Display Name:** Enter a descriptive name for the authentication rule.
- **Failed Sign-In Attempts:** Enter the number of failed sign-in attempts after which users cannot access CUC. When this parameter is set to 0, a failed sign-in attempt results in the user account being locked until manually unlocked by an administrator.
- **No Limit for Failed Sign-Ins:** Check this box so that there is no limit to the number of failed sign-in attempts, and the user is not locked out of the account.
- **Reset Every Failed Sign-In Attempt:** Enter the number of minutes after which CUC will clear the count of failed sign-in attempts, unless the failed sign-in limit is already reached and the account is locked. When this parameter is set to 0, a failed sign-in attempt results in the user account being locked until manually unlocked by an administrator.
- **Lockout Duration:** Enter the number of minutes that a user account will remain locked after the number of allowed Failed Sign-In attempts has been reached. While the account is locked, CUC prevents the users from accessing CUC by phone.
- **Administrator Must Unlock:** Check this box so that accounts remain locked until manually unlocked by the administrator.
- **Minimum Duration Between Credential Changes:** Enter the number of minutes that must elapse between password changes. This setting does not apply when administrators are changing the password in CUC administration.
- **Credential Expires After:** Enter the number of days after which the credentials will expire.
- **Never Expires:** Check this box so that passwords or PINs based on the authentication rule will never expire. This parameter is most applicable for low-security users or for accounts that more than one person

can access. When this box is checked, the user is still able to change passwords or PINs at any time.

- **Expiration Warning Days:** Enter the number of days before passwords or PINs will expire so that CUC will warn users that a password or PIN is about to expire. A value of 0 means that CUC will not warn users that a password or PIN is about to expire.
- **Minimum Credential Length:** Enter the required number of digits for user passwords and PINs. In general, shorter passwords and PINs are easier to use, but longer passwords and PINs are more secure. It is recommended to require eight or more digits. When you change the minimum credential length, users are required to use the new length the next time that they change the password or PIN.
- **Stored Number of Previous Credentials:** Enter a value for the number of previous passwords or PINs that CUC stores for a user. When a user enters a new password or PIN, CUC compares it to the stored passwords or PINs, and rejects it if it matches a password or PIN in the history. A value of 0 means that CUC will not store any previous passwords or PINs for the user.
- **Check for Trivial Passwords:** Check this box to have CUC verify that a new password or PIN meets the following criteria when the passwords or PINs are changed by using CUC administration, messaging assistant, or the CUC conversation:
- The digits are not all the same, such as 9999.
- The digits are not consecutive, such as 1234 or 4321.
- The password or PIN is not the same as the primary extension that is assigned to the user.

d. Click **Save** when finished.

Step 2. Create a new user template.

a. Navigate to **Templates > User Templates** and click the **Add New** button.

b. From the Based-on Template drop-down list, choose the system default **voicemailusertemplate**.

c. Configure the following settings on the new template:

- **Alias:** Enter an alias for the template.
- **Display Name:** Enter a display name for the template. This can be the same name used for the alias above.
- **Mailbox Store:** Choose the mailbox store in which you want to create the mailboxes for user accounts that you create using this template.
- **Outgoing Fax Server:** Choose the applicable fax server for the user, if any.

- **Phone System:** Select the phone system that the template uses. In most cases, only one phone system is configured.
- **Generate SMTP Proxy Address from Corporate Email Address:** When you check this box, CUC automatically creates a new SMTP proxy address for the value in the corporate email address field. An SMTP proxy address allows CUC to map the sender to a user. It also allows CUC to map the message recipients to users or contacts by comparing the SMTP addresses in the message header to its list of SMTP proxy addresses. You must configure applicable SMTP proxy addresses when either Cisco ViewMail for Microsoft Outlook with IMAP or the Single Inbox Feature to Send Messages is used.

d. Click **Save** when finished.

User Templates Basics

Key Topic

Many parameters must be set for a user. The mailbox behavior can best be adjusted with user templates. The most important user template settings that should be configured include the Name, Phone, and Location. Figure 28-2 illustrates the main components in User Template Basics.

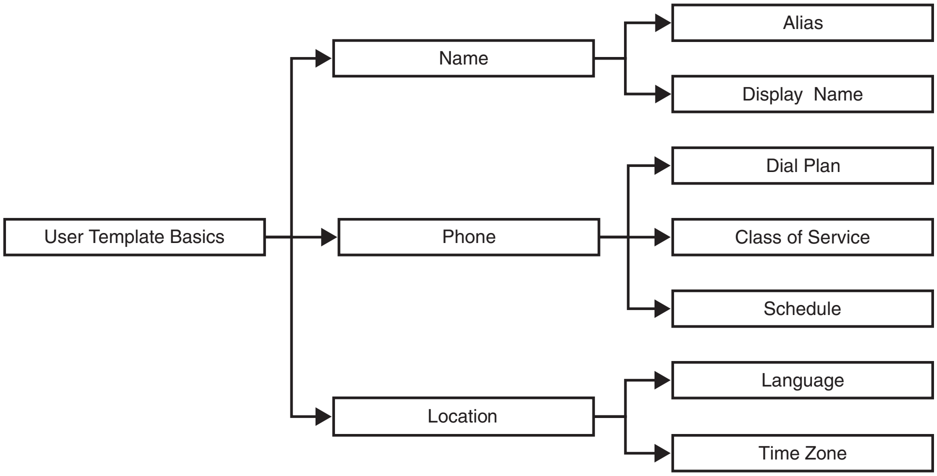


Figure 28-2 *User Template Basics Main Components*

The Name is an alias, which is actually the name of the user template, such as “manager,” which is selected during the end-user creation process. The name generation for users can also be selected, where the default is First Name followed by the Last Name.

The dial plan is set in the Phone section of the template. The dial plan sets the class of service (CoS) for the CUC user, which in turn sets the features the user can access, such as using IMAP to receive voice messages on Cisco Jabber. The dial plan sets the class of service for a user by indicating the partition to which the user belongs and in which search space the user can search, such as when sending messages via the TUI. The schedule is also set in the Phone section of the template; it defaults to weekdays. The schedule should be changed to All Hours; otherwise, the mailbox will not answer calls in the evening hours or on the weekend.

The Location is used to set the language, which is important in a multinational deployment. The language is also important in a single site, where different groups might expect callers from only certain countries, such as a hotline number. The time zone must be set so that a user in San Jose or a user in London will be informed about the correct time when a message was left. To configure user template basics settings in the CUC, first view the default user template basics settings. Clicking Save after you create the new user template described in the previous section will redirect the administrator to the Edit User Template Basics configuration page. Configure the following settings and then click Save:

- **Display Name Generation:** Choose the format for displaying the names of new users who are associated with this template: First Name then Last Name, such as John Doe; or Last Name then First Name, such as Doe, John.
- **Partition:** Choose the partition to which the object belongs. Partitions are grouped into search spaces, which are used to define the scope of objects, such as users and distribution lists, that a user or outside caller can reach while interacting with CUC. Most objects can belong to only one partition; the exception is users, who can have their primary extension in one partition and alternate extensions in other partitions. A partition can belong to more than one search space.
- **Search Scope:** Choose a search space to apply to the user account.
- **Class of Service:** Choose the class of service to which the user should be assigned. The class of service controls many user settings and makes features available.
- **Active Schedule:** Choose a schedule from the list to specify the days and times that the Standard and Closed greetings play, and choose the action that CUC takes after the greeting. The active schedule is set to Weekdays by default. Set it to All Hours so that callers can leave a message at any time.
- **Set for Self-Enrollment at Next Login:** Check this box to ask the user to do the following at the next login:
  - Record a name and a standard greeting.
  - Set a password.
  - Choose whether to be listed in the directory.
- **List in Directory:** Check this box to list the user in the directory, which outside callers can use to reach users.
- **Time Zone:** Choose the desired time zone for the user, or check the Use System Default Time Zone box. The default time zone is the time zone that is set on the CUC server. Change the settings only for users who are located in a different time zone from the CUC server. The following items use the user time zone setting:

- **Message Received Time:** When a user listens to messages by phone, CUC announces the time that a message was received by using the local time that is specified for the user.
- **Message Notification Schedule:** The schedule that is displayed on the user message notification pages and in the Cisco Unity Assistant uses the local time that is specified for the user.

- **Language:** Choose the language in which the CUC conversation plays instructions to users. Click the Use System Default Language option or choose a language from the drop-down list. This setting does not apply to the voice-recognition conversation. The language settings for users also control the language that is used for TTS.

Default Class of Service

The term *class of service (CoS)* can be misleading. CoS in this context has nothing to do with CoS in Cisco Unified Communications Manager or in QoS. In the context of CUC users, CoS describes which features the CUC users have permission to use. There are two default CoS profiles: system and voicemail user. The voicemail user CoS, which is the CoS profile of concern, supports the following by default:

- Timers define recording times for users who are assigned to the class of service. Default recording times are as follows: for the name, 30 seconds; for the greeting, 90 seconds, and for the total message length, 300 seconds.
- Users are listed in the directory by default, so all users can be found when searching users via a directory call handler.
- Features that can be licensed are disabled, such as the ability to access voicemail using an IMAP client, web inbox, TTS, voice recognition, personal transfer rules, video greeting, and so on.
- Other features, such as web inbox or call transfer rules, are also disabled by default because they could generate additional cost to the company.
- Only the administrator can set alternate extensions. Otherwise, the feature could open a security hole within the CUC solution.
- The number of private distribution lists and the members per private distribution list can be limited.
- Call transfer for outgoing or transferred calls can be restricted.

The class of service hierarchy can be divided into three main categories: timers, features, and restriction. Timers allow CoS control over recording times. Features allow CoS control over features that are disabled by default. Restrictions allow CoS control over distribution lists and tables. Figure 28-3 illustrates the class of service hierarchy within the CUC.

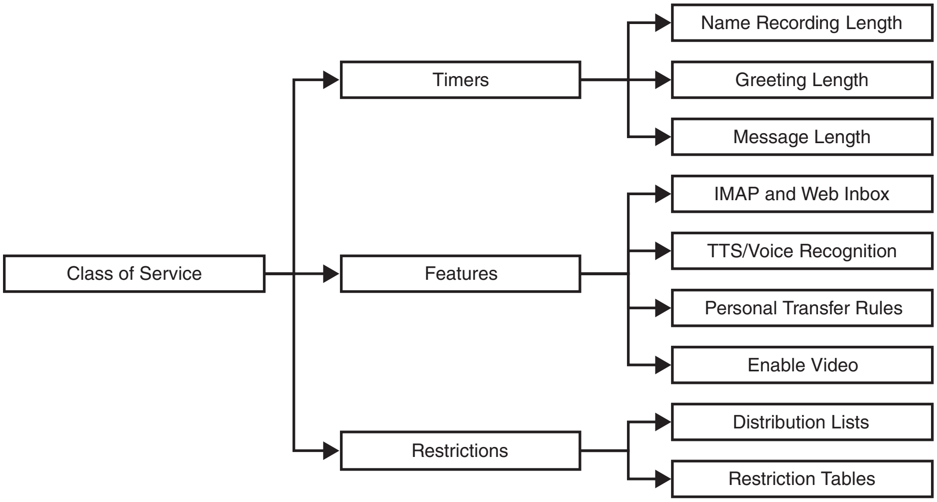


Figure 28-3 *Class of Service Hierarchy Within CUC*

Password Settings and Roles

The passwords use the previously described authentication rules. If an authentication rule were created to allow a minimum credential length of three and a trivial password, with this authentication rule, the password could be set to 123 for all new users. Settings can also be configured to require the user to change the password at next login. For security purposes, you should disable the use of trivial passwords and specify a minimum length of five digits for the PIN, which is used for the TUI to access voice messages. The web application password is used to access the CUC user options page.

When calling the CUC system pilot number, the system might ask the caller for a password, which is actually the PIN. For security reasons, do not enable the Does Not Expire check box so that passwords will need to be changed on a regular basis. Single password sign-in can be offered for the web application when an LDAP integration is set up with LDAP authentication to the Active Directory server. The PIN cannot be set in the Active Directory. Therefore, the PIN must be administered in the CUC administration. Under Roles, the user can be assigned to an administrator group, such as the user administrator. With the new access rights, the user can create new users. Using Roles, you can also create a custom user who has access to certain features or rights. By default, users do not have a defined administrator role. To configure password settings in the user templates, follow these steps:

Step 1. From the user template, select **Edit > Password Settings** from the menus at the top of the page. Notice that any user who is created from this template will be forced to change the PIN at next sign-in. Also notice that Authentication Rule is set to Recommended Voice Mail Authentication Rule, which you would have modified earlier.

Step 2. Configure the following settings as needed and then click **Save**.

- **Choose PIN:** Select one of the following PIN options:
  - **Voicemail:** Choose this option to change the settings that are associated with the voicemail password of a user.

  - **Web Application:** Choose this option to change the settings that are associated with the web application password of a user. If CUC is integrated with an LDAP directory, and if LDAP authentication is configured, the web application password must be changed in the LDAP directory.

- **Locked by Administrator:** Check this box to prevent a user from accessing CUC.

- **User Cannot Change:** Check this box to prevent the user from changing the password. This setting is most applicable for accounts that more than one person can access. When selecting this box, also check the Does Not Expire box.

- **User Must Change at Next Login:** Check this box for temporary passwords. The user must set a new password at next login to CUC. To help protect the accounts from unauthorized access and toll fraud, encourage users to specify long passwords that include eight or more digits, and nontrivial passwords. You can also use the settings on the Edit Authentication Rule page to require users to specify long and nontrivial passwords.

- **Does Not Expire:** Check this box to prevent CUC from prompting the user to change passwords. This check box is most applicable for low-security users or for accounts that more than one person can access. When this box is checked, the user is still able to change passwords at any time. When this box is not checked, the Credential Expires After field controls the password expiration, which the selected authentication rule sets.

- **Authentication Rule:** Choose the authentication policy to apply to the selected user password settings.

Step 3. From the user template, choose **Edit > Change Password**.

Step 4. From the Choose PIN drop-down list, select **Voicemail** or **Web Application**.

Step 5. Enter the PIN to use with the user template and confirm the PIN.

Step 6. Click **Save** when finished.

Transfer Rules and Greetings

Key Topic

Transfer rules are used to reach users. A standard rule is enabled, but it cannot be modified. With greetings, users can personalize their mailboxes. An error greeting plays if the caller enters invalid digits. There are three predefined transfer rules: standard, alternate, and closed. The standard rule is enabled without an end date and cannot be modified. The alternate rule might replace the standard rule with an end date, such as between Christmas and New Year's day. An alternative transfer rule could be used instead of the standard transfer rule. If the schedule for the user is set to weekdays only, the closed rule is used on the weekend and after business hours.

Users can individualize their greetings in different ways. A standard greeting might be "John Doe is not available." The name "John Doe" is generated automatically from the display name by CUC. The alternate greeting is used for personalization of the voice mailbox. The closed greeting can be played on weekends if the schedule is set to weekdays. The holiday greeting allows you to have a personalized greeting for callers, which is played on a holiday. In addition, three rarely used system greetings exist:

- **Busy:** Played when the extension is busy
- **Error:** Played if the caller entered invalid digits
- **Internal:** Played to internal users only

The standard greeting is enabled by default. Other parameters to define include what callers hear before, during, and after the greeting, or the option for callers to select the language. Figure 28-4 illustrates the transfer rules and greetings available on the CUC.

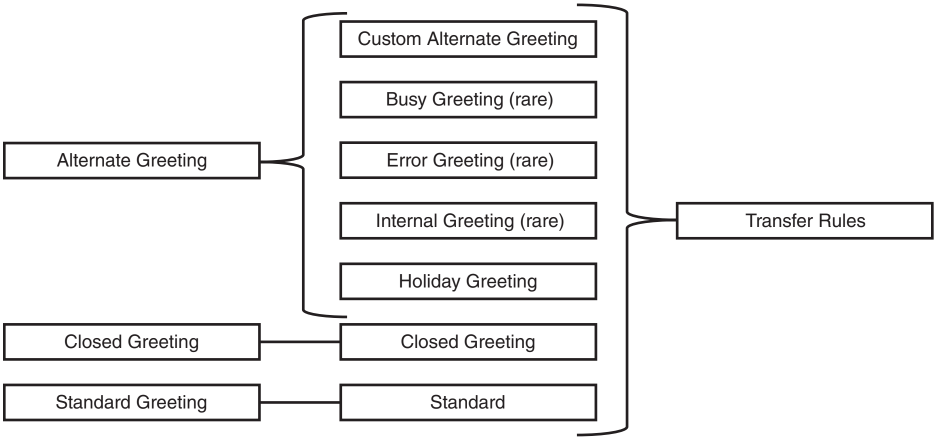


Figure 28-4 *Transfer Rules and Greetings on the CUC*

Call Actions

After the greeting, the caller can be offered various options to process the active call. The commonly used standard option is the call action to take a message. On the weekend or during the holidays, the caller might be directed to another greeting, or the call is ended after playing a message. A transfer to a call handler can also be selected, such as a system call handler, interview call handler, or a directory call handler. The call handler must already exist to be selected during the configuration.

With conversation, the call can be sent to the broadcast or greeting administrator. A mailbox could be created that allows external dial in, which allows the administrator to rerecord greetings. This function could be useful on a day when there is bad weather. The administrator can rerecord a greeting, such as “We are closed today for everyone’s safety due to icy conditions on the roads.” The caller can be transferred to an external number, such as the mobile number of the originally called user. The caller can also be offered an opportunity to sign into a mailbox with an ID and PIN. Directory numbers that a team uses with a shared mailbox could forward the caller to another user mailbox if a user does not answer the call when the phone number is dialed. Figure 28-5 illustrates various call actions that could occur after a greeting is played to the caller.

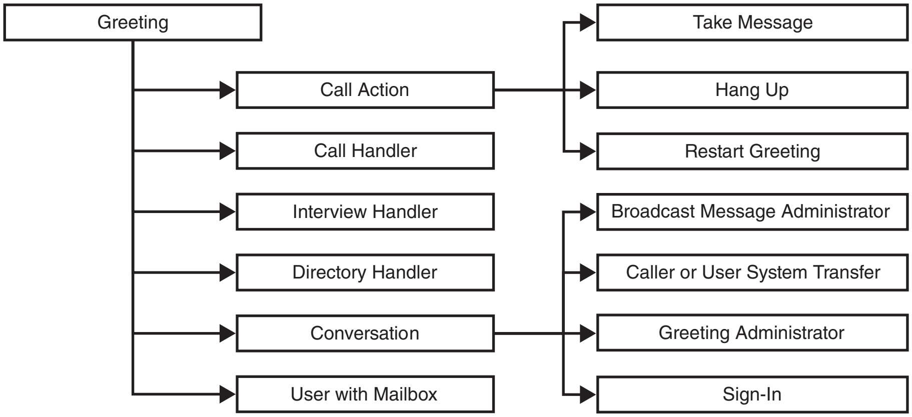


Figure 28-5 *Call Action Options After a Greeting*

Message Actions and Caller Input

The message settings can influence the TUI experience of a caller. A caller who leaves a message can be allowed to edit the message after speaking or to rerecord the message. The message can be marked with normal or urgent importance, or the caller can be asked to choose a message priority, which will have an impact on the message notifications because the user can choose to be notified for all or only urgent messages. After the caller leaves the message, the standard message actions are available, as mentioned in the previous section: call actions, call handler selection, conversation, user with mailbox.

The message action can be selected for voicemail, email, or fax. The actions that can be selected are Accept, Reject, or Relay the Message. A relay address must be specified if the messages need to be relayed.

If the caller enters a digit during the announcement "the called party is not available," an action can be specified per digit. Predefined actions are specified. You can use the asterisk (*) for sign-in and use 0 for the operator. The other digits can be customized with the standard call actions. For example, if a caller selects digit 8, that caller could be transferred to a helpdesk. A custom action can be set up to send the message immediately with urgent priority. Figure 28-6 illustrates message actions and caller input settings that can be configured on the CUC.

Perform the following steps to configure message settings on the CUC.

Step 1. From the user template, select **Edit > Message Settings** from the menu selection at the top of the page.

Step 2. Configure the appropriate settings here and then click **Save**.

- **Maximum Message Length:** Set the recording length, in seconds, that is allowed for messages that callers leave. The default message length is 300 seconds. Users may want to limit the length of messages from callers. However, some departments, such as customer service, may want to permit much longer messages.

- **Callers Can Edit Messages:** Check this box to allow callers to be prompted to listen to, add to, rerecord, or delete their messages. Try to provide balance between giving callers the additional control of editing messages and having voice-messaging ports that are tied up for additional time.
- **Language That Callers Hear:** Choose the language in which system prompts are played to callers. The language setting affects system prompts, such as "you may record your message at the tone." Select from the following options:
  - **Use System Default Language:** CUC plays the system prompts in the system default language.
  - **Inherit Language from Caller:** CUC determines the language to use for system prompts on a per-call basis, depending on the language that is set by the handler or the routing rule that processed the call.
- **Unidentified Callers Message Urgency:** Indicate the action that CUC allows when a caller leaves a message:
  - **Mark Normal:** Messages that callers leave are never marked urgent.
  - **Mark Urgent:** All messages that callers leave are marked urgent. This setting may be useful for sales or technical support calls.
  - **Ask Callers:** CUC asks callers whether to mark their messages as urgent. This setting affects the message notification feature.
- **After Message Action:** Configure the action that CUC performs after a caller leaves a message. By default, the call handler option is set to goodbye, which ends the call with a message. You can configure other call actions to be taken, or you can send a call to any call handler or any user with a mailbox.

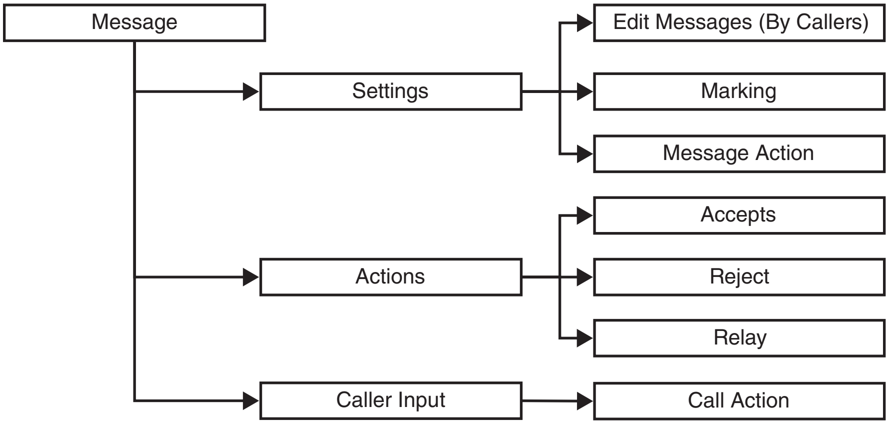


Figure 28-6 *Message Actions and Caller Input Settings on CUC*

TUI Experience

The TUI experience can be modified for the caller and for the CUC user. In the phone menu, the following parameters can be changed. The default value appears in parentheses:

Key Topic

- Conversation volume from low to high (medium); conversation speed from slow to fast (normal)
- Time format (12 hours)
- Timers for entering digits, such as how long to wait for the next digit when entering a name (3 seconds)

After the call, the call action can be selected. For the playback of messages, the following parameters can be modified:

- The volume and speed can be set for playback of the messages.
- Counters can be announced for new messages, faxes, or emails.
- Counter announcement for saved messages can be enabled.
- The order of playing new or saved messages can be set (urgent first, followed in order, based on incoming time).
- Enable the playback of incoming messages from the sender: extension, message number, time of sending the message, and so on.
- Confirm deletions of new and saved messages.

The final task to be covered in this chapter that pertains to the user templates in the CUC covers setting up the TUI. To configure TUI template settings, view the default phone menu settings and then do the following:

Step 1. From the user template, select **Edit > Phone Menus** from the menu selection at the top of the page.

Step 2. Edit the following settings as necessary and then click **Save**.

- **Touchtone Conversation Menu Style:** Choose one of the following options for users when they use a touchtone conversation. Note that the voice-recognition conversation does not offer full and brief menu styles.
  - **Full:** Users hear comprehensive instructions; select this option for a new user.
  - **Brief:** Users hear abbreviated versions of the full menus; select this option for a more experienced user.
- **Conversation Volume:** Choose the volume level at which users hear the CUC conversation: Low, Medium, or High. Users can also adjust the volume temporarily from their phones.
- **Conversation Speed:** Choose the speed at which CUC plays prompts to users: Slow, Normal, Fast, or Fastest.

- **Time Format:** Choose the time format that CUC should use to play timestamps when users listen to their messages by phone:
  - **12-Hour Clock:** This is the default time format. Users hear message timestamps in a 12-hour clock format. For example, users hear "1:00 p.m." when listening to the timestamp for a message that was left at 1:00 p.m.
  - **24-Hour Clock:** Users hear message timestamps in a 24-hour clock format. For example, users hear "1300" when listening to the timestamp for a message that was left at 1:00 p.m.
- **Touchtone Conversation:** Choose the touchtone conversation style that users hear when they listen to and manage their messages by phone. Select either full or brief menu style with each conversation style.
- **Use Voice Recognition Input Style:** Check this box when the user prefers to use voice recognition as the primary way to interact with CUC by phone. When this box is checked, the touchtone conversation setting is used only as a backup when the voice-recognition services are unavailable.
- **Enable Message Locator:** Check the Finding Messages with Message Locator box to allow users to find voice messages from other users and from unidentified callers when they check messages by phone. When this box is checked, users are prompted to find messages from the main menu in the CUC conversation. Users can use the Message Locator feature to search their new and saved messages for messages from a particular user, extension, or phone number based on ANI or caller ID information.

Cisco Unity Connection End Users

Key Topic

If the user templates are predefined, only some individual selections in settings need to be configured when a new user is created in CUC. When creating a user, select the user template, such as the employee user template. The individual parameters that need to be set are a unique alias (ID), the first and last names, a mailbox store if more CUC servers are set up, and the extensions.

The alternate extension is not required but increases productivity and improves the user experience. You can set up alternate extensions, such as the mobile and home phone numbers, so the user can dial the CUC pilot number from these devices and use the personal login, where only the PIN needs to be entered. If a nondefined extension calls in to the CUC system, the standard opening greeting is played by default. Figure 28-7 illustrates the main parameters that need to be configured when creating a new user in CUC manually.

Single or new users can be manually configured very quickly via user templates. If several users need to be created, the users can be added in bulk from a *.csv file, or the users can be imported from an Active Directory or Cisco Unified Communications Manager server. Users can also be migrated and imported from the legacy Cisco Unity server. The COBRAS tool helps administrators migrate users from a Cisco Unity system to a CUC system. The users can be imported with or without their messages.

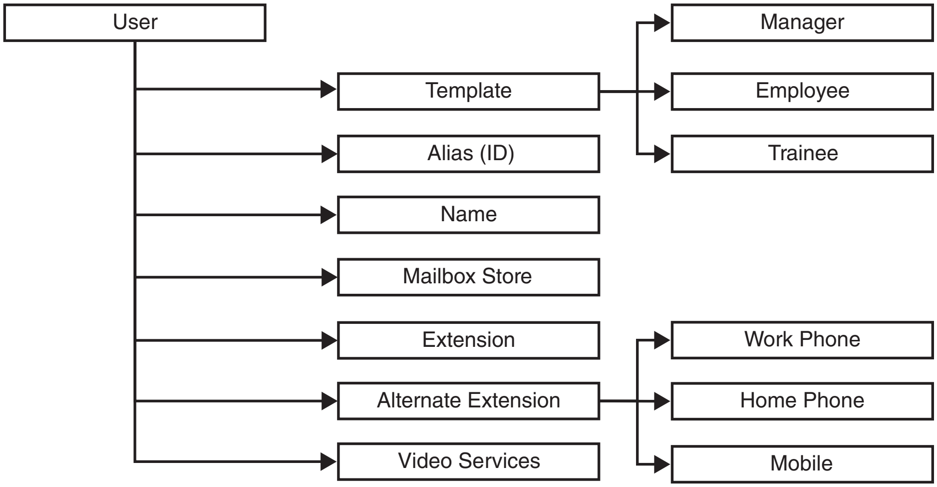


Figure 28-7 *CUC End-User Parameters*

Use the following steps to configure a user in CUC:

Step 1. Create a mailbox for the user.

a. On the Cisco Unity Connection Administration page, navigate to **Users > Users.**

b. Click **Add New**, and on the window that appears, enter the following information:

- **User Type:** Choose the user type, **User With Mailbox** or **User Without Mailbox**, from the drop-down list.
- **Based on Template:** Choose the previously configured or modified user template.
- **Alias:** Enter a unique text name for the user.
- **First Name and Last Name:** Adding the first and last names generates the display name automatically. The voice-recognition conversation may have trouble recognizing display names that contain special characters and diacritical marks. When a user, contact, or distribution list does not have a recorded name, CUC tries to play the display name or the concatenated first and last names.
- **Mailbox Store:** Choose the mailbox store in which the mailbox for the user was created.
- **Extension:** Enter the extension that the phone system uses to connect to the user.
- **Outgoing Fax Number:** Enter the phone number of the fax machine to which the user sends faxes for printing.

c. Click the **Save** button when finished.

Step 2. Create an alternative extension for the user.

a. On the configuration page for the user, select **Edit > Alternate Extensions** from the menu options at the top of the page.

b. Click the **Add New** button.

c. On the Administrator Defined Alternative Extension window, enter the following configuration:

- **Phone Type:** Choose the type of phone from the drop-down list.
- **Display Name:** Enter a descriptive name for the alternate extension.
- **Phone Number:** Enter a unique phone number for the alternate extension. Alternate extensions can be used for various reasons, such as processing multiple line appearances on user phones, mobile numbers, an assistant handling a manager's voicemail, and so on.
- **Partition:** Select the partition by which this extension will be restricted.

Key Topic

Alternate extensions can make calling CUC from an alternate device more convenient, such as a mobile phone, a home phone, or a phone at another worksite. CUC processes all calls from the alternate number in the same way that it processes calls from a primary extension, if ANI or caller ID is passed along to CUC from the phone system. This means that CUC associates the alternate phone number with the user account, and when a call comes from that number, CUC prompts the user to enter a password and sign in. When entering characters in the phone number field, consider the following:

- Enter an extension up to 40 characters in length. SIP integrations can use up to 40 alphanumeric characters.
- Each extension must be unique within the partition.
- For SIP integrations, a valid alias for a SIP URL can be entered. For example, if the URL is SIP:jdoe@cisco.com, enter **jdoe**. Spaces are not allowed.

Step 3. Click **Save** when finished.

To create an alternate name for the user, do the following:

Step 1. On the configuration page for the user, select **Edit > Alternate Names** from the menu selection at the top of the page.

Step 2. In the First Name field, enter a first name, and in the Last Name field, enter the last name.

Step 3. Click the **Add New** button when finished.

This is all the administrator must do to prepare the voice mailbox for a user. At this point, the user can dial into the voice mailbox to complete the setup as follows:

Step 1. From the line on the phone of the user, press the message button or dial the voicemail pilot number.

Step 2. When prompted, enter the PIN followed by **#**.

Step 3. When prompted to configure a recorded name, follow the prompts and record the name of the user.

Step 4. Record a personal greeting if one is desired, such as "I am sorry I am not available to take your call. Please leave a message after the tone."

Step 5. When you are prompted to enter a new PIN, set the PIN followed by **#**. Enter the PIN a second time followed by **#**.

Step 6. Ensure that you are listed in the corporate directory if you want your listing available there.

Alternative to creating users manually one at a time on the CUC, users can be imported from the Cisco Unified Communications Manager. Before importing users from Cisco Unified Communications Manager into CUC, the Cisco AXL Web Service must be enabled on the Cisco Unified Communications Manager. On the CUC, set up a Cisco Unified Communications Manager Administrative XML (AXL) server under the Phone System, which contains the Cisco Unified Communications Manager:

- **IP Address:** Enter the IP address (or host name in full URL format) of the AXL server to which CUC connects.
- **Port:** Enter the AXL server port to which CUC connects. This setting must match the port that the AXL server uses. If a non-SSL port is entered (typically port 80 or 8080), choose a non-SSL version in the Cisco Unified Communications Manager Version field. If an SSL-enabled port is entered (typically port 443 or port 8443), choose an SSL-enabled version in the Cisco Unified Communications Manager Version field.
- **User Name and Password:** Enter the username and password that CUC uses to log on to the AXL server.

After all the settings have been configured, click the Test button to test the connection. A message should be displayed, such as "Test message successfully sent to AXL server <*IP_address*>:443." If the test verification shows a successful result, users can be imported from the Cisco Unified Communications Manager to the CUC. On the CUC, navigate to **Users > Import Users**. To find Cisco Unified Communications Manager users, choose the type of user to import:

Key Topic

- In a co-resident configuration, the users are imported from the default switch.
- In a standalone configuration, choose the Cisco Unified Communications Manager server with the applicable user accounts. Only Cisco Unified Communications Manager servers from which an AXL server is configured appear in the list.
- Choose the user template on which to base the new user accounts. The template affects most user settings. For importing Cisco Unified Communications Manager users, only templates for users with voicemail appear in the list.

When making changes for the end user in Cisco Unified Communications Manager, such as a name change, navigate to **Users > Sync Users.** Choose the relevant users and synchronize them. After the synchronization, the changes will be reflected under **Users > Users.**

Alternative to importing users from the Cisco Unified Communications Manager to CUC, users can be imported from LDAP. The process used to set up LDAP communication on the CUC is the same as it is on the Cisco Unified Communications Manager. On CUC, the Cisco DirSync service must be activated first. In the Navigation menu in the top-right corner of the screen, select Cisco Unified Serviceability and then click Go. Navigate to **Tools > Service Activation** and check the box beside Cisco DirSync. Click Save and confirm the service is activated.

Once the DirSync service is running, an administrator must enable LDAP on the CUC. In the Navigation menu in the top-right corner of the screen, select Cisco Unity Connection Administration and then click Go. Navigate to **System Settings > LDAP > Setup** and configure the following to enable the LDAP system:

- **Enable Synchronizing from LDAP Server:** Check this box so that CUC gets basic information on CUC users from the LDAP directories that are specified on the LDAP directory page. Data is synchronized only for the CUC users who are created by importing users from the LDAP directory. CUC does not automatically create new CUC users when new users are added to the LDAP directory. When LDAP synchronization is enabled, CUC user data for the fields that were imported from the LDAP directory cannot be changed. Change data in the LDAP directory and do one of the following to update the data in CUC:
  - Manually resynchronize CUC data with LDAP data by using the Perform Full Sync Now button on the LDAP directory page.
  - If automatic resynchronization is configured on the LDAP directory page, wait for the next automatic resynchronization to occur.
- **LDAP Server Type:** Choose the type of LDAP server from which CUC gets the user data.
- **LDAP Attribute for User ID:** For LDAP users whose data is imported into CUC, choose the field in the LDAP directory that should appear in the Alias field in CUC. This field must have a value for every user in the LDAP directory. In addition, every value for that field must be unique. LDAP users who do not have any value in this field are not imported into CUC.

After LDAP synchronization has been enabled, the LDAP directory settings must be configured in the CUC. Navigate to **System Settings > LDAP > LDAP Directory Configuration** and configure the following settings:

- **LDAP Configuration Name:** Enter a name for the LDAP configuration. If several LDAP configurations with different LDAP user search bases are added, enter a name that identifies the users in the current search base.
- **LDAP Manager Distinguished Name:** Enter the name of an administrator account in the LDAP directory that has access to data in the LDAP user search base that the

LDAP User Search Base field specifies. CUC uses this account to synchronize CUC data with LDAP data.

- **LDAP Password:** Enter the password for the account that is specified in the LDAP Manager Distinguished Name field.
- **LDAP User Search Base:** Enter the location in the LDAP directory that contains the user data that should be synchronized with CUC user data.

Enter the location in the LDAP directory that contains the user data that should be synchronized with CUC user data. CUC imports all users into the tree or subtree (domain or organizational unit) that the search base specifies. A CUC server or cluster can import LDAP data only from subtrees with the same directory route, such as from the same Active Directory forest. Synchronization can be set up to perform only once or on a regular basis at set intervals. Select the appropriate synchronization setting with the following considerations:

- **Perform Sync Just Once:** Check this box to resynchronize user data in the CUC database with user data in the LDAP directory one time, rather than at regular intervals. If CUC users have already been created from LDAP data, this resynchronization imports updated LDAP data for the existing CUC users. However, if new users have been added to the LDAP directory, this resynchronization does not create new CUC users. Manually create new CUC users by importing them.
- **Perform a Re-Sync Every <*Interval*>:** To resynchronize user data in the CUC database with user data in the LDAP directory at regular intervals, specify the frequency with which the resynchronizations should occur. The minimum interval is six hours. The first resynchronization occurs on the date and time that are specified in the Next Re-sync Time field.

It is important for an administrator to identify user fields that can be populated through an LDAP synchronization and which fields cannot be populated. The rules for field population are the same on the CUC server as they are on the Cisco Unified Communications Manager. Refer to Chapter 16, “LDAP Integration with Cisco Unified Communications Manager,” for a refresher on those fields.

The last setting that should be set up for an LDAP synchronization is the LDAP server address and port 389. When pointing to a Microsoft global catalog, use port 3268 instead.

This section has provided information on how to add users to CUC manually, import users from Cisco Unified Communications Manager, and import users from an LDAP directory. Another way to import users into the CUC system is to use the Bulk Administration Tool. The Bulk Administration Tool allows administrators to import users in bulk from a *.csv file. Navigate to **Tools > Bulk Administration Tool** and configure the following settings:

Key Topic

- **Select Operation:** Choose the applicable bulk operation: Create, Update, Delete, or Export users.
- **Select Object Type:** Choose the applicable type of object: Users (without mailbox), Users with Mailbox, System Contacts, Distribution Lists, Unified Messaging Accounts, Branches, or Video Service Accounts.

- **Override CSV Fields When Creating User Accounts:** Choose Yes or No to indicate whether to override individual CSV field settings with the settings from a user template.
- **Select File:** Enter the complete path of the CSV file and the Failed Objects Filename report file.

Cisco Unity Connection Voice Mailboxes

During the user creation process, the CUC administrator can enable or disable the self-enrollment feature for the user's voicemail box. A new voicemail box needs to be initialized first. This operation can be performed or disabled by the administrator, or it can be performed by the end user after first login.

The user can decide to list a profile in the CUC directory. If a caller selects to dial by name, the directory call handler will search in the directory list for directory list–enabled users. The voice name can be rerecorded. By default, CUC generates the name from the display name, such as John Doe. When John Doe is not available, CUC announces that John Doe is not available instead of using the extension number assigned to that user. Finally, the greeting can be changed from the standard greeting to an alternate personalized greeting.

A voicemail box belongs to a user. A voicemail box needs a storage device. To store the incoming voice messages, a message store on a CUC server must be selected. In a cluster between two CUC servers, the database is shared between both Cisco Unity Connection servers in an active-active relationship. Should one server fail, the other server will retain a copy of all the messages. Figure 28-8 illustrates the active-active relationship between two CUC servers in a cluster.

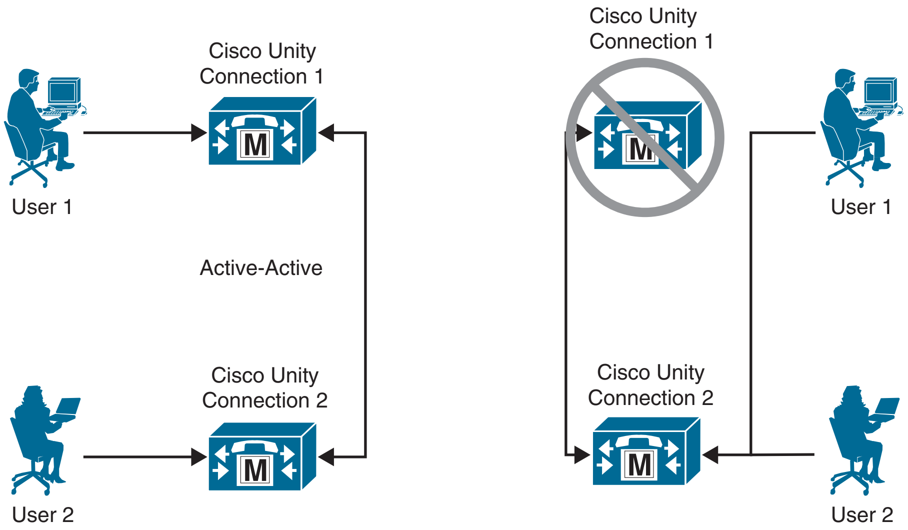


Figure 28-8 *Shared Data Between Two CUC Nodes in a Cluster*

The mailbox store is mostly an informational page. Most of the fields are grayed out, and the page lists the number of mailboxes and their current size. To view the mailbox store, navigate to **Message Storage > Mailbox Stores**. The following fields are available from this page:

- **Display Name:** Enter a name that describes the mailbox store, such as the department whose mailboxes are stored in the mailbox store.
- **Mail Database:** Enter the system name for a specified CUC mailbox store.
- **Server:** Enter the name of the CUC server.
- **Mounted:** To enable complete CUC functionality, check the Access Enabled box. If the Access Enabled box is not checked, CUC users cannot check messages, and mailbox store settings cannot be changed in CUC administration. However, callers can still leave messages, which are queued for delivery when the mailbox store is available again.
- **Number of Mailboxes:** This field shows the number of voice mailboxes in the database that is specified in the Mail Database field.
- **Current Size Before Warning:** This field shows the amount of hard disk space that all messages in the mailbox store currently consume.
- **Maximum Size Before Warning:** If the mailbox store reaches 90 percent of this value in megabytes, CUC logs a warning in the system log file. If the mailbox store reaches 100 percent of this value, CUC logs an error in the system log.
- **Creation Date:** This field shows the date and time when the mailbox store was created.

Administrators can manage the mailbox store membership. They can assign the user membership to a mailbox store by choosing the user and moving that user to another mailbox store. This process can be performed by navigating to **Message Storage > Mailbox Stores Membership**. If more storage space is required, you can create a new message store. Select the user and move that user to another message store if necessary.

The message aging policy will actively manage the storage space for new messages by monitoring what happens with saved and deleted messages. The message aging policy can be managed in the CUC by navigating to **Message Storage > Message Aging > Aging Policies**. The Default System Policy will delete only permanently deleted messages after 15 days. The option for moving new and saved messages can be set in an aging policy as well. Consider the following settings when creating or modifying an aging policy:

- **Enabled:** If message aging rules are selected, check this box to enforce the rules, or uncheck this box to ignore the rules. If no message aging rules are selected, this check box has no effect. The default is Enabled.
- **Move New Messages to the Saved Messages Folder in x Days:** When this aging rule is enabled, CUC automatically moves new messages to the Saved Messages folder the specified number of days after they were received. This option is most commonly used when the message aging for a user is set to Accept and Relay the Message, which causes messages to be forwarded to an email address. If the user always checks voice messages by using the email inbox instead of by using the CUC, checking this box prevents the user's CUC inbox from filling up.

- **Move Saved Messages to the Deleted Items Folder in x Days:** When this aging rule is enabled, CUC automatically moves messages to the Deleted Items folder the specified number of days after they were last saved.
- **Permanently Delete Messages in the Deleted Items Folder in x Days:** When this aging rule is enabled, CUC automatically deletes messages the specified number of days after they are moved to the Deleted Items folder.

One final setting worth mentioning in regard to mailbox settings on the CUC is the mailbox quotas setting. This setting specifies the maximum space per user for message storage in CUC on the system or user level. To set the mailbox quotas level, navigate to **Message Storage > Mailbox Quotas > Mailbox Quotas**. Set the mailbox quota to generate a warning, prevent sending of new messages, or prevent receiving new messages. The following descriptions explain the settings for the mailbox quotas:

Key Topic

- **Warning Quota:** When a user is configured to use system settings for voice mailbox quotas, or on the user level, and when that user's mailbox reaches the size that is specified in the Warning Quota field, the user is warned that the mailbox is reaching the maximum size allowed. The default warning quota is 12 MB. The value for Warning Quota must be smaller than the value for Send Quota, and the value for Send Quota must be smaller than the value for Send/Receive Quota.
- **Send Quota:** The user is prevented from sending any more voice messages.
- **Send/Receive Quota:** The user is prevented from sending or receiving any more voice messages.
- **Full Mailbox Check for Outside Caller Messages:** This setting indicates whether CUC first determines if a user mailbox is full before allowing an outside caller to leave a message for the user. When this box is checked, if the user mailbox is full, the outside caller is not allowed to leave a message. When this box is not checked, CUC does not determine whether the mailbox is full, so the outside caller is allowed to leave the message even if the mailbox is full.

Note that this last setting is applicable only to outside callers. If a CUC user logs on and sends a message to another user, CUC always checks whether the user mailbox is full regardless of whether this setting is enabled or not. The default setting is that the check box is not checked.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 28-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 28-2 Key Topics for Chapter 28

Key Topic Element	Description	Page Number
Paragraph	User Templates in CUC	677
List	User-Related Settings in CUC	678
Paragraph	Three Most Important User Template Settings	681
Paragraph	Three Predefined Transfer Rules	685
List	TUI Parameters That Can Be Changed	689
Paragraph	User Settings Needed for Adding a User Manually to the CUC	690
List	Alternate Extensions for CUC Users	692
List	Types of Users to Import into CUC from CUCM	693
List	Bulk Administration Tool Settings	695
List	Mailbox Store Settings	697
List	Message Aging Settings	697
List	Mailbox Quota Settings	698

Define Key Terms

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

COBRAS, CoS (on CUC), IMAP, TTS, TUI

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the user-related parameters that can be defined within the CUC.
2. Explain the three predefined transfer rules on the CUC.
3. List the five methods of adding users to the Cisco Unity Connection server.

CHAPTER 29

Deploying the Webex Application

This chapter covers the following topics:

Webex App Overview: This topic will review the features and functions of the Webex app when it's deployed with a Cisco Unified Communications Manager.

Register Webex App to Cisco Unified Communications Manager: This topic will examine all the configuration components required to support Webex App registration to the Cisco Unified Communications Manager.

Migrate Cisco Jabber Clients to Webex App: This topic will examine the extra configuration components needed to migrate existing Cisco Jabber clients to Webex App.

These days, every technology is moving toward a more cloud-centric environment. Although there will always be a need for the on-premises solutions we have all been using for so many years, those deployments will become the exceptions to the rule as more companies move to the cloud. Cisco is bridging the gap between on-premises systems and the cloud with several different hybrid solutions. One such solution allows the use of the Webex App with the Cisco Unified Communications Manager. This chapter will delve into how to deploy and use Webex App through the Cisco Unified Communications Manager. The topics discussed in this chapter follow:

- Webex App Overview
    - Webex App Features
    - User Experience with Webex App
    - Architecture for Deploying Webex App
- Register Webex App to Cisco Unified Communications Manager
    - Configure Service Profile
    - Configure UC Service
    - Configure End Users
- Migrate Cisco Jabber Clients to Webex App
    - On-Premises Unified Communications Requirements
    - Jabber-to-Webex Migration Process

This chapter covers the following objective from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 6.4 Deploy Webex App

"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 29-1 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 29-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Webex App Overview	1–3
Register Webex App to Cisco Unified Communications Manager	4–6
Migrate Cisco Jabber Client to Webex App	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 the 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 devices can support the Webex App when registered to the Cisco Unified Communications Manager?

a. Any computer, smartphone, or tablet is supported if the Cisco Unified CSF device is used.

b. Any computer using the Cisco Unified CSF device, or any smartphone using the TCT device, is supported.

c. Any MAC, Windows, or Chromebook computer is supported using the Cisco Unified CSF device.

d. Only Apple iPhones are supported using the TCT device.

2. Which of the following statements is true?

a. Jabber can support Desk Phone mode or Soft Phone mode. Webex can only support Soft Phone mode.

b. Webex and Jabber can support Desk Phone mode or Soft Phone mode.

c. Webex can support Desk Phone mode or Soft Phone mode. Jabber can only support Soft Phone mode.

d. Neither Jabber nor Webex can support Desk Phone mode. They can only support Soft Phone mode.

3. Which of the following calls using the Webex App (Unified CM) would be categorized as "calls through the Cisco Unified Communications Manager environment"?
   - a. Ad hoc meetings from a group space in the Webex App.
   - b. Joining a meeting while paired through Room, Desk, or Board devices.
   - c. Desk phone control (DPC) calls.
   - d. One-to-one calls that are placed directly in the Webex App to a free user in the consumer organization.
4. What version of the Cisco Unified Communications Manager is required to support Webex App installation on both Android and Apple phones?
   - a. 11.5(1) SU3 or later.
   - b. 11.5(1) SU8 or later.
   - c. 12.0 or later.
   - d. 14.0 or later.
   - e. Neither Android not Apple phones can support Webex App when registered to the Cisco Unified Communications Manager.
5. An engineer is preparing the Cisco Unified Communications Manager to support Webex App registration. What is the first setting that needs to be configured?
   - a. UC Services
   - b. Service Profile
   - c. End User Settings
   - d. Device Phone
6. Which of the following devices uses a display with less than 600dp?
   - a. iPhone
   - b. iPad
   - c. Android Tablet
   - d. Android Phone
7. How is the Common Identity established on Webex Control Hub?
   - a. By matching the user's email attribute in on-premises Unified Communications and the Webex platform
   - b. By matching the user's sAMAcountName attribute in on-premises unified communications and the Webex platform
   - c. By performing LDAP synchronization on Cisco Unified Communications Manager
   - d. By performing CSV import on the Webex platform
   - e. By comparing the user's first and last name in on-premises unified communications and the Webex platform
8. Which two services can Webex App use from the service profile in Cisco Unified Communications Manager? (Choose two.)
   - a. Mailstore
   - b. Voicemail
   - c. CTI
   - d. Conferencing

  - **e.** Directory
  - **f.** IM and Presence Service

9. Which UC Service Configuration parameter will enable the Cisco Jabber migration tool to copy contacts to Webex App?

  - **a.** EnableJabber2TeamsMigration
  - **b.** WebexTeamsDownloadURL
  - **c.** EnableJabber2WebexMigration
  - **d.** EnableWebexMigration
  - **e.** EnableWebexMigrationTool

Foundation Topics

Webex App Overview

The Calling in Webex App (Unified CM) solution lets you register Webex App directly to your Cisco Unified Communications Manager call control environment (on-premises enterprise, Business Edition 6000/7000, Cisco Unified Communications Manager Cloud, or delivered through an HCS partner solution).

This solution enhances the calling experience for end users, allowing them to directly make calls in Webex App through the Cisco Unified Communications Manager environment, use midcall features, and control their desk phone from Webex App.

When dialing from Webex App, users can use the same dial strings or prefixes as they do on their desk phones; Webex App functions like any other desk phone registered to the Cisco Unified Communications Manager. Cisco Unified Communications Manager calls that are established in Webex App use the configuration that's in place for the Cisco Unified Communications Manager deployment (such as location, bandwidth settings, point to point media, and so on).

As an administrator of Calling in Webex App (Unified CM), you reuse your existing Cisco Unified Communications Manager and Mobile and Remote Access (MRA) configuration you may have already had in place. The deployment model is similar to Jabber. The same device types are used: In Soft Phone mode, Webex App registers as a SIP device with the product type "Cisco Unified Client Services Framework" or CSF for desktop, TCT or BOT for mobile, and TAB for tablets. Alternatively, Webex App can connect to Cisco Unified Communications Manager using computer telephony integration (CTI) to control the user endpoints.

The Webex App makes its primary connection to the Webex cloud to get its service configuration (messaging, meetings, presence, contact lists, calling behavior, and so on). The Webex app will also retrieve the address for the Cisco Unified Communications Manager from the Webex cloud so that it can obtain the following configuration settings from the Cisco Unified Communications Manager. These settings are the same settings used by Cisco Jabber providing specific calling functionality to users:

- Initial Cisco Unified Communications Manager discovery through DNS query to discover any configured voice services domain. (In a multicluster environment, Intercluster Lookup Service is also leveraged to determine which cluster the Cisco Unified Communications Manager user is homed to.)

- An outside domain (MRA deployment) is also discovered. (If the Webex domain does not match the existing Voice Services Domain, you can set a Voice Services Domain in Webex Control Hub and associate it with specific users.)
- UC service profiles (for voicemail through Unity Connection, CTI services, and advanced calling functionality through supported parameters in the Jabber config service profile or XML file).
- Single sign-on (SSO) credentials if an Identity Provider (IdP) is integrated.
- Oath tokens, including refresh and expiry timers. (Users need to reauthenticate if a session expires.)
- Certificate validation.

Webex App Features

Integrating the Webex App with the Cisco Unified Communications Manager provides many feature sets in Webex App for desktop (Windows and Mac) and mobile (Android, iPad, and iPhone). You can answer calls with and without video, place calls and end calls, mute and unmute the microphone in a call, and enter DTMF tones when you need to make menu selections. Webex operates in both Desk Phone mode and Soft Phone mode, the same as Cisco Jabber. In the Webex App, users who are in the same organization can see the presence indicator of other users during an active call. Many other features are supported on the Webex App when registered to the Cisco Unified Communications Manager, and each one holds significant value. Although there are too many to name here, the following is a list of some of the more common features:

Key Topic

- **Call pickup:** If a user is in a customer support role and their coworker isn't able to answer an incoming call to their phone, the support user gets a notification in Webex App if both are in the same pickup group. That user can answer the call from the notification in the app. The user can also pick up the calls in other pickup groups.
- **Call recording:** You can determine how much control users have over recording calls. Depending on the setup, incoming and outgoing calls may be recorded automatically, or you may be able to decide which calls you want to record. If you enable users with call recording, they can start and stop recordings at their own discretion. When a call is being recorded, that recording continues whether a user moves the call to another device, merges the call with another active call, or makes a conference call. They're presented with a visual indicator letting them know when a call is being recorded.
- **Call waiting:** When a user is already in call and someone else calls, the called user can choose how they want to handle the incoming call. For example, the user can put the active call on hold and answer the second call.
- **Conference calls:** When users are on a call with someone else, they might want to add other people into the call to start a conference call right away. They can add up to eight other people into conference calls started in this way.
- **Control your video device from the app:** Users can start or stop sharing a video on a connected video device right from the app. For example, if users are connected to a

Cisco Webex Board and they don't want to share video, they no longer have to walk up to the board and turn off the video. They can turn it off from the app.

- **Hold/resume:** Users can place a call on hold and resume it in Webex App.
- **Hunt groups:** Users can sign in or out of a hunt group from Call Settings. When they're signed in and a call comes into a group that they belong to, they'll see the hunt group number on the incoming call notification.
- **Merge:** Users can take two active calls and merge them into a single conference call in Webex App.
- **Mirror self-view:** By default, when users share video during a call, they can see themselves just like they're looking in a mirror. If they text behind them and want to read it easily instead of having to read it backwards, they might want to turn off the **Mirror my video view** setting. This setting doesn't affect the way other people in the meeting see them.
- **Move a call into a meeting:** Users in a call can take advantage of advanced meetings features such as transcriptions, real-time translations, notes, action items, recordings, and whiteboarding. They just move that call into a full-featured meeting. Before moving the call into a meeting, users can even invite other people into the discussion.
- **Multiline:** Users can use up to eight phone lines with Webex App and leverage advanced calling features on each line, such as call forward, transfer, hunt group, shared lines, and voicemail. They can also assign different ringtones to each line. In addition, users can turn on presence for shared lines so that the line status is displayed for them.
- **Park and retrieve calls:** A user can park a call on one device and that user or someone else can retrieve the call from another device.
- **Resume from different devices:** A user can put a call on hold from the desktop app and resume it on mobile. Conversely, they can put a mobile call on hold and resume it on a desk phone. They can go any direction between desk phone, mobile, and desktop just by putting the call on hold and resuming wherever it's convenient.
- **Screen sharing:** Share content from a computer screen during a call in Webex App. Users can choose a specific application to share, rather than having to share their whole screen. If a user answers on a desk phone, a screen share is still possible. The phone user sees the shared screen from the phone if it supports video; otherwise, they'll see the shared screen from the app. Users can share their screen regardless of whether the person they called is using a cloud-registered device or an on-premises device. The screen share is still sent with a high frame rate (30 FPS), high resolution (1080p), and includes audio.
- **Switch between front and back cameras:** On mobile phones or tablets, you can switch between front-facing and back-facing cameras.
- **Transfer:** Users can redirect a connected call within Webex App. The target is the user to which another user wants to transfer the call.

- **Virtual cameras:** During a call, users can choose to use a virtual camera. A virtual camera, such as an application, driver, or software, can be used to create an overlay of video, images, or feeds.

Any desk phones or Extension Mobility profiles that are associated with the user's Cisco Unified Communications Manager account are listed as an available device to connect to in Webex App for Windows or Mac. If the device is selected, Cisco Unified Communications Manager calls that are dialed from or answered in Webex App use that desk phone. Users can start or stop the call, enter DTMF input (which the phone acknowledges), and use the midcall features documented in the preceding feature list. Users can also join meetings from Webex App in Desk Phone control mode. Users can access the description of their desk phone right from their desktop app and personalize that description to something that makes sense. They can hover over the phone description and then click the pencil icon to change the name. If more than one desk phone is assigned to users, customizing each description can be helpful.

User Experience with Webex App

The user experience with the Webex App is pretty consistent for most types of calls; however, some differences in how calls are routed should be noted. Table 29-2 lists what types of Webex App calls go through Cisco Unified Communications Manager and what types of Webex App calls or meetings instead go "over the top" as calls to cloud microservices.

Key Topic

Table 29-2 Comparison of Calls Through Cisco Unified Communications Manager and Calls/Meetings Through the Cloud

Calls Through Cisco Unified Communications Manager Environment	Calls and Meetings Through Webex Cloud
Calls initiated directly from a 1:1 space or from a contact card in the Webex App.	Ad hoc meetings from a group space in the Webex App.
Searching and then calling a user in the Webex App.	Using the Join button in the Webex App to join an ad hoc or scheduled meeting.
Dialing directory numbers or PSTN numbers from the Call button in the Webex App.	Dialing on-premises Directory URIs from the Call button in the Webex App. (Depends on the Cisco Unified Communications Manager SIP Address Routing setting in Control Hub.)
Desk phone control (DPC) calls. (For outgoing calls, dial a directory or PSTN number in the Webex App and take the call on the Cisco Unified Communications Manager device; for incoming calls, answer the call in Webex App and take the call on the device.)	Joining a meeting while paired through Room, Desk, or Board devices.
	One-to-one calls that are placed directly in the Webex App to a free user in the consumer organization, to a user in another organization, or to a user in the same organization who doesn't have a directory number. (Numbers are not shared across organizations, so they don't appear in contact cards.) These are classified as a call on Webex App.

For users who are paired to a cloud-registered Room, Desk, or Board device, Cisco Unified Communications Manager registration in the Webex App stays active. Incoming calls to a user's directory number are presented in Webex App and, when accepted, calls are answered on the desktop app and do not use the paired Room, Desk, or Board device. If the Webex device is configured in Control Hub as a Workspace that is enabled for Hybrid Calling, the user can dial from Webex App and the call then starts on the Webex device using that device's directory number as the caller ID on the receiving end. A user cannot answer an incoming call to a paired device. If the Webex device is not in a Workspace that's enabled for Hybrid Calling, the directory number or PSTN dialing fails and an error message is presented in the user's Webex App.

For users who are in desk phone control mode in Webex App, media (that is, audio and video) for 1:1 calls to users with contact cards and calls that are started from the search or dial view go through the on-premises desk phone. Media for group space meetings, Webex meetings whether scheduled or ad hoc, and calls to users without contact cards go through the on-premises desk phone.

For scenarios involving a call going to voicemail, incoming calls that don't go through Cisco Unified Communications Manager do not roll over to voicemail and continue to ring until the user answers or declines. Incoming calls that go through Cisco Unified Communications Manager, such as to a user's corporate directory number, roll over to voicemail.

Architecture for Deploying Webex App

The architecture used to support Webex App deployments differs based on whether the app is used on the network or remotely. When the Webex App is being used on the network, it will still make a connection directly with Webex Control Hub through the firewall for IM and Presence capabilities. The Control Hub will then redirect the application to register to the Cisco Unified Communications Manager for on-premises-based calling. User synchronization must exist between user accounts on Cisco Unified Communications Manager and Webex Control Hub before this setup will work. Cisco recommends using Lightweight Directory Access Protocol (LDAP) synchronization on Cisco Unified Communications Manager and then setting up Webex Control Hub with Active Directory (AD) synchronization through the Directory Connector. Other services, such as Cisco Unity Connection, can also be used with the Webex App in this scenario. Messages can be sent, presence status can be observed, and calls can be placed once registration has been completed to Webex Control Hub and Cisco Unified Communications Manager.

The Directory Connector is an application that can be downloaded from the Webex Control Hub and installed on a Windows server where Microsoft AD lives. Alternatively, Directory Connector can be installed on any computer being managed by AD. Once installed, Directory Connector can be configured and will act as the liaison between AD and Webex Control Hub. User synchronization happens automatically once users exist in Webex Control Hub and Cisco Unified Communications Manager that have the same email address associated with their accounts. Figure 29-1 illustrates an architecture where Webex App is used on a network.

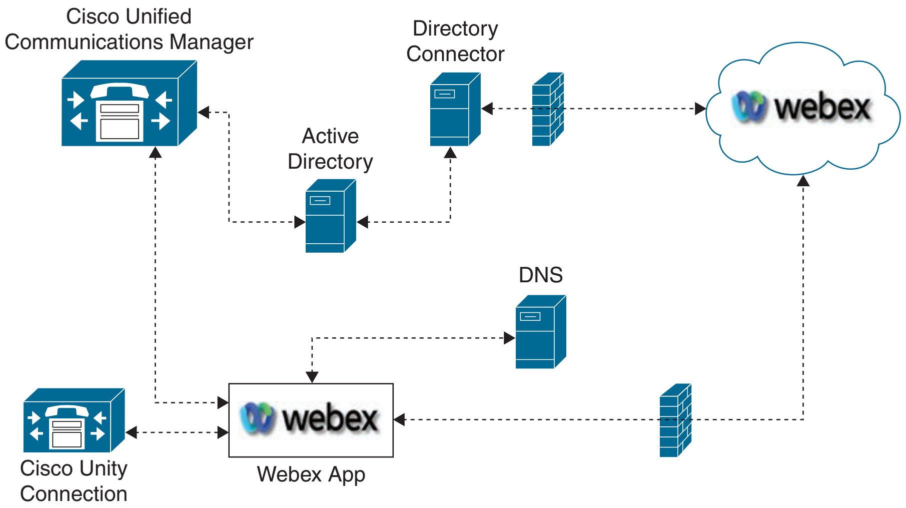


Figure 29-1 *Architecture for Deploying Webex App on a Network*

When the Webex App is being used remotely, another set of server components must be used to allow communication through the firewall between Webex App and Cisco Unified Communications Manager. These servers are the Expressway Core and Expressway Edge setup for MRA. All other components and configuration requirements remain the same for Cisco Unified Communications Manager, Webex Control Hub, and user synchronization. Figure 29-2 illustrates an architecture where Webex App is used remotely.

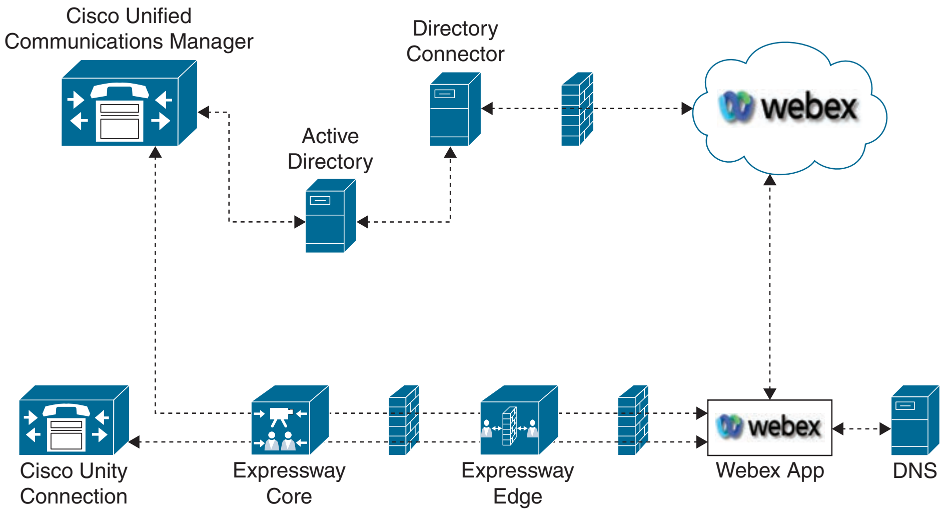


Figure 29-2 *Architecture for Deploying Webex App Remotely*

Register Webex App to Cisco Unified Communications Manager

To enable Calling in Webex App (Unified CM), you must use one of the supported Cisco Unified Communications Manager–based Cisco call control solutions and ensure that you're on the minimum supported version or later. For example, Cisco Unified Communications Manager and Android release 11.5(1) SU3 or later are required for Firebase Cloud Messaging (FCM). If you need to support iOS, release 11.5(1) SU8 is required for Apple push notifications (APN). If you upgrade the Cisco Unified Communications Manager from version 11.5, you might need to be sure you're on the correct SU version to support iOS or Android. Correct versions might vary if you're using a Hosted Collaboration Solution (HCS) or a Cisco Unified Communications Manager Cloud solution. Check current documentation before deploying. Additionally, the Cisco Expressway Edge and Core traversal pair for MRA requires version X8.11.4 or later for Calling in Webex App (Unified CM). Added security is provided starting with this release and later.

Many Cisco Unified Communications Manager features are automatically available in Webex App after you configure your environment; however, certain features need to be preconfigured in Cisco Unified Communications Manager for them to work in Webex App. There are too many features to list in this chapter; however, the following is a sampling of some features:

- Auto-answer on a directory number that is assigned to the user
- The Call Park feature
- Call Recording
- Dial plan mapping
- The Dial via Office (DvO) feature and DvO-R (DvO-Reverse)
- Extend and Connect feature
- Multiple phone lines
- Cisco Unified Survivable Remote Site Telephony (SRST)
- Voicemail in Webex App through Cisco Unity Connection
- Wi-Fi to LTE Call Handoff
- Wireless access point (AP) location monitoring

When using Calling in Webex App (Unified CM) over your corporate Wi-Fi network, Cisco recommends that you design your Wi-Fi network to eliminate gaps in coverage as much as possible, including in areas such as elevators, stairways, and outside corridors. Ensure that all access points assign the same IP address to the mobile device. Calls are dropped if the IP address changes during the call. Ensure that all access points have the same service set identifier (SSID) because the hand-off might be much slower if the SSIDs do not match. Ensure that all access points broadcast their SSID. If the access points do not broadcast their SSID, the mobile device may prompt the user to join another Wi-Fi network, which interrupts the call. Ensure that the enterprise firewall is configured to allow the passage of Session Traversal Utilities for NAT (STUN) packets.

Conduct a thorough site survey to minimize network problems that could affect voice quality. Cisco recommends that you verify nonoverlapping channel configurations, access point coverage, and required data and traffic rates. Eliminate rogue access points, and identify and mitigate the impact of potential interference sources.

There are many other requirements you may need to verify before setting up your environment to use the Webex App. Be sure to consult the most recent deployment guide before proceeding in a production environment. Once you have met all the prerequisites for supporting Webex App in your environment, you can proceed with the configurations needed.

Configure UC Services and Service Profile

The first setting that needs to be configured in the Cisco Unified Communications Manager to support the Webex App is UC Services. UC services go hand-in-hand with a service profile, which allows you to bundle UC services together. First, you must create a CTI service that provides Webex App with the devices associated with the user. You can also create a voicemail service if you want users to have access to voicemail in Webex App. At the end, create a service profile to add the UC services that later get applied to end-user accounts.

First, set up the relevant UC services for your Calling in Webex App (Unified CM) deployment. The CTI service is required. The UC Services provides Webex App with the location of the CTI service, which retrieves a list of devices that are associated with the user. Add Cisco Unified Communications Manager services to specify the address and other settings for the service. The CTI UC service provides Webex App with the location of the CTI service, which retrieves a list of devices associated with the user. The voicemail service ties into the existing Unity Connection deployment and provides voicemail retrieval to users when they are associated with the corresponding service profile. To set up the relevant UC services for your Calling in Webex App (Unified CM) deployment, use the following steps:

Key Topic

Step 1. Open the Cisco Unified CM Administration interface. Select **User Management > User Settings > UC Service**. The **Find and List UC Services** window opens.

Step 2. Select **Add New**. The **UC Service Configuration** window opens.

Step 3. In the **Add a UC Service** section, select **CTI** from the **UC Service Type** drop-down list. Select **Next**.

Step 4. Provide details for the CTI service as follows:

a. Specify a name for the service in the **Name** field. The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.

b. Specify the CTI service address in the **Host Name/IP Address** field. Enter the address in the form of a hostname, IP address, or fully qualified domain name (FQDN). This value corresponds to the Cisco Unified Communications Manager publisher that's running the CTI Manager service. You'll create a second service for the subscriber.

c. Specify the port number for the CTI service in the **Port** field.

Step 5. Save your changes.

Set up the voicemail service if you have Unity Connection deployed and want to integrate voicemail access into Webex App. The voicemail service ties into your existing Unity Connection deployment and provides voicemail retrieval to users when they are associated with the corresponding service profile. If you're configuring voicemail access for Webex App users, ensure that you identify a directory number in your Cisco Unified Communications Manager deployment to use for voicemail system access. To set up the voicemail service, perform the following steps:

Key Topic

Step 1. Return to **User Management > User Settings > UC Service** and then click **Add New**.

Step 2. Choose **Voicemail** and then click **Next**.

Step 3. Provide details for the voicemail service as follows:

a. Specify a name for the service in the **Name** field. The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.

b. Specify the voicemail address in the **Host Name/IP Address** field. Enter the address in the form of a fully qualified domain name (FQDN). Otherwise, the certificate validation step fails.

NOTE By default, the client always uses port 443 and the HTTPS protocol to connect to the voicemail server. For this reason, any value you specify does not take effect.

Step 4. Save your changes.

After you add and configure Cisco Unified Communications Manager services, you add them to a service profile. You can also apply additional configuration in the service profile, as needed, by following these steps:

Key Topic

Step 1. Open the **Cisco Unified CM Administration** interface and go to **User Management > User Settings > Service Profile**.

Step 2. Create a new service profile and enter a name for it in the **Name** field.

Step 3. Select **Make this the default service profile for the system** if you want the service profile to be the default for the cluster.

Step 4. Add your UC services under **Voicemail Profile** and **CTI Profile**.

Step 5. Set **Credential source for voicemail service** to **Unified CM – IM and Presence**.

Step 6. Complete any additional configurations and then click **Save**.

Configure End Users

For Calling in Webex App (Unified CM) to work, you must create new users or configure existing users on Cisco Unified Communications Manager with the settings in the list that follows. If you use LDAP synchronization, these settings may already be in place.

Step 1. From **Cisco Unified CM Administration**, go to **User Management** > **End Users**, choose any criteria, click **Find**, and then open the user account that you want to configure.

Step 2. Verify that **Mail ID** contains the user’s email address.

NOTE If you're using server information for configuration and not SRV records, your users' Webex App email addresses must match their Cisco Unified Communications Manager email addresses—at a minimum, the user ID portion before the domain must match.

Step 3. Under the user's **Service Settings**, check the **Home Cluster** box.

Configure this setting on the Cisco Unified Communications Manager where each user is homed and where their devices are registered.

Optionally, you can choose your service profile from the **UC Service Profile** drop-down list you created earlier (with CTI service and voicemail) if you need to make user-level overrides.

Step 4. Save your changes and then you'll assign applicable roles to the user.

Step 5. Click **Add to Access Control Group**.

Step 6. Click the corresponding check box for each access control group you want to assign to the end users.

At a minimum you should assign the user to the following access control groups:

- Standard CCM End Users
- **Standard CTI Enabled:** This option is used for desk phone control.

Certain phone models require additional control groups, as follows:

- For Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- For Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

To make the Webex App a soft phone client, create at least one device for every user you're configuring for Calling in Webex App (Unified CM). Webex App for desktop and mobile registers to Cisco Unified Communications Manager using the same soft phone device types as Cisco Jabber. If you want any user to only have desk phone control and no soft phone functionality, you do not need to create a desktop CSF device for them. The steps that follow outline how to create a device for the Webex App soft phone client:

Step 1. Log in to the **Cisco Unified CM Administration** interface.

Step 2. Select **Device > Phone**. The **Find and List Phones** window opens.

Step 3. Select **Add New**.

Step 4. From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.

For Webex App users, you can only create one type of device per platform for a user, although you can create multiple devices for each user. For example, you can create one dual-mode mobile device and one CSF device, but not two CSF devices. Webex App uses density-independent pixels (dp) to identify Android devices. A dp is a unit of length for screen size, typically used in mobile software to scale an app display to different screen sizes. Devices with displays that are 600dp or greater are identified as tablets; devices with less than 600dp are identified as phones. The following is a list of devices that can be used for the Webex app depending on the platform you are using.

- **Cisco Unified Client Services Framework:** Select this option to create a CSF device for Webex App for Mac or Webex App for Windows.
- **Cisco Dual Mode for iPhone:** Select this option to create a TCT device for Webex App for iPhone users.
- **Cisco Jabber for Tablet:** Select this option to create a TAB device for Webex App on an iPad, Android tablet, or Google Chromebook. For Android, Webex App identifies devices with displays that are 600 density-independent pixels (dp) or greater as a tablet. The device shows the Tablet UI left and right layout, the right panel shows the space chat content or profile detail page, and you should choose the TAB soft phone device type in Cisco Unified Communications Manager.
- **Cisco Dual Mode for Android:** Select this option to create a BOT device for Webex App for Android phone users. Webex App identifies devices with displays that are under 600dp as a phone. The device shows the Phone UI vertical layout, and you can choose the BOT soft phone device type in Cisco Unified Communications Manager.

Users can be signed in to phone service on one device type for each platform (for example, Webex App for a Windows device and Webex App for an iPhone). Users can’t be signed in to phone service on more than one device type on the same platform (for example, Webex App for an iPad and Webex App for an Android tablet). While Chromebook users require a TAB device to use Calling in Webex App Unified CM, phone service does work for a user with both a Chromebook and an Android phone signed in at the same time.

Step 5. From the **Owner User ID** drop-down list, select the user for whom you want to create the device.

Step 6. In the **Device Name** field, use the applicable format to specify a name for the device. Table 29-3 identifies acceptable formats for each device type.

Key Topic

Table 29-3 Device Name Format for Soft Phone Devices

Device Type	Required Format
Cisco Unified Client Services Framework	Valid characters: a–z, A–Z, 0–9. 15-character limit.
Cisco Dual Mode for iPhone	The device name must begin with *TCT*. For example, if you create a TCT device for the user Tanya Adams, whose username is tadams, enter **TCTTADAMS**. Must be uppercase. Valid characters: A–Z, 0–9, period (.), underscore (_), and hyphen (-). 15-character limit.

Device Type	Required Format
Cisco Jabber for Tablet	The device name must begin with *TAB*. For example, if you create a TAB device for the user Tanya Adams, whose username is tadams, enter **TABTADAMS**. Must be uppercase. Valid characters: A–Z, 0–9, period (.), underscore (_), and hyphen (-). 15-character limit. For Android, Webex App identifies devices with displays that are 600dp or greater as a tablet.
Cisco Dual Mode for Android	The device name must begin with *BOT*. For example, if you create a BOT device for the user Tanya Adams, whose username is tadams, enter **BOTTADAMS**. Must be uppercase. Valid characters: A–Z, 0–9, period (.), underscore (_), and hyphen (-). 15-character limit. For Android, Webex App identifies devices with displays that are less than 600dp as a phone.

Step 7. For mobile devices only (TCT, BOT, and TAB), in the **Product Specific Configuration Layout** section, enter any designated emergency numbers in **Emergency Numbers** to route emergency calls through the user's mobile provider.

You can enter a comma-separated list of additional emergency numbers that users can direct dial. These numbers must contain only numerical digits; Cisco does not allow spaces, dashes, or other character.

Emergency numbers as defined on the device are always dialed direct using the mobile network instead of through the enterprise environment. Use direct-dial numbers for users who frequently travel to countries other than the country of their mobile network provider, if the emergency number differs depending on the location, or if your organization uses a dedicated security number.

Step 8. Select **Save**.

Step 9. Click **Apply Config**.

After you create and configure each device, you must add a directory number to the device, as follows:

Step 1. Locate the **Association Information** section on the **Phone Configuration** window.

Step 2. Click **Add a new DN**.

Step 3. In the **Directory Number** field, specify a directory number.

Step 4. In the **Users Associated with Line** section, click **Associate End Users**.

Step 5. In the **Find User where** field, specify the appropriate filters and then click **Find**.

Step 6. From the list that appears, select the applicable users and click **Add Selected**.

Step 7. Specify all other required configuration settings, as appropriate.

Step 8. Select **Apply Config**.

Step 9. Select **Save**.

Next, you will need to associate the users with their assigned devices, as follows. A soft phone device for Webex App should not be associated to multiple users if you intend to use different service profiles for these users.

Step 1. Open the Unified CM Administration interface.

Step 2. Select **User Management > End User**.

Step 3. Find and select the appropriate user. The End User Configuration window opens.

Step 4. Select **Device Association** in the Device Information section.

Step 5. Associate the user with devices as appropriate.

Step 6. Return to the **End User Configuration** window and then select **Save**.

Once you have associated the user with the device, the final step is to set the **User Owner ID** field in the device configuration:

Step 1. Select **Device > Phone**.

Step 2. Find and select the appropriate device. The **Phone Configuration** window opens.

Step 3. Locate the **Device Information** section.

Step 4. Select **User** as the value for the **Owner** field.

Step 5. Select the appropriate user ID from the **Owner User ID** field.

Step 6. Select **Save**.

Your Webex App is now ready to use. Up to this point we have covered how to deploy calling with Webex App (Unified CM) from a greenfield deployment. In most cases, a company using the Cisco Unified Communications Manager for calling already used Jabber as its soft client of choice. Those customers who want to migrate from Jabber to the Webex App have a few more steps to take.

Migrate Cisco Jabber Clients to Webex App

To migrate a Cisco Jabber user to the Cisco Webex App, you must have an existing working environment for Cisco Jabber on-premises and a Webex Control Hub subscription. The migration process includes registering Cisco Jabber locally and via Mobile and Remote Access (MRA) for calling services and creating a service profile so that Cisco Jabber can access additional services. These services include computer telephony integration (CTI) and desktop phone control, Cisco Unified Communications Manager IM and Presence Service, voicemail, and Cisco Webex for conferencing. Although Cisco Jabber can use all these services, they are not mandatory for you to configure. For example, if you do not use CTI to control physical phones or you do not use voicemail, you do not have to include these services in the service profile. However, a working environment is required before you can prepare Webex Control Hub to support Cisco Jabber user migration to Cisco Webex App.

If you are planning to use calling from the Cisco Unified Communications Manager, you do not need to use the migration wizard through Cloud Connected Unified Communications. This tool is used to migrate calling from on-premises to the cloud. Before you can use the migration wizard on Webex Control Hub, you must meet several requirements. On Webex Control Hub, complete the following tasks:

Key Topic

- **Access the Webex Control Hub with full administrative privileges:** To access and configure Webex Control Hub, you must have administrative privileges. With full administrative privileges, you can verify who has sufficient privileges by checking user account roles in the Control Hub.
- **Add a cluster of Cisco Unified Communications Managers and IM and Presence Service servers to Cloud Connected UC:** Add on-premises servers to Cloud Connected UC to enable Webex to gather the required information about users and clusters.
- **Activate Deployment Insight services for Cisco Unified Communications Managers and IM and Presence Service servers:** Responsible for collecting configuration details from on-premises servers that connect to the cloud.
- **Remove Hybrid Calling, if used:** This outdated feature should be removed and Cisco Expressway Hybrid should be decommissioned before you assign Calling in Webex App in Cisco Unified Communications Manager.
- **Synchronize users to Common Identity:** User synchronization is an important and mandatory part of migration because a common identity between two different solutions needs to be established. This piece is required when you plan to use the Webex Control Hub for IM and Presence, as mentioned earlier in this chapter.

Cisco Jabber uses the following:

- User identification with *username@domain*
- Directory services from an LDAP server or from Cisco Unified Communications Manager User Data Service (UDS)
- Contact pictures from LDAP attributes or a web server

Cisco Webex App uses the following:

- User identification with a user's email address
- Directory services from the Webex platform
- Contact pictures from the Webex platform

Although there are multiple options for adding users to Webex Control Hub, Cisco recommends that you synchronize users with Webex Control Hub. Typically, users in Cisco Unified Communications Manager are already synchronized from the Active Directory, so you should use Cisco Directory Connector or the User and Contact Synchronization tool that is built in to the Cloud Connected UC function to synchronize users to the Webex platform. If you need a refresher on how to use Directory Connector, review Chapter 23, "Adding Users and Devices in Webex Control Hub." A Common Identity is established by matching email attributes on the Cisco Unified Communications Manager end-user list and Webex Control Hub users list. When the mail parameter of a user on the Webex platform does not match the end user on Cisco Unified Communications Manager, that user is not considered to be the same individual and will not be in the list for migrating from Cisco Jabber to the Webex App.

When you synchronize users to Webex Control Hub, make sure that all users are synchronized, even if you do not want them to use Webex services. Webex App uses directory services from the Cisco Webex users list and will not be able to find unsynchronized user information when searching contacts with Webex. Therefore, you should ensure that all users with common information, telephone, and mobile numbers are synchronized.

Webex App obtains user pictures or avatars from the Webex platform, and you must either add user avatars manually on the Webex platform or synchronize them with Cisco Directory Connector. Cisco Directory Connector can obtain user pictures from a web server or an Active Directory attribute and send them to the Webex platform.

On-Premises Unified Communications Requirements

Consider the following when you prepare Cisco Unified Communications Manager to allow Cisco Jabber migration to Webex App:

- You must enable Cisco Jabber migration of contacts and preferences to Webex App.
- You must enable Webex to use voicemail and CTI control features.

You can create a service profile on Cisco Unified Communications Manager by using the UC Service Profile drop-down so that the migration tool in Cisco Jabber can migrate contacts and preferences to Webex App as follows:

- Contacts
- Directory contacts
- Custom contacts
- Federated contacts
- Preferences
- Notification settings
- Audio and video device selection
- Video preferences for incoming calls

When you enable the Cisco Jabber migration tool, Cisco Jabber synchronizes the contact list and preference data to the Webex App on the user's device. Webex App writes the data to the user profile service in the Cisco Webex platform. A user can either run the migration tool on Cisco Jabber manually from the Help menu or wait for Cisco Jabber to present the tool sometime between 5 minutes and 3 hours later. When you migrate Cisco Jabber users to the Webex App, you need to create a service profile to continue using voicemail and CTI control features. Cisco Jabber relies on the service profile in Cisco Unified Communications Manager to enable the following services:

- Voicemail
- Mailstore
- Conferencing
- Directory
- IM and Presence Service
- CTI
- Video Conference Scheduling Portal
- Cisco Jabber Client Configuration

The Webex App relies on the service profile in Cisco Unified Communications Manager to enable the following services:

- **Voicemail:** Access visual voicemail services with Webex App.
- **CTI:** Allow desk phone control mode with Webex App.
- **Cisco Jabber Client Configuration:** Allow advanced calling functions with Webex App. The rest will be ignored, so it is recommended that you use only relevant Cisco Jabber configuration parameters for the Webex App.

The remaining services are ignored and can be deleted after Cisco Jabber is successfully migrated to Webex App.

Jabber-to-Webex Migration Process

Migrating Cisco Jabber to the Webex App involves preparing Cisco Unified Communications Manager with an extra service profile and configuring Cisco Webex Control Hub with onboarding Webex Cloud Connected UC, enabling Deployment Insight services, and establishing a Common Identity. When all prerequisites are met, you can run the migration wizard on Cisco Webex Control Hub and decide which users to migrate to Webex App by choosing different user filtering and Unified Communications calling options.

In Cisco Unified Communications Manager, prepare two service profiles for migration. The first will be used to transfer Cisco Jabber contact and preference data to Cisco Webex and for filtering when the migration wizard is run on the Webex Control Hub. After users are migrated to Webex, the second profile is used to allow Webex to use CTI control and access visual voicemail services.

Key Topic

The high-level configuration steps on Cisco Unified Communications Manager are as follows:

Step 1. Duplicate the Cisco Jabber Client Configuration Service in the service profile that Cisco Jabber users currently use:

- Add the **EnableJabber2TeamsMigration** parameter and set the value to **true**.
- **Optional:** Add **WebexTeamsDownloadURL** and set the value to a Webex download location.

Step 2. **Optional:** Add a new Cisco Jabber Client Configuration Service that will be used for the Webex App.

Duplicate the service profile in Cisco Unified Communications Manager that Cisco Jabber users currently use and set the new UC service as Cisco Jabber Client Configuration profile to Common, Desktop, and Mobile options. The duplicate service profile is used in migrating Cisco Jabber to Webex App to enable the Cisco Jabber migration tool and as a user filtering option with the Webex migration wizard.

Step 3. Create a new service profile in Cisco Unified Communications Manager and configure the following parameters:

- **Voicemail profile:** The Voicemail UC Service that Cisco Jabber users currently use.
- **CTI profile:** The CTI UC Service that Cisco Jabber users currently use.
- **Jabber Client Configuration profile:** The Jabber Client Configuration UC Service that the Webex App should use.

Voicemail, CTI, and Jabber Client Configuration profiles are optional and depend on your environment. If you do not use voicemail or desktop phone control, you do not need to configure the voicemail and CTI parameters. You do not have to set the Jabber Client Configuration profile if Webex App is not using advanced calling options.

Step 4. Configure a service profile in Cisco Unified Communications Manager for migration of end users from Cisco Jabber to Webex App.

You can set a UC Service Profile on an individual end user or use the Cisco Unified Communications Manager bulk tool. Now you are ready to migrate Cisco Jabber users using Webex Cloud Connected UC to the Webex App. The high-level configuration steps on the Webex Control Hub are as follows:

Step 1. Run the **Migrate Jabber to the new Webex** wizard to prepare all required information for migrating Cisco Jabber to the Webex App. Refer to Chapter 23 for more information on where and how this wizard is configured.

The **Migrate Jabber to the Webex App** window displays the user counts, which include the number of already-migrated users, all users configured in Cisco Unified Communications Manager, all Cisco Unified Communications Manager users in Common Identity, and all Cisco Unified Communications Manager users not in Common Identity. You can only migrate Cisco Unified Communications Manager users in Common Identity.

Step 2. Create a new migration task to prepare a user list and settings that should be used for migration. You need to provide the unique **Task name** and check all **Prerequisites** before you can continue to the next step.

To complete the migration task wizard, you need to go through the **Task name**, **Cluster selection**, **Settings**, **User selection**, and **Review** steps.

Step 3. On the **Cluster selection** page, choose a cluster from which Cisco Jabber users will be migrated to Webex App.

The **Cluster selection** page displays the number of available users who are ready for migration. This number is the difference between the total number of Cisco Unified Communications Manager users in Common Identity and the number of already-migrated users.

Step 4. On the **Settings** page, configure the calling options and behavior when calls are made from Webex App using the following options:

- **Calling in Webex App (Unified CM)**
- **Use my user's email domain**
- **Use UC Manager Profile for calling**
- **Open Cisco Jabber from Webex App**

Step 5. Choose the users you want to migrate to Webex App.

Step 6. Review any configuration errors or warnings and solve them, if needed, before you continue with the wizard.

Step 7. Finish the migration task and verify that the task has completed successfully before verifying the Webex App user migration.

Once you're all set up, users will eventually be prompted to migrate Jabber to Webex; however, you can force this action, instead of waiting for it to initiate, by following these steps:

Step 1. Open the Jabber client and click the gear icon in the top-right corner. Go to **Help > Move data to Webex**. This option is available only because you enabled it with a Jabber Client Configuration profile. Remember that you configured the **EnableJabber2TeamsMigration** option under the Jabber Client Configuration profile. This will start the Cisco Jabber-to-Webex migration tool, which moves contacts and preferences from Cisco Jabber to Webex.

Step 2. Click **Next** on the wizard that appears on the screen and follow the prompts through the process. This will allow the user to choose what they want to migrate, such as contacts, preferences, or both.

Step 3. Click the **Move to Webex** button when finished. The **Webex** window is now displayed. When the migration is complete, you will see the message "You're all moved over!"

Step 4. Click **Restart Webex.** Once the app reboots, verify the **Contacts.** You should now see the contacts that were moved from Cisco Jabber to Webex.

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 35, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 29-4 lists a reference of these key topics and the page numbers on which each is found.

Table 29-4 Key Topics for Chapter 29

Key Topic Element	Description	Page Number
List	Webex App features	704
Table 29-1	Comparison of Calls Through Cisco Unified Communications Manager and Calls/Meetings through the Cloud	706
Steps	Configure CTI UC Service	710
Steps	Configure Voicemail UC Service	711
Steps	Configure Service Profile	711
Table 29-3	Device Name Format for Soft Phone Devices	713
List	Webex Control Hub requirements for Jabber Migration	716
List	Service Profile services used by Webex App	718
List	Steps for Jabber migration on Cisco Unified Communications Manager	719

Define Key Terms

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

Webex App, CSF, TCT, BOT, TAB, CTI, DPC, FCM, APN, UC Services, Service Profile, dp, Webex Control Hub, Cloud Connected UC, Common Identity

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the four different soft-phone devices used to register Webex App to the Cisco Unified Communications Manager.
2. List the five Webex Control Hub requirements for Jabber migration to Webex App.
3. List the three services Webex App relies on within the service profile on the Cisco Unified Communications Manager.

This part covers the following topics:

- **Chapter 30, Troubleshooting Endpoints:** This chapter will identify the logs available on Cisco Unified IP phones and Cisco CE software-based endpoints. This chapter will also cover common registration issues, call setup issues, and media issues related to these endpoint devices.
- **Chapter 31, Cisco Unified Communications Manager Reports:** This chapter will examine how the Dialed Number Analyzer and CAR tool can be used in the CUCM to troubleshoot issues related to registration, call setup, and media-related issues. Along with the CAR tool, this chapter will also examine how to use CDR and CMR reports to view user reports, system reports, and device reports on the Cisco Unified Communications Manager.
- **Chapter 32, Real-Time Monitoring Tool (RTMT):** The Real-Time Monitoring Tool is a complex but granular tool used by top-level engineers to troubleshoot Cisco UC and Telepresence systems. This chapter will provide a brief overview of the Real-Time Monitoring Tool and how to use this tool to monitor activity over the Cisco Unified Communications Manager.
- **Chapter 33, Understanding the Disaster Recovery System:** This chapter will explain how to create a backup of the Cisco Unified Communications Manager configuration and how to do a restore of those configuration settings in the event they need to be recovered after a disaster.
- **Chapter 34, Monitoring Voicemail in Cisco Unity Connection:** This chapter will identify how to generate reports on the Cisco Unity Connections server and through the Cisco Unified Serviceability page. This chapter will also identify how to use those reports to perform troubleshooting and maintenance on the Cisco Unity Connection server.

Part VIII

Troubleshooting Collaboration Components

CHAPTER 30

Troubleshooting Endpoints

This chapter covers the following topics:

Accessing Logs on Cisco Unified IP Phones: This topic will provide a brief description of how to access logs on Cisco Unified IP phones.

Accessing Logs on CE Software-Based Endpoints: This topic will provide a detailed explanation about the different types of logs available on CE software-based endpoints and how to access these logs.

Call Signaling and Quality: This topic will explain how to use some of the tools on Cisco CE software-based endpoints to capture signaling and media information from the endpoint. This topic will also identify common issues related to registration, call setup, and media for Cisco Unified IP phones and Cisco Telepresence endpoints.

Troubleshooting Cisco Jabber: This topic will introduce some of the troubleshooting tools available on the Cisco Jabber client, as well as common registration, call setup, and media issues that Cisco Jabber can encounter.

This chapter draws off previous chapters to describe how Cisco Unified IP phones, Cisco Telepresence endpoints, and Cisco Jabber can be supported when registration, call setup, and media issues occur. Each device has some tools that can be used to troubleshoot issues, which will also be discussed in this chapter. Topics discussed in this chapter include the following:

- Accessing Logs on Cisco Unified IP Phones
- Accessing Logs on CE Software-Based Endpoints
  - Log Collection
  - Log Bundle
- Call Signaling and Quality
  - Signaling and Media Detailed Capture
  - Common Registration Issues
  - Common Call Setup Issues
  - Common Media Issues
- Troubleshooting Cisco Jabber

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 1.4 Troubleshoot these network components in a Cisco Collaboration solution
  - 1.4.a DNS (A/AAA, SRV, Reverse Pointer Record [PTR])
  - 1.4.b NTP
- 2.1 Troubleshoot these elements of a SIP conversation
  - 2.1.a Call set up and tear down
  - 2.1.b SDP
- 2.5 Troubleshoot SIP 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 30-1 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 30-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Accessing Logs on Cisco Unified IP Phones	1
Accessing Logs on CE Software-Based Endpoints	2–5
Call Signaling and Quality	6–10
Troubleshooting Cisco Jabber	11

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 must an administrator do before accessing logs on the Cisco Unified IP phone through the web interface?
   - **a.** Nothing, the web interface is always available to the administrator.
   - **b.** Set the username and password for the phone on the phone.
   - **c.** Set the username and password for the phone on the CUCM.
   - **d.** Enable access to the web interface of the phone on the CUCM.

2. What menu location can an administrator use to access log files on a CE software-based endpoint web interface?
   a. **Maintenance > System Logs**
   b. **Status > Logs > Event Logs**
   c. **Maintenance > Current Logs**
   d. **Status > Current Logs**
3. On a CE software-based endpoint, what is the difference between Start Extended Logging and Include a Full Packet Capture?
   a. Start Extended Logging includes a packet capture with signaling only, but Include a Full Packet Capture includes a packet capture with signaling and media.
   b. Start Extended Logging includes a full debug level with no packet capture, but Include a Full Packet Capture includes a packet capture with signaling and media.
   c. Start Extended Logging includes a full debug level with signaling packet capture, but Include a Full Packet Capture includes a packet capture with signaling and media.
   d. Start Extended Logging includes a full debug level with no packet capture, but Include a Full Packet Capture includes a packet capture with signaling only.
4. Which of the following log files contain general information on all previous calls made by the endpoint?
   a. Status.txt
   b. Journal.log
   c. Call_history.txt
   d. Latest-provisioning.log
5. How many historical log files are stored in the log bundle when it is downloaded?
   a. 1
   b. 2
   c. 5
   d. 11
6. Which of the following statements is true about the following logs available on CE software-based endpoints?
   a. Call information from the Call Control page is available after the call ends.
   b. Call information from the Status page is available during a call or after the call ends.
   c. Call information from the Call Logs page is available after the call ends or if a call attempt fails to connect.
   d. All of these answers are correct.
7. When you are reading a detailed debug capture of a SIP call, what indictor marks the beginning of the SDP media capabilities exchange?
   a. M=
   b. V=
   c. CSeq: SDP
   d. A=

8. When an administrator suspects a Webex Room Kit endpoint is not registering to the CUCM due to a network reachability error, which of the following commands can be used to ping the CUCM from the CLI of the endpoint?
   a. **Systemtools network ping**
   b. **Xcommand network ping**
   c. **Xconfiguration network ping**
   d. **xstatus network ping**
9. When a user tries to place a call and only dead air is heard, what is the probable cause of this issue?
   a. Misconfigured dial plan
   b. CAC
   c. IP reachability issue to the CUCM
   d. Firewall or ACL blocking media
10. A user has called in a complaint that the audio and video were out of sync while in a video call from a SIP endpoint. What can an engineer do to prevent this issue from happening again?
    a. Reprovision the available bandwidth for that endpoint.
    b. Nothing; lip synchronization is not supported over SIP natively.
    c. Change the codec used in the CUCM Regions settings.
    d. Change the CAC settings in the CUCM.
11. Which of the following is a TCP port that Cisco Jabber uses for XMPP communication?
    a. 8443
    b. 5222
    c. 5060
    d. 2748

Foundation Topics

Accessing Logs on Cisco Unified IP Phones

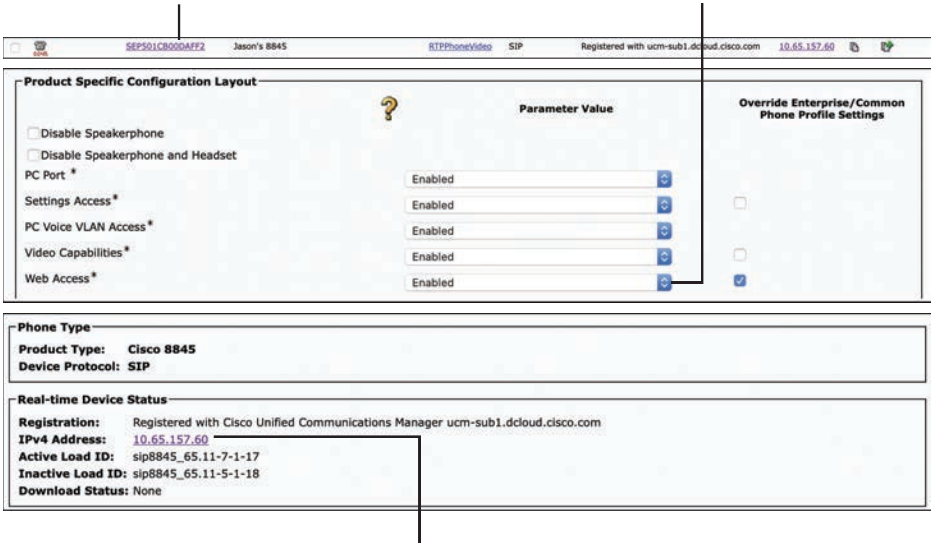
Key Topic

Cisco Unified IP phones can display status messages that show the most recent events from the phone on the screen display itself. These messages can indicate settings such as if a DHCP server can be reached and the address that is assigned to the phone. The status messages are available on all types of Cisco Unified IP phones. To check the status messages on a Cisco Unified IP Phone 8800 series, you can navigate to **Applications > Administrator Settings > Status**. Three types of status messages are available: Status Messages, Network Statistics, and Call Statistics. The Call Statistics menu allows you to check the Average (Avg) and Max Jitter, Receiver (Rcvr) Lost Packets, and Latency to verify that the call meets the general QoS requirements for the video traffic type. Beyond these status menus, no more logs are available from these phones on the endpoint itself. However, many more logs are available through the web interface of these phones.

Before you can access the logs available from the web interface of the Cisco Unified IP Phones 7800 series and 8800 series, you must configure some settings on the Cisco Unified Communications Manager first. From the Cisco Unified Communications Manager Administration page, navigate to **Device > Phone**. Select a Cisco Unified IP phone from the list by clicking on the MAC address, and then scroll down to the Web Access setting. Using the drop-down menu, change this setting from Disabled, which is the default, to Enabled. Then click Save and Apply Config from the buttons across the top of the screen. After the phone has been reset, you should be able to log in to the phone through the web interface. Figure 30-1 illustrates how to configure all these settings.

Navigate to Device > Phone and select the MAC address of the phone.

Change the Web Access setting to Enabled.



□ SEP501CB00DAFF2 Jason's 8845 RTPPhoneVideo SIP Registered with ucm-sub1.dcloud.cisco.com 10.65.157.60

Product Specific Configuration Layout

	Parameter Value	Override Enterprise/Common Phone Profile Settings
□ Disable Speakerphone		
□ Disable Speakerphone and Headset		
PC Port *	Enabled	
Settings Access*	Enabled	□
PC Voice VLAN Access*	Enabled	
Video Capabilities*	Enabled	□
Web Access*	Enabled	☑

Phone Type

Product Type: Cisco 8845
Device Protocol: SIP

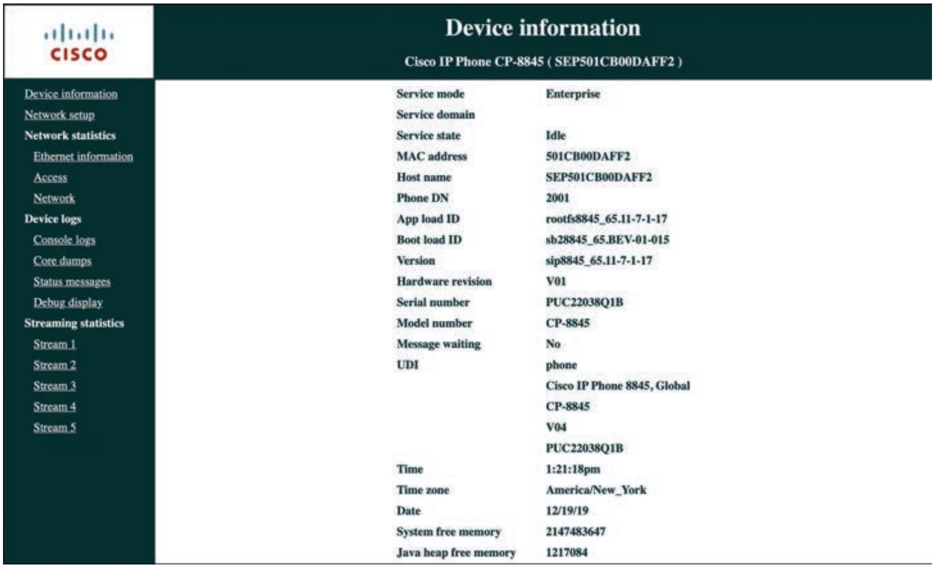
Real-time Device Status

Registration: Registered with Cisco Unified Communications Manager ucm-sub1.dcloud.cisco.com
IPv4 Address: 10.65.157.60
Active Load ID: sip8845_65.11-7-1-17
Inactive Load ID: sip8845_65.11-5-1-18
Download Status: None

Click on or navigate to the IP address of the Cisco Unified IP Phone.

Figure 30-1 *Configure CUCM for IP Phone Web Interface Access*

In a new web browser tab, navigate to the IP address of the Cisco Unified IP phone. This IP address can be identified on the Cisco Unified IP phone or on the endpoint itself by navigating to **Application > Phone Information**. You do not need to use HTTPS, and you do not need to enter a username or password. No settings on the phone can be changed from the web interface. Only logs can be accessed from the web interface, but a lot more logs are available to the administrator. Figure 30-2 illustrates the web interface and logs available on a Cisco Unified IP Phone 8845.



Device information

Cisco IP Phone CP-8845 (SEP501CB00DAFF2)

Service mode	Enterprise
Service domain	
Service state	Idle
MAC address	501CB00DAFF2
Host name	SEP501CB00DAFF2
Phone DN	2001
App load ID	rootfs8845_65.11-7-1-17
Boot load ID	sb28845_65.BEV-01-015
Version	sip8845_65.11-7-1-17
Hardware revision	V01
Serial number	PUC22038Q1B
Model number	CP-8845
Message waiting	No
UDI	phone Cisco IP Phone 8845, Global CP-8845 V04 PUC22038Q1B
Time	1:21:18pm
Time zone	America/New_York
Date	12/19/19
System free memory	2147483647
Java heap free memory	1217084

Figure 30-2 *Cisco Unified IP Phone 8845 Web Interface Logs*

Accessing Logs on CE Software-Based Endpoints

Many different types of logs are available on Cisco Telepresence endpoints running CE software. Historically, administrators had to access these logs from the CLI, and they often had to use other tools to extract these logs, such as the Microsoft WinSCP tool. Cisco has made many enhancements to the web interface of these endpoints, making access to these logs much easier. You can use the following steps to access the logs from the web interface of an endpoint.

Step 1. Open a web browser and enter the IP address of the endpoint in the address bar.

Step 2. From the login screen, enter the username and password assigned to the endpoint. By default, CE software-based endpoints use **admin** as the username and the password field is left blank.

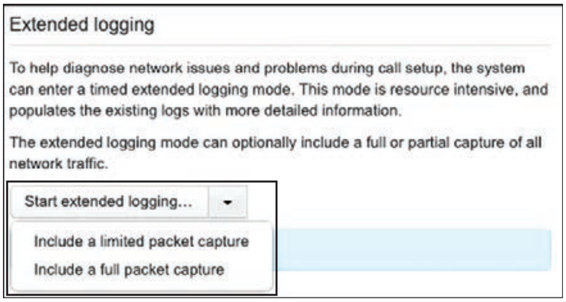
Step 3. Once logged in, navigate to **Maintenance > System Logs**.

The System Logs page is divided into three main sections.

- Download Log Archive
- Start/Stop Extended Logging
- Manually Browse Current Logs or Historic Logs

Log Collection

Extended logging enables additional debugging including SIP tracing. Historically, this debug level had to be enabled from the CLI and then retrieved from the eventlog.application.log file. Now Cisco has added the ability to turn on this debug trace directly from the web interface. When Start Extended Logging is selected, the extended logging is turned on and will last for 10 minutes. Two other options exist for enabling extended logging. The Include a Limited Packet Capture option will not only turn on the extended logging but will also capture log information in a separate pcap file. The "limited" component signifies that media information will not be captured, only signaling data. This option will also last for 10 minutes when enabled. If media information is needed because of media issues, you should select the Include a Full Packet Capture option. This option will collect all the data previously noted; plus, it will also capture all the RTP traffic. Because this type of trace will include much more information, this option will last only 3 minutes. Figure 30-3 illustrates the menu options on the CE endpoint web interface used to enable these extended logging options.


Extended logging

To help diagnose network issues and problems during call setup, the system can enter a timed extended logging mode. This mode is resource intensive, and populates the existing logs with more detailed information.

The extended logging mode can optionally include a full or partial capture of all network traffic.

Start extended logging...
Include a limited packet capture
Include a full packet capture

- Extended Logging
  - Enables additional debugs, including SIP tracing
  - Lasts 10 minutes
- Include a Limited Packet Capture
  - Starts pcap, which will filter out RTP media
  - Lasts 10 minutes
- Include a Full Packet Capture
  - Captures all traffic, including RTP
  - Lasts 3 minutes

Figure 30-3 *Extended Logging Options from CE Endpoint Web Interface*

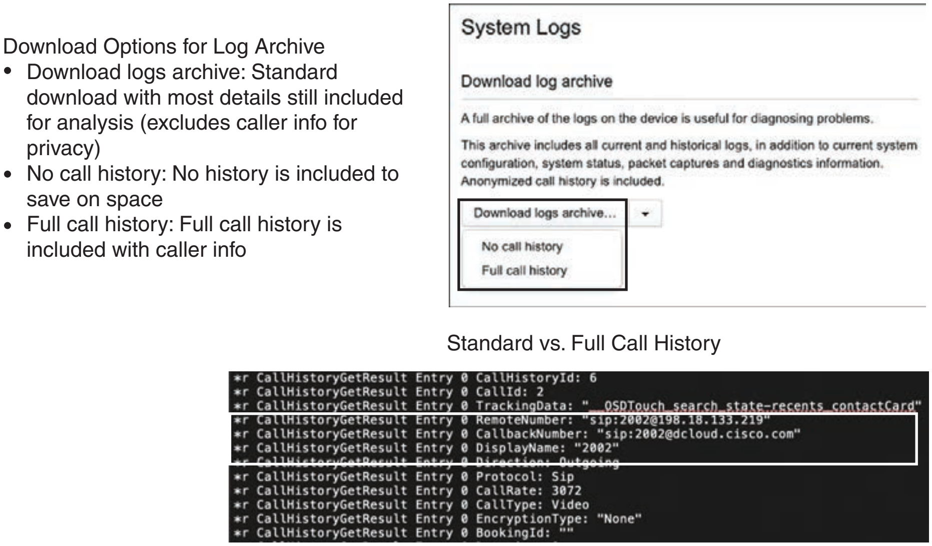
When one of the options from Figure 30-3 is selected, an indicator flag will notify the administrator that extended logging is active and will indicate the total time allotment. Also, the packet capture file will be displayed in the GUI. This file can be downloaded directly by clicking the hyperlink, or it can be included in the log bundle when downloaded.

Much like with enabling extended logging, three options are available when downloading the logs archive:

Key Topic

- **Download Logs Archive:** Selecting this option will enable a standard download with most details still included for analysis. Call info is excluded from this standard download to ensure the caller's privacy.
- **No Call History:** Selecting this option will download the same log information as Download Logs Archive, except no "history" log information will be included to save on space.
- **Full Call History:** Selecting this option will download the exact same information as the standard download, including caller information. Only three lines are different between this option and the standard option.

Figure 30-4 illustrates the three log archives that can be downloaded and the three lines that distinguish the standard logs archive from the full call history.



Download Options for Log Archive
- Download logs archive: Standard download with most details still included for analysis (excludes caller info for privacy)
- No call history: No history is included to save on space
- Full call history: Full call history is included with caller info

System Logs

Download log archive

A full archive of the logs on the device is useful for diagnosing problems.

This archive includes all current and historical logs, in addition to current system configuration, system status, packet captures and diagnostics information. Anonymized call history is included.

Standard vs. Full Call History

```
*r CallHistoryGetResult Entry 0 CallHistoryId: 6
*r CallHistoryGetResult Entry 0 CallId: 2
*r CallHistoryGetResult Entry 0 TrackingData: "_OSDTouch_search_state-recents_contactCard"
*r CallHistoryGetResult Entry 0 RemoteNumber: "sip:2002@198.18.133.219"
*r CallHistoryGetResult Entry 0 CallbackNumber: "sip:2002@dcloud.cisco.com"
*r CallHistoryGetResult Entry 0 DisplayName: "2002"
*r CallHistoryGetResult Entry 0 Direction: Outgoing
*r CallHistoryGetResult Entry 0 Protocol: Sip
*r CallHistoryGetResult Entry 0 CallRate: 3072
*r CallHistoryGetResult Entry 0 CallType: Video
*r CallHistoryGetResult Entry 0 EncryptionType: "None"
*r CallHistoryGetResult Entry 0 BookingId: ""
```

Figure 30-4 *System Logs Download Options from CE Endpoint Web Interface*

Log Bundle

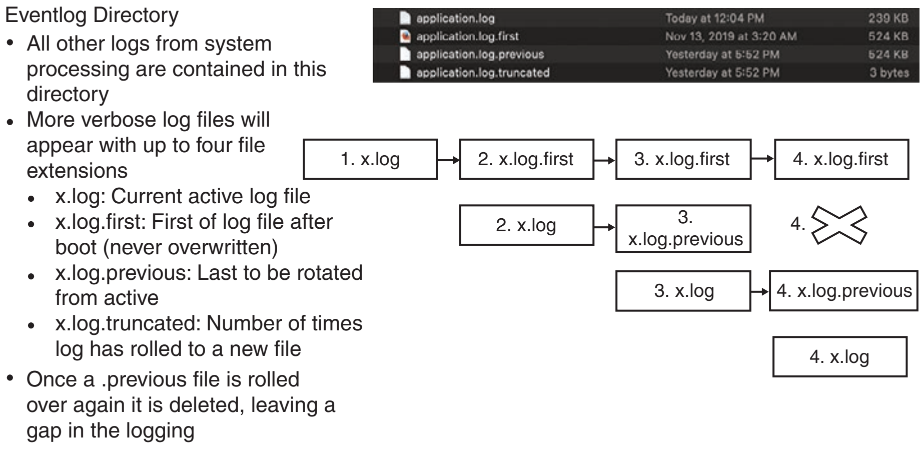
When the log archive files have been downloaded, they will be zipped in a tar.gz file. After that file is uncompressed and opened, two or three other folders will be included. There will always be a *current* and an *old* folder. If extended logging was enabled with a packet capture before the log archive was downloaded, there will be a third folder that includes the pcap file that was created. The current folder contains all log files and information from the current boot of the system. The old folder contains historical log bundles created at shutdown. When the current folder is opened, the following files are available. This is not an exhaustive list; rather, it is a list of the most likely logs an administrator would use, with a description of each file.

Key Topic

- **Call_history.txt:** Contains general info on all previous calls made by the system
  - Protocol
  - Negotiated call rate
  - Start/end times
  - Disconnect information
  - Media statistics
  - Direction
- **Configuration.txt:** Includes all system configuration settings set through the web GUI and CLI
  - Same as running xConfiguration in the CLI
  - Good for quick reference of settings without needing to access system directly or if troubleshooting issue from some time ago
  - Always pulled at the time of log collection

- **Status.txt:** Includes all system status outputs
  - Same as running xStatus in the CLI
  - Useful as a quick health check for processes such as provisioning or peripheral connections
  - Always pulled at the time of log collection
- **Peripherals.txt:** Contains information on all connected peripherals
  - Same information included in status.txt
  - Good for quick reference without having to sort through other noise
- **Journal.log (also known as messages.log):** Contains low-level system information and boot processes
  - Also includes kernel messages from kernel.log
  - Useful for troubleshooting system crashes
- **Latest-provisioning.log:** Present if the system is provisioned by CUCM
  - Contains the most recently pushed cnf.xml file
  - Useful to validate configuration from CUCM without needing access to CUCM
- **Latest-valid-provisioning.log** contains config after parsing is complete

The eventlog folder, also included in the current folder, contains a directory of log files that offer more verbose information. The logging capacity on these endpoints is finite, but the system will take measures to ensure the most relevant information is stored. Eventlog files will use up to four file extensions before older data is lost. Figure 30-5 illustrates how these four file extensions are created within the CE software-based endpoint event log. The boxes in the figure illustrate how these file extensions work. Note that **x** in these examples indicates any eventlog file. The description that follows uses application.log as a point of reference and works from the top left toward the bottom right.



Eventlog Directory

- All other logs from system processing are contained in this directory
- More verbose log files will appear with up to four file extensions
  - x.log: Current active log file
  - x.log.first: First of log file after boot (never overwritten)
  - x.log.previous: Last to be rotated from active
  - x.log.truncated: Number of times log has rolled to a new file
- Once a .previous file is rolled over again it is deleted, leaving a gap in the logging

```
application.log              Today at 12:04 PM          239 KB
application.log.first        Nov 13, 2019 at 3:20 AM    524 KB
application.log.previous     Yesterday at 5:52 PM       524 KB
application.log.truncated    Yesterday at 5:52 PM       3 bytes
```

Figure 30-5 *Event Log File Extension Operation on CE Software-Based Endpoints*

1. The first x.log box represents an event log that is created when the endpoint first boots up, such as the application.log.
2. Once this log fills up, the data is saved under a new filename, such as application.log.first. The data in log.first logs will never be overwritten or deleted. Once this original content has been renamed, new logged information can be captured in the application.log file (second row).
3. When this second application.log file fills up, it too needs to be renamed, so application.log.previous will be used. Once this second set of content has been renamed, new logged information can be captured in the application.log file (third row). The log.first file does not change from when it was originally created.
4. When this third application.log file fills up, it too needs to be renamed, and application.log.previous will be used again. Two files with the same name cannot exist, so the first application.log.previous file is deleted, creating a gap in the logging. Once this third set of content has been renamed, new logged information can be captured in the application.log file (fourth row).

You may have noticed from Figure 30-5 that there is another file extension called x.log.truncated. This is not a renamed log file as previously described. This file is a logged reference point that tracks how many times an **x** log has rolled over since the last reboot of the endpoint. Many logs are included in the Event Log folder, most of which will never be referenced by a system administrator. The following is a list of the most commonly used event logs, with a description of the information found in these logs:

Key Topic

- **All.log:**
  - All logs rolled into a single file
  - Quick glance at what's happening
  - Overwrites quickly
  - Specific log files referenced by tagging in all.log.
- **Application.log:**
  - Includes application-level debugging (including additional debugs enabled)
  - Includes Call setup and signaling
  - Includes Registration information
  - Includes Provisioning information
  - Includes Phonebook searches
  - Includes Configuration changes
- **Main.log:**
  - Process and system monitoring
  - Boot information, software version, option keys
  - Place to look for boot issues or crashes

- **Audit.log:**
  - Logs commands from all connected devices
  - Includes physically connected devices, such as touch and network connected
  - Includes any configuration changes from users or management devices

Historical bundles are similar to the current directory but contain slightly less diagnostic info. All of the same event logs are included in each historical log. Each time the system reboots, all the logs in the current log files are compressed into a single historical log file. The log.tar.gz is always a reference to the most recently created historical log. After the next reboot, the log.tar.gz file is renamed with a numeric value, such as log.x.tar.gz, where x is a number value (0–9). When all historic log slots are full, the oldest historic log will be deleted. This deletion is based on the timestamp, not on the numeric value associated with the name. Although up to 11 historical log files can exist in the Cisco CE software-based endpoint, the log bundle will only contain the previous five historical log files. All historical log files are cleared on a factory reset.

Call Signaling and Quality

The web interface of Cisco Telepresence CE software-based endpoints provides three basic places to check for call info:

Key Topic

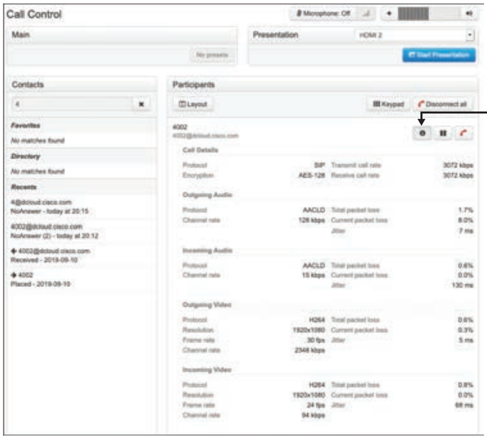
- Call Control Page
- Status
- Call Logs

These quick reference locations are perfect for a quick understanding of call negotiation or basic media statistics, or to augment additional troubleshooting. The Call Control and Status pages will display call statistic information only while a call is active. However, Call Logs pages are available for previous calls or call attempts.

Select the Call Control menu from the top of the screen to view the Call Control settings. If there is an active call, you will see the connected party's alias listed in the Participants section with three buttons beside the listing. The last two are used to place the call on hold or hang up the call. The first button, the information button, is an *i* with a circle around it. Figure 30-6 illustrates how the Call Control Details page will appear.

The information button is used to display the call details. Information that can be observed from the call in Figure 30-6 includes that this call is an encrypted SIP call and that the call rate was placed at 3 Mbps. Also, AAC-LD is the audio codec being used, H.264 is the video codec being used, and incoming audio and incoming video have a high jitter rate.

From the menus at the top of the page, navigate to **Setup > Status**. A list of menus will appear in the column to the left. Select MediaChannels from the menu. This will display status information about any current calls that are connected at the immediate time. Status provides useful information, such as the UDP media ports used by both source and destination endpoints.



Contacts: 4

Favorites
No matches found

Directory
No matches found

Recents
4@dcloud.cisco.com
NoAnswer - today at 20:15
4002@dcloud.cisco.com
NoAnswer (2) - today at 20:12
4002@dcloud.cisco.com
Received - 2019-09-10
4002
Placed - 2019-09-10

4002
4002@dcloud.cisco.com

Call Details

Protocol	SIP	Transmit call rate	3072 kbps
Encryption	AES-128	Receive call rate	3072 kbps

Outgoing Audio

Protocol	AACLD	Total packet loss	1.7%
Channel rate	128 kbps	Current packet loss	8.0%
		Jitter	7 ms

Incoming Audio

Protocol	AACLD	Total packet loss	0.6%
Channel rate	15 kbps	Current packet loss	0.0%
		Jitter	130 ms

Outgoing Video

Protocol	H264	Total packet loss	0.6%
Resolution	1920x1080	Current packet loss	0.3%
Frame rate	30 fps	Jitter	5 ms
Channel rate	2348 kbps		

Incoming Video

Protocol	H264	Total packet loss	0.8%
Resolution	1920x1080	Current packet loss	0.0%
Frame rate	24 fps	Jitter	68 ms
Channel rate	94 kbps		

Click On the “i” Button

- This call is an encrypted SIP call
- The call rate was placed at 3 Mbps
- AAC-LD is the audio codec being used
- H.264 is the video codec being used
- Incoming audio and incoming video have a high jitter rate

Figure 30-6 *Call Control Details Page on the Cisco CE Software-Based Endpoint*

The call logs offer information after a call ends or for calls that never connected. Next, navigate to **Maintenance > Call Logs**. A list of all calls or call attempts since the last reboot will be listed in this log. From this page, you can access some basic information, such as the direction of the call, how long the call was connected, and the reason for the call ending. Select any of these call listings to view more detailed information. The following valuable information can be observed from this log:

Key Topic

- Remote number
- Call direction, protocol, and call rate
- Disconnect cause
- Disconnect cause code
- Media statistics averages (packet loss/jitter)

Signaling and Media Detail Capture

This chapter has already discussed how to enable extended logging, how to perform a packet capture, and how to pull this information from the endpoints. This section will introduce how to read the log information after it is captured. Debug log information is accessed in the eventlog.application.log file. There will be a lot of information to drill through to find what you need. The easiest way to find the call debug information is to use the search tool. The actual SDP information, which is available only in a debug, always begins with v=0. You can use this variable to find the specific call information you are looking for. Example 30-1 illustrates how some of the information captured in a debug will appear in the application.log file.

Example 30-1 *Debug Log from eventlog.application.log After Extended Logging Was Enabled and a Call Was Placed*

```
SipPacket I: SIP Msg: Outgoing => INVITE, CSeq: 100 INVITE, Remote: 14.49.23.20:5060,
CallId: 88b866e5f94fdfb3e0214208bd6a34fe, SessionId: 0eaf314a5f335bdbb6823e427b11968
0;remote=00000000000000000000000000000000
SipPacket[2]: INVITE sip:20001@tkratzke.local SIP/2.0
SipPacket[2]: Via: SIP/2.0/TCP 14.0.70.171:39293;branch=xxxx;rport
SipPacket[2]: Call-ID: 88b866e5f94fdfb3e0214208bd6a34fe
SipPacket[2]: CSeq: 100 INVITE...
SipPacket[2]: v=0
SipPacket[2]: m=video 21008 RTP/AVP 99 97 126 123
SipPacket[2]: b=TIAS:6000000
SipPacket[2]: a=rtpmap:99 H265/90000
SipPacket[2]: a=fmtp:99 level-id=90;max-lsr=125337600;max-lps=2088960;max-tr=22;max-
tc=20;max-fps=6000;x-cisco-hevc=529
SipPacket[2]: a=rtpmap:97 H264/90000
SipPacket[2]: a=fmtp:97 packetization-mode=0;profile-level-id=428016;max-
br=5000;max-mbps=490000;max-fs=8160;max-smbps=490000;max-fps=6000
! Output truncated for brevity
```

Key Topic

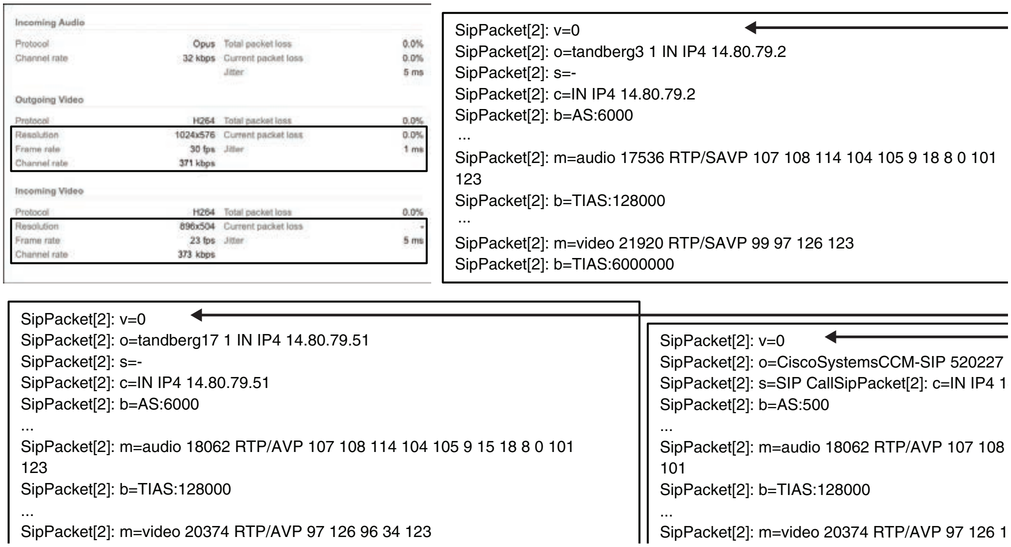
In Example 30-1, the shaded header information is all the information you will see in the application log file about each call when no debug is enabled. All the information below the header, which has been truncated for obvious reasons, is shown only when a debug is enabled. The m= represents the beginning of the SDP media capabilities exchange based on what codecs the endpoint supports. Audio will always be displayed first, followed by primary video, which is followed by content sharing. The example has omitted the audio SDP negotiation. Note that 21008 is the RTP port this endpoint wants to use to send the media, which is video in this case. A different port would be used for audio or content sharing, and different ports are used for media going in the other direction. The 99 97 126 123 numbers are SIP cause codes for codecs that this endpoint supports. You will always find a description for each number in the a= lines below, so you don't need to memorize what each one of these is. The preferred codec is always the first number in the list, and each number following is in sequential order of preference. Notice that 99 represents H265/90000 and 97 represents H264/90000. The 90000 is just the Hertz rate. The next line below each of these identifies the bandwidth rate requested with each codec.

Packet captures are tagged in a file called pcap. You will need special tools, such as Wireshark, to open and read this file. Reading a pcap file is not an intuitive process. You must know what you are looking for in order for the information to make any sense. Each line in a pcap file is a different packet that was sent. When one of these packet lines is selected, a new window is opened, usually at the bottom of the page, showing specific header information about the packet selected. Each of these new lines of information can be expanded so that engineers can drill down into the different OSI layers of information sent.

Because a pcap file contains a lot of information, an easy way to filter the information is to locate a distinguishing attribute you are trying to investigate, such as the UDP port used for video communications, and then filter the packets based on that port. There is another, and perhaps easier, way to filter information using Wireshark. Navigate to **Telephony > RTP**

> RTP Streams. This tool will filter out the data for you and provide a summary of all the detected RTP streams in the capture. It will provide the source and destination address, identify the payload type, and identify packet loss and jitter values. This information might help in isolating where along the connection path a loss of data was detected.

Now that you know how to read these detailed log files, the following explanation will illustrate how these logs can be used to troubleshoot a call media issue that the Cisco Technical Assistance Center (TAC) gets lots of calls about. Figure 30-7 illustrates the logs used to troubleshoot this issue.



```
Incoming Audio
Protocol                 Opus   Total packet loss     0.0%
Channel rate          32 kbps   Current packet loss   0.0%
                                Jitter                5 ms

Outgoing Video
Protocol                 H264   Total packet loss     0.0%
Resolution           1024x576   Current packet loss   0.0%
Frame rate             30 fps   Jitter                1 ms
Channel rate         371 kbps

Incoming Video
Protocol                 H264   Total packet loss     0.0%
Resolution            896x504   Current packet loss      -
Frame rate             23 fps   Jitter                5 ms
Channel rate         373 kbps
```

```
SipPacket[2]: v=0
SipPacket[2]: o=tandberg3 1 IN IP4 14.80.79.2
SipPacket[2]: s=-
SipPacket[2]: c=IN IP4 14.80.79.2
SipPacket[2]: b=AS:6000
...
SipPacket[2]: m=audio 17536 RTP/SAVP 107 108 114 104 105 9 18 8 0 101
123
SipPacket[2]: b=TIAS:128000
...
SipPacket[2]: m=video 21920 RTP/SAVP 99 97 126 123
SipPacket[2]: b=TIAS:6000000
```

```
SipPacket[2]: v=0
SipPacket[2]: o=tandberg17 1 IN IP4 14.80.79.51
SipPacket[2]: s=-
SipPacket[2]: c=IN IP4 14.80.79.51
SipPacket[2]: b=AS:6000
...
SipPacket[2]: m=audio 18062 RTP/AVP 107 108 114 104 105 9 15 18 8 0 101
123
SipPacket[2]: b=TIAS:128000
...
SipPacket[2]: m=video 20374 RTP/AVP 97 126 96 34 123
```

```
SipPacket[2]: v=0
SipPacket[2]: o=CiscoSystemsCCM-SIP 520227
SipPacket[2]: s=SIP CallSipPacket[2]: c=IN IP4 1
SipPacket[2]: b=AS:500
...
SipPacket[2]: m=audio 18062 RTP/AVP 107 108
101
SipPacket[2]: b=TIAS:128000
...
SipPacket[2]: m=video 20374 RTP/AVP 97 126 1
```

Figure 30-7 *Call Information Details Log and SIP Debug Logs Used for Troubleshooting Media Issue*

Imagine two endpoints in a basic call through the Cisco Unified Communications Manager. When they call each other, the audio quality is good; however, their video is pixelated and blurry. At first investigation, the Call Information Details from the Call Control menu on the endpoint reveal that video bandwidth is not getting the quantity requested. In Figure 30-7, the top-left screenshot reveals that only 371 kbps bandwidth has been allocated for outgoing video, and only 373 kbps has been allocated for incoming video. When extended logging is enabled, the SIP call setup log initially shows the source endpoint that initiated the call is requesting 6 Mbps for this call for video. The next part of the log, represented in the middle-left log, shows that the destination endpoint can also support 6 Mbps in this call, so the issue doesn't seem to be with the destination endpoint.

Further investigation in the log file finally reveals the issue, represented in the middle-right log. The source endpoint is actually requesting 500 kbps total bandwidth for this call, divided between audio at 128 kbps and video at 372 kbps. Something obviously renegotiated the bandwidth for the call. Since both endpoints are registered to the Cisco Unified Communications Manager, a quick check reveals that only 500 kbps has been provisioned for video calls, which is causing poor video quality during the call.

Common Registration Issues

Chapter 9, "Endpoint Registration," covered the registration process to the Cisco Unified Communications Manager. Understanding this registration process is important because any of these registration components could cause registration to fail. As a review, Cisco Unified IP phones and Cisco Telepresence endpoints require these elements to register successfully with Cisco Unified Communications Manager:

1. The phone must be on a correct voice and video VLAN that has network connectivity to Cisco Unified Communications Manager.
2. The phone must have a correct IP address, network mask, and default router, which the DHCP server can assign, or you can configure manually at the phone.
3. The phone must have a correct TFTP server address from which to download the configuration. The DHCP server assigns the option 150 TFTP IP address, or you can configure it manually at the phone.
4. There must be IP connectivity to the Cisco TFTP and Cisco Unified Communications Manager servers.
5. The phone must be able to exchange SCCP or SIP messages with Cisco Unified Communications Manager servers, without any filters applied.
6. The phone must be a known device to Cisco Unified Communications Manager. The phone must also be configured manually with the correct MAC address or must be able to use autoprovisioning.
7. If security is implemented in the Cisco Unified Communications network, the phone must have correct security elements applied. This configuration is performed on Cisco Unified Communications Manager, but the phone can cache old invalid information, such as trust lists.

Several factors can cause a "Phone not registered" message on a Cisco Unified IP phone. If a phone does not power up, the cause might be disabled PoE at the switch port or a switch that uses an incompatible PoE mechanism. Cisco switches support two types of PoE: Cisco proprietary and standards-based IEEE 802.3X. Cisco Unified IP phones support only the standards-based option. The IEEE standards for PoE are 802.3af and 802.3at. Some Cisco phones support the latter, which could cause issues. If a user were to connect an 802.3at device to an 802.3af supported switch, certain features on that phone would not work, which could include the phone not having enough power to fully boot up. The result is a cyclical reboot, where the phone begins to power on but shuts down during the boot process and starts the boot sequence all over again. Although PoE-related issues are not the most common issues found in a Cisco Collaboration network, they can occur. Figure 30-8 illustrates the more common issues that administrators will come across in a Cisco Collaboration network causing registration failures.

Key Topic

The phone might get an incorrect VLAN from the switch, so call control servers might be unreachable. You can configure each port on a Cisco Catalyst switch to which the Cisco Unified IP phones connect with two independent VLANs. Although one of the VLANs is called a Voice VLAN for historical reasons, it is also used to carry video traffic between the phone and the switch. This auxiliary VLAN carries tagged traffic using an IEEE 802.1Q header with the configured VVID. The Data VLAN stretches from the switch through the phone to the computer, which connects at the PC port of the phone. This VLAN is untagged. Although two VLANs are the recommended setup, the switch does not need to use separate VLANs for voice and video traffic and data traffic. One VLAN can be used for everything. The biggest advantage of using two VLANs is that the phone separates traffic types that have very different QoS requirements. Two VLANs also perform traffic classification that can be reused later downstream.

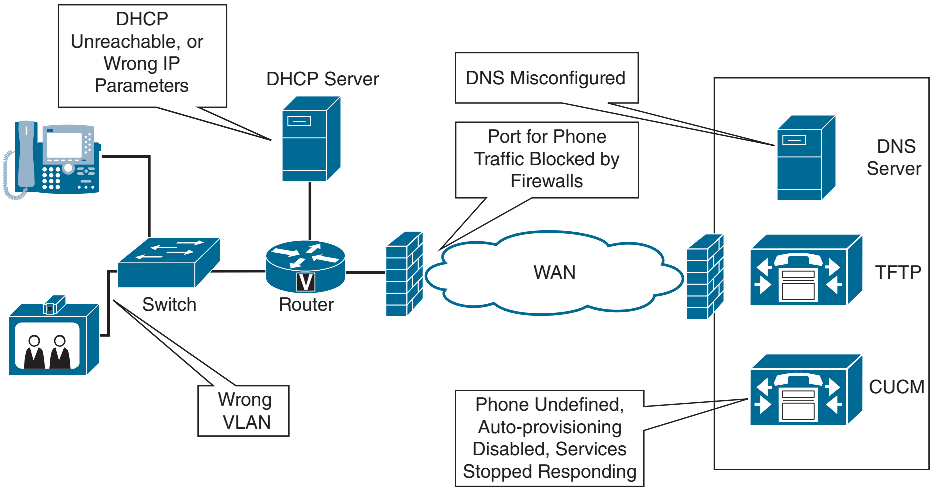

DHCP Unreachable, or Wrong IP Parameters
DHCP Server
DNS Misconfigured
Port for Phone Traffic Blocked by Firewalls
DNS Server
Switch
V
Router
WAN
TFTP
CUCM
Wrong VLAN
Phone Undefined, Auto-provisioning Disabled, Services Stopped Responding

Figure 30-8 *Common Registration Issues in a Cisco Collaboration Network*

DHCP servers can be unreachable because a router is placed between the phone and the DHCP server path. Remember that DHCP requests are broadcasts that spread out on the local IP subnet only. The router must be configured to relay these broadcasts on the IP subnet on which the DHCP server connects. The DHCP server can run out of IP addresses and therefore has none to assign. The DHCP server can also be misconfigured and assign incorrect IP parameters. A Cisco Unified IP phone can obtain IP parameters from three general types of DHCP servers:

Key Topic

- DHCP server running as a service at Cisco Unified Communications Manager
- DHCP server that is implemented at a Cisco IOS router
- Third-party DHCP server—for example, a Microsoft Windows server

If the phone has incorrect IP parameters, you can erase them and wait until the phone obtains new parameters from the DHCP server. To erase network settings on the Cisco Unified IP Phone 7800 and 8800 series, choose **Applications > Administrator Settings > Reset Settings > Network Settings** and confirm that the network settings have been erased. If IP parameters are not being received from the DHCP server, consider network-connectivity problems. Verify Layer 2 connectivity to the switch first. Another potential issue might be that the DHCP server has assigned all its available addresses to other endpoints and does not have an address to assign. The DHCP server might use an incorrect configuration and assign incorrect IP parameters to the phone. For example, an incorrect default router or network mask can cause incorrect routing outbound from the phone. Also remember that option 150 must be configured on the DHCP server for the phones to obtain configuration settings from the TFTP server. Example 30-2 shows a typical router-based DHCP server configuration.

Example 30-2 *Sample Router-Based DHCP Server Configuration*

```
ip dhcp pool video-phones
   network 10.250.20.0 255.255.255.0
    dns-server 10.192.126.10 10.192.126.11
    default-router 10.250.20.2
    domain-name cisco.com
    option 150 ip 10.192.5.97
```

After the phone obtains correct IP parameters, it sends registration packets that follow the IP routed path. If the route does not exist in either direction, the traffic does not reach the servers that are required to complete the registration process. The Cisco Unified IP phone requires IP connectivity to the Cisco TFTP server and Cisco Unified Communications Manager. In small deployments, these two servers can be collocated on the same physical platform, but for larger deployments, they need to be separate for scalability reasons. You can verify IP connectivity by using two options:

Key Topic

- Ping the servers from a switch, by using an extended ping with the source IP address from the voice and video VLAN. This VLAN is the same VLAN that the phones use to communicate with the servers.
- Ping the servers from a computer in the voice and video VLAN that receives IP parameters from the DHCP server for the same IP subnet as the phone. If using this option, ensure that you do not connect the computer to the PC port of the phone because from there it might be assigned to a completely different VLAN.

If **ping** fails, use **traceroute** to verify the routed path. Be aware, however, that company security policies might intentionally block ping and traceroute, whereas other traffic types can pass. You can also verify IP routing tables at the downstream routers. Do not forget about the opposite direction. If ping succeeds, there might still be issues at firewalls. Firewalls can let the ping pass but block the ports that are required for successful registration, such as TFTP, SCCP, SIP, or instantiated RTP/RTCP ports.

If you suspect that broken IP connectivity to the Cisco Unified Communications Manager is causing the registration issue from a Cisco Telepresence endpoint, you can verify the IP connectivity directly from the CE software-based endpoints. Log in to the CLI as admin and display the network settings that the endpoint uses. Verify that the IP settings and VLAN are correct. Try to ping the call control server from the CLI by using the **systemtools network ping** *IP_address* command. If the ping shows lost packets, you can verify the IP routed path by using the **systemtools network traceroute** *IP_address* command. You can also use the **systemtools network netstat** command to verify that the network processes are running and listening on the correct protocol ports.

DNS, if used, can also contribute to failed communication with the call control servers resulting in a failed registration attempt. DNS can be unavailable or unreachable in the IP network. DNS can also be misconfigured, meaning that it resolves names to incorrect IP addresses. If a DNS server is used to address Cisco Unified Communications servers, you should verify that the DNS server resolves names to correct IP addresses. To verify name resolution, use the **ns lookup** command followed by the DNS name of the Cisco Unified Communications Manager and Cisco TFTP server, if a separate TFTP exists, instead of the

IP address. Remember that this test must be performed from the same VLAN that is used for voice and video devices. Otherwise, the verification procedure does not check IP connectivity to the DNS server. If names do not resolve at all, ping the DNS server by its IP address. If no response is received, troubleshoot IP connectivity to the DNS server. If names resolve to incorrect IP addresses, check and correct the DNS database. If DNS names resolve to correct IP addresses but no response to the ping is received, troubleshoot IP connectivity to Cisco Unified Communications Manager and the Cisco TFTP server.

Firewalls might block the types of network protocols that are required during the registration process. Cisco Unified IP phones use TFTP to download configuration and use SCCP or SIP to complete the registration process. The firewalls in the path must open ports for these protocols:

Key Topic

TFTP uses UDP port 69 and then uses ephemeral ports for the actual file download.

- SCCP uses TCP port 2000. Secure SCCP uses TLS ports 2443 and 2445.
- SIP uses TCP or UDP port 5060. The port that is used depends on how SIP is provisioned on Cisco Unified Communications Manager. Secure SIP uses TLS port 5061.

If no network connectivity issues exist but the Cisco Unified IP phone still cannot register, settings on the Cisco Unified Communications Manager could prevent registration from occurring. Administrators should verify that endpoint configuration exists and that the correct MAC address is configured in Cisco Unified Communications Manager. If autoprovisioning is used instead of manual configuration, verify that autoprovisioning is enabled and that enough directory numbers are left in the pool. Verify that the required services are running on the Cisco Unified Communications Manager and Cisco TFTP server. Also, verify that Cisco Unified Communications Manager has not reached the limit of maximum registered phones because of licensing or configured limitations.

The Cisco Unified IP phone and Telepresence endpoint supports digital certificates, device authentication, and encryption. Phones can use the IEEE 802.1X data link layer authentication protocol to connect to a Cisco Catalyst switch that implements this security mechanism. Phones that support 802.1X must be configured correctly; otherwise, the data link layer authentication will prevent the phone from registering. Phones that do not support 802.1X must be provided with some other means to access the voice network. Cisco Unified IP phones and Telepresence endpoints also provide security by default with these automatic security features:

- Signing of the phone configuration files
- Support for phone-configuration file encryption
- HTTPS with Cisco Tomcat and other web services (MIDlets)

These security features are provided by default, even without implemented security for signaling and media and without running the Cisco CTL client. If the Cisco Unified IP phone does not have an existing CTL file, it trusts the first ITL file automatically, as it trusts the CTL file. Subsequent ITL files must be signed by the same TFTP private key, or the Trust Verification Service must be able to return the certificate that corresponds to the signer. The ITL file contains the ITL. The ITL file has the same format as the CTL file and is basically a smaller, leaner version of the CTL file. These attributes apply to the ITL file:

- Unlike the CTL file, the system builds the ITL file automatically when you install the cluster, and the ITL file is updated automatically if the contents need to be changed.
- The ITL file does not require eTokens. It uses a soft eToken (the TFTP private key).
- The Cisco Unified IP phones download the ITL file at bootup time or during reset, just after downloading the CTL file (if present).

Key Topic

- The CTL and ITL files can prevent a Cisco Unified IP phone from registering if the phone was moved to a different Cisco Unified Communications Manager cluster and the files that are stored at the phone still refer to the original cluster of the phone. In these circumstances, you must manually erase the CTL and ITL files from the phone to let the phone build or download new files as it boots.

Common Call Setup Issues

The components that are involved in call setup depend on the chosen deployment model. Cisco Unified Communications Manager can be deployed in single-site or multisite models, or as a single cluster or multiple clusters. The components also depend on whether the network interconnects with any other networks, such as video-capable ISDN (H.320) or traditional H.323 systems. Generally, two traffic types are used for each call:

- Call signaling traffic
- Call bearer traffic for audio and video

In most deployments, the components or mechanisms involved in call setup include dial plans, digit manipulation, and call privilege policies, which are implemented at the call control systems such as Cisco Unified Communications Manager and gateways. If any of these components are misconfigured, a call might fail to set up. Figure 30-9 illustrates the components involved with call setup in a Cisco Collaboration solution.

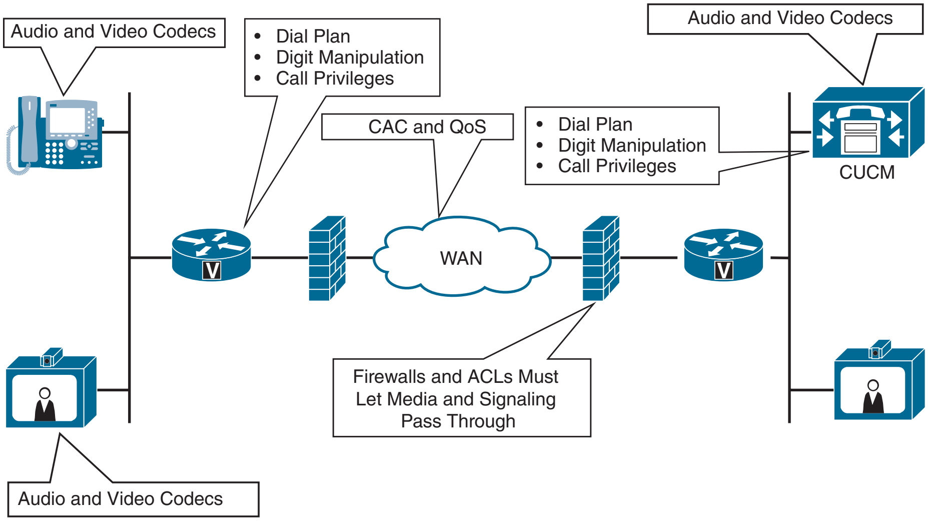


Figure 30-9 *Cisco Collaboration Call Setup Components*

If firewalls or access lists are implemented along the call path, they must allow call signaling and audio and video media to pass through to them for a call to set up. Media port numbers are dynamically negotiated during the call setup. Therefore, firewall adjustments must be implemented to track these negotiations and open proper ports through which the media will flow.

Key Topic

Some additional components can affect the call setup process. Audio and video codecs are implemented at endpoints and gateways. During the setup of a video call, the endpoints negotiate the codec that is used to encode and decode audio and video traffic. If two endpoints cannot agree on a common codec, the call setup will fail. Call Admission Control (CAC), if implemented, can block the call as it is being set up because of the existence of too many calls between two sites across the WAN. CAC is used to guard network resources from oversubscription, which can affect the quality of existing calls. Gateways might implement media transcoding functions when passing the media from one network to another. Gateways require DSP resources to perform these processing-intensive functions. Starting with Cisco IOS Release 15.0(1)M, if a DSP is required but is not available, when the phone goes off-hook, the caller receives a fast-busy tone. Prior to Cisco IOS Release 15.0(1)M, the caller would hear dead air.

When troubleshooting call setup issues, you must make correct judgments concerning the potential cause at the beginning of the troubleshooting procedure. Many distinct components are involved in the call. Many common call-setup issues relate solely to call control components. Based on the type of issue, you can deduce what might be causing the problem. For example, getting a reorder tone during dialing is almost certainly the result of an incorrect dial plan. Table 30-2 lists the most common endpoint call setup issues and the probable causes to check related to these issues.

Key Topic

Table 30-2 Common Endpoint Call Setup Issues and Probable Causes

Call Setup Issue	Probable Causes
Reorder tone during and at the end of dialing	Misconfigured CUCM Components: ■ Misconfigured dial plan ■ Insufficient calling privileges ■ Misconfigured digit manipulation
	CAC can also cause this issue
No ring-back tone	IP reachability issues to CUCM
	Gateway may block or drop audio
	ISDN may not provide ring-back tone
Unexpected second dial tone	Misconfigured dial plan
Video is not set up, only audio	Video codec mismatch
	CAC (such as RSVP Video Desired Mode)
	Regions
Dead air is heard	Firewall or ACL blocking media
One-way audio or video	Firewall or ACL blocking media in one direction, or CAC
Call is dropped after dialed	Audio or video codec mismatch
Call is dropped in the middle of the call	Repeatable issues are usually due to network connectivity events, but could also be caused by CAC or permission on the CUCM

The first call-setup issue listed is the reorder tone heard during and at the end of dialing. It's important to remember that Cisco Unified IP phones and collaboration endpoints that register to the Cisco Unified Communications Manager are also controlled by it. Therefore, issues can often be diagnosed with only this call control element, which provides all intelligence and features to the endpoints.

Misconfiguring Cisco Unified Communications Manager components can cause a reorder tone during and at the end of dialing. These components could include misconfiguring the dial plan, insufficient calling privileges for the type of call, or misconfigured digit manipulation at the call control component. CAC can also block the call. Cisco Unified Communications Manager or a separate component in the voice and video network can implement CAC, such as an H.323 gatekeeper or an RSVP-enabled router. If CAC blocks the call, you usually see the message "Not Enough Bandwidth" on the IP phone display or Cisco Telepresence endpoint. If the caller does not have the appropriate privileges to dial the number, the call is blocked. Several companies have a policy to block international numbers or costly premium numbers, such as 900 numbers, for many employees.

IP reachability problems to Cisco Unified Communications Manager can cause no ring-back tone. Alternatively, a gateway, if it is used, might not cut through the audio, or another network, such as ISDN or H.323, simply might not provide the ring-back tone. You should verify that IP connectivity to Cisco Unified Communications Manager is stable. If the affected call was placed outbound to the public switched telephone network (PSTN), additional tools on the gateway or at the network edge may be needed to assess where the issue resides.

An unexpected second dial tone during dialing is typically caused by a misconfigured dial plan on a call control component. The Cisco Unified Communications Manager administrator can try to identify the issue by using the Cisco Unified Communications Manager Dialed Number Analyzer. You must work from the Cisco Unified Communications Manager to diagnose and solve this issue because it cannot be solved at the endpoint level.

If only audio was set up for the call and not video, this issue could indicate a mismatch of video codecs between the endpoints. It could also indicate that CAC has blocked more resource-demanding video. Cisco Unified Communications Manager might have CAC configured to set up only audio if the WAN runs out of bandwidth. This behavior is called RSVP video desired mode. Try to isolate the video codec cause by dialing the same destination from another endpoint model that might support a different set of codecs. To isolate the CAC cause, you can try dialing the destination later, when more bandwidth might be available.

Dead air after the call is set up indicates a media-blocking function in the routed path. An ACL entry might be blocking RTP audio traffic. You can use the ACL packet-logging feature, which will log the denied packets on the router console. Voice and video protocol inspection engines are required at the firewall for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the Cisco Adaptive Security Appliance (ASA) to perform a deep packet inspection instead of passing the packet through the fast path. Several common inspection engines are enabled on the Cisco ASA appliance by default, but you might need to enable others depending on your network.

One-way calling between the same two endpoints means that the call can be set up in one direction only. This issue is typically caused by calling privileges. This behavior might also be intentional and might not be an issue. CAC is a direction-oriented mechanism and can block a call in one direction while allowing media to flow in the opposite direction. You should consider asymmetric bandwidth utilization in typical TCP/IP networks. A firewall or ACL that blocks a call setup in one direction can also cause the one-way calling issue. Use the packet-logging feature to identify the traffic that a firewall or access list denies. To isolate weak calling privileges, use the Cisco Unified Communications Manager Dialed Number Analyzer, or place the same call from the IP phone of a manager, who is expected to have higher calling privileges.

A call dropping immediately after it is dialed is typically caused by a mismatch of audio codecs; however, a mismatch of video codecs can also cause this issue. The behavior depends on endpoint algorithms if the call is dropped because of mismatched video codecs or is degraded to audio only. Try to place a test call from a different endpoint model that might support a different set of codecs. The Cisco Unified Communications Manager administrator should also check the codecs that are enabled for the affected endpoint or use the trace utility to see the sequence of events that led to the dropped call behavior.

Calls that are dropped in the middle of a conversation are usually caused by a network connectivity event. Make sure that the event is repeatable and not transient before you start troubleshooting. Check the IP connectivity between the endpoints in both directions. You can power-cycle the affected endpoints to initialize their software and then try to make a call again.

Key Topic

Calling issues on Cisco Telepresence CE software-based endpoints are like the potential issues of standard Cisco Unified IP phones. Because of the complex setup, a great variety of problems can be experienced when setting up a call with a Cisco Telepresence CE software-based endpoint. Cisco Telepresence CE software-based endpoints can register to the Cisco Unified Communications Manager or to the Cisco Expressway. Depending on the provisioning model, you should verify that the dial plan is correct and that calls can be successfully routed through that call control server. Also, related to the dial plan at the Cisco Unified Communications Manager, the caller can be blocked because of insufficient calling privileges. IP connectivity problems also contribute to failed call setup. Issues with IP routing, firewall configuration, and access lists that filter out audio or video in the routed path can all prevent a call from being successfully set up. CAC is used to maintain a good quality of media. In essence, CAC sets up a bandwidth limit that can accommodate a certain number of calls. If this bandwidth is consumed, no additional calls are admitted, and the calls fail to set up.

Common Media Issues

From the source of video information until the video is displayed at the remote endpoint, the video media might be subject to several factors that influence its final quality. Video call setup negotiates video parameters end to end, so the local endpoint adjusts its behavior according to the far-end endpoint capabilities, and vice versa. At the local endpoint that generates the video stream, a camera might not be properly tuned to local environmental conditions. As a result, the camera might not be able to focus on an object, such as because of a dark room or narrow contrast range. Figure 30-10 illustrates common issues that can affect media quality within a Cisco Collaboration solution.

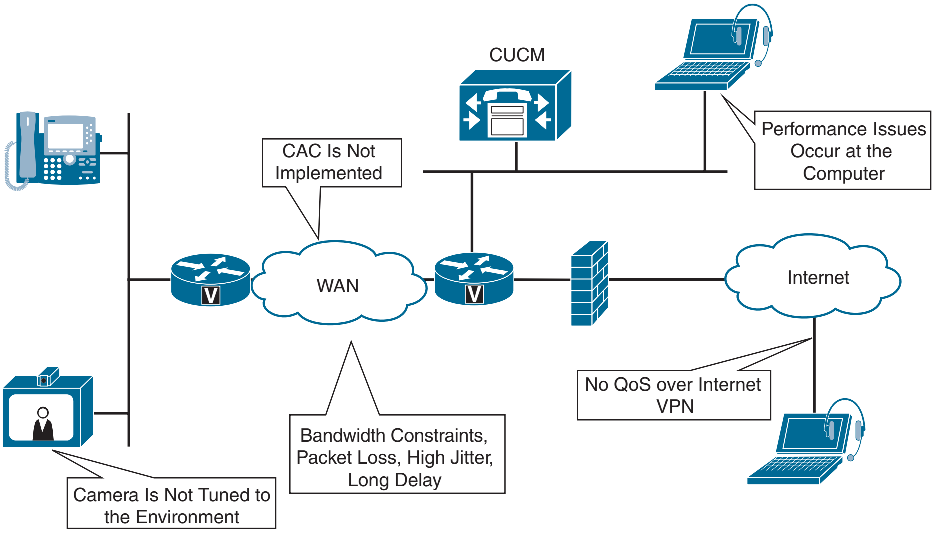

CUCM
Performance Issues Occur at the Computer
CAC Is Not Implemented
WAN
V
V
Internet
No QoS over Internet VPN
Bandwidth Constraints, Packet Loss, High Jitter, Long Delay
Camera Is Not Tuned to the Environment

Figure 30-10 *Media Quality Issues Within a Cisco Collaboration Solution*

The result of each video-encoding algorithm is the video bit rate. Because the video bit rate is dynamic and depends on many factors, it might be calculated and provisioned incorrectly across the WAN. When the video stream is transferred over the WAN, bandwidth reservation might be insufficient. High packet loss and high jitter can cause the far-end video decoder to miss video information, and the resulting video can be jerky. High end-to-end delay makes an interactive video call a bad experience.

If CAC is not implemented in the network, there is no control over the bandwidth that is available for video. All video calls might struggle because of lack of bandwidth per call, when too many calls exist. In addition to CAC, voice and video have specific traffic behavior and QoS requirements. Voice generally requires the network to meet the following characteristics in each direction:

Key Topic

- Jitter, or the variation in delay, should be less than 30 ms.
- One-way end-to-end delay for an interactive call must be less than 150 ms.
- Packet loss should generally be less than 1 percent. However, the speech quality of some audio codecs decreases rapidly when reaching a 0.5-percent packet loss, such as G.729A or G.729AB.
- Voice traffic should be marked with a DSCP EF to benefit from specific queuing behavior while transferred.

Video has requirements that are similar to voice. The only considerable difference is that video demands much more bandwidth, and its bandwidth requirements vary greatly. Video traffic should be marked with DSCP AF41 to benefit from bandwidth guarantees while transferred end to end. Many deployments mark voice and video the same. Packet loss results in a poor user experience and can usually be seen by artifacts on the screen. You can view call statistics to determine whether the network is experiencing the packet loss.

Key Topic

Call statistics can be checked on Cisco CE software-based endpoints using the web interface, as previously discussed, using the on-screen display, and using the CLI. Call statistics include packet loss, jitter, and delay statistics for incoming and outgoing audio and video channels. 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 from the CLI. 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.

If the CE software-based endpoint monitor displays an image outside of the monitor frame, be aware that most monitors will overscan TV resolutions such as 720p and 1080p. To fix this issue, you must enter the monitor menu system and find the appropriate setting. Different monitors use different terms, but look for something like Just Scan, Pixel by Pixel, or Underscan. Some monitors have this option for the native resolution of the display only. If you cannot find the option, go to the Endpoint Administrator Settings menu, change the video-output resolution, and try again.

If you cannot get any audio from the CE software-based endpoint when it is connected to a monitor by using HDMI, check whether the video output resolution for HDMI 1 is set to 800 × 600 or 1900 × 1200. Because of an issue with these two resolutions, they are run in DVI mode (DVI over HDMI), which does not support audio. To check or change the video-output resolution, navigate to **System > Configuration > Video > Output > HDMI 1 > Resolution** and choose another video output resolution for HDMI 1, or use the audio from Audio Line Out 1 and 2. If the audio on the dual stream is out of sync with the dual-stream video, be aware that Cisco CE software-based endpoints do not support lip synchronization between audio and video over SIP.

When you install but cannot control a second Cisco PrecisionHD camera on your CE software-based endpoint codec, you need to use a Video System Control Architecture (VISCA) cascading cable to connect the cameras. The VISCA cascading cable connects the first and second cameras. You need to configure the video-input source to set which camera you should control when this particular video-input source is active. To configure the second camera, which is connected to video input source 2, execute the CLI command **xConfiguration Video Input Source 2 CameraControl CameraId: 2**.

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 no-processing 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 CE software-based endpoints supports a maximum of 340 ms on all the audio bandwidth.

Cisco ClearPath is an innovative technology that can improve the quality of video while minimizing the effect of packet loss in networks with uncontrolled quality of data transmission. This technology is a set of algorithms for compensation of network losses in the communication channel and can work with any image quality, up to full high definition. Table 30-3 summarizes the major elements that influence media quality in a Cisco Collaboration solution.

Key Topic

Table 30-3 Major Elements Influencing Media Quality in a Cisco Collaboration Solution

Element	Description
Input video peripherals	Video input peripheral quality, lens, exposure range, focus capabilities, lighting conditions
Video codec	Selection of video codec, performance, and capabilities of video codec
Output video peripherals	Video output peripheral quality: screen, image-enhancing capabilities
Amount of video information	Video resolution, frames per second, object-moving behavior, background complexity, resulting video bit rate
Network QoS	Network, packet loss, jitter and delay characteristics, CAC, differentiated services in converged network
Correct bandwidth provisioned	Bandwidth overhead calculation and provisioning
CPU utilization	Computer hosting Cisco Jabber running many applications

Input-video peripheral quality has a direct influence on the quality of the video information that is produced. The following are major characteristics of the input-video peripheral:

- The quality of the lens that the camera uses
- The exposure range that the camera can process
- The focus capabilities
- The recommended lighting conditions for which the camera is designed

Selection of the video codec must consider the performance requirements, codec capabilities, and limitations in terms of its susceptibility to declined QoS, such as higher jitter. H.264 standards do not cover precisely how to encode and decode a video stream or how to recover from issues, such as from missed frames. Some of these functions are left to the vendor-endpoint implementations, which Cisco has revolutionized with technologies like ClearPath.

An output-video peripheral can have a strong impact on how video information is presented at the far end. Screens that are not tuned to contrast and brightness according to surrounding conditions can greatly affect how the video is experienced. Vendors also implement various video-enhancing capabilities, such as sharpening and noise reduction, that can improve the final media content perceived by the far-end participants.

The amount of video information has an impact on how much bandwidth the associated video stream requires in terms of video bit rate. Parameters that influence the video bit rate are video resolution, number of frames per second, and object moving behavior or complexity of the background behind the object.

The quality of video information can decline most rapidly with decreasing QoS in the video-transport network. High packet loss and high jitter can have a strong influence on video decoding behavior and can cause rapid degradation in video quality. High end-to-end delay is a problem for human conversation and makes it difficult to continue as normal. If the network carries multiple traffic types, differentiated services must be implemented to provide each traffic type with its own QoS requirements.

When calculating bandwidth requirements for an expected video stream, bandwidth overhead is seldom considered. Failure to consider bandwidth overhead leads to insufficient bandwidth reservation and packet loss. In a Cisco Unified Communications network, some additional bandwidth overhead above the expected video-stream bit rate must be considered. The network designer must address this situation.

The computer that hosts the client requires available processor time to encode and decode a video stream. If the computer runs too many applications and processor utilization is high, there might be no processor time left for the software-based video codec within the client. Processing power is also reduced when the computer runs on batteries. Endpoint-to-endpoint interoperability is also important when it comes to video quality. Video that is coded on an endpoint can appear inadequate on one endpoint but look perfect on another endpoint.

Troubleshooting Cisco Jabber

A few Cisco Jabber tools can be used to help troubleshoot issues. You can display message notifications that are collected during the registration process, whenever you change the operational mode, or whenever you choose a different deskphone device. Navigate to **Help > Show Error Notifications** to see whether any error or warning messages have been logged.

If a user encounters a problem with Cisco Jabber, that user can create a problem report. The user can enter a description of the problem, and the description is included in an autogenerated report. The report contains logs from the user's computer, and the report is saved to the desktop. The user can then send this file to the system administrator to help analyze the problem. The problem report can be generated from the Cisco Jabber interface, or it can be created from outside the application by navigating to **Start > All Programs > Cisco Jabber > Cisco Jabber Problem Report**. Use the following steps to create the problem report from Cisco Jabber:

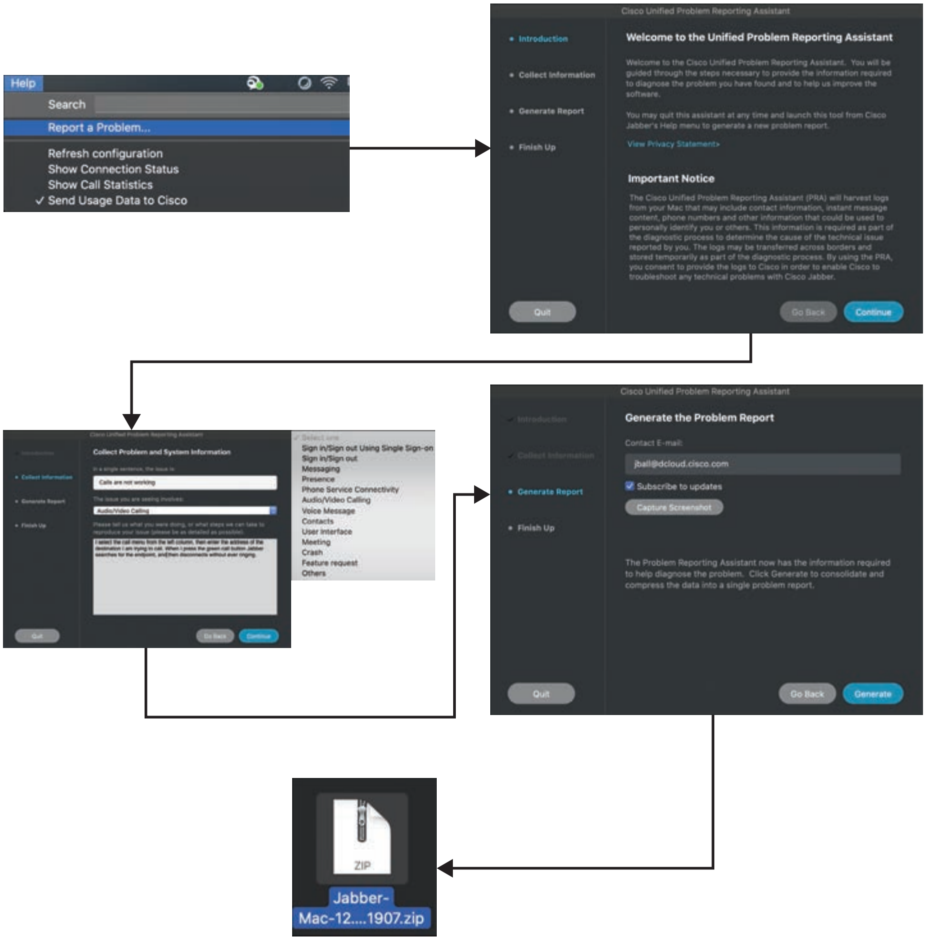
Step 1. On the Cisco Jabber client, navigate to **Help > Report a Problem**.

Step 2. Navigate through the three separate windows to create the report. In the first window, read through the welcome message, which has an important notice, and click **Continue**.

Step 3. In the second window, provide a single-sentence explanation of the issue, choose the problem category from the drop-down list, and optionally enter a more detailed problem description. Click **Continue**.

Step 4. In the third window, you can optionally attach a file to the report and click **Generate**. A copy of the report is saved to your computer desktop.

Cisco Jabber saves the problem report to the computer desktop as a .zip file. The file contains all the logs that are collected at the computer. You can unzip these files and assess the issue yourself, or send this .zip file to Cisco TAC for further analysis. Figure 30-11 illustrates the procedure to generate a problem report from Cisco Jabber.



Welcome to the Unified Problem Reporting Assistant

Welcome to the Cisco Unified Problem Reporting Assistant. You will be guided through the steps necessary to provide the information required to diagnose the problem you have found and to help us improve the software.

You may quit this assistant at any time and launch this tool from Cisco Jabber's Help menu to generate a new problem report.

Important Notice

The Cisco Unified Problem Reporting Assistant (PRA) will harvest logs from your Mac that may include contact information, instant message content, phone numbers and other information that could be used to personally identify you or others. This information is required as part of the diagnostic process to determine the cause of the technical issue reported by you. The logs may be transferred across borders and stored temporarily as part of the diagnostic process. By using the PRA, you consent to provide the logs to Cisco in order to enable Cisco to troubleshoot any technical problems with Cisco Jabber.

Collect Problem and System Information

In a single sentence, the issue is: Calls are not working

The issue you are seeing involves: Audio/Video Calling

Please tell us what you were doing, or what steps we can take to reproduce your issue (please be as detailed as possible): I select the call menu from the left column, then enter the address of the destination I am trying to call. When I press the green call button Jabber searches for the endpoint, and then disconnects without ever ringing.

Generate the Problem Report

Contact E-mail: jball@dcloud.cisco.com

☑ Subscribe to updates

The Problem Reporting Assistant now has the information required to help diagnose the problem. Click Generate to consolidate and compress the data into a single problem report.

Figure 30-11 *Problem Report from Cisco Jabber*

When Cisco Jabber is set to Automatic Registration, it is hard-coded to always try registering to the cloud first. Then it will try to register with Cisco Unified Communications Manager IM and Presence Service or the Cisco Unified Communications Manager. Last, it will try to send the registration communication to the Expressway Edge. The Cisco Jabber client can also be configured to manually search for any one of these services.

The client registers with different services of Cisco Unified Communications Manager, depending on whether the client operates in deskphone or softphone mode. Cisco Jabber shares all IP parameters with the host computer. These parameters must be set properly at the computer, which must have IP connectivity to Cisco Unified Communications Manager IM and Presence Service, Cisco Unified Communications Manager, and the Cisco TFTP server, if the client operates as a softphone. Cisco Unified Communications Manager CTI Manager is the service that is usually run with other services on Cisco Unified Communications Manager. For larger deployments, Cisco Unified Communications Manager CTI Manager can be run on a separate server. Cisco Jabber must be able to exchange traffic with the servers for the protocols that are used during the registration process. Most communication is based on HTTPS, such as SOAP and Cisco CallManager. Cisco IP Phone Services. XMPP is also used, as are TFTP, SIP, and CTIQBE, depending on the mode of the client. You should make sure that the appropriate port numbers are open at the firewalls that are installed in the routed path:

- SOAP uses server ports TCP 8191 and TCP 8443.
- XMPP uses server port TCP 5222.
- Cisco CallManager Cisco IP Phone Services use server port TCP 8443.
- TFTP uses server port UDP 69.
- SIP registration uses server ports UDP 5060, depending on how SIP was provisioned at the servers. Secure SIP uses 5061.
- CTIQBE uses server port TCP 2748.

The registration process for Cisco Jabber starts with entering a user ID, password, and the Cisco Unified Communications Manager IM and Presence Service address. The client automatically receives from the servers all other parameters that are required during the registration in softphone or deskphone mode. If the Cisco Unified Communications Manager IM and Presence Service address was entered as an IP address rather than by name, the address will change to the Cisco Unified Communications Manager IM and Presence Service host name automatically during the SOAP configuration exchange. The host computer must be able to resolve this host name, or the address field must be rewritten manually to the IP address during each new user login. This issue is frequently the reason that the client does not register.

Cisco Jabber shows different error messages when the login fails to aid in troubleshooting. The error message “Invalid user ID or password. Please try again” indicates an issue with the user credentials. The credentials are authenticated against the local Cisco Unified Communications Manager database or the LDAP server. The credentials might have expired at either server, or the LDAP server might not be reachable by the Cisco Unified Communications Manager. The error message “Unable to connect to network. Please check your network connection” indicates network-connectivity issues, DNS-resolution issues, issues at Cisco Unified Communications Manager IM and Presence Service, or the user might not hold the license for the client.

Also, Cisco Jabber is incompatible with NAT. To traverse NAT, the client must be behind a VPN connection. NAT and firewalls can cause a range of registration issues that must be resolved with the help of a security engineer. When deploying a Cisco Adaptive Security Appliance and Cisco AnyConnect Secure Mobility Client for Cisco Jabber for Windows, you should configure NAT rules to support the Cisco AnyConnect Secure Mobility Client. If you do not configure NAT rules, the Cisco AnyConnect Secure Mobility Client cannot communicate with the Cisco ASA.

If Cisco Jabber logs in and you want to make sure that the client has registered properly, use the Server Status and Notifications window to determine whether any components failed to register. If so, you can generate a problem report that contains the logs to provide more information to diagnose the problem. Cisco Jabber is hosted on a computer with other applications; therefore, it can face very specific issues that relate to the host computer environment. Table 30-4 identifies potential issues that can arise from this specific computer environment for Cisco Jabber.

Key Topic

Table 30-4 Common Call Setup Issues on Cisco Jabber

Issue	Possible Causes
No calls possible	Softphone is not registered, or deskphone CTI control does not work. Network connectivity issues or misconfigured servers exist.
No audio (softphone mode)	Required network ports are not open on the computer that hosts the application.
One-way audio or video (softphone mode)	Computer audio or video device on either side does not work. If connected over a Cisco VPN client (for Windows), ensure that the stateful firewall is disabled.
Poor audio quality	If echo or feedback is heard, be sure to use a proper headset and not computer speakers.
Incoming video is black (permanent)	Required network ports are not open on the computer that hosts the application.
Incoming video is black (transient)	Local or far-end computer experiences lack resources to encode or decode the video signal. Camera could be muted.

When a user logs in to the client but no calls are possible, consider the operational mode that Cisco Jabber uses:

- If Cisco Jabber is in softphone mode, the client might not be successfully registered as being in softphone mode with Cisco Unified Communications Manager.
- If Cisco Jabber is in deskphone mode, the CTI control component might not work because of an unregistered hardware Cisco Unified IP phone. Alternatively, CTI communication issues might exist, or the CTI gateway might be misconfigured in Cisco Unified Communications Manager or the Cisco IM and Presence Server. Also, the called target might not be registered with the call control server.

To verify Cisco Jabber connectivity, navigate to **Help > Show Connection Status** or **Help > Show Error Notifications**. If no audio is received in softphone mode, verify that the correct RTP ports (UDP 16384 to 32766) are open on the computer firewall.

One-way audio or video in softphone mode means that voice is heard or video is seen in one direction only. If the client is connected over a Cisco VPN client (for Windows), make sure that the stateful firewall setting is disabled on the host computer. The microphone, as an audio device peripheral, or the camera also might not work at the far end. When experiencing black incoming video as a permanent issue, and when only audio works, you must also consider the firewall setup on the host computer. If black incoming video is only a transient issue, the far-end system that encodes the video or the computer that decodes the video might be experiencing a temporary lack of computing resources.

Some major elements influence video quality in a Cisco Unified Communications environment for Cisco Jabber as well. These elements are the same for Cisco Jabber as they are for any other Cisco Unified IP phone or Telepresence endpoints. Refer to the media quality discussion under the "Common Media Issues" section for a review of these elements.

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 30-5 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 30-5 Key Topics for Chapter 30

Key Topic Element	Description	Page Number
Paragraph	Status Message Types on IP Phones	727
List	Log Archive Download Options	730
List	Files Included in the Current Log Bundle Folder	731
List	Files Included in the Eventlog Folder	733
List	Call Info Logs on CE Endpoints	734
List	Information Found in Call Logs on CE Endpoints	735
Paragraph	How to Read a Detailed Debug Log	736
Paragraph	How VLANs Impact Registration	738
List	Types of DHCP Servers	739
List	Tools for Testing IP Connectivity	740
List	TFTP SIP and SCCP Ports Used	741
Paragraph	How Registration Is Impacted from CTL and ITL Files	742
Paragraph	Call Setup Issues	743
Table 30-2	Common Endpoint Call Setup Issues and Probable Causes	743
Paragraph	Call Setup Issues in CE Endpoints	745
List	QoS Characteristics	746
Paragraph	Checking Call Statistics on CE Endpoints	747
Table 30-3	Major Elements Influencing Media Quality in a Cisco Collaboration Solution	748
List	Ports Used by Cisco Jabber	751
Table 30-4	Common Call Setup Issues on Cisco Jabber	752

Define Key Terms

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

802.1x, CAC, Codec, CTL, Current Logging, DHCP, DSP, Eventlog, Extended Logging, Historical Logs, ITL, Option 150, TVS, VLAN, VVID

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the three types of log archives that can be downloaded with their descriptions.
2. What are the four major characteristics of input-video peripherals that can influence media quality?
3. List the four steps to create a problem report on Cisco Jabber.

This page intentionally left blank

CHAPTER 31

Cisco Unified Communications Manager Reports

This chapter covers the following topics:

Dialed Number Analyzer: This topic will explain how to enable, access, and use the Dialed Number Analyzer tool on the Cisco Unified Communications Manager.

CAR Tool: This topic will explain how to enable, access, and use the Cisco CDR Analysis and Reporting tool, also known as the CAR tool, on the Cisco Unified Communications Manager.

CDR and CMR Logs on CUCM: This topic will explain the information contained within and the use for call detail records (CDRs) and call management records (CMRs). These records include user reports, system reports, and device reports.

Many tools can be used to troubleshoot issues and monitor analytical data from the Cisco Unified Communications Manager. Because this book is designed to introduce administrators to the basic functions of a Cisco Collaboration solution, this chapter will cover only two of these tools. Topics discussed in this chapter include the following:

- Dialed Number Analyzer
- CAR Tool
- CDR and CMR Logs on CUCM
  - User Reports on CUCM
  - System Reports on CUCM
  - Device Reports on CUCM

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.0 (CLCOR 350-801) exam:

- 1.4 Troubleshoot these network components in a Cisco Collaboration solution
  - 1.4.c LDAP integration on Cisco UCM

“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 31-1 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 31-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Dialed Number Analyzer	1–2
CAR Tool	3–4
CDR and CMR Logs on CUCM	5–6

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. How many services must be enabled on the CUCM before the Dialed Number Analyzer tool can be used?
   - **a.** None
   - **b.** One
   - **c.** Two
   - **d.** Four
2. How does the CAR tool process CDR files from the CDR Repository?
   - **a.** Compressed tar.gz files
   - **b.** Flat files
   - **c.** Direct from the source, not from the repository
   - **d.** Both flat files and compressed tar.gz files
3. Which of the following details are included in a CMR?
   - **a.** The date and time the call was started
   - **b.** The amount of data sent and received during the call
   - **c.** The time the call connected
   - **d.** The cause for the termination of a call
4. Which of the following user reports is available to users, managers, and administrators?
   - **a.** Top N
   - **b.** Cisco IP Phone Service
   - **c.** Cisco Unified Communications Manager Assistant (IPMA)
   - **d.** Bills
5. Which of the following system reports are available to managers and administrators?
   - **a.** QoS Summary
   - **b.** Traffic Summary

   c. System Overview
   d. CDR error

6. Which of the following is a device report available through the CAR tool on the CUCM?
   a. Endpoint
   b. Trunk
   c. Jabber
   d. Gateway

Foundation Topics

Dialed Number Analyzer

Many tools are available through the Cisco Unified Communications Manager. This vast ocean of tools exists for the many different call scenarios that can be processed by the CUCM. Although this chapter will not cover all the different tools available, a few tools are worth mentioning.

The Cisco Dialed Number Analyzer (DNA) is a calling simulator that will determine whether a call between a specific source and destination alias is possible through the current configuration within the Collaboration network. When DNA is used, a call is not actually placed. The returned data shows whether the call would be possible and indicates all of the call control mechanisms that will affect this call. Therefore, when calls are not possible, DNA will show what component in the Cisco Unified Communications Manager is preventing the call from connecting, if any apply. You can use the DNA tool to troubleshoot dial plan issues and issues that relate to calling privileges in Cisco Unified Communications Manager.

The Dialed Number Analyzer installs as a feature service along with Cisco Unified Communications Manager. The DNA tool can be used to analyze dial plans after they are deployed. You can use the tool to test a dial plan by providing dialed digits as input. This tool also analyzes the dialed digits and shows details of the call. You can use these results to diagnose the dial plan and identify any problems.

The Dialed Number Analyzer allows analysis of inbound and outbound calls in a Cisco Unified Communications Manager dial plan. It analyzes the calls and provides results that show complete details, including call patterns and calling- and called-party transformations that are applied to the dialed digits.

Before you can use the Dialed Number Analyzer, a Cisco Unified Communications Manager administrator must activate and implement the service. To activate the Dialed Number Analyzer services, follow these steps:

Step 1. From the Cisco Unified Serviceability page, navigate to **Tools > Service Activation**.

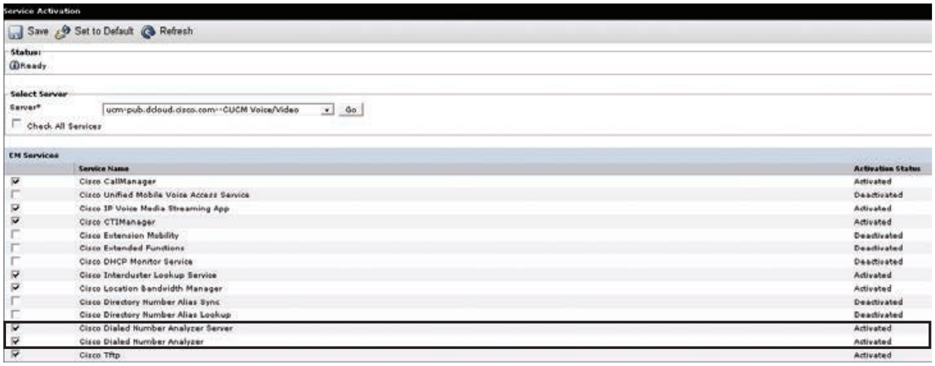
Step 2. Select the CUCM publisher from the drop-down list and click **Go**.

Step 3. Under the CM Services section, check both of the following DNA services:

- **Cisco Dialed Number Analyzer Server:** If you have more than one node in the CUCM cluster, activate this service on the node that will be dedicated to the Dialed Number Analyzer service.

- **Cisco Dialed Number Analyzer:** If you are planning to use the CUCM Dialed Number Analyzer, activate this service. This service may consume a lot of resources, so activate this service only on the CUCM node with the least amount of call-processing activity or during off-peak hours.

Step 4. Click **Save** to enable these services. Figure 31-1 illustrates how the services for the Dialed Number Analyzer can be activated.



Status:
Ready

Select Server
Server* ucm-pub.dcloud.cisco.com--CUCM Voice/Video Go
□ Check All Services

CM Services

	Service Name	Activation Status
☑	Cisco CallManager	Activated
□	Cisco Unified Mobile Voice Access Service	Deactivated
☑	Cisco IP Voice Media Streaming App	Activated
☑	Cisco CTIManager	Activated
□	Cisco Extension Mobility	Deactivated
□	Cisco Extended Functions	Deactivated
□	Cisco DHCP Monitor Service	Deactivated
☑	Cisco Intercluster Lookup Service	Activated
☑	Cisco Location Bandwidth Manager	Activated
□	Cisco Directory Number Alias Sync	Deactivated
□	Cisco Directory Number Alias Lookup	Deactivated
☑	Cisco Dialed Number Analyzer Server	Activated
☑	Cisco Dialed Number Analyzer	Activated
☑	Cisco Tftp	Activated

Figure 31-1 *Dialed Number Analyzer Services on the CUCM*

After activating DNA, you can use it to analyze call connection attempts. Although the DNA web page can be accessed from the Cisco Unified Serviceability menus, another way to access this tool may be a little bit easier. Follow these steps to access the Cisco Unified Communications Manager Dialed Number Analyzer:

Key Topic

Step 1. Navigate to **https://<*CUCM IP Address*>/dna**.

Step 2. Choose **Analysis > Phones**.

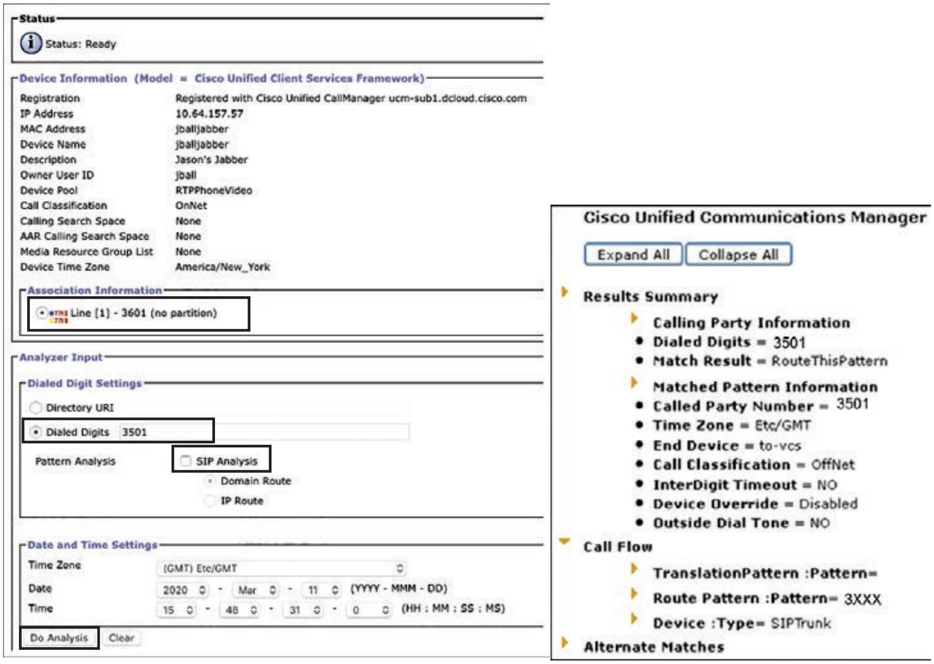
Step 3. Leave the text box next to the Find button empty and click **Find** to view a list of all available devices. Click the Device Name of the endpoint from which you want to simulate a call attempt.

Step 4. In the window that appears, do the following:

- From the Association Information section, choose **Line (1)**.
- In the Dialed Digits Settings section, choose the **Dialed Digits** radio button, and then enter the directory number of another device.
- Check the **SIP Analysis** check box.

Step 5. Click the **Do Analysis** button.

A new window will pop up with data from the analysis. You can use this data to analyze the results that appear in the results window. Figure 31-2 shows output from the Cisco Unified Communications Manager Dialed Number Analyzer.



Status

Status: Ready

Device Information (Model = Cisco Unified Client Services Framework)

Registration: Registered with Cisco Unified CallManager ucm-sub1.dcloud.cisco.com
IP Address: 10.64.157.57
MAC Address: jballjabber
Device Name: jballjabber
Description: Jason's Jabber
Owner User ID: jball
Device Pool: RTPPhoneVideo
Call Classification: OnNet
Calling Search Space: None
AAR Calling Search Space: None
Media Resource Group List: None
Device Time Zone: America/New_York

Association Information

● Line [1] - 3601 (no partition)

Analyzer Input

Dialed Digit Settings

○ Directory URI
● Dialed Digits 3501

Pattern Analysis: □ SIP Analysis
● Domain Route
○ IP Route

Date and Time Settings

Time Zone: (GMT) Etc/GMT
Date: 2020 - Mar - 11 (YYYY - MMM - DD)
Time: 15 - 48 - 31 - 0 (HH : MM : SS : MS)

Cisco Unified Communications Manager

Results Summary
- Calling Party Information
  - Dialed Digits = 3501
  - Match Result = RouteThisPattern
- Matched Pattern Information
  - Called Party Number = 3501
  - Time Zone = Etc/GMT
  - End Device = to-vcs
  - Call Classification = OffNet
  - InterDigit Timeout = NO
  - Device Override = Disabled
  - Outside Dial Tone = NO

Call Flow
- TranslationPattern :Pattern=
- Route Pattern :Pattern= 3XXX
- Device :Type= SIPTrunk

Alternate Matches

Figure 31-2 *Dialed Number Analyzer Tool and Output Results*

This output was generated from the Analyzer window, where the calling phone, number 3601, simulates dialing to the number 3501. The output window on the right side of the figure starts with a Results Summary and ends with Alternate Matches. The content of the analysis output depends on the dial plan configuration and the Analyzer window that was used to generate that output. This particular analysis shows that the called party, number 3501, is reachable by using a SIP trunk that is associated with route pattern 3XXX.

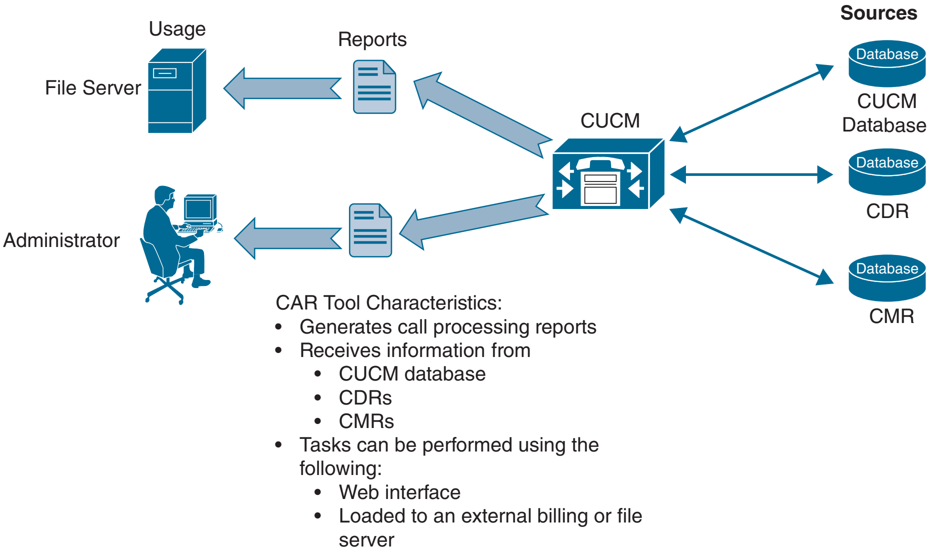
CAR Tool

All calls that the Cisco CallManager service processes can be logged by the Cisco Unified Communications Manager. This data includes different call details and call quality information. The Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) tool uses this data to provide system-generated reports to users, managers, and administrators. These reports can help monitor QoS issues, device utilization, or call statistics.

As its primary function, CAR generates reports about the users of CUCM and generates reports on the system status with respect to call processing. CAR also performs CAR database management activities. Administrators can perform these tasks in one of the following ways:

- Automatically configure the required tasks to take place
- Manually perform the tasks by using the web interface

All CAR reports use CDR data. CAR processes the CDRs from flat files that the CDR Repository service places in the CDR Repository folder structure. CAR then processes CDRs at a scheduled time and frequency. By default, CDR data loads continuously 24 hours per day and seven days per week. However, the administrator can set the loading time, interval, and duration as needed. In addition, the default setting loads only CDR records. CMR records are not loaded by default. Figure 31-3 illustrates the CAR tool characteristics previously outlined.



CAR Tool Characteristics:

- Generates call processing reports
- Receives information from
  - CUCM database
  - CDRs
  - CMRs
- Tasks can be performed using the following:
  - Web interface
  - Loaded to an external billing or file server

Figure 31-3 *CAR Tool Characteristics*

CAR is composed of a group of complementary services that administrators can activate in the Service Activation window of the Cisco Unified Serviceability page. Before CAR can be launched from the Tools menu in Cisco Unified Serviceability, you must activate the CAR services. In Cisco Unified Serviceability, navigate to **Tools > Service Activation**. Check the boxes next to the following CDR services:

- Cisco CAR Web Service
- Cisco SOAP-CDROnDemand Service (optional). (If using a third-party billing application that accesses CDR data via an HTTPS/Simple Object Access Protocol [HTTPS/SOAP] interface, activate this service.)

Certain CUCM service parameters must also be enabled to ensure that the CDR records are generated. The administrator can configure these parameters on the Service Parameters Configuration window from the Cisco Unified CM Administration page. To access the Service Parameters Configuration window, navigate to **System > Service Parameters**. Select the publisher CUCM from the first drop-down list, and then select the Cisco Call Manager service from the second drop-down list. Click the Advanced button to display the complete list of service parameters available. Table 31-2 identifies the list of service parameters that can affect CDR and CMR records.

Table 31-2 CDR and CMR Service Parameters on the CUCM

Service Parameter	Description
CDR Enabled Flag	This parameter determines whether CDRs are generated. Valid values specify True (CDRs are generated) or False (CDRs are not generated). For this required field, the default value specifies False. Enable this parameter on all servers.
CDR Log Calls with Zero Duration Flag	This parameter enables or disables the logging of CDRs for calls that never connected or that lasted less than one second. Cisco CallManager logs unsuccessful calls (calls that result in reorder, such as might occur due to a forwarding directive failure or calls that attempt to go through a busy trunk) regardless of this flag. This is a required field with a default value of False.
Call Diagnostics Enabled	Three settings can be configured under this menu option: ■ **Enabled Only When CDR Enable Flag is True:** Generates CMRs only when the CDR Enabled Flag service parameter is set to True. ■ **Enabled Regardless of CDR Enabled Flag:** Generates CMRs without regard to the setting in the CDR Enabled Flag service parameter. This parameter represents a required field. ■ The default value specifies **Disabled**, which will not generate CMRs.
Display FAC in CDR	This parameter determines whether the forced authorization codes (FAC) associated with the call display in the CDR. Valid values specify True (display authorization code in CDRs) or False (do not display authorization code in CDRs) for this required field. The default value specifies False.
Show Line Group Member DN in finalCalledPartyNumber CDR Field	This parameter determines whether the finalCalledPartyNumber field in the CDRs shows the directory number of the line group member who answers the call or the hunt pilot directory number. Valid values specify True (the finalCalledPartyNumber in CDRs will show the directory number of the phone that answered the call) or False (the finalCalledPartyNumber in CDRs will show the hunt pilot directory number). This parameter applies only to basic calls that are routed through a hunt list without future interactions, such as transfers, conference, and call park. If a feature is involved in the call, the hunt pilot directory number will show in the finalCalledPartyNumber field regardless of the setting in this parameter. The default value for this required field specifies False.

Service Parameter	Description
Add Incoming Number Prefix to CRD	This parameter determines whether CUCM adds the incoming prefix (as specified in the National Number Prefix, International Number Prefix, Subscriber Number Prefix, and Unknown Number Prefix Service Parameters) to the calling party number in the CDRs for that call. If the prefix is applied on the inbound side of the call, it is always added to the calling party number in the CDRs for that call. This occurs even if this parameter is set to False. If the prefix is applied on the outbound side, the prefix is added to the calling party number in the CDR or CDRs for that call, only if the parameter is set to True. If the Destination of the call is a gateway, CUCM will not add the prefix to the CDRs even if this parameter is enabled. This parameter is applied on a clusterwide basis. The default value for this required field specifies False.

The CAR tool provides different levels of user rights. In fact, the CAR tool provides reporting capabilities for three levels of users:

Key Topic

- Administrators are allowed to use all the features of CAR so that they can generate system reports to view system performance, verify load balancing, and troubleshoot.
- Managers can generate reports for users, departments, and QoS to help with call monitoring for budgeting or security purposes. Reports can also be used for determining the voice quality of the calls (for example, to ensure compliance with service-level agreements).
- End users can generate a billing report for their calls.

Any application or end user can act as a CAR administrator. Users who have been identified as CAR administrators have complete control over the CAR system. The administrator can modify all parameters that relate to the system and the reports. Cisco Unified Communications Manager CAR requires a minimum of one administrator.

CDR and CMR Logs on CUCM

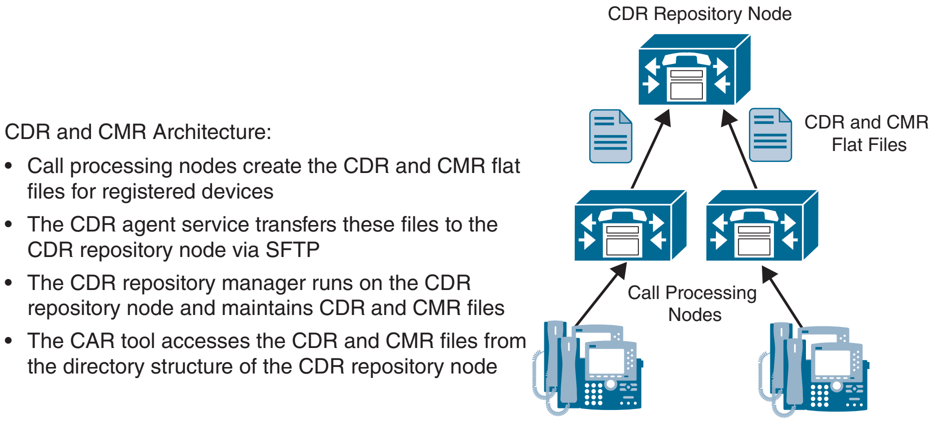
The call detail records (CDR) and call management records (CMR) architectures include different ways in which CDR and CMR files can be loaded to the CAR tool. CDRs provide details about the following:

Key Topic

- The called number
- The calling number
- The date and time that the call was started
- The time that the call connected
- The time that the call ended
- The cause for the termination of a call

CMRs include jitter, lost packets, the amount of data that was sent and received during the call, and latency. CDR data comprises CDRs and CMRs, collectively. A single call can result in the generation of several CDRs and CMRs. The CUCM records information regarding each call in CDRs and CMRs. CDRs and CMRs, known collectively as CDR data, serve as the basic information source for Cisco CAR.

The Cisco CDR Agent service transfers CDR and CMR files that CUCM generates from the local host to the CDR Repository node, where the CDR Repository Manager service runs over an SFTP connection. If the SFTP connection fails, the Cisco CDR Agent service continues to make connection attempts to the CDR Repository node until a connection is made. The Cisco CDR Agent service sends any accumulated CDR files when the connection to the CDR Repository node resumes. The CDR Repository Manager service maintains the CDR and CMR files, allocates the amount of disk space for use by CMRs and CDRs, sends the files to up to three configured destinations, and tracks the delivery result for each destination. The Cisco CAR tool accesses the CDR and CMR files in the directory structure that the CDR Repository Manager service creates. By default, the CAR tool will retain data for 60 days and up to 80 percent for a low watermark and 90 percent for a high watermark of the database. High and low watermarks can be modified for data retention in CAR, and the max age of data can be set up to 180 days. To modify these settings, navigate to **System > Database > Configure Automatic Purge**. Figure 31-4 illustrates the CDR and CMR structure within the Cisco Unified Communications Manager.



CDR and CMR Architecture:

- Call processing nodes create the CDR and CMR flat files for registered devices
- The CDR agent service transfers these files to the CDR repository node via SFTP
- The CDR repository manager runs on the CDR repository node and maintains CDR and CMR files
- The CAR tool accesses the CDR and CMR files from the directory structure of the CDR repository node

Figure 31-4 *CDR and CMR Structure on the CUCM*

The CAR tool allows CDR and CMR dump information to be exported to a location on the local computer. The CDR and CMR dump is in CSV format and can be used for external billing tools. The following procedure shows how to export CDR and CMR data:

Key Topic

Step 1. From the Cisco Unified CM CDR Analysis and Reporting page, navigate to **CDR > Export CDR/CMR**. The Export CDR/CMR Records window displays.

Step 2. In the From Date and To Date drop-down lists, choose a date range for the CDR and CMR dump.

Step 3. In the Select Records section, check the **CDR Records** box, or the **CMR Records** box, or both.

Step 4. Click **Export to File**.

Step 5. In the new window that appears, right-click **CDR Dump** or **CMR Dump** and choose **Save As** to download the files. Choose the folder to which the files will be saved on the local disk.

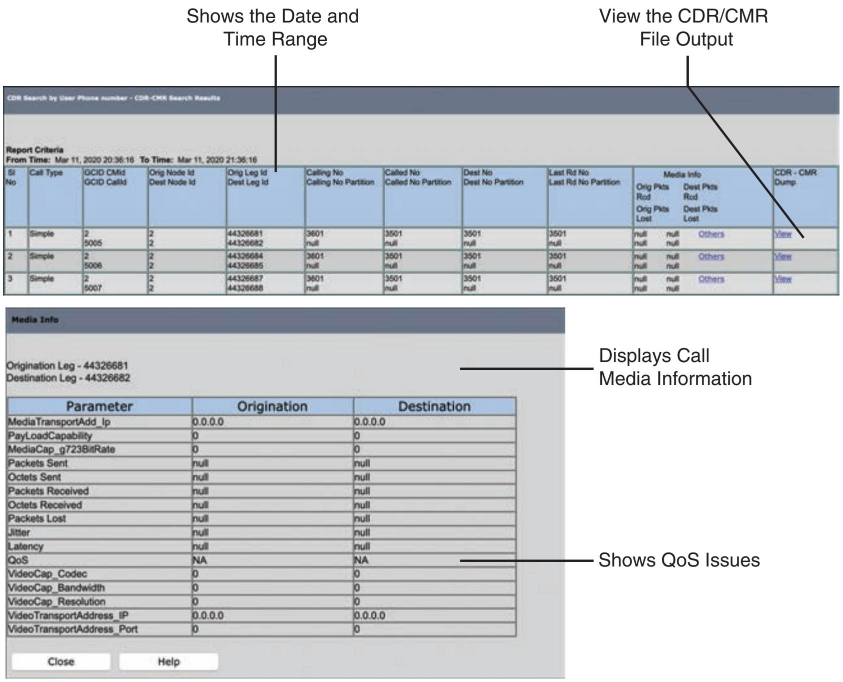
Step 6. If you check the Delete File box, the files will be deleted from the CUCM as soon as you click the Back or Close button.

The CDR Search feature can be used to display details about a phone call, such as to show QoS details. Follow these steps to search for a special call:

Step 1. Navigate to **CDR > Search > By User/Phone Number/SIP URL**. The configuration window for the CDR search appears.

Step 2. In the configuration window for CDR Search, you can specify a phone number or range. You can use the Search Internal Phone Number/SIP URL Based User link to display a search window to find configured end users in CUCM. In this window, search for a first name or last name and click **Select** to search for this user. Then, in the From Date and To Date fields, enter a date and time range. When ready, click **OK** to perform the search.

A table with the results of the CDR search will display in a new window. The result includes all call details. To send the report via email, click the Send Report button. To display the media information, click the Others link to open the details in a new window. The media information includes QoS details, such as jitter or latency values for each call. Figure 31-5 illustrates the search results generated in the table.



Shows the Date and Time Range

View the CDR/CMR File Output

CDR Search by User Phone number - CDR-CMR Search Results

Report Criteria
From Time: Mar 11, 2020 20:36:16 To Time: Mar 11, 2020 21:36:16

Sl No	Call Type	GCID CMId GCID CallId	Orig Node Id Dest Node Id	Orig Leg Id Dest Leg Id	Calling No Calling No Partition	Called No Called No Partition	Dest No Dest No Partition	Last Rd No Last Rd No Partition	Media Info Orig Pkts Rcd / Dest Pkts Rcd Orig Pkts Lost / Dest Pkts Lost	CDR - CMR Dump
1	Simple	2 5005	2 2	44326681 44326682	3601 null	3501 null	3501 null	3501 null	null null Others null null	View
2	Simple	2 5006	2 2	44326684 44326685	3601 null	3501 null	3501 null	3501 null	null null Others null null	View
3	Simple	2 5007	2 2	44326687 44326688	3601 null	3501 null	3501 null	3501 null	null null Others null null	View

Media Info

Origination Leg - 44326681
Destination Leg - 44326682

Displays Call Media Information

Parameter	Origination	Destination
MediaTransportAdd_Ip	0.0.0.0	0.0.0.0
PayLoadCapability	0	0
MediaCap_g723BitRate	0	0
Packets Sent	null	null
Octets Sent	null	null
Packets Received	null	null
Octets Received	null	null
Packets Lost	null	null
Jitter	null	null
Latency	null	null
QoS	NA	NA
VideoCap_Codec	0	0
VideoCap_Bandwidth	0	0
VideoCap_Resolution	0	0
VideoTransportAddress_IP	0.0.0.0	0.0.0.0
VideoTransportAddress_Port	0	0

Shows QoS Issues

Figure 31-5 *CDR Data Search Results on the CUCM*

User Reports on CUCM

The CAR tool can be used to generate CDR reports. Users, managers, and CDR administrators can generate user reports. The CAR tool includes user reports for Bills, Top N, Cisco Unified Communications Manager Assistant (IPMA), and Cisco IP Phone Service.

Bills user reports can be generated for an individual or based on an entire department. Individual user reports are available for users, managers, and CAR administrators. Individual bills provide call information for the date range that is specified. This report allows you to generate, view, or email summary or detailed information about individual phone bills. CAR administrators who are application users cannot generate this report.

Department user reports are available for managers and CAR administrators. Department bills provide call information and QoS ratings. A manager can generate a summary or detailed report of the calls that all users make who report to the manager or only those users whom the manager selects. A CAR administrator can generate a summary or detailed report of the calls that some or all users in the system make.

Top N user reports provide data on users based on the top charges, longest duration, or most consumed calls. By Charge user reports are available for managers and CAR administrators. The Top N by Charge reports list the top number of users who incurred a maximum charge for calls during a period that the manager or CAR administrator specifies. Reports that are generated by destinations show the destinations that incurred the maximum charges. Reports that are generated by all calls list the calls that incurred the maximum charges. By Number of Calls user reports are available for managers and CAR administrators as well. The Top N by Number of Calls report lists the users who incurred the maximum number of calls. Reports that are generated using extensions list the extensions that placed or received the greatest number of calls during the period that is specified.

The Cisco Unified Communications Manager Assistant (IPMA) user reports are available only for administrators, and they are based on Manager Call Usage or Assistant Call Usage reports. For Manager Call Usage, the Cisco Unified Communications Manager Assistant Summary and Detail reports provide call completion usage details for Cisco Unified Communications Manager assistant managers. The manager reports can include only calls that managers manage for themselves, or only calls that assistants manage for managers, or calls that both managers and assistants handle for managers. For Assistant Call Usage, the Cisco Unified Communications Manager Assistant Summary and Detail reports provide call completion usage details for Cisco Unified Communications Manager Assistants. The Assistant reports can include only calls that assistants manage for themselves, or only calls that assistants manage for managers, or calls that assistants manage for themselves and for managers.

Cisco IP Phone Service user reports are also available for CAR administrators exclusively. The Cisco IP Phone Services report shows selected Cisco IP Phone Services, the number of users who are subscribed to each of the selected services, and the utilization percentage for each of the selected services. Table 31-3 provides a summary of all the different user reports available on the Cisco Unified Communications Manager.

Key Topic

Table 31-3 User Reports on the CUCM

User Report	Method of Application	User Access Allowed
Bills	Individual	Users, Managers, or Administrators
	Department	Managers or Administrators
Top N	By Charge	Managers or Administrators
	Duration	Managers or Administrators
	By Number of Calls	Managers or Administrators
Cisco Unified Communications Manager Assistant (IPMA)	Manager Call Usage	Administrators
	Assistant Call Usage	Administrators
Cisco IP Phone Service	Shows Cisco IP Phone Services, the number of users who are subscribed to each of the selected services, and the utilization percentage for each of the selected services	Administrators

System Reports on CUCM

In addition to user reports, the CAR tool can also generate different system reports. CAR provides system reports for managers and CAR administrators. Both managers and CAR administrators can access the QoS summary report. Only CAR administrators can access all of the other reports.

Four different QoS reports can be generated using the CAR tool:

- **Detail** reports are available for CAR administrators only. The QoS Detail report provides the QoS ratings that are attributed to inbound and outbound calls on the CUCM network for the period that was specified. You can use this report to help monitor the voice quality of all calls on a user-level basis for the entire system.
- **Summary** reports are available for managers and CAR administrators. This report provides a pie chart that shows the distribution of QoS grades that are achieved for the specified call classifications and period. The report also provides a table that summarizes the calls for each QoS grade.
- **By Gateway** reports are available for CAR administrators only. This report shows the percentage of the calls for each of the chosen gateways that meet the QoS criteria that the user chooses. Reports can be generated on an hourly, daily, or weekly basis.
- **By Call Types** reports are available only for CAR administrators. This report shows the percentage of the calls for each chosen call type that meets the QoS criteria that the user chooses. Reports can be generated on an hourly, daily, or weekly basis.

Two different types of Traffic reports are available for system reporting from the CAR tool, and all Traffic reports are available only to CAR administrators. Summary reports provide information about the call volume for a period that the administrator specified. They include only those call types and QoS voice-quality categories that were chosen. You can use this report to determine the number of calls that are being made on an hourly, weekly, or daily basis. Summary by Extension reports provide information about the call volume for a period and set of extensions that the administrator specified. It includes only those call types and extensions that were chosen.

The next system report available to CAR administrators only is the Forced Authorization Code/Client Matter Code (FAC/CMC) reports. Three different types of reports can be generated here:

- **Client Matter Code** reports allow administrators to view the following information:
  - Originating and destination numbers
  - The date and time that the call originated
  - The call duration in seconds
  - The call classification for calls that relate to each chosen client matter code
- **Authorization Code Name** reports allow administrators to view the following information:
  - Originating and destination numbers
  - The date and time that the call originated
  - The call duration in seconds
  - The call classification
  - The authorization level for calls that relate to each chosen authorization code name
- **Authorization Level** reports allow administrators to view the following information:
  - Originating and destination numbers
  - The date and time that the call originated
  - The call duration in seconds
  - The authorization code name
  - The call classification for calls that relate to each chosen authorization level

Some other system reports also are useful to CAR administrators. The Cisco Unified Communications Manager MCID service tracks malicious calls. The Malicious Call Details report displays the details of malicious calls for a given date range. The Cisco Unified Communications Manager Call Precedence service allows authenticated users to preempt lower-priority phone calls. The PDF version of the CAR Precedence Call Summary report displays the call summary for the precedence values in the form of a bar chart, on an hour of the day, day of week, or day of month basis, for each of the precedence levels that were chosen. You can use the System Overview report to see a high-level picture of the CUCM network. The CDR

Error report provides statistics for the number of error records in the CAR Billing Error table and the reason for the errors. You can use this report to determine whether CAR incurred any errors with CDR data while the CDR data was loaded. Table 31-4 summarizes the system reports available through CAR as outlined in this section.

Table 31-4 System Reports on the CUCM

System Report	Method of Application	User Access Allowed
QoS	Detail	Administrators
	Summary	Managers and Administrators
	By Gateway	Administrators
	By Call Types	Administrators
Traffic	Summary	Administrators
	Summary by Extension	Administrators
Forced Authorization Code/Client Matter Code (FAC/CMC)	Client Matter Code	Administrators
	Authorization Code Name	Administrators
	Authorization Level	Administrators
Malicious Call Details	CUCM MCID service	Administrators
Precedence Call Summary	CUCM Call Precedence service	Administrators
System Overview	High-level picture of the CUCM network	Administrators
CDR Error	Error records in the CAR Billing_Air table	Administrators

Device Reports on CUCM

Device reports help CAR administrators track the load and performance of Cisco Unified Communications Manager–related devices, such as gateways or conference bridges. The following device reports are available only for CAR administrators.

Three Gateway reports are available to administrators on the Cisco Unified Communications Manager. You can use the Gateway Detail report to track issues with specific gateways. This report provides a list of calls that used the specified gateways. This report can be used to review detailed information about the chosen gateways. The administrator can specify gateways by type. The Gateway Summary report provides a summary of all the calls that went through the gateways. It also provides the total number of calls and the duration for each of the categories. The categories are Incoming, Tandem, and Outgoing (Long-Distance, Local, International, Others, OnNet). The report also provides the total calls for each QoS value for each gateway in the system. The Gateway Utilization report provides an estimate of the utilization percentage for the gateways.

The Route Pattern/Hunt Pilot reports can be generated to accommodate five different levels of information. The Route and Line Group Utilization report provides an estimated utilization percentage of the chosen route and line groups. The administrator can examine the usage based on each hour of a day or by a specified number of days of the week or month. Reports are generated for each chosen route and line group. You can use the report to analyze whether the route and line group capacity is sufficient to meet the usage requirements.

The Route/Hunt List Utilization report provides an estimated utilization percentage of the chosen route and hunt list. Reports are generated for each chosen route and hunt list. You can use the report to analyze whether the route and hunt list capacity is sufficient to meet the usage requirements. The Route Pattern/Hunt Pilot Utilization report provides an estimated utilization percentage of the chosen route patterns and hunt pilots. The CDR Hunt Pilot Call Summary report displays the call details for the specified hunt pilot. This report displays only an overview of the calls for the hunt pilots; hunt member information is not included. Finally, the Hunt Pilot Detail report displays call details for a hunt pilot number or a hunt member directory number.

Two different Conference Bridge reports are available through the CAR tool. The Conference Call Details report allows the administrator to generate and view details about conference calls and conference bridges. The summary report displays the summary information for conference calls within a chosen date and time range, but it does not contain information about each individual conference participant call log. The Conference Bridge Utilization report provides an estimate of the utilization percentage of the conference bridges. The administrator can examine the usage based on each hour of a day or by a specified number of days of the week or month.

The Voice Messaging Utilization report provides an estimate of the utilization percentage of the voice-messaging devices. Table 31-5 summarizes all the different device reports available on the CAR tool through the Cisco Unified Communications Manager.

Key Topic

Table 31-5 Device Reports on the CUCM

Device Report	Method of Application	User Access Allowed
Gateway	Detail	Administrator
	Summary	Administrator
	Utilization	Administrator
Route Pattern/Hunt Pilot	Route and Line Group Utilization	Administrator
	Route/Hunt List Utilization	Administrator
	Route Pattern/Hunt Pilot Utilization	Administrator
	Hunt Pilot Summary	Administrator
	Hunt Pilot Detail	Administrator
Conference Bridge	Conference Call Details	Administrator
	Conference Bridge Utilization	Administrator
Voice Messaging Utilization	Utilization percentage of the voice-messaging devices	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 35, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 31-6 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 31-6 Key Topics for Chapter 31

Key Topic Element	Description	Page Number
Steps	Using DNA to Analyze Call Behavior	759
Table 31-2	CDR and CMR Service Parameters on the CUCM	762
List	Levels of CAR Users	763
List	Details Provided in CDRs	763
Steps	Steps to Export CDR/CMR Data	764
Table 31-3	User Reports on the CUCM	767
Table 31-4	System Reports on the CUCM	769
Table 31-5	Device Reports on the CUCM	770

Define Key Terms

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

CAR Tool, CDR, CDR Agent Service, CDR Repository Manager Service, CDR Repository Node, CMC, CMR, DNA, FAC

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What are the steps to use the Cisco DNA tool?
2. List the three types of users who can access the CAR tool and the files they can access.
3. List all the CDR and CMR attributes that are included in the log file details.

CHAPTER 32

Real-Time Monitoring Tool (RTMT)

This chapter covers the following topics:

Cisco Unified RTMT Overview: This topic will describe the Cisco Unified Real-Time Monitoring Tool (RTMT) general parameters and how to access it.

Monitor Systems with RTMT: This topic will explain how to use the Cisco Unified RTMT for system monitoring.

Monitor the CUCM with RTMT: This topic will explain how to use the Cisco Unified RTMT to monitor the Cisco Unified Communications Manager.

The Cisco Unified Communications Manager, Cisco Unity Connection, and the IM and Presence server all include many trace files, syslog messages, and counters that indicate the current system and server health. An administrator can access these counters and files using the Cisco Unified Real-Time Monitoring Tool, or RTMT, which is a client that supports monitoring, alert definition and generation, file collection, and viewing of syslog messages. The Cisco Unified RTMT is a complex and advanced tool that should be used by engineers who know how to work with it. This chapter serves only to introduce you to the RTMT so that you can begin to explore what this tool is capable of and see how it can be used in a Cisco Collaboration solution. Topics discussed in this chapter include the following:

- Cisco Unified RTMT Overview
- Monitor Systems with RTMT
- Monitor the CUCM with RTMT

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 1.4 Troubleshoot these network components in a Cisco Collaboration solution
  - 1.4.c LDAP integration on Cisco UCM

“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 32-1 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 32-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Cisco Unified RTMT Overview	1–2
Monitor Systems with RTMT	3–4
Monitor the CUCM with RTMT	5–6

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 the AMC service parameter, what is the default value for the Data Collection Polling Rate?
   a. 15 seconds
   b. 30 seconds
   c. 150 seconds
   d. 300 seconds
2. Which of the following operating systems allows the Cisco Unified RTMT client to be downloaded?
   a. Windows
   b. MAC
   c. Chromebook
   d. All of these answers are correct.
3. Which of the following is an example of a perfmon counter on RTMT?
   a. Number of registered phones
   b. Number of active calls
   c. Voice messaging port usage
   d. All of these answers are correct.
4. How many perfmon counter charts can be displayed in RTMT for each category tab?
   a. 6
   b. 12
   c. 15
   d. 18
5. Which of the following is a gateway that can be monitored from the Gateway Activity window in RTMT?
   a. MGCP FXS
   b. MGCP PRI

c. H.323

d. All of these answers are correct.

6. Which of the following replication status values in the Database Summary window of RTMT indicates that replication is finished setting up and is working?

a. 0

b. 1

c. 2

d. 3

e. 4

Foundation Topics

Cisco Unified RTMT Overview

The Cisco Unified Real-Time Monitoring Tool (RTMT), which runs as a client application, uses HTTPS and TCP to monitor system performance, device status, device discovery, CTI applications, and voice-messaging ports. RTMT allows administrators to view a set of predefined management objects that monitor the health of Cisco Unified Communications Manager, Cisco Unity Connection, and Cisco IM and Presence Service installations. RTMT can generate various alerts in the form of emails for objects when values exceed or fall below user-configured thresholds. It can also collect and view traces in files from different services, view syslog messages in the syslog viewer, and work with performance-monitoring counters. Even when RTMT is not running as an application on the desktop, tasks, such as alarm updates, continue to take place on the server in the background. Cisco RTMT uses the following services and servlets:

Key Topic

- **Cisco AMC Service:** This service starts automatically after the installation and allows RTMT to retrieve real-time information from the server or from a server in a cluster.
- **Cisco CallManager Seviceability RTMT:** This service, which supports RTMT, starts automatically after the installation.
- **Cisco RIS Data Collector:** The Real-Time Information server maintains real-time information, such as performance counter statistics, critical alarms that are generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as RTMT, SOAP applications, and AMC to retrieve the information that is stored on the server.
- **Cisco Tomcat Stats Collector:** The Cisco Tomcat Stats Servlet allows monitoring of the Cisco Tomcat perfmon counters by using the RTMT or CLI.
- **Cisco Trace Collection Servlet:** The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces by using the RTMT client. If this service is stopped on a server, the administrator cannot collect or view traces on that server.
- **Cisco Trace Collection Service:** The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the RTMT client.

- **Cisco Log Partition Monitoring Tool:** This service, which starts automatically after the installation, monitors the disk usage of the log partition on a server.
- **Cisco SOAP-Real-Time Service APIs:** The Cisco SOAP-Real-Time Service APIs, which start automatically after installation, allow the collection of real-time information for devices and CTI applications.
- **Cisco SOAP-Performance Monitoring APIs:** The Cisco SOAP-Performance Monitoring APIs allow the use of performance monitoring counters for various applications through SOAP APIs. The service starts automatically after installation.
- **Cisco RTMT Reporter Servlet:** This service, which starts automatically after installation, allows publishing of reports for the RTMT.

As mentioned previously, the Cisco AMC Service starts automatically after installation and allows the RTMT to retrieve real-time information from the server or from a server in a cluster. The service parameters of this service can be modified to control what information is collected using the RTMT. To modify the service parameters that are associated with the RTMT, you can navigate to **System > System Parameters** from the Cisco Unified CM Administration web interface and choose the active server. From the list of services, choose Cisco AMC Service and configure or verify the following fields:

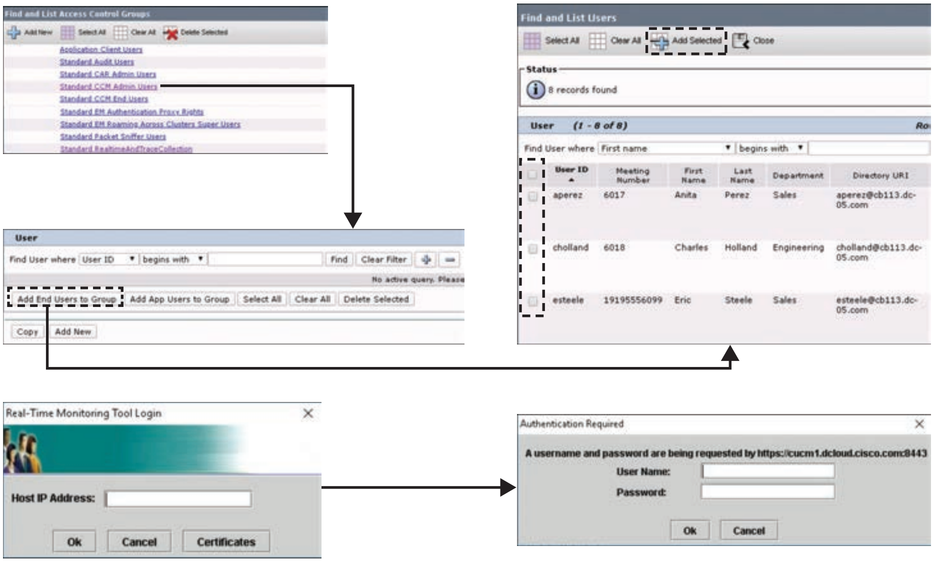
Key Topic

- **Primary Collector:** This parameter specifies the primary AMC (the server that collects clusterwide real-time information). The value must match one of the configured servers, and preferably the server with no or minimal call processing. By default, this server is the first node in the cluster.
- **Failover Collector:** The server that is specified in this parameter is used to collect real-time data when the primary AMC is down or unreachable. No data will be collected when the primary collector is not active unless the failover collector is specified.
- **Data Collection Enabled:** This parameter determines whether collecting and alerting of real-time cluster information are enabled (True) or disabled (False). The default is enabled (True).
- **Data Collection Polling Rate:** This parameter specifies the AMC collecting rate in seconds. The default is 30 seconds, the minimum is 15 seconds, and the maximum is 300 seconds.
- **Server Synchronization Period:** This parameter specifies the amount of time in seconds that the backup AMC waits at start in order to determine if the primary AMC is up and actively collecting. This parameter prevents the backup AMC from assuming the collecting task prematurely. The default is 60 seconds.

The RTMT can be installed on a client computer that works with resolutions 800×600 and higher, running any Microsoft Windows version from XP to Windows 10, or Linux with a KDE or Gnome client. Some engineers have been able to use RTMT on an Apple Mac computer by downloading the Linux version to the Mac; however, Windows is the preferred operating system that Cisco recommends using. Alternatively, Mac users can build a Windows VM using Bootcamp, Parallels, or some other VM solution, such as VMware vFusion. This solution will allow the RTMT to run on the Windows operating system while using the Mac computer. Both 32-bit and 64-bit versions of Windows operating systems are supported. Cisco Unified RTMT can be downloaded from the Cisco Unified CM Administration web interface. You need to navigate to **Applications > Plugins** and search for All Plugins. Then click the download link for Cisco Unified Real-Time Monitoring Tool–Windows or –Linux.

To use the RTMT after the application has been downloaded, an end user or application user must be enabled. The RTMT supports either end users or application users for logins. To allow end users or application users to log in to RTMT, navigate to **User Management > User Settings > Access Control Group** in the Cisco Unified CM Administration web interface. Search for the Standard CCM Admin Users group and select it to open the settings menus. Then select the Add End Users to Group or Add App Users to Group button to search for the desired user or users. Check the box beside all desired users and click the Add Select button. Perform the same action for the Standard Real-TimeAndTraceCollection group.

The RTMT is version dependent on the Cisco Unified Communications Manager, so be sure to download the latest version. There are some big changes coming to RTMT with Cisco Unified Communications Manager version 14. When starting the RTMT, enter the server IP or host name in the Host IP Address field and click OK. In the User Name field, enter the previously configured end user or application user. In the Password field, enter the password credentials of that user. Click OK to connect to the server. Figure 32-1 illustrates how to add users to groups and log in to RTMT.



8 records found

User (1 - 8 of 8)

Find User where First name begins with

	User ID	Meeting Number	First Name	Last Name	Department	Directory URI
□	aperez	6017	Anita	Perez	Sales	aperez@cb113.dc-05.com
□	cholland	6018	Charles	Holland	Engineering	cholland@cb113.dc-05.com
□	esteele	19195556099	Eric	Steele	Sales	esteele@cb113.dc-05.com

A username and password are being requested by https://cucm1.dcloud.cisco.com:8443

Figure 32-1 *Add Users to Groups and Log In to RTMT*

Key Topic

The menu bar in RTMT allows access to different tasks. Although the menu bar offers several different menus, the RTMT window is composed of the following general components. File allows administrators to save, restore, and delete existing RTMT profiles, monitor Java Heap Memory Usage, go to the Serviceability Report Archive window in Cisco Unified Serviceability, log off, or exit RTMT. From the RTMT **File > Cisco Unified Reporting** menu option, administrators can access Cisco Unified Reporting from RTMT. Edit allows administrators to configure categories for table format view, set the polling rate for devices and performance monitoring counters, hide the quick launch channel, and edit the trace settings for RTMT. Windows allows users to close a single RTMT window or all RTMT windows. Application, depending on the configuration, allows users to browse the applicable web pages for Cisco Unified CM Administration, Cisco Unified Serviceability, Cisco Unity Connection Administration, and Cisco Unity Connection Serviceability. Figure 32-2 illustrates the menus available in RTMT.

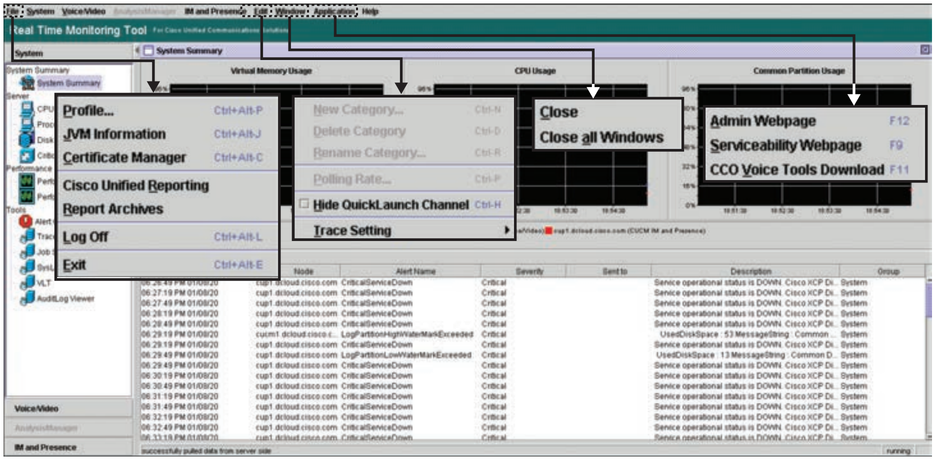
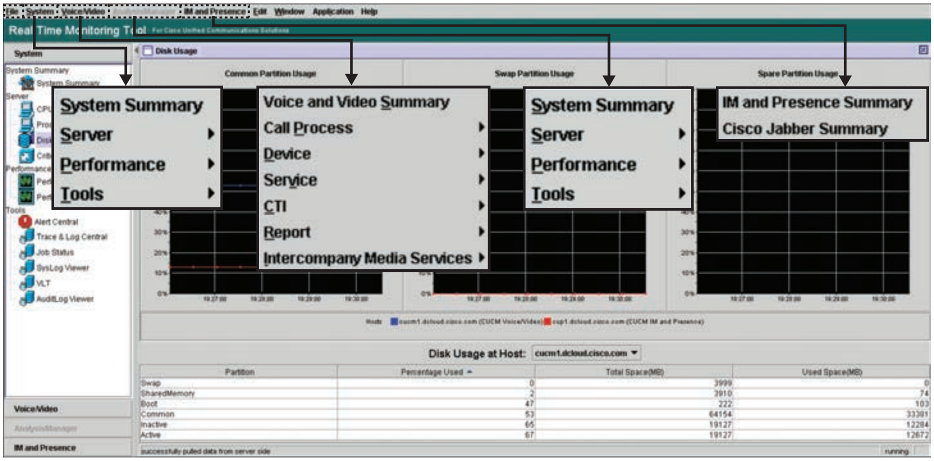


Figure 32-2 *RTMT General Menu Options*

When the Cisco Unified Communications Manager and other UC services are being monitored, RTMT menus have five additional menus: System, Voice/Video, Unity Connection, IM and Presence, and AnalysisManager. A category is composed of a group of monitored performance counters, such as Disk Usage and Critical Services in the System menu, or Call Activity and Device Summary in the Voice/Video menu. The bottom toolbar in the Cisco RTMT monitoring pane contains tabs, and each tab has an associated category name. All performance counters that are monitored in a specific tab belong to that specific category. The bottom toolbar displays any categories that the administrator accesses during an RTMT session.

Key Topic

Each additional menu contains different categories to access monitoring or troubleshooting tasks, some of which depend on the platform that is being monitored. System contains system and platform health monitoring, such as CPU and memory monitoring, or displays the current disk usage. This menu allows administrators to monitor the system summary, monitor server resources, work with performance counters, work with alerts, collect traces, and view system log messages. It also gives you access to Trace & Log Central to collect and view trace files for different services. The SysLog Viewer displays log messages from the system itself and from the hosting server. Voice/Video displays server-specific statistics and summaries. This menu allows you to view Cisco Unified Communications Manager summary information on the server, monitor call processing information, and view and search for devices, monitor services, and CTI. This item is available only when RTMT is connected to a Cisco Unified Communications Manager server. Unity Connection allows you to view the Port Monitor tool and display server-specific statistics and summaries. This item is available only when RTMT is connected to a Cisco Unity Connection server. IM and Presence allows you to view summaries for Cisco Unified IM and Presence Service and Cisco Jabber. This item is available only when RTMT is connected to a Cisco Unified IM and Presence server. AnalysisManager displays configuration or license summaries and includes tools, such as Call Path Analysis. This item is available only when RTMT is connected to a Cisco Unified Communications Manager server. Figure 32-3 illustrates four additional menus available in RTMT.



Partition	Percentage Used ▴	Total Space(MB)	Used Space(MB)
Swap	0	3999	0
SharedMemory	2	3910	74
Boot	47	222	103
Common	53	64154	33381
Inactive	65	19127	12284
Active	67	19127	12672

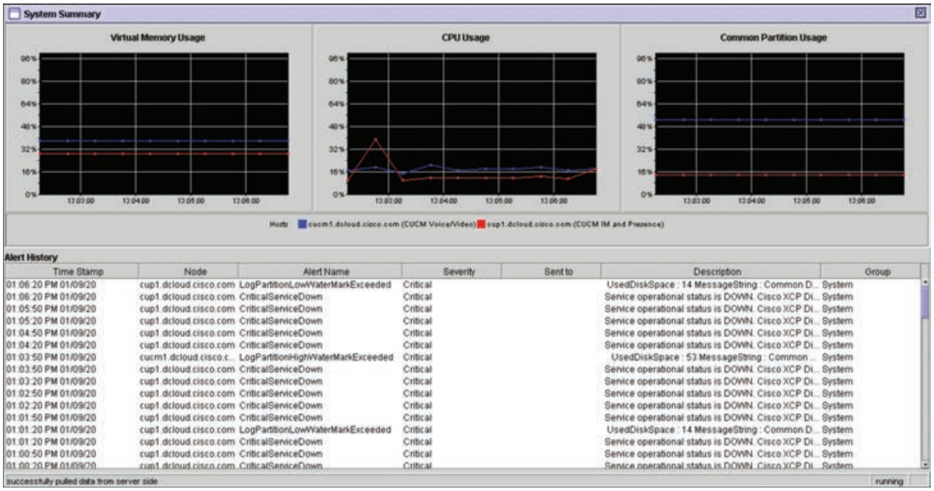
successfully pulled data from server side

Figure 32-3 *Additional RTMT Menu Options*

Monitor Systems with RTMT

When RTMT is connected to a Cisco Unified Communications Manager server, you can monitor three platform values within a single screen. The System Summary provides an overview of the Virtual Memory Usage, CPU Usage, and Common Partition Usage. The values are displayed for each cluster node in a different color, as defined in the three monitors. The Alert History, which is displayed below the monitors, provides the most recently received alert messages, with a timestamp, the node, and alert details. Figure 32-4 illustrates the System Summary menu options.

Navigate to System > System Summary



Alert History

Time Stamp	Node	Alert Name	Severity	Sent to	Description	Group
01:06:20 PM 01/09/20	cup1.dcloud.cisco.com	LogPartitionLowWaterMarkExceeded	Critical		UsedDiskSpace : 14 MessageString : Common D...	System
01:06:20 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:05:50 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:05:20 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:04:50 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:04:20 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:03:50 PM 01/09/20	cucm1.dcloud.cisco.c...	LogPartitionHighWaterMarkExceeded	Critical		UsedDiskSpace : 53 MessageString : Common ...	System
01:03:50 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:03:20 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:02:50 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:02:20 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:01:50 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:01:20 PM 01/09/20	cup1.dcloud.cisco.com	LogPartitionLowWaterMarkExceeded	Critical		UsedDiskSpace : 14 MessageString : Common D...	System
01:01:20 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:00:50 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
01:00:20 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System

successfully pulled data from server side

Figure 32-4 *System Summary Menu Options on RTMT*

The Cisco Unified Communications Manager, Cisco Unity Connection, and Cisco IM and Presence server directly update performance counters, called *perfmon counters*. The counters contain information on the system and the devices on the system, such as

Key Topic

- The number of registered phones
- The number of active calls
- The number of available conference bridge resources
- Voice-messaging port usage

The RTMT displays perfmon counters in chart or table format. The chart format displays the perfmon counter information by using loan charts. Up to six charts can be displayed for each category tab. When you open the performance monitor, the chart format is chosen by default. To change this to the table format, choose Edit in the top menu, choose New Category, and check the Present Data in Table View check box. After creating a category, you cannot change the display from the chart format to a table format, or vice versa. To add a new perfmon counter to a chart or table view, simply drag and drop a counter from the tree in the chart or table, or double-click the counter, select it from the list, and click the Add button. If you right-click an active perfmon counter, various options, such as removing the counter from the current view or setting an alert, are displayed. Figure 32-5 illustrates the performance monitor options using perfmon counters on RTMT.

Navigate to System > Performance > Open Performance Log Viewer

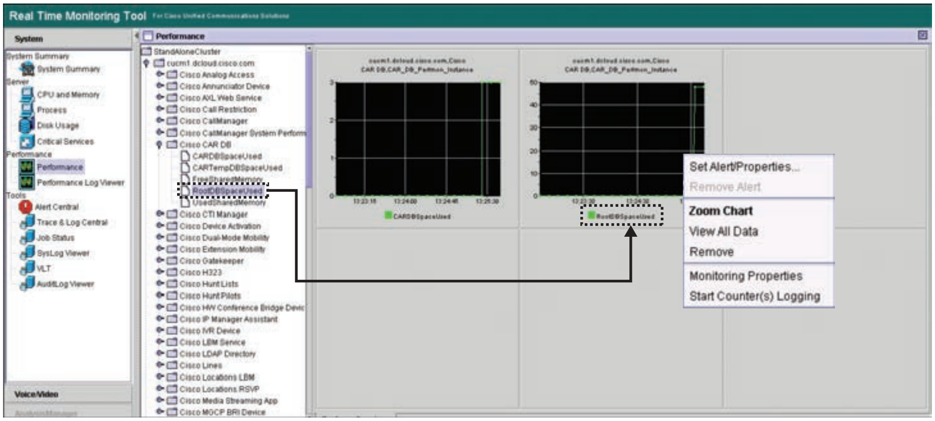


Figure 32-5 *Performance Monitor Options Using Perfmon Counters on RTMT*

The RTMT system can generate alert messages to notify administrators when a predefined condition is met, such as when an active server goes from up to down. The system can send alerts through email. RTMT supports alert defining, setting, and viewing, and contains preconfigured and user-defined alerts. Although you can perform configuration tasks for both preconfigured and user-defined alerts, you cannot delete preconfigured alerts. To access the Alert menu, from the top menu, navigate to **System > Tools > Alert**. The following menu options are available:

Key Topic

- **Alert Central:** This option comprises the history and status of every alert in the system.
- **Set Alert/Properties:** This menu category allows you to set alerts and alert properties.

- **Remove Alert:** This menu category allows you to remove an alert.
- **Enable Alert:** With this menu category, you can enable alerts.
- **Disable Alert:** You can disable an alert with this category.
- **Suspend Cluster/Node Alerts:** This menu category allows you to temporarily suspend alerts on a particular server or on an entire cluster.
- **Clear Alerts:** This menu category allows you to reset an alert (change the color of an alert item to black) to signal that an alert has been managed. After an alert has been raised, its color will automatically change in RTMT and will stay that way until you manually clear the alert. The manual clear alert action does not update the System Cleared Timestamp column in Alert Central. This column is updated only if the alert condition is automatically cleared.
- **Clear All Alerts:** This menu category allows you to clear all alerts.
- **Reset All Alerts to Default Config:** This menu category allows you to reset all the alerts to the default configuration.
- **Alert Detail:** This menu category provides detailed information on alert events.
- **Config Email Server:** In this category, you can configure the email server to allow alert notifications by email.
- **Config Alert Action:** This category allows you to set actions to take for specific alerts, and you can configure the actions to send the alerts to any desired email recipients.

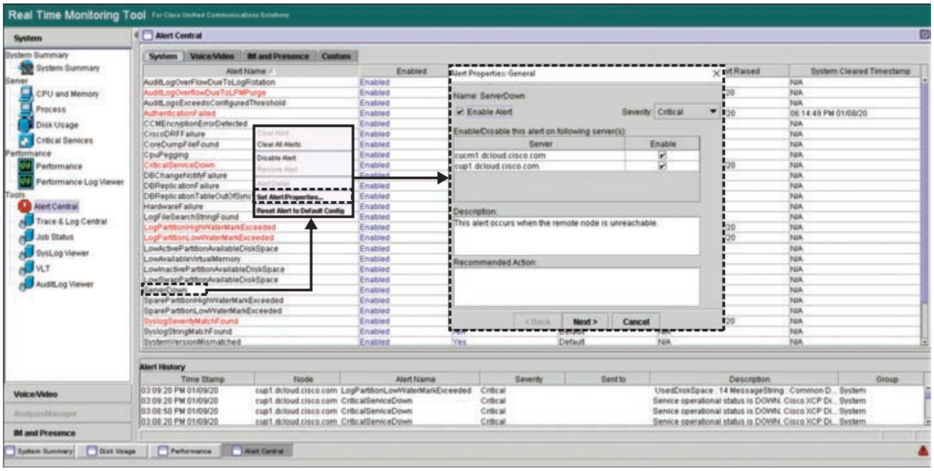
In RTMT, the administrator can configure alert notifications for perfmon counter value thresholds and set alert properties for the alert, such as the threshold, duration, frequency, and so on. RTMT predefined alerts are configured for perfmon counter value thresholds as well as event, or alarm, notifications. To configure email notification for alerts, you must define the email server in the Config Email Server menu and then define the config alert action, which is where email recipients are added.

The Alert Central monitoring window displays the Alert Status and Alert History of the alerts that the system has generated. RTMT displays both preconfigured alerts and custom alerts in Alert Central. RTMT organizes the alerts under the applicable tabs: System, Voice/Video, Unity Connection, IM and Presence, and Custom. As administrator, you can enable or disable preconfigured and custom alerts in Alert Central, but you cannot delete preconfigured alerts.

You can access Alert Central by navigating in the RTMT menus to **System > Tools > Alert > Alert Central**. To sort alert information in the Alert Status pane, click the up/down arrow that is displayed in the column heading. For example, click the up/down arrow that displays in the Enabled or in the Safe Range columns. You can sort Alert History information by clicking the up/down arrow in the columns in the Alert History page. To see Alert History that is out of view in the pane, use the scroll bar on the right side of the pane. To enable, disable, or remove an alert, from the Alert Status window, right-click the alert and choose Disable Alert or Remove Alert, depending on what you want to accomplish.

To customize alarm settings, right-click a specific alert and choose Set Alert/Properties. You can define different options such as Threshold, Alarm Frequency, and Schedule. You can also specify User-Defined Email Text and Trigger Alert Action settings. In addition, you can remove only user-defined alerts from RTMT. The Remove Alert option appears grayed out when choosing a preconfigured alert. Figure 32-6 illustrates the Alert Central settings.

Navigate to System > Tools > Alert > Alert Central



Alert Name	Enabled	System Cleared Timestamp
AuditLogOverFlowDueToLogRotation	Enabled	N/A
AuditLogOverflowDueToLPMPurge	Enabled	N/A
AuditLogsExceedsConfiguredThreshold	Enabled	N/A
AuthenticationFailed	Enabled	06:14:49 PM 01/08/20
CCMEncryptionErrorDetected	Enabled	N/A
CiscoDRFFailure	Enabled	N/A
CoreDumpFileFound	Enabled	N/A
CpuPegging	Enabled	N/A
CriticalServiceDown	Enabled	N/A
DBChangeNotifyFailure	Enabled	N/A
DBReplicationFailure	Enabled	N/A
DBReplicationTableOutOfSync	Enabled	N/A
HardwareFailure	Enabled	N/A
LogFileSearchStringFound	Enabled	N/A
LogPartitionHighWaterMarkExceeded	Enabled	N/A
LogPartitionLowWaterMarkExceeded	Enabled	N/A
LowActivePartitionAvailableDiskSpace	Enabled	N/A
LowAvailableVirtualMemory	Enabled	N/A
LowInactivePartitionAvailableDiskSpace	Enabled	N/A
LowSwapPartitionAvailableDiskSpace	Enabled	N/A
ServerDown	Enabled	N/A
SparePartitionHighWaterMarkExceeded	Enabled	N/A
SparePartitionLowWaterMarkExceeded	Enabled	N/A
SyslogSeverityMatchFound	Enabled	N/A
SyslogStringMatchFound	Enabled	N/A
SystemVersionMismatched	Enabled	N/A

Alert Properties: General

Name: ServerDown

☑ Enable Alert   Severity: Critical

Enable/Disable this alert on following server(s):

Server	Enable
cucm1.dcloud.cisco.com	☑
cup1.dcloud.cisco.com	☑

Description:

This alert occurs when the remote node is unreachable.

Recommended Action:

< Back   Next >   Cancel

Alert History

Time Stamp	Node	Alert Name	Severity	Sent to	Description	Group
03:09:20 PM 01/09/20	cup1.dcloud.cisco.com	LogPartitionLowWaterMarkExceeded	Critical		UsedDiskSpace : 14 MessageString : Common D...	System
03:09:20 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
03:08:50 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System
03:08:20 PM 01/09/20	cup1.dcloud.cisco.com	CriticalServiceDown	Critical		Service operational status is DOWN. Cisco XCP Di...	System

Figure 32-6 *RTMT Alert Central Settings*

Key Topic

The Trace & Log Central feature in RTMT allows administrators to configure on-demand trace collection for a specific date range or an absolute time. As administrator, you can collect trace files that contain search criteria that were specified and save the trace collection criteria for later use. You can also schedule one recurring trace collection and download the trace files to an SFTP or FTP server on the network or collect a crash dump file. After you collect the files, you can view them in the appropriate viewer within RTMT. You can also view traces on the server without downloading the trace files by selecting the Remote Browse feature. You can also use the Remote Browse feature to download the traces to the local PC:

Step 1. Double-click **Remote Browse from Trace and Log Central**, choose **Trace Files**, and then click **Next**.

Step 2. In the Select UCM Services/Application tab, select the desired services.

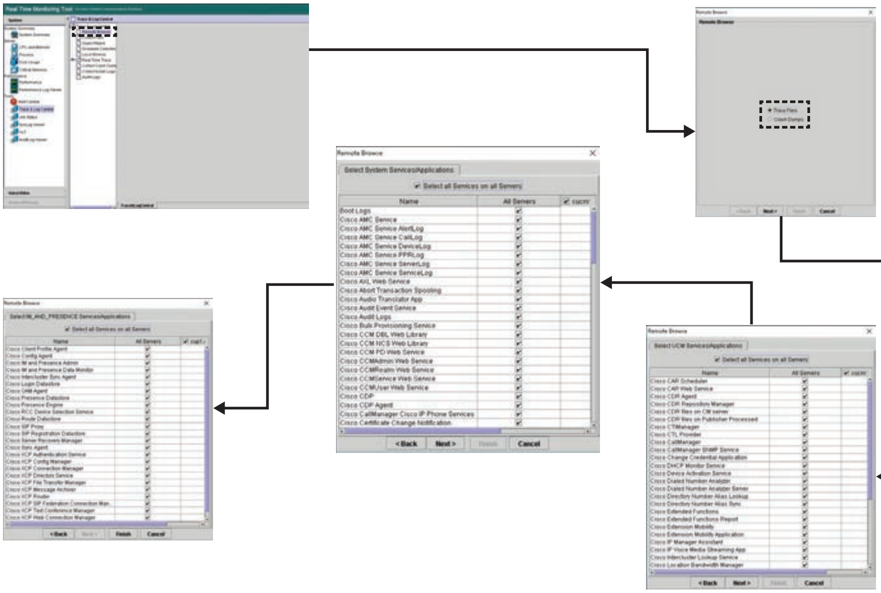
Step 3. To select all options available, check the **Select All Services on All Servers** check box and click **Next**. The Select System Services/Application tab appears.

Step 4. Select a service or check the **Select All Services on All Servers** check box, and then click **Next** again.

Step 5. Finally, the Select IM_AND_PRESENCE Services/Application tab appears. Select a service or check the **Select All Services on All Servers** check box. At least one box must be checked on one of the three pages.

Step 6. When done, click **Finish**. Cisco Unified Communications Manager then will perform the query and display the results.

Figure 32-7 illustrates the steps required to set up Remote Browse from the RTMT.



Remote Browse

Select System Services/Applications

☑ Select all Services on all Servers

Name	All Servers	☑ cucm
Boot Logs	☑	
Cisco AMC Service	☑	
Cisco AMC Service AlertLog	☑	
Cisco AMC Service CallLog	☑	
Cisco AMC Service DeviceLog	☑	
Cisco AMC Service PPRLog	☑	
Cisco AMC Service ServerLog	☑	
Cisco AMC Service ServiceLog	☑	
Cisco AXL Web Service	☑	
Cisco Abort Transaction Spooling	☑	
Cisco Audio Translator App	☑	
Cisco Audit Event Service	☑	
Cisco Audit Logs	☑	
Cisco Bulk Provisioning Service	☑	
Cisco CCM DBL Web Library	☑	
Cisco CCM NCS Web Library	☑	
Cisco CCM PD Web Service	☑	
Cisco CCMAdmin Web Service	☑	
Cisco CCMRealm Web Service	☑	
Cisco CCMService Web Service	☑	
Cisco CCMUser Web Service	☑	
Cisco CDP	☑	
Cisco CDP Agent	☑	
Cisco CallManager Cisco IP Phone Services	☑	
Cisco Certificate Change Notification	☑	

Remote Browse

Select UCM Services/Applications

☑ Select all Services on all Servers

Name	All Servers	☑ cucm
Cisco CAR Scheduler	☑	
Cisco CAR Web Service	☑	
Cisco CDR Agent	☑	
Cisco CDR Repository Manager	☑	
Cisco CDR files on CM server	☑	
Cisco CDR files on Publisher Processed	☑	
Cisco CTIManager	☑	
Cisco CTL Provider	☑	
Cisco CallManager	☑	
Cisco CallManager SNMP Service	☑	
Cisco Change Credential Application	☑	
Cisco DHCP Monitor Service	☑	
Cisco Device Activation Service	☑	
Cisco Dialed Number Analyzer	☑	
Cisco Dialed Number Analyzer Server	☑	
Cisco Directory Number Alias Lookup	☑	
Cisco Directory Number Alias Sync	☑	
Cisco Extended Functions	☑	
Cisco Extended Functions Report	☑	
Cisco Extension Mobility	☑	
Cisco Extension Mobility Application	☑	
Cisco IP Manager Assistant	☑	
Cisco IP Voice Media Streaming App	☑	
Cisco Intercluster Lookup Service	☑	
Cisco Location Bandwidth Manager	☑	

Remote Browse

Select IM_AND_PRESENCE Services/Applications

☑ Select all Services on all Servers

Name	All Servers	☑ cup1
Cisco Client Profile Agent	☑	
Cisco Config Agent	☑	
Cisco IM and Presence Admin	☑	
Cisco IM and Presence Data Monitor	☑	
Cisco Intercluster Sync Agent	☑	
Cisco Login Datastore	☑	
Cisco OAM Agent	☑	
Cisco Presence Datastore	☑	
Cisco Presence Engine	☑	
Cisco RCC Device Selection Service	☑	
Cisco Route Datastore	☑	
Cisco SIP Proxy	☑	
Cisco SIP Registration Datastore	☑	
Cisco Server Recovery Manager	☑	
Cisco Sync Agent	☑	
Cisco XCP Authentication Service	☑	
Cisco XCP Config Manager	☑	
Cisco XCP Connection Manager	☑	
Cisco XCP Directory Service	☑	
Cisco XCP File Transfer Manager	☑	
Cisco XCP Message Archiver	☑	
Cisco XCP Router	☑	
Cisco XCP SIP Federation Connection Man...	☑	
Cisco XCP Text Conference Manager	☑	
Cisco XCP Web Connection Manager	☑	

Figure 32-7 *Remote Browse Under Trace and Log Central in the RTMT*

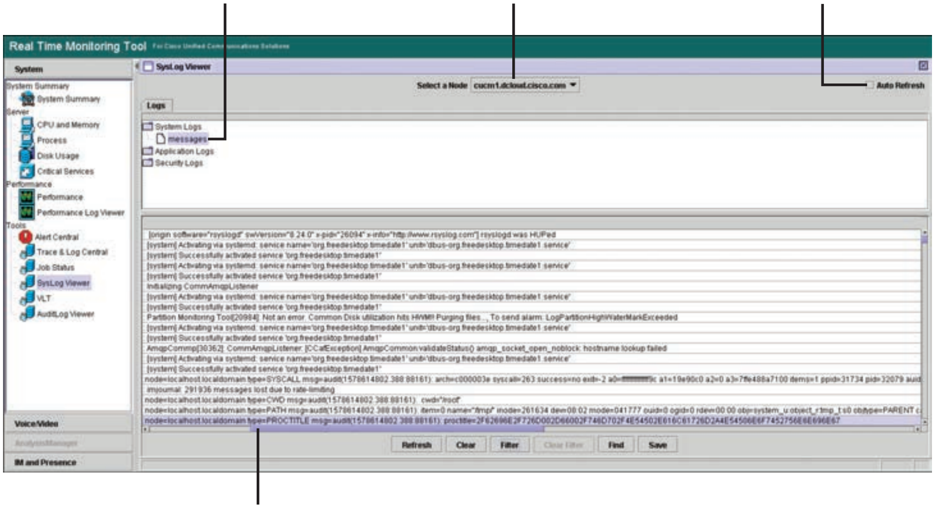
After a message states that Remote Browse is ready, click Close. After the query is performed, RTMT will display the results. You can now open a file by double-clicking it, or can select a file to download or delete. To refresh a specific service or a specific server in a cluster, click the service or server name, and then click the Refresh button. To refresh all services or all servers in a cluster that display in the tree hierarchy, click the Refresh All button.

The Syslog Viewer displays various error messages from the system, application, and security log. To access the syslogs of a specific node, select the node from the drop-down menu in the top center of the window. When the node is chosen, the log appears in the window below. Next, open a log file folder and click Messages. The syslog messages from the chosen folder are now displayed. To filter the results, click the Filter button, and then choose the options to filter from the drop-down boxes displayed in the popup window. To remove the filter, click the Clear Filter button. All logs are displayed after the filter is cleared. To automatically refresh the screen, check the Auto Refresh check box in the upper-right corner of the window. Syslog messages also display the syslog definition, which includes recommended actions, in an adjacent pane when the syslog message is double-clicked. Figure 32-8 illustrates the Syslog viewer under Alert Central in RTMT.

Select the Log File

Select the Node

Check Box to Auto Refresh the Message Output



```
[origin software="rsyslogd" swVersion="8.24.0" x-pid="26094" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
[system] Activating via systemd: service name='org.freedesktop.timedate1' unit='dbus-org.freedesktop.timedate1.service'
[system] Successfully activated service 'org.freedesktop.timedate1'
[system] Activating via systemd: service name='org.freedesktop.timedate1' unit='dbus-org.freedesktop.timedate1.service'
[system] Successfully activated service 'org.freedesktop.timedate1'
Initializing CommAmqpListener
[system] Activating via systemd: service name='org.freedesktop.timedate1' unit='dbus-org.freedesktop.timedate1.service'
[system] Successfully activated service 'org.freedesktop.timedate1'
Partition Monitoring Tool[20984]: Not an error. Common Disk utilization hits HWM!! Purging files..., To send alarm: LogPartitionHighWaterMarkExceeded
[system] Activating via systemd: service name='org.freedesktop.timedate1' unit='dbus-org.freedesktop.timedate1.service'
[system] Successfully activated service 'org.freedesktop.timedate1'
AmqpCommp[30362]: CommAmqpListener: [CCafException] AmqpCommon::validateStatus() amqp_socket_open_noblock: hostname lookup failed
[system] Activating via systemd: service name='org.freedesktop.timedate1' unit='dbus-org.freedesktop.timedate1.service'
[system] Successfully activated service 'org.freedesktop.timedate1'
node=localhost.localdomain type=SYSCALL msg=audit(1578614802.388:88161): arch=c000003e syscall=263 success=no exit=-2 a0=[redacted]c a1=19e90c0 a2=0 a3=7ffe488a7100 items=1 ppid=31734 pid=32079 auid
imjournal: 291936 messages lost due to rate-limiting
node=localhost.localdomain type=CWD msg=audit(1578614802.388:88161):  cwd="/root"
node=localhost.localdomain type=PATH msg=audit(1578614802.388:88161): item=0 name="/tmp/" inode=261634 dev=08:02 mode=041777 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:tmp_t:s0 objtype=PARENT c
node=localhost.localdomain type=PROCTITLE msg=audit(1578614802.388:88161): proctitle=2F62696E2F726D002D66002F746D702F4E54502E616C61726D2A4E54506E6F7452756E6E696E67
```

Use the Toolbar to Navigate Through the Log Output

Figure 32-8 *Syslog Viewer Under Alert Central in RTMT*

Monitor the CUCM with RTMT

Several tools available in the Real-Time Monitoring Tool are used specifically for monitoring the Cisco Unified Communications Manager. This section will introduce a few of these tools to help you get started using RTMT. Specifically, this section will cover how to use the Voice and Video Summary, Gateway Activity, Profile, Device Search, and Database Summary windows.

In a single monitoring pane, the RTMT allows an administrator to monitor information about a Cisco Unified Communications Manager server or about all servers in a cluster if applicable. You can use the menus at the top of the RTMT window to navigate to **Voice/Video > Voice and Video Summary**. As shown in Figure 32-9, in the Voice and Video Summary window, you can view information on the following predefined objects:

Key Topic

- Registered phones
- Calls in progress
- Active MGCP gateway ports and channels

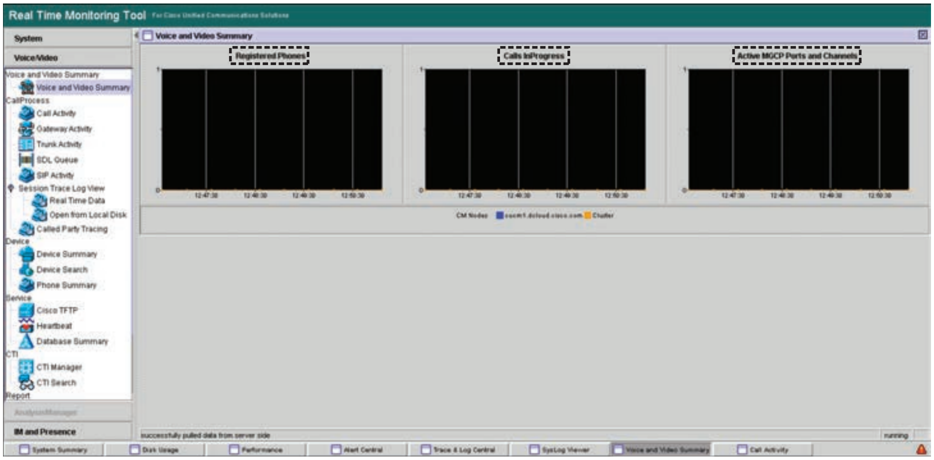
Gateway Activity provides an overview of the current gateway usage in Cisco Unified Communications Manager. You can access the Gateway Activity window by navigating in RTMT to **Voice/Video > Call Process > Gateway Activity**. There you can use the Gateway Type drop-down menu in the top center of the screen to select any of the following gateway types to monitor:

32

Key Topic

- MGCP FXS
- MGCP FXO

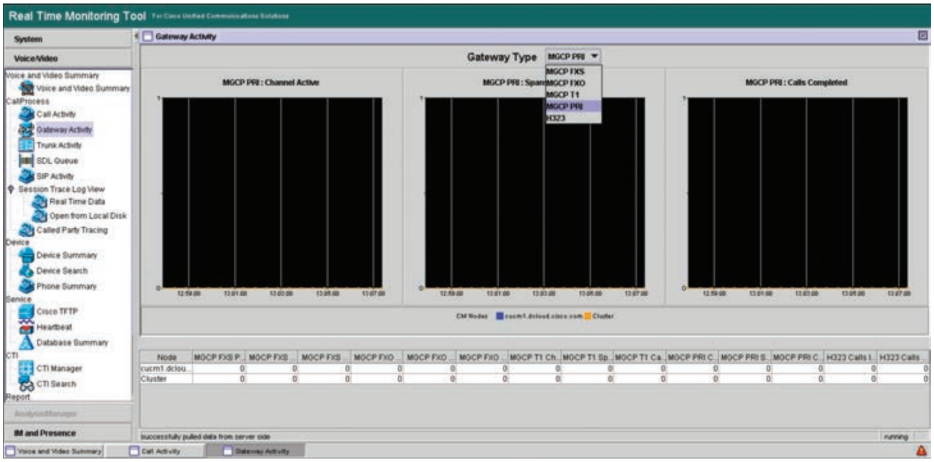
- MGCP T1
- MGCP PRI
- H.323


Navigate to Voice/Video > Voice and Video Summary

successfully pulled data from server side

Figure 32-9 *Voice and Video Summary Window in RTMT*

Gateway Activity monitoring includes the number of calls in progress for a particular gateway type. It also includes the number of calls that were completed for each gateway type for a particular server or for an entire cluster. This type of monitoring provides a summary of all calls in progress or completed calls for a specific gateway type. It does not display calls on a per gateway basis, however. Figure 32-10 illustrates the Gateway Activity window in RTMT.


Navigate to Voice/Video > Call Process > Gateway Activity

Node	MGCP FXS P...	MGCP FXS ...	MGCP FXS ...	MGCP FXO ...	MGCP FXO ...	MGCP FXO ...	MGCP T1 Ch...	MGCP T1 Sp...	MGCP T1 Ca...	MGCP PRI C...	MGCP PRI S...	MGCP PRI C...	H323 Calls I...	H323 Calls ...
cucm1.dclou...	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cluster	0	0	0	0	0	0	0	0	0	0	0	0	0	0

successfully pulled data from server side

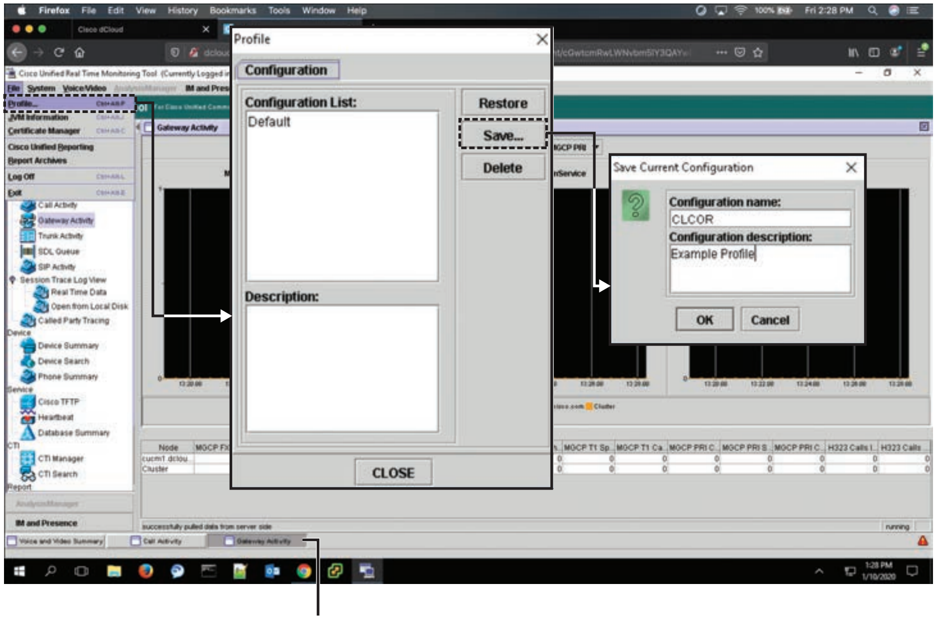
Figure 32-10 *RTMT Gateway Activity Window*

The Profile window allows administrators to use and save different views for later use without the need to open the performance counters again. After you have logged in to a server, the RTMT launches the monitoring module from the local cache. The RTMT can also be launched from a remote server when the local cache does not contain a monitoring module that matches the back-end version. The RTMT includes a default profile that is called Default. The first time that you use the RTMT, the default profile is initiated and displays an empty page in the monitor pane. You can then configure RTMT to display information, such as multiple tabs and different performance counters for different features, in the monitor pane of RTMT and save the framework configuration in a profile. You can restore the profile at a later time during the same session or the next time that you log in to the RTMT. By creating multiple profiles so that each profile displays unique information, you can quickly display different information simply by switching between the different profiles.

Key Topic

To set up a new profile in RTMT, navigate in the menus at the top of the page to **File > Profile**. You will see the Default profile created already, but do not select it from the list. Click the Save button, and a new popup window will appear. Enter a Configuration Name and, optionally, a Configuration Description for the new profile, and then click OK. To open a previously saved profile, select the desired profile from the Configuration List on the Profile popup window, and then click the Restore button. Figure 32-11 illustrates how to create a new profile in the RTMT.

Navigate to Voice/Video > Call Process > Gateway Activity



Configuration List:
Default

Description:

Configuration name: CLCOR

Configuration description: Example Profile

RTMT can handle multiple tabs at the same time.

Figure 32-11 *How to Create a New Profile in RTMT*

The Device Search window allows an administrator to search for specific devices and display their status in the Cisco Unified Communications Manager. The Device Search menu includes the following items on which you can search:

- Phones
- Gateway devices
- H.323 devices
- CTI devices
- Voicemail devices
- Media resources
- Hunt list
- SIP trunk

You can access the Device Search window on the RTMT by navigating to **Voice/Video > Device > Device Search**. Then double-click the desired item to open a popup window with the Status selection menu. The status options include Registered, Unregistered, Partial Registered, Rejected, Any Status, and Devices Only Configured in Database. You can also search by any model or a specific device model, and set up criteria that include several different attributes. Within the phone search, you can also search based on phone protocol. The RTMT queries Cisco RIS to find a matching device. Results are displayed in a table with the following information:

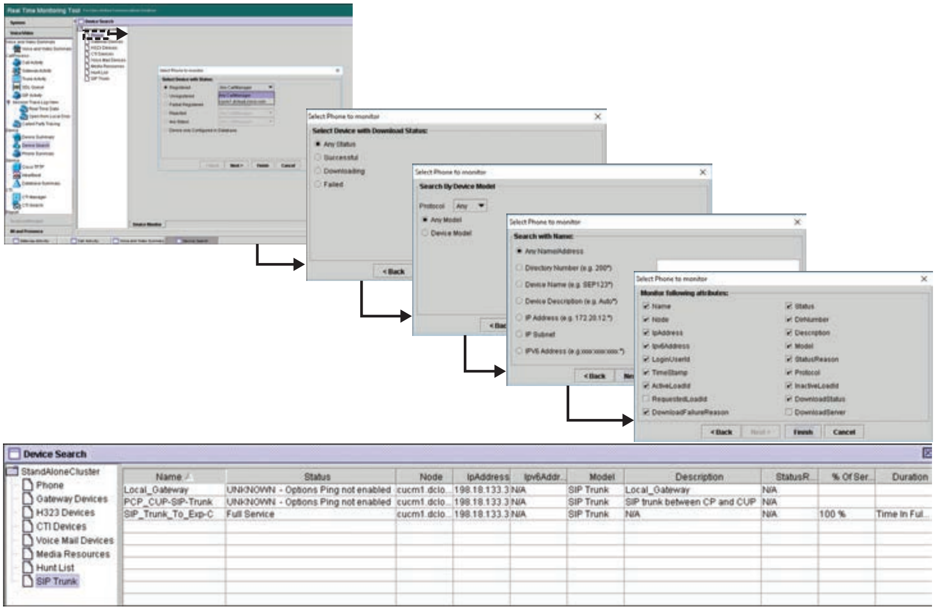
- A row for each matched device
- A column for each of the specified attributes
- A timestamp of the device that has been opened or closed
- The application that controls the device media

Results are displayed in a table with a row for each matched device in a column for each of the specified attributes. You can define the table parameters as shown in Figure 32-12. Some devices may not provide information for all search criteria. For example, if you want to monitor a phone for ActiveLoadId, InactiveLoadId, DownloadStatus, and StatusReason, the download status results display Unknown for phone models that cannot provide this information. Figure 32-12 illustrates the Device Search menu options and table in the RTMT.

The Database Summary window monitors the state of the database and database replication in a Cisco Unified Communications Manager cluster. You can access the Database Summary window by navigating in the RTMT to **Voice/Video > Service > Database Summary**. The Database Summary monitors five different values that are important for troubleshooting database issues. Each pane displays the value for each node in the cluster and the cluster summary. For troubleshooting, the replication status indicates whether the replication of the database from the publisher is working or not. This state is indicated with a value between 0 and 4; each value determines a specific state of the replication status:

Key Topic

- **0:** Not started, no subscribers exist, or the Cisco Database Layer Monitor service is not running and has not been running since the subscriber was installed.
- **1:** Started; replication is currently being set up.
- **2:** Finished; replication setup is complete and working.
- **3:** Broken; replication failed during setup and is not working.
- **4:** Replication is not set up correctly.



Select Phone to monitor

Select Device with Download Status:

● Any Status
○ Successful
○ Downloading
○ Failed

< Back

Select Phone to monitor

Search By Device Model

Protocol: Any

● Any Model
○ Device Model

Select Phone to monitor

Search with Name:

● Any Name/Address
○ Directory Number (e.g. 200*)
○ Device Name (e.g. SEP123*)
○ Device Description (e.g. Auto*)
○ IP Address (e.g. 172.20.12.*)
○ IP Subnet
○ IPV6 Address (e.g.xxxx:xxxx:xxxx:*)

< Back

Select Phone to monitor

Monitor following attributes:

☑ Name	☑ Status
☑ Node	☑ DirNumber
☑ IpAddress	☑ Description
☑ Ipv6Address	☑ Model
☑ LoginUserId	☑ StatusReason
☑ TimeStamp	☑ Protocol
☑ ActiveLoadId	☑ InactiveLoadId
□ RequestedLoadId	☑ DownloadStatus
☑ DownloadFailureReason	□ DownloadServer

< Back | Next > | Finish | Cancel

Device Search

StandAloneCluster
- Phone
- Gateway Devices
- H323 Devices
- CTI Devices
- Voice Mail Devices
- Media Resources
- Hunt List
- SIP Trunk

Name	Status	Node	IpAddress	Ipv6Addr...	Model	Description	StatusR...	% Of Ser...	Duration
Local_Gateway	UNKNOWN - Options Ping not enabled	cucm1.dclo...	198.18.133.3	N/A	SIP Trunk	Local_Gateway	N/A		
PCP_CUP-SIP-Trunk	UNKNOWN - Options Ping not enabled	cucm1.dclo...	198.18.133.3	N/A	SIP Trunk	SIP trunk between CP and CUP	N/A		
SIP_Trunk_To_Exp-C	Full Service	cucm1.dclo...	198.18.133.3	N/A	SIP Trunk	N/A	N/A	100 %	Time In Ful...

Figure 32-12 *RTMT Device Search Menu Options and Output Table*

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 35, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 32-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 32-2 Key Topics for Chapter 32

Key Topic Element	Description	Page Number
List	Servers and Servlets Used by RTMT	774
List	AMC Service Parameters	775
Paragraph	General Menu Components in RTMT	776
Paragraph	Additional RTMT Menu Options	777
List	Perfmon Counter Information	779
List	Alert Options	779
Paragraph	Remote Browse	781
List	Predefines Objects in the Voice and Video Summary Window	783
List	Gateway Types in the Gateway Activity Window	783
Paragraph	Steps to Create a Profile in RTMT	785
List	Five Values of Database Summary	787

Define Key Terms

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

Perfmon Counters, Remote Browse, RIS, RTMT, Servlet

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. In addition to the four main menu components of the RTMT, what are the five menus added when UC servers are being monitored?
2. Explain the steps to set up Remote Browse through RTMT.
3. List the five different values of the Database Summary with their explanations.

This page intentionally left blank

CHAPTER 33

Understanding the Disaster Recovery System

This chapter covers the following topics:

Disaster Recovery System Overview: This topic will describe the features of the Disaster Recovery System. This system provides complete data backup and restore capabilities for all servers in a Cisco Unified Communications Manager cluster, Cisco Unity Connection, or Cisco Unified Communications Manager IM and Presence server.

Backup Cisco Unified Communications Solutions: This topic will describe the backup process for Cisco Unified Communications solutions.

Restore Cisco Unified Communications Solutions: This topic will describe the steps for performing a restore using the Restore Wizard.

One of the most important administrative functions is the backup and restore procedure on Cisco Unified Communications Manager, Cisco Unity Connection, or Cisco Unified Communications Manager IM and Presence server. Organizations depend on the competency of administrators to keep the IP telephony network functioning properly and to restore operations when an outage occurs for any reason. Therefore, knowing how to perform backups and setting a proper schedule and timing for the backup are crucial. Topics discussed in this chapter include the following:

- Disaster Recovery System Overview
- Backup Cisco Unified Communications Solutions
- Restore Cisco Unified Communications Solutions

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 1.4 Troubleshoot these network components in a 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 33-1 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 33-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Disaster Recovery System Overview	1–2
Backup Cisco Unified Communications Solutions	3–4
Restore Cisco Unified Communications Solutions	5–6

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 is a capability of the Disaster Recovery System?
   a. Backups can only be performed manually.
   b. Backups can only be scheduled.
   c. Backups require a remote SFTP server.
   d. A user interface for performing backup tasks is available from any Cisco UC server.
2. Which of the following components is used to perform the actual backup and restore the UC services?
   a. Master Agent
   b. Local Agent
   c. Backup/Restore Agent
   d. Backup/Restore Service
3. What is the first step to backing up the CUCM using the Disaster Recovery System?
   a. Configure the backup scheduler.
   b. Initiate a manual backup of the system.
   c. Create a backup device.
   d. Enable the backup service.
4. Which of the following features is used to back up licensing within the UC solutions?
   a. CDR_CAR
   b. UCM
   c. ELM
   d. SELFCARE
5. When you are restoring settings from an SFTP server, what should be the next step after you choose the Type?
   a. Select the features to be restored.
   b. Select the file integrity check.
   c. Select the node to restore settings to.
   d. Choose the SFTP server to restore settings from.

6. How many jobs does History display for previous backup or restore processes?
   a. 20
   b. 10
   c. 40
   d. 30

Foundation Topics

Disaster Recovery System Overview

The Disaster Recovery System (DRS) allows administrators to perform regularly scheduled automatic or user-invoked manual data backups. The DRS performs a cluster-level backup. In a cluster-level backup, the system collects backups for all servers in a cluster to a central location and archives the backup data to a physical storage device. The DRS restores its own settings, such as the backup device settings and schedule settings, as part of the platform backup or restore. The DRS backs up and restores drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, the administrator does not need to reconfigure the DRS backup device and schedule. When performing a system data restoration, the administrator can choose which nodes should be restored. The DRS includes the following capabilities:

- A user interface for performing backup and restore tasks
- A distributed system architecture for performing backup and restore functions, including monitoring the current backup status and providing a history log
- Scheduled or manual backups
- Backups archived to a physical drive or remote SFTP server

The DRS cannot be used for migration between different Cisco Unified Communications Manager releases. Before restoring a server, the administrator should ensure that the version that is installed on the server matches the version of the backup file that should be restored. The DRS supports only matching versions of the application for restore procedures.

Key Topic

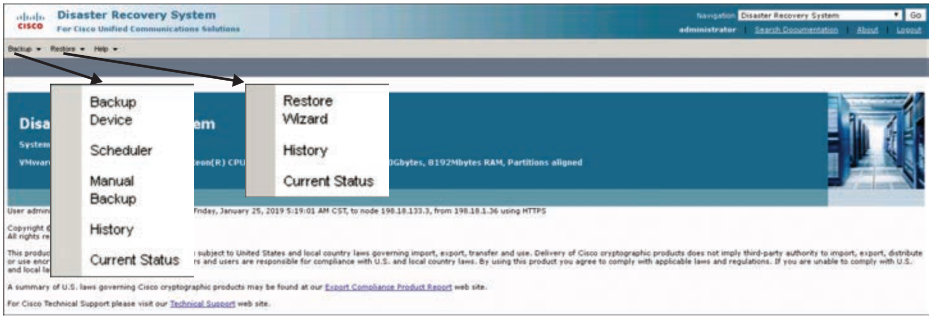
The DRS uses two components: the Master Agent and the Local Agent. They provide the features for the various DRS tasks. The system automatically starts the Master Agent service on each node of the cluster, but the Master Agent is functional only on the first node. The Master Agent on the subsequent nodes does not perform any functions. The Master Agent performs the following duties: stores systemwide component registration information, maintains a complete set of scheduled tasks in an XML file, and updates this file when it receives updates of schedules from the user interface. The Master Agent sends executable tasks to the applicable Local Agents, as scheduled. The Local Agents execute immediate backup tasks without delay. The Master Agent stores backup data on a local attached drive or at a remote network location. The administrator accesses the Master Agent through the DRS user interface to perform activities such as the following:

- Configuring backup devices
- Scheduling backups by adding new backup schedules

- Viewing or updating an existing schedule
- Displaying the status of executed schedules
- Performing system restoration

The server has a Local Agent to perform backup and restore functions as well. Each server in a cluster, including the server that contains the Master Agent, must have its own Local Agent to perform backup and restore functions for its server. The Local Agent runs backup and restore scripts on the server. In a cluster, the Local Agent runs backup and restore scripts on each node in the cluster. By default, a Local Agent is automatically activated on each node of the cluster.

The DRS web interface is separated into two menus: one for backup tasks and one for restore tasks. To access the DRS, select Disaster Recovery System from the Navigation drop-down list in the upper-right corner of the screen on the Cisco Unified Communications Manager, Cisco Unified IM and Presence server, or Cisco Unity Connection web interface window. You can also directly access this Disaster Recovery web interface by entering the address **https://<*server_IP*>/DRF/** in the address bar of a web browser. The DRS feature is also available in Cisco Unified Contact Center Express. You can log in to the DRS by using the same administrator username and password used for the Cisco Unified CM Operating System Administration web interface. Figure 33-1 illustrates the menu options available using the DRS.



In the Navigator drop-down menu, select Disaster Recovery System.
OR
In the Address bar enter https://<IP_Address>/drf.

Disaster Recovery System
For Cisco Unified Communications Solutions
Navigation Disaster Recovery System
Go
administrator | Search Documentation | About | Logout
Backup
Restore
Help
Backup Device
Scheduler
Manual Backup
History
Current Status
Restore Wizard
History
Current Status
Disa
em
System
VMwar
eon(R) CPU
0Gbytes, 8192Mbytes RAM, Partitions aligned

User admin Friday, January 25, 2019 5:19:01 AM CST, to node 198.18.133.3, from 198.18.1.36 using HTTPS

Copyright All rights re

This produc subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encr rs and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local la

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For Cisco Technical Support please visit our Technical Support web site.

Figure 33-1 *Disaster Recovery System Menus*

For UC services, the platform, traces, syslogs, and license information will be backed up or restored. Additionally, the MOH, BAT BPS, CCM Preferences, TFTP Phone Device Profiles, SNMP Syslog Components, Cluster Management, and CEF are all backed up. The other components that are backed up or restored depend on the product type, as summarized in Table 33-2. This table identifies the differences and similarities between the backup and restore processes for each Cisco UC application.

Table 33-2 Disaster Recovery System Components

Cisco Unified Communications Manager	Cisco IM and Presence Server	Cisco Unity Connection
Platform	Platform	Platform
Cisco License Manager	Cisco License Manager	Cisco License Manager
Trace Collection Tool	Trace Collection Tool	Trace Collection Tool
Syslog	Syslog	Syslog
Cisco Unified CM DB	Cisco Unified Communications Manager IM and Presence Service DB	Cisco Unity Connection DB
TFTP/MOH Files	XCP Data	Mailbox Store
CDR/CAR Data	CUP Data	Greetings

Backup Cisco Unified Communications Solutions

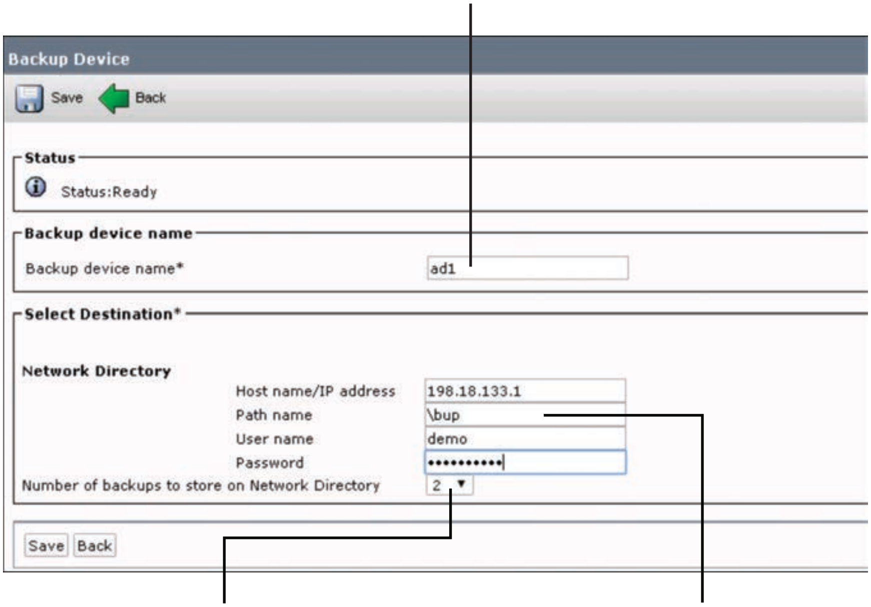
The first step in creating a backup is to select a *backup device*. The backup device is a compilation of settings used to discover the database to which the backup information will be saved. Because no backup devices are created at the time of installation, you will need to create a new one. To create a new backup device from the DRS menus, navigate to **Backup > Backup Device** and click the Add New button. The DRSs use SFTP to store and retrieve these backup files, whether from a local or remote storage system. All files will be stored in the .tar format. The backup device configuration window allows you to determine the backup location. When you're using Network Directory as the desired destination for a backup, SFTP will be used. You define a Backup Device Name and enter the Host Name/IP Address, Path Name, User Name, and Password settings for the SFTP server. The Path name is the root of the SFTP software folder plus a subfolder denoted by a backslash (\). When ready, click Save. After the backup devices are created, click the Back button to view all backup devices. Figure 33-2 illustrates how to create a backup device.

The *scheduler* allows administrators to perform automatic backups in specific time frames. The backup process is resource intensive and can take longer for a larger database. It is advisable that you schedule backups during off hours or during a maintenance window. To create a scheduled backup task from the DRS menus, navigate to **Backup > Scheduler**. Then click Add New to create a new schedule. Define a Schedule Name for the scheduled backup and select the Device Name that should be used to save the backup files. Next, select the features for the backup scheduler. In Figure 33-3, CDR_CAR, IM_AND_PRESENCE, UCM, SELFCARE, and PLM are the features that can be selected in a Cisco Unified Communications Manager cluster. For Cisco Unity Connection, you can choose the following features:

- CONNECTION_DATABASE
- CONNECTION_GREETINGS_VOICENAMES
- CONNECTION_MESSAGES_UNITYMDXDB1
- CUC

After the features have been selected, define the time when the backup process should start. The schedule can be created to run Once or on a Daily, Weekly, or Monthly basis at a specific time. When you're finished configuring the schedule, click Save. Once the schedule has been saved, click the Back button to go back to the schedule list. Locate the newly created backup schedule and check the box beside it. Click the Enable Selected Schedules button to activate the schedule. Figure 33-3 illustrates the settings used to schedule a backup through the DRS.

Define a name for
the backup device.



Backup Device

Status

Status:Ready

Backup device name

Backup device name* ad1

Select Destination*

Network Directory

Host name/IP address 198.18.133.1
Path name \bup
User name demo
Password ••••••••••
Number of backups to store on Network Directory 2

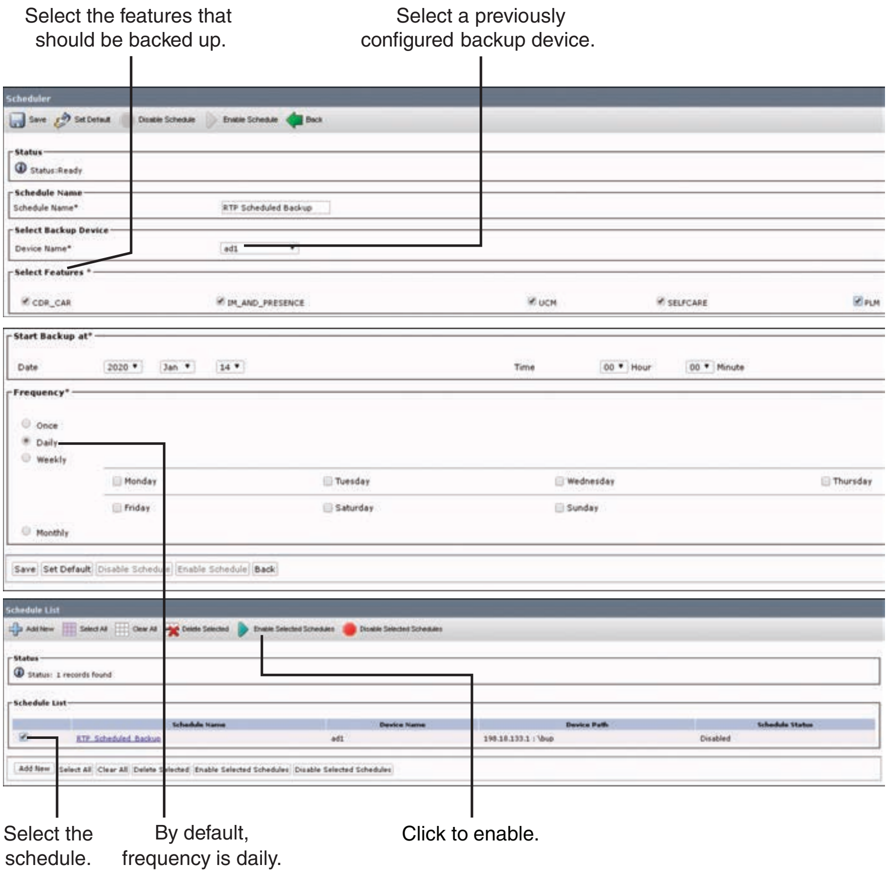
Up to 10 backups can be stored on the
network directory; the default is 2.

The Disaster Recovery System
needs write access to the SFTP path.

Figure 33-2 *Creating a Backup Device*

A *manual backup* is one that starts immediately. To immediately run a manual backup, navigate to **Backup > Manual Backup**. Choose the Backup Device that should be used for the manual backup from the Device Name drop-down list. Select the features, which include the same features as a scheduled backup, and then click Start Backup.

Backup Status is a table that displays the status of a backup as each component is being backed up. When you're starting a manual backup, the status is automatically displayed, but you can navigate to **Backup > Current Status** to view the status of the manual backup if the page gets lost. As the backup procedure is being completed, you see the status of each component that is being backed up and its progress. Information about the status of each component can be viewed in the log file in the lower-right portion of the screen. Figure 33-4 illustrates how to start a manual backup and view the current status of that backup.



Select the features that should be backed up.

Select a previously configured backup device.

Status

Status:Ready

Schedule Name

Schedule Name* RTP Scheduled Backup

Select Backup Device

Device Name* ad1

Select Features *

☑ CDR_CAR ☑ IM_AND_PRESENCE ☑ UCM ☑ SELFCARE ☑ PLM

Start Backup at*

Date 2020 Jan 14 Time 00 Hour 00 Minute

Frequency*

○ Once
● Daily
○ Weekly

□ Monday □ Tuesday □ Wednesday □ Thursday
□ Friday □ Saturday □ Sunday

○ Monthly

Status

Status: 1 records found

Schedule List

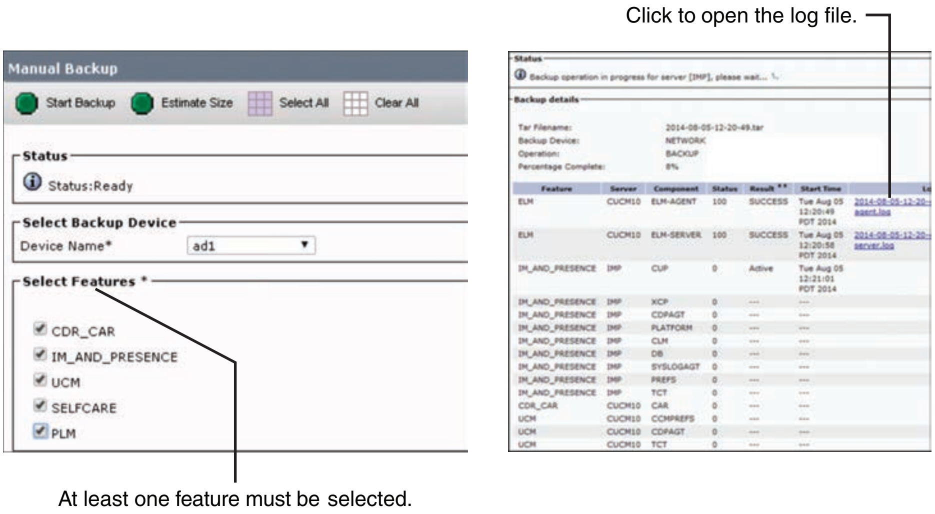
	Schedule Name	Device Name	Device Path	Schedule Status
☑	RTP Scheduled Backup	ad1	198.18.133.1 : \bup	Disabled

Select the schedule.

By default, frequency is daily.

Click to enable.

Figure 33-3 *Schedule a Backup Through the Disaster Recovery System*



Click to open the log file.

Status

Status:Ready

Select Backup Device

Device Name* ad1

Select Features *

☑ CDR_CAR
☑ IM_AND_PRESENCE
☑ UCM
☑ SELFCARE
☑ PLM

Status

Backup operation in progress for server [IMP], please wait...

Backup details

Tar Filename: 2014-08-05-12-20-49.tar
Backup Device: NETWORK
Operation: BACKUP
Percentage Complete: 8%

Feature	Server	Component	Status	Result **	Start Time	Lo
ELM	CUCM10	ELM-AGENT	100	SUCCESS	Tue Aug 05 12:20:49 PDT 2014	2014-08-05-12-20- agent.log
ELM	CUCM10	ELM-SERVER	100	SUCCESS	Tue Aug 05 12:20:58 PDT 2014	2014-08-05-12-20- server.log
IM_AND_PRESENCE	IMP	CUP	0	Active	Tue Aug 05 12:21:01 PDT 2014	
IM_AND_PRESENCE	IMP	XCP	0	---	---	
IM_AND_PRESENCE	IMP	CDPAGT	0	---	---	
IM_AND_PRESENCE	IMP	PLATFORM	0	---	---	
IM_AND_PRESENCE	IMP	CLM	0	---	---	
IM_AND_PRESENCE	IMP	DB	0	---	---	
IM_AND_PRESENCE	IMP	SYSLOGAGT	0	---	---	
IM_AND_PRESENCE	IMP	PREFS	0	---	---	
IM_AND_PRESENCE	IMP	TCT	0	---	---	
CDR_CAR	CUCM10	CAR	0	---	---	
UCM	CUCM10	CCMPREFS	0	---	---	
UCM	CUCM10	CDPAGT	0	---	---	
UCM	CUCM10	TCT	0	---	---	

At least one feature must be selected.

Figure 33-4 *Manual Backup and Current Status Through the Disaster Recovery System*

Restore Cisco Unified Communications Solutions

The Restore Wizard is embedded in the Backup and Restore System. It is used if a recovery from a server failure is needed. Before restoring Cisco Unified Communications Manager, the administrator must ensure that the hostname, IP address, version, and deployment type of the server being restored matches the hostname, IP address, version, and deployment type of the backup file that should be restored. To access the Backup and Restore System, navigate to **Restore > Restore Wizard** and use the following steps:

Key Topic

Step 1. Choose the Backup Device that should be used for the restore process, and then click **Next**.

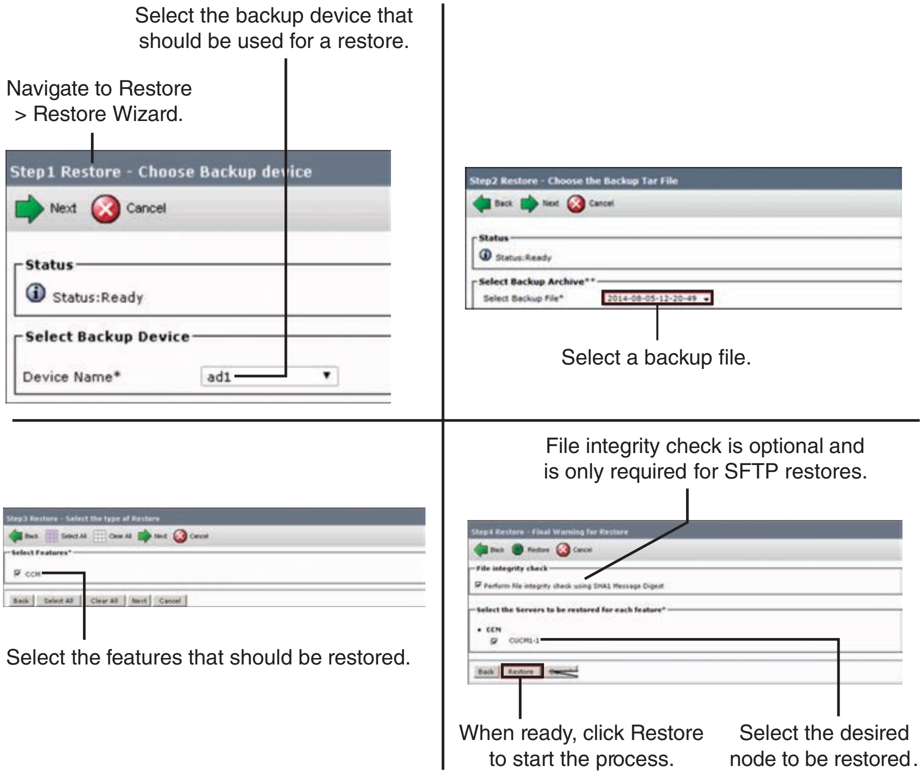
Step 2. The Restore Wizard will check for valid backup files on the backup device. Select the desired backup file from the drop-down list and click **Next**.

Step 3. Once the restore device and backup file have been selected, choose the Type of restore. The type of restore is simply the features that should be restored. This selection depends on the features that are contained in the backup file. For example, if the backup file contains only the CCM feature, you cannot restore the CDR_CAR feature from this file. Once the Type has been selected, click **Next**.

Step 4. Choose file integrity check. The file integrity check is optional and is required only in the case of SFTP backups. Be aware that the file integrity check process consumes a significant amount of CPU and network bandwidth, which slows down the restore process considerably. Next, choose the server node to restore for each feature. If you choose the first node to restore the data, the DRS automatically restores the database on the subsequent nodes. Also, after you choose the node to which the data is to be restored, any existing data on that server is overwritten. When ready, click **Restore** to start the restore process. Figure 33-5 illustrates the steps required to run the Restore Wizard from the DRS.

When the restore process starts, the restore status will be displayed. As the restore procedure for a component is being completed, you can view the status as each component of each server is being restored. Information on the status of each component can be viewed in the log file in the lower-right portion of the screen. After the restore procedure has successfully completed, a reboot of the restored server is required for all changes to take effect. Even if restoring only the first node, you must restart all nodes in the cluster. Restart the subsequent nodes before restarting the first node. Figure 33-6 illustrates the restore status screen that displays after a restore is initiated from the DRS.

The history can be used to show the previous backup and restores. From the Backup History window and Restore History window, you can view the backups or restores that have been performed, including the filename, storage location, completion date, result, and features that were backed up or restored. Navigate to **Backup > History** to display the Backup History window or navigate to **Restore > History** to display the Restore History window. Each history displays the latest 20 jobs.



Select the backup device that should be used for a restore.

Navigate to Restore > Restore Wizard.

Step1 Restore - Choose Backup device

Status

Status:Ready

Select Backup Device

Device Name* ad1

Step2 Restore - Choose the Backup Tar File

Status

Status:Ready

Select Backup Archive**

Select Backup File* 2014-08-05-12-20-49

Select a backup file.

Step3 Restore - Select the type of Restore

Select Features*

☑ CCM

Select the features that should be restored.

File integrity check is optional and is only required for SFTP restores.

Step4 Restore - Final Warning for Restore

File integrity check

☑ Perform file integrity check using SHA1 Message Digest

Select the Servers to be restored for each feature*

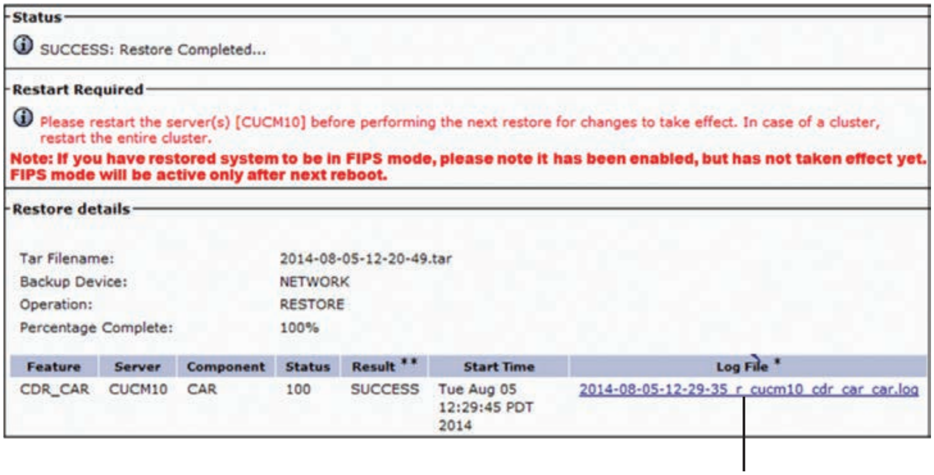
- CCM

  ☑ CUCM1-1

When ready, click Restore to start the process.

Select the desired node to be restored.

Figure 33-5 *Restore Wizard Steps on the Disaster Recovery System*



Status

SUCCESS: Restore Completed...

Restart Required

Please restart the server(s) [CUCM10] before performing the next restore for changes to take effect. In case of a cluster, restart the entire cluster.

Note: If you have restored system to be in FIPS mode, please note it has been enabled, but has not taken effect yet. FIPS mode will be active only after next reboot.

Restore details

Tar Filename: 2014-08-05-12-20-49.tar

Backup Device: NETWORK

Operation: RESTORE

Percentage Complete: 100%

Feature	Server	Component	Status	Result **	Start Time	Log File *
CDR_CAR	CUCM10	CAR	100	SUCCESS	Tue Aug 05 12:29:45 PDT 2014	2014-08-05-12-29-35_r_cucm10_cdr_car_car.log

Click to open the log file.

Figure 33-6 *Restore Wizard Restore Status Screen*

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 35, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 33-3 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 33-3 Key Topics for Chapter 33

Key Topic Element	Description	Page Number
Paragraph	Master Agent Explained	792
Table 33-2	Disaster Recovery System Components	794
Paragraph	Backup Device	794
List	Features That Can Be Backed Up	794
Steps	Steps to Run the Restore Wizard	797

Define Key Terms

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

Backup Device, Backup Status, Cluster-Level Backup, Local Agent, Manual Backup, Master Agent, Restore Wizard, Scheduler

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the activities that can be performed in the DRS through the Master Agent.
2. List all the features that can be backed up from the CUCM.

CHAPTER 34

Monitoring Voicemail in Cisco Unity Connection

This chapter covers the following topics:

Generate Reports on Cisco Unity Connection: This topic will describe the different reports and parameters for reporting in Cisco Unity Connection.

Generate Reports in Cisco Unified Serviceability: This topic will describe the different reports for Cisco Unified Serviceability.

Use Reports for Troubleshooting and Maintenance: This topic will describe how reports help an administrator maintain and manage Cisco Unity Connection.

This chapter will describe the monitoring options and different reports that are available in Cisco Unity Connection. Some of the reports help actively maintain and manage Cisco Unity Connection. Topics discussed in this chapter include the following:

- Generate Reports on Cisco Unity Connection
- Generate Reports in Cisco Unified Serviceability
- Use Reports for Troubleshooting and Maintenance

This chapter covers the following objectives from the Cisco Collaboration Core Technologies v1.1 (CLCOR 350-801) exam:

- 1.4 Troubleshoot these network components in a 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 34-1 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 34-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Generate Reports on Cisco Unity Connection	1–2
Generate Reports in Cisco Unified Serviceability	3–4
Use Reports for Troubleshooting and Maintenance	5–6

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. How many different reports are available through Cisco Unity Connection Serviceability?
   - **a.** 2
   - **b.** 4
   - **c.** 10
   - **d.** 20
2. What is the default number of days that data is kept in the report database?
   - **a.** 7 days
   - **b.** 30 days
   - **c.** 90 days
   - **d.** 120 days
3. Which of the following is a report generated through the Cisco Unified Serviceability web page?
   - **a.** Alert report
   - **b.** Port Activity Report
   - **c.** Message Report
   - **d.** Mailbox Store Report
4. Over what period of time do the server report settings represent data?
   - **a.** 5 minutes
   - **b.** 15 minutes
   - **c.** 1 hour
   - **d.** 24 hours
5. A user tries to log in to her voice mailbox, but she receives a message that the mailbox has been locked. What should be the next step the user takes to gain access to the mailbox?
   - **a.** Log in to CUC and unlock the mailbox.
   - **b.** Log in to the CUCM and unlock the mailbox.
   - **c.** Contact the IT support staff to unlock the mailbox in CUC.
   - **d.** Contact the IT support staff to unlock the mailbox in CUCM.
6. Which of the following reports should administrators view on a regular basis as part of their maintenance duties?
   - **a.** Unused Voice Mail Accounts Report
   - **b.** Outcall Billing Summary Report

c. Phone Interface Failed Logon Report

d. User Lockout Report

Foundation Topics

Generate Reports on Cisco Unity Connection

In Cisco Unity Connection, available from the Navigator menu in the top-right corner of the screen, administrators can choose between two different serviceability web pages to access tools and generate reports. Cisco Unified Serviceability is available on the Cisco Unified Communications Manager, Cisco Unified IM and Presence server, and Cisco Unity Connection. It offers two different types of reports: alert reports and server reports. The Cisco Unity Connection Serviceability web page is available only through the Cisco Unity Connection server, and it allows 20 different reports to be generated. Table 34-2 identifies the different reports available through Cisco Unity Connection Serviceability.

Table 34-2 Reports Available Through Cisco Unity Connection Serviceability

Report Name	Description of Output
Phone Interface Failed Logon	Includes the following information for every failed attempt to sign into Unity Connection by phone: ■ Name of user, alias, caller ID, and extension of user who failed to sign in ■ Date and time the failed login occurred ■ Whether the maximum number of failed sign-ins has been reached for the user
Users	Includes the following information for each user: ■ Last name, first name, and alias ■ Information that identifies the Unity Connection or Cisco Business Edition server associated with the user ■ Billing ID, class of service, and extension ■ Whether the account is locked ■ Whether the user has enabled personal call transfer rules
Message Traffic	Includes totals for the following traffic categories: Voice Fax Email Nondelivery receipt (NDR) Delivery receipt Read receipt Hourly totals Daily totals

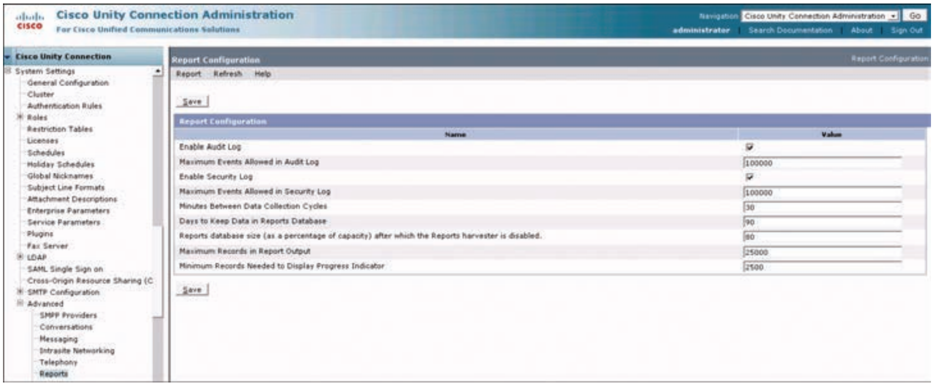
Report Name	Description of Output
Port Activity	Includes the following information for voice-messaging ports: ■ Name ■ Number of inbound calls handled ■ Number of outbound MWI calls handled
	■ Number of outbound AMIS calls handled ■ Number of outbound notification calls handled ■ Number of outbound TRAP calls handled ■ Total number of calls handled
Mailbox Store	Includes the following information about the specified mailbox stores: ■ Mail database name ■ Display name ■ Server name ■ Whether access is enabled ■ Mailbox store size ■ Last error ■ Status ■ Whether the mail database can be deleted
Dial Plan	Includes a list of the search spaces configured on the Unity Connection or Cisco Business Edition server, with an ordered list of partitions assigned to each search space. If the server is part of a digital network, also lists the search spaces and associated partition membership on every other Unity Connection location on the network.
Dial Search Scope	Includes a list of all users and their extensions in the specified partition that is configured in the Unity Connection directory. If a partition is not specified, lists all users and their extensions for all partitions that are configured in the directory.
User Phone Login and MWI	Includes the following information about phone logins, MWI activity, and message notifications to phone devices per user: ■ Name, extension, and class of service ■ Date and time for each activity ■ The source of each activity ■ Action completed (for example, Login, MWI On or Off, and Phone Dialout) ■ Dialout number and results (applicable only for message notifications to phone devices) ■ The number of new messages for a user at time of login

Report Name	Description of Output
User MessageActivity	Includes the following information about messages sent and received, per user: ■ Name, extension, and class of service ■ Date and time for each message ■ Type of message ■ Action completed (for example, new message or message saved) ■ Information on the message sender
Distribution Lists	Includes the following information: ■ Name and display name of the list ■ Date and time the list was created (date and time are given in Greenwich Mean Time) ■ A count of the number of users included in the list ■ If the Included List Members check box is checked, includes a listing of the alias of each user who is a member of the list
User Lockout	Includes user alias, number of failed login attempts for the user, credential type (a result of 4 indicates a login attempt from the Unity Connection conversation; a result of 3 indicates a login attempt from a web application), and the date and time that the account was locked. (Date and time are given in Greenwich Mean Time.)
Unused Voicemail Accounts	Includes user alias and display name, and the date and time that the user account was created. (Date and time are given in Greenwich Mean Time.)
Transfer Call Billing	Includes the following information for each call: ■ Name, extension, and billing ID of the user ■ Date and time that the call occurred ■ The phone number dialed ■ The result of transfer (connected, ring-no-answer (RNA), busy, or unknown)
Outcall BillingDetail	Includes the following information, arranged by day and by the extension of the user who placed the call: ■ Name, extension, and billing ID ■ Date and time the call was placed ■ The phone number called ■ The result of the call (connected, ring-no-answer [RNA], busy, or unknown) ■ The duration of the call in seconds
Outcall BillingSummary	Arranged by date and according to the name, extension, and billing ID of the user who placed the call, and includes a listing of the 24 hours of the day, with a dialout time in seconds specified for each hour span.

Report Name	Description of Output
Call Handler Traffic	Includes the following information for each call handler and use for each hour of a day: ■ Total number of calls ■ Number of times each key on the phone keypad was pressed ■ Extension ■ Invalid extension ■ Number of times the After Greeting action occurred ■ Number of times the caller hung up
System Configuration	Includes detailed information about all aspects of the configuration of the Unity Connection system.
SpeechView Activity Report By User	Includes the total number of transcribed messages, failed transcriptions, and truncated transcriptions for a given user during a given time period. If the report is run for all users, then the output is broken out by user.
SpeechView Activity Summary Report	Includes the total number of transcribed messages, failed transcriptions, and truncated transcriptions for the entire system during a given time period. When a message is sent to multiple recipients, the message is transcribed only once, so the transcription activity is counted only once.
HTTPS Networking Sync Error Report	(Applicable only for HTTPS Networking) Includes the following information associated with the directory objects that do not synchronize during directory synchronization: ■ Creation Date ■ Failed ObjectID ■ USN ■ Object Type ■ Location Display Name ■ HTTP(S) Link ■ Error Message

To limit the number of events in log files or the days for which log data will be kept, you can modify the reporting parameters. On the Cisco Unity Connection Administration web page, navigate to **System Settings > Advanced > Reports**, and observe the following parameters that can be set for reporting. Figure 34-1 illustrates the Report Configuration fields available in Cisco Unity Connection.

Check the Enable Audit Log check box to enable the audit log. When this box is unchecked, stored procedures stop writing to the audit log. In the default setting, the check box is checked. The Maximum Events Allowed in Audit Log setting allows administrators to enter the maximum number of audit events that are allowed in the audit log table. When the maximum threshold is reached, the oldest events are removed. You can enter a number between 1 and 100,000. The default setting is 100,000.



Report Configuration

Name	Value
Enable Audit Log	☑
Maximum Events Allowed in Audit Log	100000
Enable Security Log	☑
Maximum Events Allowed in Security Log	100000
Minutes Between Data Collection Cycles	30
Days to Keep Data in Reports Database	90
Reports database size (as a percentage of capacity) after which the Reports harvester is disabled.	80
Maximum Records in Report Output	25000
Minimum Records Needed to Display Progress Indicator	2500

Figure 34-1 *Cisco Unity Connection Report Configuration Fields*

Check the Enable Security Log check box to enable or disable the security log. If this setting is set to disabled, stored procedures stop writing to the security log. In the default setting, the check box is checked. The Maximum Events Allowed in Security Log parameter is the maximum number of security events that are allowed in the security log table. You can enter values between 1 and 100,000. When the maximum threshold is reached, the oldest events are removed. The default setting is 100,000.

The Minutes Between Data Collection Cycles parameter allows administrators to enter the amount of time to wait, in minutes, between cycles of gathering report data. The default setting is 30 minutes.

The Days to Keep Data in Reports Database parameter allows administrators to enter the number of days to keep data in the report database. If more than this number of days is specified in the time range for the report, this setting still limits the number of days of data. The default setting is 90 days.

The Reports Database Size (as a Percentage of Capacity) After Which the Report Harvester Is Disabled parameter allows administrators to enter the maximum percentage of the disk capacity that the reports database is allowed to occupy. When the reports database reaches this percentage, the Cisco Unity Connection Report Data Harvester service, which is located in Cisco Unity Connection Serviceability, is turned off so that the database does not grow. The default setting is 80 percent.

The Maximum Records in Record Output parameter is the maximum number of records that can be included in the report output. You can enter a value between 5000 and 30,000. The default setting is 25,000 records. If the report output is generated to HTML, the maximum number of records that are returned in the output is 250, even if the Maximum Records and Report Output setting is set higher than 250. Maximum Records in Report Output Setting for the User Message Activity Report is restricted to 15,000 records instead of the default of 25,000 records because of the size of the report.

The Minimum Records Needed to Display Progress Indicator parameter requires administrators to enter a value between 1 and 10,000. If the number of records in the requested report is more than this value, a report confirmation page appears before running a report. A progress indicator is also displayed while the report is being generated. The purpose of the progress indicator is to warn that the requested report is large and likely to take a long time to complete. In Cisco Unity Connection, reports are generated from within a browser, and the browser session must be kept open while the report is being generated. Depending on the size of the database and the type of report being generated, that report can take a long time to generate. Meanwhile, the browser cannot be used for any other purpose, and the Cisco Unity Connection Administration session must remain open. The default setting is 2500 records.

Perform the following steps to generate and view a Cisco Unity Connection Serviceability user report:

Key Topic

Step 1. To connect to Cisco Unity Connection Serviceability, enter **https://<*IP_address*>/cuservice** in the address bar of the browser.

Step 2. Once logged in, navigate to **Tools > Report** and select **User Report**.

Step 3. Leave the settings as the default values and click **Generate Report**.

Select the applicable file format for the report output. If the fields are available, set a date range by selecting the beginning and ending month, day, year, and time. Set other parameters, as applicable, and then click **Generate Report**. To view the report output, select any of the following file formats:

- **Web Page:** The output appears in the browser window.
- **Comma-Delimited File:** A file download dialog box opens, asking whether to open or save the file.
- **PDF File (Portable Document Format):** A file download dialog box opens, asking whether to open or save the file.

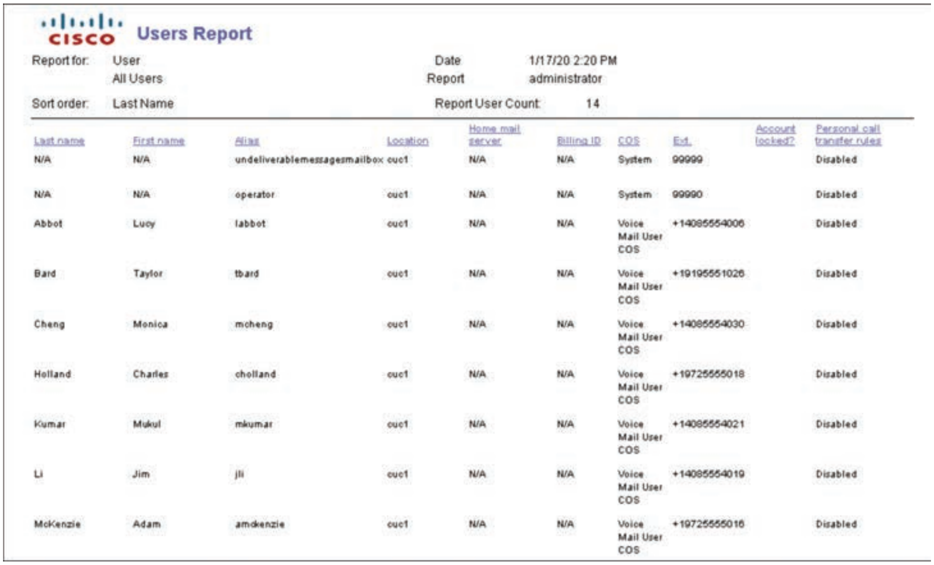
For the user report, you can filter the result by User, Distribution List, or CoS. When you are selecting the user class, the options are All Users or Selected User. When you choose Selected User, every user must be selected to be included in the user report. You can also sort the results by Last or First Name, Extension, or CoS. Click **Generate Report** to create the output.

Step 4. View the Report Output.

The users are sorted by their last name. Cisco Unity Connection system users like the operator are displayed with the last name "N/A" and are listed first. Figure 34-2 illustrates the output from a user report. This user report includes the following information for each user:

Key Topic

- Last name, first name, and alias
- Information that identifies the Cisco Unity Connection server that is associated with the user
- Billing ID, CoS, and extension
- Whether the account is locked
- Whether the user has enabled personal call transfer rules



Users Report

Report for: User
All Users

Date 1/17/20 2:20 PM

Report administrator

Sort order: Last Name

Report User Count 14

Last name	First name	Alias	Location	Home mail server	Billing ID	COS	Ext.	Account locked?	Personal call transfer rules
N/A	N/A	undeliverablemessagesmailbox	cuc1	N/A	N/A	System	99999		Disabled
N/A	N/A	operator	cuc1	N/A	N/A	System	99990		Disabled
Abbot	Lucy	labbot	cuc1	N/A	N/A	Voice Mail User COS	+14085554006		Disabled
Bard	Taylor	tbard	cuc1	N/A	N/A	Voice Mail User COS	+19195551026		Disabled
Cheng	Monica	mcheng	cuc1	N/A	N/A	Voice Mail User COS	+14085554030		Disabled
Holland	Charles	cholland	cuc1	N/A	N/A	Voice Mail User COS	+19725555018		Disabled
Kumar	Mukul	mkumar	cuc1	N/A	N/A	Voice Mail User COS	+14085554021		Disabled
Li	Jim	jli	cuc1	N/A	N/A	Voice Mail User COS	+14085554019		Disabled
McKenzie	Adam	amckenzie	cuc1	N/A	N/A	Voice Mail User COS	+19725555016		Disabled

Figure 34-2 *Cisco Unity Connection Serviceability User Report*

Generate Reports in Cisco Unified Serviceability

The Cisco Serviceability Reporter service generates daily reports in Cisco Unified Serviceability. Each report provides a summary composed of different charts that display the statistics for that particular report. The Cisco Serviceability Reporter generates reports once a day on the basis of logged information. You must activate the Cisco Serviceability Reporter service for the Cisco Unified Serviceability Reports to function. Cisco recommends that you activate the Cisco Serviceability Reporter service only on a non-call-processing server. As mentioned at the beginning of the previous section, two types of Cisco Unified Serviceability reports are generated for each day:

Key Topic

- **Alert report:** Contains any alerts that were generated along with their severity
- **Server report:** Contains statistics on the server performance for the day

The following steps outline how to generate alert and server reports using Cisco Unified Serviceability:

Step 1. In the Cisco Unified Serviceability web page, on Cisco Unity Connection, navigate to **Tools > Serviceability Reports Archive**.

Step 2. Select the latest available report, which is usually the report for the previous day, and open the alert report. Remember that these reports are generated from the previous day's activity. If you start the Cisco Serviceability Reporter service and then try to view the data in the reports, there may not be enough information to process.

Step 3. These reports allow you to check the number of alerts per Cluster, Server, and Top 10 Alerts. Select the first of the Top 10 Alerts and gather additional information about the alert on Cisco.com.

The alert report includes the following statistics. For more details on a particular alert, use the Cisco Unified Real-Time Monitoring Tool (RTMT).

Key Topic

- **The Number of Alerts per Severity for the Cluster Statistic:** Shows alerts per severity level in the Cisco Unity Connection cluster (active-active pair) as follows:
- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug
- **The Number of Alerts per Server Statistic:** Shows the number of alerts per Cisco Unity Connection server.
- **The Top 10 Alerts in the Cluster Statistic:** Shows the top 10 alerts. Following are three examples of possible alerts:
- 140 LowAvailableVirtualMemory alerts
- 140 LowSwapPartitionAvailableDiskSpace alerts
- 3 SyslogSeverityMatchFound alerts

Step 4. Open the server report for the same day.

Step 5. Check the following values, which are presented in percentages:

- CPU per Server
- Virtual Memory per Server
- Hard Disk Usage for Common/Spare Partition

The following information is shown in the server report:

Key Topic

- **Percentage of CPU per Server:** A line chart displays the percentage of CPU usage for each server in a cluster. Each data value in a chart represents the average CPU usage for one 15-minute period. If no data exists for the server, Cisco Serviceability Reporter does not generate a line that represents that server. If there are no lines to generate, Cisco Serviceability Reporter does not create the chart. The message "No data for Service Statistics report available" is displayed.
- **Percentage of Memory Usage per Server:** A line chart displays the percentage of memory usage for the server (%MemoryInUse). In a cluster configuration, there is one line per server in the cluster for which data is available. Each data value in the chart represents the average memory usage for a 15-minute period of time. If no data exists, Cisco Serviceability Reporter does not generate the chart.

- **Percentage of Hard Disk Usage of the Common Partition per Server:** A line chart displays the percentage of the space usage for the common partition on the server (%DiskSpaceInUse) or on each server in a cluster configuration. Each data value in the chart represents the average disk usage for a 15-minute period. If no data exists, Cisco Serviceability Reporter does not generate the chart. The same report is available for the spare partition. As long as there is no installation in the second partition, no information is available.

Use Reports for Troubleshooting and Maintenance

Now that I've covered the different reports available through the Cisco Unity Connection server, this section will examine how these reports can be used for troubleshooting and some maintenance tasks. Reports discussed in this section that can be used for troubleshooting include the User Lockout Report and the Port Activity Report. Reports discussed in this section that can be used for maintenance tasks include the Mailbox Store Report, the Unused Voice Mail Accounts Report, and the various named billing reports.

The Phone Interface Failed Logon Report shows all users who have entered a wrong PIN in the past. When generating the report, you can select which list to display from the following two choices for a user:

- List All Failed Logins
- List Only the Last Failed Login

In addition, you can specify a timeframe, such as all failed logins in the past week. Entries in this report indicate that a user might have issues logging in to the voice mailbox. Another option is that someone is trying to hack into a mailbox of another user. This report should be viewed together with the User Lockout Report. Figure 34-3 illustrates the Phone Interface Failed Logon Report options.

The User Lockout Report includes the user alias, the number of failed logins attempted for the user, credential type, and the date and time the account was locked. You can sort the report result by the following criteria:

- Alias
- Time of last lockout

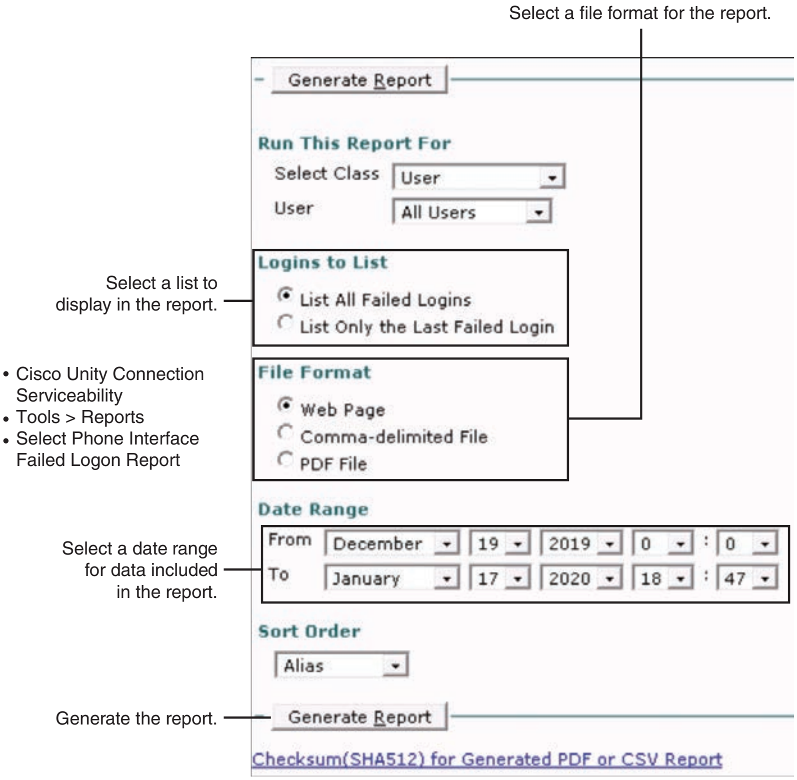
After a user is locked out, the user will normally request IT support. The IT support staff will unlock the mailbox so that the user can log in again. Locked-out users should be contacted to determine if there is a problem. A security policy might specify that IT support staff should contact users instead of simply unlocking all accounts on a weekly basis. If users are not aware that their account has been locked, someone else might have tried to hack the mailbox. Using the time of last lockout and call detail records (CDRs), the IT staff might be able to identify the hacker. Figure 34-4 illustrates the options for generating the User Lockout Report.

When a user is locked out, you can reset the password or PIN so the user can access Cisco Unity Connection again. From the Cisco Unity Connection Administration web page, navigate to **Users > Users.** Select a user, and choose **Edit > Password Settings** from the menus at the top of the screen. The following lockout-related information is available:

Key Topic

- **Failed Sign-In Attempts:** Indicates the number of failed sign-in attempts that have occurred for this password or PIN. The number is reset to zero after a successful sign-in has occurred or when an administrator selects the Unlock Password button.
- **Time of Last Failed Sign-In Attempt:** Indicates the date and time of the most recent failed sign-in attempt for this password or PIN.
- **Time Locked by Administrator:** Indicates the date and time that a user password or PIN was locked by an administrator.
- **Time Locked Due to Failed Sign-In Attempts:** Indicates the date and time that a user password or PIN was locked because the maximum number of allowed failed sign-in attempts was reached.

Choose the Unlock Password button to unlock the user password or PIN. When selected, Unlock Password will also reset the Failed Sign-In Attempts to zero and delete the Time Locked value. If a user cannot remember the password or PIN or is locked out again, you can change the password or PIN. Navigate to **Edit > Change Password** and enter a new password or PIN. The user should be instructed to change the password after the first login. Figure 34-5 illustrates the menu options under the Edit Password Settings (Voicemail) menu.



Select a file format for the report.

Select a list to display in the report.

- Cisco Unity Connection Serviceability
- Tools > Reports
- Select Phone Interface Failed Logon Report

Select a date range for data included in the report.

Generate the report.

Generate Report

Run This Report For
Select Class User
User All Users

Logins to List
● List All Failed Logins
○ List Only the Last Failed Login

File Format
● Web Page
○ Comma-delimited File
○ PDF File

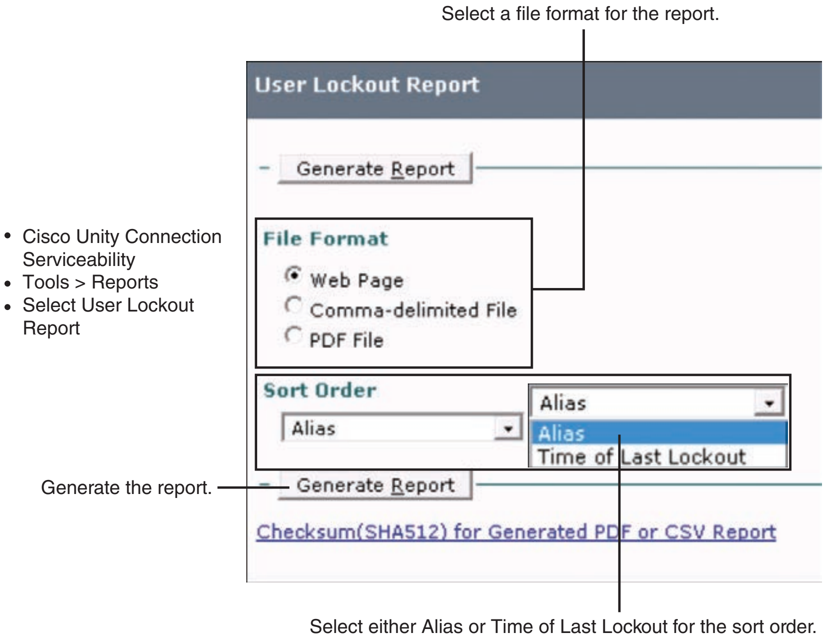
Date Range
From December 19 2019 0 : 0
To January 17 2020 18 : 47

Sort Order
Alias

Generate Report

Checksum(SHA512) for Generated PDF or CSV Report

Figure 34-3 *Phone Interface Failed Logon Report Options*



Select a file format for the report.

- Cisco Unity Connection Serviceability
- Tools > Reports
- Select User Lockout Report

Generate the report.

Select either Alias or Time of Last Lockout for the sort order.

User Lockout Report

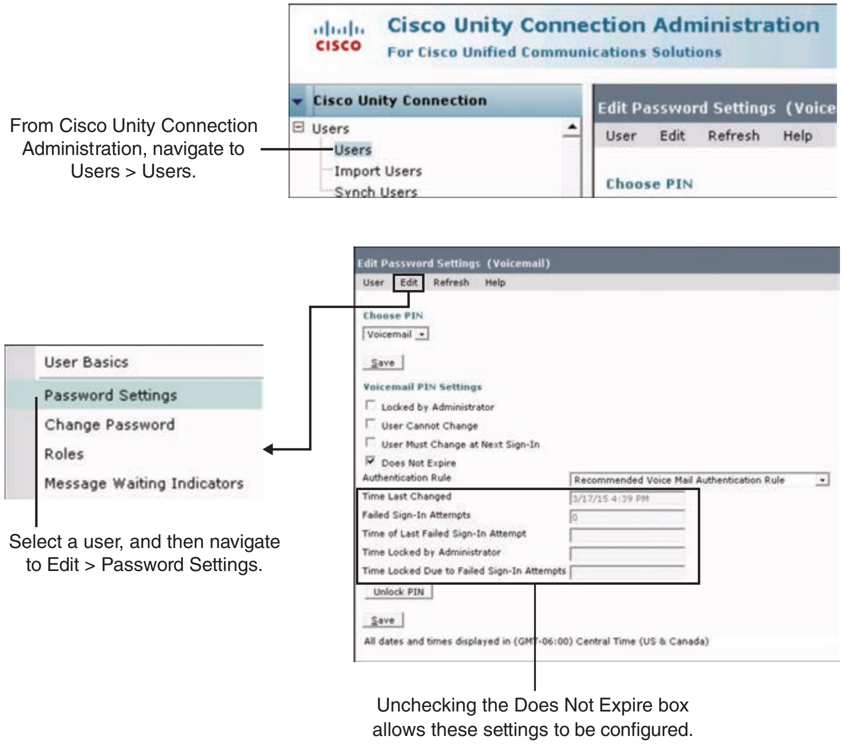
File Format

● Web Page
○ Comma-delimited File
○ PDF File

Sort Order

Alias

Figure 34-4 *User Lockout Report Options*



From Cisco Unity Connection Administration, navigate to Users > Users.

Select a user, and then navigate to Edit > Password Settings.

Unchecking the Does Not Expire box allows these settings to be configured.

Edit Password Settings (Voicemail)

Choose PIN

Voicemail

Voicemail PIN Settings

□ Locked by Administrator
□ User Cannot Change
□ User Must Change at Next Sign-In
☑ Does Not Expire

Authentication Rule	Recommended Voice Mail Authentication Rule
Time Last Changed	3/17/15 4:39 PM
Failed Sign-In Attempts	0
Time of Last Failed Sign-In Attempt	
Time Locked by Administrator	
Time Locked Due to Failed Sign-In Attempts	

All dates and times displayed in (GMT-06:00) Central Time (US & Canada)

Figure 34-5 *Edit Password Settings (Voicemail) Menu Options*

Administrators should check the Port Activity Report on a regular basis to ensure that all Cisco Unity Connection ports are active and in use. The Port Activity Report includes the following information for voice messaging ports:

- Name of the port
- Number of inbound calls processed
- Number of outbound MWI calls processed
- Number of outbound AMIS calls processed
- Number of outbound notification calls processed
- Number of outbound TRAP calls processed
- Total number of calls processed

The distribution mechanism in the line group configuration on Cisco Unified Communications Manager controls the incoming calls. When single ports are configured to offer only TRAP functionality, you can verify that this configuration is reflected in the Port Activity Report.

Some reports should be viewed on a regular basis, such as the Mailbox Store Report and the Unused Voice Mail Accounts Report. The Mailbox Store Report includes the following information about the specified mailbox stores:

- Mail database name
- Display name
- Server name
- Whether access is enabled
- Mailbox store size
- Last error
- Status
- Whether the mail database can be deleted

The Unused Voice Mail Accounts Report includes the user alias, display name, and the date and time that the user account was created. Check this report on a regular basis to identify unused voicemail accounts. If an employee left the company, unused voicemail accounts are a security risk.

Three different kinds of billing reports are available. The Transfer Call Billing Report includes the following information for each call:

- Name, extension, and billing ID of the user
- Date and time that the call occurred
- The phone number dialed
- The result of the transfer (connected, RNA, busy, or unknown)

The Outcall Billing Detail Report includes the following information, arranged by day and by the extension of the user who placed the call:

- Name, extension, and billing ID
- Date and time the call was placed
- The phone number called
- The result of the call (connected, RNA, busy, or unknown)
- The duration of the call in seconds

The Outcall Billing Summary Report is arranged by date and according to the name, extension, and billing ID of the user who placed the call. This report is a listing of 24 hours of the day, with a dial-out time in seconds specified for each hour span.

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 35, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 34-3 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 34-3 Key Topics for Chapter 34

Key Topic Element	Description	Page Number
Table 34-2	Reports Available Through Cisco Unity Connection Serviceability	802
Steps	Generate a Cisco Unity Connection Serviceability User Report	807
List	Information in a User Report	807
List	Two Types of Cisco Unified Serviceability Reports	808
List	Statistics Included in an Alert Report	809
List	Information Included in the Server Report	809
List	Display Options for Phone Interface Failed Login Report	810
List	Sort Options for User Lockout Report	810
List	User Lockout Related Information	811
List	Port Activity Report Information	813
List	Mailbox Store Report Information	813

Define Key Terms

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

Alert Report, AMIS, Cisco Unified Serviceability, Cisco Unity Connection Serviceability, MWI, Server Report, TRAP

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. List the information included in a user report.
2. List the information included in a server report.
3. What are the three different kinds of billing reports available through the Cisco Unity Connection?

This part covers the following topics:

- **Chapter 35, Final Preparation:** This chapter, along with the Introduction of the book, will suggest hands-on activities and a study plan to help you complete your preparation for the exam.

Part IX

Final Preparation

CHAPTER 35

Final Preparation

The first 34 chapters of this book cover the technologies, protocols, design concepts, and considerations required for your preparation in passing the Cisco Implementing and Operating Cisco Collaboration Core Technologies (CLCOR 350-801) exam. This is the exam required for the CCNP Collaboration, CCIE Collaboration, and Cisco Certified Specialist–Collaboration Core Certifications. If you are pursuing the CCNP Collaboration certification, you still need to select and pass a concentration exam in addition to the Core exam to achieve that certification. If you are preparing for the CCIE certification, you must also pass the hands-on 8-hour lab.

Chapters 1 through 34 cover the information necessary to pass the exam. However, most people need more preparation than simply reading the first 34 chapters of this book. This chapter, along with the Introduction of the book, suggests hands-on activities and a study plan that will help you complete your preparation for the exam.

Hands-on Activities

As mentioned, you should not expect to pass the CLCOR 350-801 exam by just reading this book. The CLCOR 350-801 exam requires hands-on experience with many of the Cisco technologies, tools, and techniques discussed in this book. These include Cisco routers, switches, firewalls, Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Server, Cisco Unity Connection, Cisco Expressway Core, Cisco Expressway Edge, Webex Control Hub, Cisco Unified IP phones, Cisco Telepresence endpoints, Cisco Jabber soft client, Webex App, and the different APIs supported by those products. The most effective way to learn the skills necessary to pass the exam is to build your own lab, break it, and fix it. Building your own lab can be very expensive for the Cisco Collaboration solution; therefore, Cisco provides free lab access to Cisco partners through dCloud. Simply navigate to https://dcloud.cisco.com and log in with your CCO ID. Then you can browse though many different lab scenarios and topologies across five different data centers globally. You may still want to purchase a VPN router and some Telepresence endpoints and UC phones to use with the dCloud labs. You may also find some helpful videos with demonstrations on YouTube. We recommend the Collab Crush channel.

Suggested Plan for Final Review and Study

This section lists a suggested study plan from the point at which you finish reading this book through Chapter 34 until you take the Implementing and Operating Cisco Collaboration Core Technologies (CLCOR 350-801) exam. You can ignore this five-step plan, use it as is, or modify it to better meet your needs:

Step 1. **Review key topics and DIKTA questions:** You can use the table at the end of each chapter that lists the key topics in each chapter or just flip through the pages looking for key topics. Also, reviewing the “Do I Know This Already?” (DIKTA) questions from the beginning of the chapter can be helpful for review.

Step 2. **Review the exam blueprint:** Cisco maintains a list of testable content known as the Implementing and Operating Cisco Collaboration Core Technologies (CLCOR 350-801) exam blueprint. Review it and make sure you are familiar with every item listed. You can download a copy at https://learningcontent.cisco.com/documents/marketing/exam-topics/350-801-CLCOR-v1.1.pdf.

Step 3. **Complete memory tables:** Open Appendix A, "Answers to the "Do I Know This Already?" Quizzes and Q&A Sections" from the book's website and print the entire thing or print the tables by major parts. Then complete the tables.

Step 4. **Study "Q&A" sections:** Go through the review questions at the end of each chapter to identify areas in which you need more study.

Step 5. **Use the Pearson Cert Practice Test engine to practice:** The Pearson Test Prep practice test software provides a bank of unique exam-realistic questions available only with this book.

Summary

The tools and suggestions listed in this chapter have been designed with one goal in mind: to help you develop the skills required to pass the Implementing and Operating Cisco Collaboration Core Technologies (CLCOR 350-801) exam to achieve the CCNP Collaboration certification.

This book has been developed from the beginning both to present you with a collection of facts and to help you learn how to apply those facts. Regardless of your experience level before reading this book, it is our hope that the broad range of preparation tools, and even the structure of the book, will help you pass the exam with ease. We wish you success in your exam and hope that our paths cross again as you continue to grow in your IT and Collaboration career.

This part covers the following topics:

- **Chapter 36, CCNP and CCIE Collaboration Core (CLCOR) 350-801 Exam Updates:** This chapter is a living document. After the initial publication of this book, Cisco Press will provide supplemental updates in this chapter as a digital download for any minor exam updates.

Part X

Exam Updates

Chapter 36: CCNP and CCIE Collaboration Core (CLCOR) 350-801 Exam Updates

CHAPTER 36

CCNP and CCIE Collaboration Core (CLCOR) 350-801 Exam Updates

The Purpose of This Chapter

For all the other chapters, the content should remain unchanged throughout this edition of the book. This chapter , however, will change over time, with an updated online PDF posted so you can see the latest version of the chapter even after you purchase this book.

Why do we need a chapter that updates over time? For two reasons:

1. To add more technical content to the book before it is time to replace the current book edition with the next edition. This chapter will include additional technology content and possibly additional PDFs containing more content.
2. To communicate detail about the next version of the exam, to tell you about our publishing plans for that edition, and to help you understand what that means to you.

After the initial publication of this book, Cisco Press will provide supplemental updates as digital downloads for minor exam updates. If an exam has major changes or accumulates enough minor changes, we will then announce a new edition. We will do our best to provide any updates to you free of charge before we release a new edition. However, if the updates are significant enough in between editions, we may release the updates as a low-priced standalone eBook.

If we do produce a free updated version of this chapter, you can access it on the book's companion website. Simply go to the companion website page and go to the "Exam Updates Chapter" section of the page.

If you have not yet accessed the companion website, follow this process:

Step 1. Browse to www.ciscopress.com/register.

Step 2. Enter the print book ISBN (even if you are using an eBook): 9780138200947.

Step 3. After registering the book, go to your account page and select the Registered Products tab.

Step 4. Click the Access Bonus Content link to access the companion website. Select the **Exam Updates Chapter** link or scroll down to that section to check for updates.

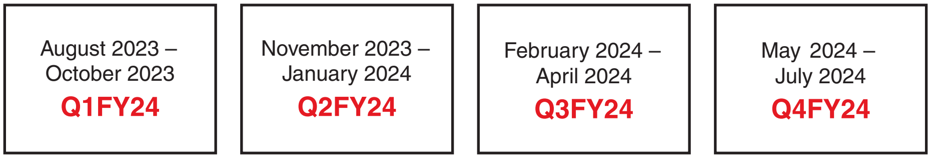
About Possible Exam Updates

Cisco introduced CCNA and CCNP in 1998. For the first 25 years of those certification tracks, Cisco updated the exams on average every 3–4 years. However, Cisco did not pre-announce the exam changes, so exam changes felt very sudden. Usually, a new exam would be announced, with new exam topics, giving you 3–6 months before your only option was to take the new exam. As a result, you could be studying with no idea about Cisco's plans, and the next day, you had a 3–6 month timeline to either pass the old exam or pivot to prepare for the new exam.

Thankfully, Cisco changed its exam release approach in 2023. Called the Cisco Certification Roadmap (https://cisco.com/go/certroadmap), the new plan includes these features:

- Cisco considers changes to all exam tracks (CCNA, CCNP Enterprise, CCNP Security, and so on) annually.
- Cisco uses a pre-defined annual schedule for each track, so even before any announcements, you know the timing of possible changes to the exam you are studying for.
- The schedule moves in a quarterly sequence:
  - Privately review the exam to consider what to change.
  - Publicly announce if an exam is changing, and if so, announce details like exam topics and release date.
  - Release the new exam.
- Exam changes might not occur each year. If changes occur, Cisco characterizes them as minor (less than 20% change) or major (more than 20% change).

The specific dates for a given certification track can be confusing because Cisco organizes the work by fiscal year quarters. Figure 36-1 spells out the quarters with an example 2024 fiscal year. Because Cisco's fiscal year begins in August, the first quarter (Q1) of fiscal year (FY) 2024 begins in August 2023, for example.



August 2023 – October 2023 Q1FY24	November 2023 – January 2024 Q2FY24	February 2024 – April 2024 Q3FY24	May 2024 – July 2024 Q4FY24

Figure 36-1 *Cisco Fiscal Year and Months Example (FY2024)*

Focus more on the sequence of the quarters to understand the plan. Over time, Cisco may make no changes in some years and minor changes in others.

Impact on You and Your Study Plan

Cisco's new policy helps you plan, but it also means the exam might change before you pass the current exam. That impacts you, affecting how we deliver this book to you. This chapter gives us a way to communicate in detail about those changes as they occur. However, you should watch other spaces as well.

For some other information sources to watch, bookmark and check these sites for news:

- **Cisco:** Check the Certification Roadmap page: https://cisco.com/go/certroadmap. Make sure to sign up for automatic notifications from Cisco on that page.
- **Publisher:** This page contains new certification products, offers, discounts, and free downloads related to the more frequent exam updates: https://www.ciscopress.com/newcert
- **The Cisco Learning Network:** Subscribe to the CCNA Community at Visit cs.co/9780138200947, where you should find ongoing discussions about exam changes over time. If you have questions, search for "roadmap" in the CCNA community, and if you do not find an answer, ask a new question!

As changes arise, we will update this chapter with more detail about exam and book content. At that point, we will publish an updated version of this chapter, listing our content plans. That detail will likely include the following:

- Content removed, so if you plan to take the new exam version, you can ignore that content when studying.
- New content planned per new exam topics, so you know what's coming.

The remainder of the chapter shows the new content that may change over time.

News about the Next Exam Release

This statement was last updated in 2023, before the publication of the *CCNP and CCIE Collaboration Core (CLCOR) 350-801 Official Cert Guide*.

This version of this chapter has no news to share about the next exam release.

At the most recent version this chapter, the 350-801 exam version number was Version 1.1.

Updated Technical Content

The current version of this chapter has no additional technical content.

This page intentionally left blank

This part covers the following topics:

- **Appendix A, Answers to the "Do I Know This Already?" Quizzes and Q&A Sections:** This appendix will provide the answers to the quizzes at the beginning and end of each chapter.
- **Glossary:** The glossary will provide definitions for all the key terms in the book.

Part XI

Appendices

Appendix A: Answers to the “Do I Know This Already?” Quizzes and Q&A Sections

Glossary

APPENDIX A

Answers to the “Do I Know This Already?” Quizzes and Q&A Sections

Chapter 1

Do I Know This Already?

1. C
2. D
3. B
4. D
5. B
6. A
7. D

Answers to the Q&A

1. Call Manager is an IP PBX.
2. ISDN using H.320, IP using H.323, and IP using SIP
3. Email, fax, and voicemail
4. Vocal communication with Webex and People Insights

Chapter 2

Do I Know This Already?

1. D
2. B
3. D
4. A
5. C
6. B
7. B
8. A
9. C
10. D

Answers to the Q&A

1. The technical properties of a sound wave are as follows: Cycle, Period (time), Wavelength (distance), Pressure, Amplitude.

2. The three digital signal rate forms are DS0, DS1, and DS3. A DS1 is equivalent to a T1 T-carrier rate form with 24–64 kbps circuits, and a DS3 is equivalent to a T3 T-carrier rate form with 28 T1 circuits.
3. G.711, G.722, and G.729 are the top three audio codecs used by the ITU. iLBC, iSAC, and AAC-LD are the three audio codecs used by SIP mentioned in this book.

Chapter 3

Do I Know This Already?

1. C
2. A
3. A
4. B
5. C
6. A
7. D
8. A
9. B
10. D
11. C
12. B

Answers to the Q&A

1. In composite video, all the video information is combined into a single line level. In component video, a video signal is split into two or more component channels.
2. The two main digital cameras are charge-coupled device (CCD) image sensors and complementary metal-oxide-semiconductor (CMOS) image sensors. Three main light-filtration techniques are Foveon X3 sensors, 3CCD (also known as three-chip cameras), and Bayer.
3. Transform blocks are broken down into 16×16 luma (Y) samples and 8×8 chroma (Cb and Cr) samples.
4. In SIP communications, the protocol to be employed is called Binary Floor Control Protocol (BFCP). In H.320 and H.323 communications, the additional protocol to be employed is called H.239.

Chapter 4

Do I Know This Already?

1. C
2. A
3. B
4. A
5. D
6. C

7. A
8. C
9. B
10. C
11. A
12. D

Answers to the Q&A

1. The six components that make up a video system are
   - Audio Input: Microphones
   - Audio Output: Speakers
   - Video Input: Camera
   - Video Output: Display
   - Endpoint: AKA Codec
   - Cables and connectors
2. The five functions of the menu settings on an endpoint are to place calls, answer calls, change administrator settings, adjust PTZ camera controls, and share content.
3. The four categories of reflections are direct sound, early reflections, incoherent late reflections (or reverberation), and coherent late reflections (or echo).
4. The three positions used in the three-point lighting technique are the key light, fill light, and back light.

Chapter 5

Do I Know This Already?

1. D
2. C
3. A, E, H, and I
4. B
5. D
6. C
7. B
8. C
9. B
10. D
11. C
12. A
13. C
14. B

Answers to the Q&A

1. BRI supports 2 B-channels at 64 Kbps each and 1 D-channel at 16 Kbps. PRI comes in T-carrier, J-carrier, and E-carrier. T- and J-carrier support 23 B-channels at 64 Kbps each and one D-channel at 64 Kbps. E-carrier supports 30 B-channels at 64 Kbps each and two D-channels at 64 Kbps each.
2. E.164 aliases are numeric only with up to 15 digits, H.323 IDs can be alphanumeric and special characters but do not support spaces, and prefixes are registered numeric aliases that are used to route calls to bridges and gateways.
3. Obtain power, load locally stored image, CDP discovery, obtain VLAN information, DHCP Discovery, TFTP Get, receive CTL file and TFTP information, send registration request to CUCM, receive OK when registration is complete.
4. IETF has STUN, TURN, and ICE for NAT traversal; Cisco has Assent for NAT and firewall traversal; and ITU has H.460.17, H.460.18, and H.460.19 for NAT and firewall traversal.

Chapter 6

Do I Know This Already?

1. A, C, and F
2. A
3. C
4. D
5. B
6. D
7. C and D
8. C
9. A
10. B
11. C
12. B
13. C
14. B

Answers to the Q&A

1. Webex Room Kit Series (Room Kit Mini, Room Kit, Room Kit Plus, Room Kit Pro), Webex 55 (Single/Dual), Webex 70 (Single/Dual), Webex Board
2. See the following table.

Feature	Cisco Expressway	Cisco VCS
Server Components	Expressway Core Expressway Edge	VCS Control VCS Expressway
Registration Licensing	Included with CUCL and CUWL user licenses (Registration supported on X8.9 or later)	Device Registration Licenses required (2500 max per server)

Feature	Cisco Expressway	Cisco VCS
Call Licensing	Internal and mobile calling included Rich Media Session (RMS) Licenses required for B2B and B2C calling	Nontraversal Call Licenses required Traversal Call Licenses required
Microsoft Interop License	Requires RMS licenses	Requires Option Key
FindMe License	Available	Requires Option Key
Device Provisioning License	Requires Option Key (Free)	Requires Option Key (Free)
Clustering Capabilities	Up to 6 servers	Up to 6 servers

3. Prime Collaboration Provisioning, Prime Collaboration Assurance, and Prime Collaboration Analytics
4. See the following commands:

```
Switch(config)# mls qos
Switch(config)# interface fastethernet 0/1
Switch(config-if)# mls qos trust cos
```

Chapter 7

Do I Know This Already?

1. A
2. D
3. B
4. B
5. B
6. C
7. B

Answers to the Q&A

1. 7811—1 line, 7821—2 lines, 7841—4 lines, 7861—16 lines
2. 8851—2 KEM, 8851NR—2 KEM, 8861—3 KEM, 8865—3 KEM, 8865NR—3 KEM
3. Busy lamp field, call forwarding, call hold, call pickup, call park, call transfer, call waiting, do not disturb, and extension mobility/hot desking

Chapter 8

Do I Know This Already?

1. D
2. B
3. C
4. B
5. A
6. B

7. C
8. D
9. D
10. D
11. D
12. A, D, and E

Answers to the Q&A

1. DX70, DX80, SX10, SX20, SX80, MX200G2, MX300G2, MX700, MX800
2. Floor stand, table stand, wheel base, and wall mount
3. Webex Room Kit Mini, Webex Room Kit, Webex Room Kit Plus, Webex Room Kit Pro, Webex Room 55, Webex Room 70, Webex Board 55s, Webex Board 70s, Webex Board 85
4. Room Kit Pro: Codec Pro, Quad Camera, and Touch 10

   Room Kit Pro Precision 60: Codec Pro, Precision 60 camera, and Touch 10

   Codec Pro: Codec only
5. Triple 4k camera cluster with automated alignment

   Three thin bezel 70-inch LCD displays

   One powerful single codec, allowing five simultaneous streams

   H.265 HEVC-capable supporting 1080p 60 fps

   Eighteen positioning microphones

   Nineteen special audio speakers

   Two three-headed dongles that support HDMI, Display Port, and Mini Display port connections

   An integrated LED lighting bar

   Requires only a single 10/15 amp circuit requiring 950 watts of power to run the whole system

Chapter 9

Do I Know This Already?

1. B
2. C
3. C
4. A
5. C
6. A and F
7. D
8. A
9. D
10. D

Answers to the Q&A

1. Prestandard PoE, also called inline power, supports up to 7W power; 801.3af PoE supports up to 15W of power; and 802.3at, also called PoE+, supports up to 25.5W of power.
2. SW1(config-if)# **switchport mode access**

   ```
   SW1(config-if)# switchport access vlan 100
   SW1(config-if)# switchport voice vlan 200
   ```
3. Option 150 and Option 66
4. Phone configuration files

   Phone firmware files

   Certificate trust list (CTL) files

   Identity trust list (ITL) files

   Tone localization files

   User interface (UI) localization and dictionary files

   Ringer files

   Softkey files

   Dial plan files for SIP phones
5. Request-URI:

   To:

   From:

   Call-ID:

   CSeq:

   Contact:

Chapter 10

Do I Know This Already?

1. B
2. B
3. A
4. C
5. D
6. A
7. B
8. D
9. A
10. C
11. A

Answers to the Q&A

1. TRC5 Remote Control, Touchscreen, Touch 10 Controller, Web Interface, CLI
2. Windows PC, Mac PC, Smartphone, Tablet, VHS Player, Blu-ray Player, Apple TV, TV Tuner, etc.

3. CUCM, Spark (or Webex is acceptable), TMS, VCS
4. Five multisite layouts are as follows:
   - **Auto:** The default layout family, as given by the local layout database, will be used as the remote layout.
   - **Equal:** All video participants will have equal-sized panes as long as there is enough space on the screen.
   - **Overlay:** The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small PIPs. Transitions between active speakers are voice switched.
   - **Prominent:** The active speaker, or the presentation if present, will be a larger picture, while the other participants will be smaller pictures. Transitions between active speakers are voice switched.
   - **Single:** The active speaker, or the presentation if present, will be shown in full screen. The other participants will not be shown at all. Transitions between active speakers are voice switched.

Chapter 11

Do I Know This Already?

1. C
2. A
3. A
4. C
5. D
6. D
7. C

Answers to the Q&A

1. Upload the cop.sgn file to CUCM, restart the TFTP service, and push the software out to the endpoints.
2. The steps for manually upgrading a Cisco CE software-based endpoint are as follows:

Step 1. Using a Web browser, navigate to the web interface of the endpoint, and log in with the appropriate username and password.

Step 2. Navigate to **Maintenance > Software Upgrade**.

Step 3. Click the Browse button and select the pkg file that was previously downloaded, and then click Open.

Step 4. The detected version of the software load should appear on the screen. After confirming the version is correct, click the blue Install software button.

Step 5. The software will upload to the endpoint. This part of the process could take several minutes. Once the upload process is complete, the upgrade will automatically initialize.

Step 6. This process will take several more minutes to complete. Once the upgrade has completed, the endpoint will reboot.

3. Through the TMS web interface or through the back end on the Windows Server
4. CLI, Web Interface, and TMS

Chapter 12

Do I Know This Already?

1. A
2. B
3. D
4. A
5. C
6. B
7. D
8. A
9. D
10. B

Answers to the Q&A

1. Spanning Tree Protocol 802.1d (STP), Rapid Spanning Tree Protocol 802.1w (RSTP), and Multiple Instance Spanning Tree Protocol 802.1s (MISTP)
2. Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP)
3. Multiprotocol Label Switching (MPLS), Cisco Voice and Video Enabled IP Security Virtual Private Network (IPSec V3PN), and Dynamic Multipoint Virtual Private Network (DMVPN)
4. Cisco 1100-8P ISR LTE Advanced, Cisco 1100-4P ISR with DSL, Cisco 1101-4P, and Cisco 1101-4PLTEP

Chapter 13

Do I Know This Already?

1. D
2. B
3. C
4. A
5. C
6. A
7. A
8. F
9. B

10. C
11. C
12. B
13. A
14. C

Answers to the Q&A

1. Latency, jitter, packet loss, and bandwidth delay
2. Voice, Interactive Video, Streaming Video, Call Signaling, IP Routing, Network Management, Mission-Critical Data, Transactional Data, Bulk Data, Best Effort Data, Scavenger
3. Delay less than 150 ms, jitter less than 30 ms, and a packet loss less than 1 percent
4. See the following table:

Traffic Type	DSCP (PHB)	802.1p UP	802.11e UP
Voice	46 (EF)	5	6
Video	34 (AF41)	4	5
Voice and Video Signaling	24 (CS3)	3	4

5. The switch commands are as follows:

```
Switch(config)# mls qos
Switch(config)# interface type number
Switch(config-if)# mls qos trust cos
```

The router commands are as follows:

```
Router(Config)# class-map class-map-name
Router(config-cmap)# match protocol protocol
Router(config)# policy-map name
Router(config-pmap)# class name
Router(config-pmap-c)# priority bandwidth-in-kbps
Router(Config)# interface type number
Router(Config-if)# service-policy {input | output}
policy-map-name
```

Chapter 14

Do I Know This Already?

1. B
2. D
3. C
4. C
5. B
6. A

Answers to the Q&A

1. _cisco-uds._tcp.fqdn. 7200 10 10 8443 cucm.fqdn and _cuplogin._tcp.fqdn. 7200 10 10 8443 imp.fqdn.
2. Five reasons for NTP:
   - Cisco IP phones display date and time information. This information is obtained from Cisco Unified Communications Manager.
   - CDR and CMR, which are used for call reporting, analysis, and billing, include date and time information.
   - Alarms and events in log files, as well as trace information in trace files, include time information. Troubleshooting a problem requires correlation of information that is created by different system components, such as Cisco Unified Communications Manager, Cisco IOS gateway, and so on. This problem solving is possible only if all devices in the network have the same correct time information.
   - Some Cisco Unified Communications Manager features are date-based or time-based and therefore rely on correct date and time. These features include time-of-day routing and certificate-based security features.
   - Certificates include a validity period. If a system that receives a certificate has an invalid future date, it may consider the received certificate to be invalid or expired.
3. Cisco Emergency Responder, Cisco Paging Server, UCCE, UCCX, Unified CVP, Cisco Prime Collaboration, TMS

Chapter 15

Do I Know This Already?

1. D
2. A and C
3. B
4. C
5. C
6. D
7. B
8. C
9. C
10. A

Answers to the Q&A

1. The eight feature services are as follows:
   - Performance and Monitoring Services
   - Directory Services
   - CM Services
   - CTI Services

- Database and Admin Services
- Location-based Tracking Services
- Security Services
- CDR Services

2. Enterprise parameters are used to define clusterwide system settings, and these parameters apply to all devices and services across all nodes within the entire cluster. After installation of all Cisco Unified Communications Manager nodes and activation of the feature services, enterprise parameter default values should be verified, and modified if required, before deploying endpoints.
3. The most important service parameters for the Cisco CallManager service are the following:
    - **T302 Timer:** This setting specifies the interdigit timer for variable-length numbers. Reducing the default value will speed up dialing (shorter post-dial delay).
    - **CDR and CMR:** Call detail records and call management records are the bases for call reporting, accounting, and billing. The service parameters are used to enable CDRs and CMRs (both are disabled by default). While the CDR service parameter can be easily found by using the search function (the parameter is named CDR Enabled Flag), it is more challenging to find the CMR parameter (the parameter is named Call Diagnostics Enabled).
    - **Clusterwide Parameters (System-Location and Region):** This section lists various codecs of voice media-streaming applications. These codecs can be modified or disabled if needed.
4. 1:1 and 2:1.
5. Lossless compression searches content for statistically redundant information that can be represented in a compressed state without losing any original information. By contrast, lossy compression searches for nonessential content that can be deleted to conserve storage space.

Chapter 16

Do I Know This Already?

1. D
2. B
3. A
4. C
5. B
6. C
7. D
8. C
9. C
10. D

Answers to the Q&A

1. End-user attributes are as follows:

   Personal and Organizational Settings:

   - User ID
   - Last Name
   - Middle Name
   - First Name
   - Phone Numbers
   - Mail ID
   - Manager User ID
   - Department

   Password

   Cisco Unified Communications Manager Settings:

   - PIN
   - [SIP] Digest Credentials
   - Associated PC/Site Code
   - Controlled Devices
   - Extension Mobility
   - Directory Numbers Associations
   - Mobility Information
   - Multilevel Precedence and Preemption Authorization (MLPP)
   - CAPF Information
   - Permissions Information (Groups and Roles)

2. Steps to enable synchronization are as follows:

Step 1. Change the Navigation drop-down to Cisco Unified Serviceability and click **Go**.

Step 2. Navigate to **Tools > Service Activation**, select the Publisher server from the list, and click **Go**.

Step 3. Check the box next to the **Cisco DirSync** service and click **Save**.

Step 4. Once the service has been verified as Active, change the Navigation drop-down to **Cisco Unified CM Administration** and click **Go**.

Step 5. Navigate to **System > LDAP > LDAP System**.

Step 6. Check the box beside the Enable **Synchronizing from LDAP Server** setting.

Step 7. In the LDAP Server Type drop-down menu, select the type of LDAP server that will be used for this deployment, such as Microsoft Active Directory.

Step 8. In the LDAP Attribute for User ID drop-down menu, select the attribute that will be used to identify user accounts within the LDAP directory database.

3. Steps to enable authentication are as follows:

Step 1. Navigate to **System > LDAP > LDAP Authentication.**

Step 2. Check the box beside **Use LDAP Authentication for End Users**.

Step 3. Enter the LDAP Manager Distinguished Name followed by the LDAP Password and Confirm Password.

Step 4. The LDAP User Search Base should be the main search base for the whole domain. Any users in the LDAP directory that have not been synchronized with the Cisco Unified Communications Manager will not be able to log in.

Step 5. Finally, enter the address for the LDAP server in the Host Name or IP Address for Server field. Enter the LDAP Port and check the **Use TLS** box if a secure connection is being used for LDAP authentication.

Step 6. Click **Save** when finished.

Chapter 17

Do I Know This Already?

1. B
2. D
3. B
4. C and H
5. D
6. A
7. B
8. A
9. C
10. C

Answers to the Q&A

1. To manually add a phone to an end user, do the following:

Step 1. In the Cisco Unified Communications Manager Administration, navigate to **User Management > User/Phone Add > Quick/User Phone Add.**

Step 2. Click **Find** and select the end user for whom you want to add a new phone.

Step 3. Click the **Manage Devices** button. The Manage Devices window appears.

Step 4. Click **Add New Phone**. The Add Phone to User popup displays.

Step 5. From the Product Type drop-down list, select the phone model.

Step 6. From the Device Protocol drop-down, select **SIP** or **SCCP** as the protocol. Note that some Cisco phones and endpoints support only SIP, so SCCP will not be an option.

Step 7. In the Device Name text box, enter the device MAC address.

Step 8. From the Universal Device Template drop-down list, select a universal device template.

Step 9. (Optional) If the phone supports expansion modules, enter the number of expansion modules that you want to deploy.

Step 10. If you want to use Extension Mobility to access the phone, check the **Is Extension Mobility Template** check box.

Step 11. Click **Add Phone**. The Add New Phone popup closes. The Cisco Unified Communications Manager adds the phone to the user and uses the universal device template to configure the phone.

Step 12. If you want to make additional edits to the phone configuration, click the corresponding Pencil icon to open the phone in the Phone Configuration window.

2. The main steps to Self-Provisioning are as follows:

Step 1. Enable the Cisco CTI Manager and Self-Provisioning IVR Services.

Step 2. Configure auto-registration on Publisher CUCM.

Step 3. Create a CTI route point for Self-Provisioning IVR.

Step 4. Create a dial-in extension for Self-Provisioning IVR.

Step 5. Create an application user for Self-Provisioning IVR.

Step 6. Configure the system for Self-Provisioning.

3. The steps to set up BAT are as follows:

Step 1. Set up the template for data input.

Step 2. Define a format for the CSV data file.

Step 3. Collect the data for each device in the bulk transaction.

Step 4. Upload the data files choosing the relevant target and function for the transaction.

Step 5. Validate the data input files with the Cisco Unified Communications Manager database.

Step 6. Submit jobs for execution.

Step 7. Schedule jobs.

Step 8. Execute jobs to insert the devices into the Cisco Unified Communications Manager database.

Chapter 18

Do I Know This Already?

1. C
2. B
3. C
4. D

5. C
6. B
7. A, B, and C
8. A
9. D
10. B

Answers to the Q&A

1. Components of a well-designed dial plan are as follows:
   - Endpoint addressing (numbering plan)
   - Call routing and path selection
   - Digit manipulation
   - Calling privileges
   - Call coverage
2. CSS and partition mechanisms:

   Partitions:
   - Voicemail ports
   - Directory numbers
   - Route patterns
   - SIP route patterns
   - Translation patterns

   CSSs:
   - Voicemail ports
   - Phones
   - Phone lines
   - Trunks
   - Gateways
   - Translation patterns
3. The hunt distribution algorithms are as follows:
   - Try the next member; then try the next group in the hunt list.
   - Try the next member but do not go directly to the next group.
   - Skip remaining members and go directly to the next group.
   - Stop hunting.

Chapter 19

Do I Know This Already?

1. D
2. A
3. C
4. B
5. E
6. A
7. B

Answers to the Q&A

1. Call-routing source components:
   - IP phones
   - Trunks
   - Gateways
   - Translation patterns
   - Voicemail ports
2. Call-routing target components:
   - Translation patterns
   - Voicemail ports
   - Directory numbers
   - Directory URIs
   - Route patterns and SIP route patterns
   - Call park numbers
3. Transformation pattern steps:
   - **a.** Configure calling party transformation patterns.
   - **b.** Configure called party transformation patterns.
   - **c.** Optionally Configure transformation profiles.

Chapter 20

Do I Know This Already?

1. C
2. D
3. A
4. B
5. B
6. D

Answers to the Q&A

1. Firewall traversal protocols:
    - Assent
    - H.460.18/19
2. RMS Services:
    - B2B and B2C Communications
    - Microsoft Interoperability
3. TDM Gateway models:
    - ISR
    - ASR

Chapter 21

Do I Know This Already?

1. A
2. D
3. A and B
4. B
5. D
6. C
7. B
8. C and D
9. D
10. A
11. B
12. D
13. A

Answers to the Q&A

1. First, MRA is only supported for SIP; there is no H.323 support in the MRA solution. Second, certificates are required for MRA; there is no way to build the traversal zones with a basic TLS or TCP SIP connection. TLS Verify is required for MRA. Third, some specific settings must be configured to enable MRA on the Expressway servers. Fourth, the zones created between the Cisco Expressway Core and Cisco Expressway Edge servers are not the same traversal client zone and traversal server zone used in a standard firewall traversal solution. Finally, the DNS SRV records that need to be created are different from what is required for a traditional firewall traversal solution.
2. DNS A-records and SRV records

    Firewall ports and considerations

    Certificate requirements and recommendations

    HTTPS reverse proxy settings

3. Endpoint sends an SRV lookup for _cisco-uds._tcp.<domain> but the lookup fails.

   Endpoint sends an SRV lookup for _collab-edge._tcp.<domain> and the lookup is found. The communication is routed to the Expressway-E.

   Endpoint goes through a TLS handshake with the Expressway-E.

   Endpoint sends an HTTP Get message to the Expressway-E. The message is proxied to the Expressway-C.

   Expressway-C sends an SRV lookup for _cisco-uds._tcp.<domain> and the lookup is found. The communication is routed to the CUCM.

   Endpoint registers to the CUCM.

4. Enable MRA on both Cisco Expressways (Core and Edge).

   Configure MRA on the Expressway Core.

   Configure a secure traversal zone connection between the Expressway Edge and the Expressway Core.

5. Enable MRA on both Cisco Expressways (Core and Edge).

   Enable OAuth Authentication in Cisco Unified Communications Manager and Expressway.

   Onboard Cisco Unified Communications Manager to the cloud for MRA activation code onboarding.

   Configure MRA Service Domains.

   Configure MRA Access Control to allow activation code onboarding.

   Check that the Trusted Cisco Manufacturing Certificates (MICs) installed.

   Provision the phone in the Cisco Unified Communications Manager database using any accepted provisioning method.

Chapter 22

Do I Know This Already?

1. A
2. C
3. D
4. B
5. A
6. D
7. C
8. B
9. A
10. D

Answers to the Q&A

1. The three types of Meetings available in a Webex solution are as follows:

   - Webex Personal Rooms
   - Webex Webinars
   - Webex Events

2. The three Webex Calling PSTN options are as follows:
   - Cloud Connected PSTN (CCP)
   - Cisco PSTN
   - On-premises PSTN through Local Gateway

Chapter 23

Do I Know This Already?

1. D
2. C
3. D
4. B
5. A
6. D
7. A
8. C
9. C
10. E

Answers to the Q&A

1. The four main steps to set up Cloud Connected Unified Communications through the Webex Control Hub are as follows:

Step 1. Enable Cloud Connected Unified Communications.

Step 2. Install and sync Agent Files.

Step 3. Verify and assign clusters.

Step 4. Ensure Deployment Insight Service is enabled.

2. The three directory management options available for user import to the Webex Control Hub are as follows:
   - Microsoft Active Directory (AD)
   - Microsoft Azure Active Directory (Azure AD)
   - Okta
3. The three areas of communication when using directory synchronization through the Directory Connector are as follows:
   - Control Hub
   - Directory Connector Management Interface
   - Directory Synchronization Service
4. The six types of workspaces available when registering a Shared Usage device are as follows:
   - **Desk:** Individual | Capacity 1
   - **Focus:** High concentration | Capacity 1–2

- **Huddle:** Brainstorm/collaboration | Capacity 2–5
- **Meeting Room:** Dedicated meeting space | Capacity 6–20
- **Open Space:** Unstructured agile | Capacity 2–100
- **Other:** Unspecified

Chapter 24

Do I Know This Already?

1. D
2. D
3. C
4. A, E, F
5. C
6. B, E
7. B
8. A, B
9. B
10. D

Answers to the Q&A

1. The three PSTN options for Webex Calling are as follows:
    - Cloud Connected PSTN (CCP)
    - Cisco PSTN
    - Premises-based PSTN
2. The five series of Cisco routers that support the Local Gateway are:
    - ISR 1100 Series
    - ISR 4000 Series
    - Catalyst 8000 Edge Platforms
    - Cloud Service Router 1000v
    - Catalyst 8000v
3. The four companies that offer third-party routers to support the Local Gateway are as follows:
    - Oracle
    - AudioCodes
    - Mediant
    - Ribbon

4. The two rules you must follow when creating multiple locations in the Webex Control Hub for Webex Calling are as follows:
   - You cannot assign multiple Local Gateways to a single location. Only one Local Gateway can be assigned per location.
   - You can assign a single Local Gateway to multiple locations.

Chapter 25

Do I Know This Already?

1. B
2. A
3. B
4. D
5. C
6. C
7. D
8. C
9. A
10. B

Answers to the Q&A

1. The four criteria for call pickup are as follows:
   - A user can only be assigned to one call pickup.
   - A call pickup can only have users from the same location.
   - A location may have multiple call pickups.
   - Call pickup names must be unique.
2. The Cisco DECT devices that can register to Webex Control Hub are as follows:
   - Cisco IP DECT DBS 110 Single-Cell Base Station
   - Cisco IP DECT DBS 210 Multi-Cell Base Station (up to 254 bases)
   - Cisco DECT Handsets (6823 and 6825)
3. To configure their own Webex Calling features, users should go here in the user portal:
   - Go to **https://settings.webex.com** and select **Webex Calling**.
   - From the calling user portal, go to **Call Settings**.
   - Toggle on (and configure if necessary) all the settings you want to use.

Chapter 26

Do I Know This Already?

1. B
2. D

3. A
4. A
5. C
6. B
7. A
8. C
9. D
10. B

Answers to the Q&A

1. Settings should be configured in the following order for Webex Calling both in Webex Control Hub and Local Gateway:
    1. Locations
    2. Numbers
    3. Call Routing
    4. Local Gateway (on the Cisco IOS-XE router)
    5. Gateway (on Webex Control Hub)
2. The three PSTN options for Webex Calling are as follows:
    - Cisco PSTN
    - Cloud Connected PSTN
    - Premises-based PSTN
3. The three-step process the Cisco Unified Communications Manager would use to route calls from Cisco UBE to Local Gateway is as follows:
    1. The via URI uses an inbound dial peer to point to a dial peer group.
    2. The outbound dial peers in the DPG then re-route the call to Webex.
    3. Webex will then find the registered phone matching the dialed alias and connect the call.

Chapter 27

Do I Know This Already?

1. D
2. D
3. C
4. A
5. B
6. C
7. A

Answers to the Q&A

1. CUCM SIP integration with CUC:

Step 1. Configure a SIP trunk security profile.

Step 2. Configure a SIP trunk to CUC.

Step 3. Configure the voice mail pilot and the voice mail port.

Step 4. Configure a route pattern.

2. System call handlers are used for greetings and can offer the caller different call actions depending on the digit that the caller selects. Directory call handlers allow callers to search for users on the CUC system or on connected voice-messaging systems. Interview call handlers allow the system to ask the caller questions and record the answers.
3. Direct routing rules:
   - **Attempt Sign-In:** Calls from users are routed to the user login conversation.
   - **Opening Greeting:** Calls forwarded from an extension that is not associated with a user account are routed to the opening greeting.

Forwarded routing rules:

- **Attempt Forward:** All calls forwarded from a user extension or routed to the user greeting.
- **Opening Greeting:** Calls forwarded from an extension that is not associated with a user account are routed to the opening greeting.

Chapter 28

Do I Know This Already?

1. A
2. C
3. C
4. B
5. D
6. A
7. D
8. A
9. B
10. B

Answers to the Q&A

1. CUC user-related settings are as follows:
   - Enterprise and service parameters on the highest level
   - General settings on the system level
   - User templates on the mid-level
   - User settings on the low level
2. There are three predefined transfer rules: standard, alternate, and closed. The standard rule is enabled without an end date and cannot be modified. The alternate rule might replace the standard rule with an end date, such as between Christmas and New Year's

day. An alternative transfer rule could be used instead of the standard transfer rule. If the schedule for the user is set to weekdays only, the closed rule is used on the weekend and after business hours.

3. Methods to add users to CUC are as follows:
   - Manually add users.
   - Import users from CUCM.
   - Import users from LDAP.
   - Use the Bulk Administration Tool.
   - Migrate users from Cisco Unity using COBRAS.

Chapter 29

Do I Know This Already?

1. D
2. B
3. D
4. B
5. A
6. D
7. A
8. B, C
9. A

Answers to the Q&A

1. The four different soft phone devices used to register Webex App to the Cisco Unified Communications Manager are as follows:
   - Cisco Unified Client Services Framework
   - Cisco Dual Mode for iPhone
   - Cisco Jabber for Tablet
   - Cisco Dual Mode for Android
2. The five Webex Control Hub requirements for Jabber migration to Webex App are as follows:
   - Access the Webex Control Hub with full administrative privileges.
   - Add a cluster of Cisco Unified Communications Managers and IM and Presence Service servers to Cloud Connected UC.
   - Activate Deployment Insight services for Cisco Unified Communications Managers and IM and Presence Service servers.
   - Remove Hybrid Calling, if used.
   - Synchronize users to Common Identity.

3. The three services Webex App relies on within the Service Profile on the Cisco Unified Communications Manager are as follows:

   - Voicemail
   - CTI
   - Cisco Jabber Client Configuration

Chapter 30

Do I Know This Already?

1. D
2. A
3. B
4. C
5. C
6. C
7. B
8. A
9. D
10. B
11. B

Answers to the Q&A

1. The three types of logs archives that can be downloaded are as follows:
   - **Download Logs Archive:** Selecting this option will enable a standard download with most details still included for analysis. Call info is excluded from this standard download to ensure the caller's privacy.
   - **No Call History:** Selecting this option will download the same log information as the Download Logs Archive, except no history log information will be included to save on space.
   - **Full Call History:** Selecting this option will download the exact same information as the standard download including caller information. Only three lines are different between this option and the standard option.

2. The four major characteristics of input-video peripherals that can influence media quality are as follows:
   - The quality of the lens that the camera uses
   - The exposure range that the camera can process
   - The focus capabilities
   - The recommended lighting conditions for which the camera is designed

3. Steps for creating problem reports on Cisco Jabber are as follows:

Step 1. On the Cisco Jabber client, navigate to **Help > Report a Problem**.

Step 2. Navigate through the three separate windows to create the report. In the first window, choose the problem area and click **Next**.

Step 3. In the second window, choose the problem category and optionally enter a brief problem description. Click **Next**.

Step 4. In the third window, you can optionally attach a file to the report and click **Save Report**. A copy of the report is saved to your computer desktop.

Chapter 31

Do I Know This Already?

1. C
2. B
3. B
4. D
5. A
6. D

Answers to the Q&A

1. The steps to use the Cisco DNA tool are as follows:

Step 1. Navigate to **https://<*CUCM IP Address*>/dna**.

Step 2. Choose **Analysis > Phones**.

Step 3. Leave the text box next to the Find button empty and click **Find** to view a list of all available devices. Click on the **Device Name** of the endpoint from which you want to simulate a call attempt.

Step 4. In the window that appears, do the following:

a. From the Association Information section, choose **Line (1)**.

b. In the Dialed Digits Settings section, choose the **Dialed Digits** radio button, and then enter the directory number of another device.

c. Check the **SIP Analysis** check box.

Step 5. Click the **Do Analysis** button.

2. The three types of users who can access the CAR tool and the files they can access are as follows:

- Administrators are allowed to use all the features of CAR so that they can generate system reports to view system performance, verify load balancing, and troubleshoot.

- Managers can generate reports for users, departments, and QoS to help with call monitoring for budgeting or security purposes. Reports can also be used for determining the voice quality of the calls (for example, to ensure compliance with service-level agreements).

- End users can generate a billing report for their calls.

3. The CDR and CMR attributes that are included in the log file details are as follows:

   CDR:

   - The called number
   - The calling number
   - The date and time that the call was started
   - The time that the call connected
   - The time that the call ended
   - The cause for the termination of a call

   CMR:

   - Jitter
   - Lost packets
   - The amount of data that was sent and received during the call
   - Latency

Chapter 32

Do I Know This Already?

1. B
2. A
3. D
4. A
5. D
6. C

Answers to the Q&A

1. The five menus that are added to the RTMT when UC servers are being monitored are as follows:
   - System
   - Voice/Video
   - Unity Connection
   - IM and Presence
   - AnalysisManager
2. To set up Remote Browse through the RTMT, complete the following steps:

Step 1. Double-click **Remote Browse from Trace and Log Central**, choose **Trace Files**, and then **click Next.**

Step 2. In the Select UCM Services/Application tab, select the desired services.

Step 3. To select all options available, check the **Select All Services on All Servers** check box and click **Next**. The Select System Services/Application tab appears.

Step 4. **Select a service or check the Select All Services on All Servers** check box, and then click **Next** again.

Step 5. Finally, the Select IM_AND_PRESENCE Services/Application tab appears. Select a service or check the **Select All Services on All Servers** check box. At least one box must be checked on one of the three pages.

Step 6. **When** done, click **Finish.** Cisco Unified Communications Manager will perform the query and display the results.

3. The five different values of the Database Summary are as follows:
   - **0:** Not started, no subscribers exist, or the Cisco Database Layer Monitor service is not running and has not been running since the subscriber was installed.
   - **1:** Started; replication is currently being set up.
   - **2:** Finished; replication setup is complete and working.
   - **3:** Broken; replication failed during setup and is not working.
   - **4:** Replication is not set up correctly.

Chapter 33

Do I Know This Already?

1. D
2. B
3. C
4. D
5. B
6. A

Answers to the Q&A

1. Activities that can be performed in the DRS through the Master Agent are as follows:
   - Configuring backup devices
   - Scheduling backups by adding new backup schedules
   - Viewing or updating an existing schedule
   - Displaying the status of executed schedules
   - Performing system restoration
2. CDR_CAR, IM_AND_PRESENCE, UCM, SELFCARE, and PLM are the features that can be selected within a Cisco Unified Communications Manager cluster.

Chapter 34

Do I Know This Already?

1. D
2. C
3. A

4. B
5. C
6. A

Answers to the Q&A

1. The information included in a user report is as follows:
    - Last name, first name, and alias
    - Information that identifies the Cisco Unity Connection server that is associated with the user
    - Billing ID, CoS, and extension
    - Whether the account is locked
    - Whether the user has enabled personal call transfer rules
2. The information included in a server report is as follows:
    - **Percentage of CPU per Server:** A line chart displays the percentage of CPU usage for each server in a cluster. Each data value in a chart represents the average CPU usage for one 15-minute period. If no data exists for the server, Cisco Serviceability Reporter does not generate a line that represents that server. If there are no lines to generate, Cisco Serviceability Reporter does not create the chart. The message “No data for Service Statistics report available” is displayed.
    - **Percentage of Memory Usage per Server:** A line chart displays the percentage of memory usage for the server (%MemoryInUse). In a cluster configuration, there is one line per server in the cluster for which data is available. Each data value in the chart represents the average memory usage for a 15-minute period of time. If no data exists, Cisco Serviceability Reporter does not generate the chart.
    - **Percentage of Hard Disk Usage of the Common Partition per Server:** A line chart displays the percentage of the space usage for the common partition on the server (%DiskSpaceInUse) or on each server in a cluster configuration. Each data value in the chart represents the average disk usage for a 15-minute period. If no data exists, Cisco Serviceability Reporter does not generate the chart. The same report is available for the spare partition. As long as there is no installation in the second partition, no information is available.
3. The three types of billing reports are as follows:
    - Transfer Call Billing Report
    - Outcall Billing Detail Report
    - Outcall Billing Summary Report

This page intentionally left blank

GLOSSARY

NUMERICS

+E.164 alias An international phone number written with a plus sign (+) before the phone number to indicate that the number is in international (E.164) format.

3CCD A technique that determines colors by sending light through a prism, which separates the light into the RGB spectrum frequencies. Each color is measured on an individual light-sensitive chip. Also known as *three-chip cameras*.

3G-SDI 3G Serial Digital Interface; a video interface that consists of a single 2.970 Gbps serial link that allows you to replace dual-link HD-SDI.

802.11e The standard used for wireless networks. Both 802.1p and differentiated services code point are the standards to set priorities on wired networks. This standard is commonly referred as user priority, and it is important to map the UP to its appropriate DSCP value.

802.1d A Layer 2 protocol known as Spanning Tree Protocol that runs on bridges and switches. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network.

802.1p An IEEE standard that allows Layer 2 CoS to be applied from the switch. Eight different classes of service are expressed in a 3-bit PCP field in a q header added to the frame.

802.1Q An IEEE standard often referred to as Dot1Q. It is the networking standard that supports VLANs on an IEEE 802.3 Ethernet network. This standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also contains provisions for a quality-of-service prioritization scheme commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.

802.1s Multiple Instance Spanning Tree Protocol (MISTP).

802.1w Rapid Spanning Tree Protocol (RSTP).

802.1x A data link layer authentication protocol used by Cisco IP phones to connect to a Cisco Catalyst switch that implements this security mechanism. Phones that support 802.1x must be configured correctly; otherwise, the data link layer authentication will prevent the phone from registering.

802.3af An IEEE standard for PoE that supports up to 15W of power to any device that supports PoE.

802.3at An IEEE standard also known as PoE+ that can support up to 25.5W of power to any device that supports this standard.

A

AAAA-records A type of lookup record that resolves 128-bit IPv6 addresses to URLs.

AAR Automated alternate routing; a type of routing that automatically reroutes calls through the PSTN or another network when the system blocks a call due to insufficient bandwidth.

absorption The complete dissipation of sound waves within an object of obstruction. Absorption is similar to transmitting through an object.

ACG Automatic gain control; a function that makes dynamic adjustments to gain, typically on a microphone signal, to maintain an optimal level for different speakers.

ACL Access control list; a function of a router that controls ingress and egress traffic based on protocol or port.

acoustical power A measure of amplitude over time.

AD Active Directory; a Microsoft Corporate Directory product used for user and device management and LDAP integrations.

AD forest The topmost logical container in an Active Directory configuration that contains domains, users, computers, and group policies.

ad hoc "On the fly"; a call escalation function through a Cisco Unified Communications Manager allowing a point-to-point call to escalate to a multipoint call using an external conferencing resource to host the call.

AD LDS Active Directory Lightweight Directory Services; an independent mode of Microsoft Active Directory that provides dedicated directory services for applications.

AD tree A collection of domains within a Microsoft Active Directory network. The term refers to the fact that each domain has exactly one parent, leading to a hierarchical tree structure. A group of Active Directory trees is known as a forest.

ADAM Active Directory Application Mode; a part of Microsoft's fully integrated directory services available with Windows Server 2003 and built specifically to address directory-enabled application scenarios.

ADCS Active Directory Certificate Service; a service that runs on a Microsoft Windows Server. This service can be used to sign private certificates for use within an enterprise.

ADDTS Add Traffic Stream; a message sent from a wireless client that is preparing to place a call to an access point to indicate the TSPEC. The access point can then accept or reject the ADDTS request based on whether bandwidth and priority treatment are available.

Advanced Networking An option key on the Expressway Edge servers that enables a second NIC so that when the Expressway Edge is placed in a DMZ, one NIC can communicate with the internal network and the second NIC can securely communicate with the public Internet. Calls can then be bridged across these two NICs through the Expressway Edge.

AEC Acoustic Echo Cancellation; a method that works by comparing the audio input from a near-end mic against the audio input from a far-end mic and subtracting the common delayed audio.

Agent Install file A package that must exist on Cisco UC applications for CCCUC to function. Webex uses components in these files to install telemetry modules used to extract user and device data, as well as log information so that it can all be monitored through the cloud.

AI Artificial intelligence.

alert report A Cisco Unified Serviceability report generated on the CUC that contains any alerts that were generated along with their severity.

aliasing A form of distortion caused when a digital signal is converted back to analog form by a digital-to-analog converter; false frequency components appear that were not in the original analog signal.

AMIS Audio Messaging Interchange Specification analog; a protocol that provides a mechanism for transferring voice messages between different voice-messaging systems.

amplitude The measure of the magnitude of change in each oscillation of a sound wave. Most often this measurement is peak-to-peak, such as the change between the highest peak amplitude value and the lowest trough amplitude value, which can be negative.

analog signal A continuous signal that contains a time variable representative of some other time-varying quality, such as the voltage of the signal may vary with the pressure of the sound waves.

ANI Automatic number identification; a service that provides the receiver of a telephone call with the number of the calling phone.

Announcement Files The Announcement Files feature is an announcement repository that helps manage audio files from a common location that are used in various services, such as Auto Attendant announcements, Music on Hold, or Call Queue announcements.

annunciator A device that allows spoken messages or call process tones to be played during a call. They use the SCCP protocol for communication, but they can be used by either SIP or SCCP phones.

Anonymous call rejection A user configurable feature that allows users to reject all incoming calls from unidentified or blocked caller IDs.

aperture The diameter of the hole through which light enters a camera. The size of the aperture controls the amount of light entering your lens to the camera sensors.

API Application programming interface; a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service.

APN Apple Push Notifications is a platform notification service created by and used exclusively for Apple smart devices. APN allows third-party applications to send push notifications to Apple devices.

application users Users who are associated with Cisco Unified Communications features or applications, such as Cisco Unified Contact Center Express or Cisco Unified CM Assistant. These applications must authenticate with Cisco Unified Communications Manager, but these internal "users" do not have an interactive login and serve purely for internal communications between applications.

A-record A mapping record used by Domain Name Servers to map a URI address to an IP address. A-records consist of a host name and domain name, which make up the URI, and an IP address.

ARP Address Resolution Protocol; the protocol used to map IP network addresses to the hardware MAC addresses used by a data link protocol.

ASR Aggregation Services Router; a type of router used in edge routing for high-bandwidth applications in large enterprise businesses.

assent A protocol that requires two components: a traversal server and a traversal client. The traversal server resides outside the firewall or in a 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. Only two ports are required to be opened on the firewall because Assent will multiplex the media so all RTP traffic uses one port and all RTCP traffic uses a second port. In addition to the firewall traversal capabilities of Assent, NAT traversal is built into the protocol as well. Also, Assent can be used with both the SIP and H.323 communication standards.

asymmetric cryptography The same process as symmetric cryptography, except that the identity of the communicating parties can be authenticated using public-key cryptography.

Auto Attendant A feature that ensures calls are answered and that callers' needs are met. You can add greetings, set up menus, and route calls to an answering service, a hunt group, a voicemail box, or a real person. You can create a 24-hour schedule or provide different options when your business is open or closed.

autoframing An AI technology built into some of the Cisco Telepresence endpoints that allows individual zoomed-in video switching between participants who are speaking within a video meeting room. Autoframing technology can follow participants in a room using speech detection and facial recognition.

auto-registration A setting in the CUCM that uses a generic template to automatically register all devices that communicate with the TFTP service on the CUCM.

AXL Administrative XML Web Service; an XML/SOAP-based interface that provides a mechanism for inserting, retrieving, updating, and removing data from the Unified Communications configuration database. Developers can use AXL and the provided WSDL to create, read, update, and delete objects such as gateways, users, devices, route patterns, and much more.

B

B2B Shorthand for "business-to-business." This term refers to sales your business makes to other businesses rather than to individual consumers.

B2BUA Back-to-back user agent; a logical network element in SIP applications. It is a type of SIP UA that receives a SIP request, then reformulates the request, and sends it out as a new request.

B2C Shorthand for “business-to-consumer.” This term refers to sales your business makes to individual consumers rather than to other businesses.

backup device A compilation of settings used to discover the database to which the backup information will be saved.

backup status A table that displays the status of a backup as each component is being backed up.

balanced audio cable A cable that is characterized by three wires, two of which carry the identical signal 180 degrees out of phase with each other. The third is the ground that encompasses the other two wires to protect them from outside noise. This allows for better isolation of the signal from EMI noise.

bandwidth The rate that data bits can successfully travel across a communication path.

Base64-Encoded Format An encoding method for certificates that converts binary to plain ASCII text.

BAT Bulk Administration Tool; a feature of the CUCM that allows administrators to push bulk settings to many phones by using a CSV file.

Bayer A filter within a camera that lets about one-third of each color in and maps the saturation levels of each color per pixel in a mosaic type of effect.

BFCP Binary Floor Control Protocol; the IETF standard for content sharing over SIP.

bidirectional mic A directional mic that picks up equally in two directions, usually 180 degrees opposed.

bit depth The size of a packet sample, which is measured in bits per sample.

BOT Cisco Dual Mode for Android is the option to select to create a device BOT for Webex App on Android phones.

BPS Bulk Provision Service; a service that administers and maintains all jobs that are submitted through the Bulk Administration menu of the Cisco Unified Communications Manager Administration.

Branch Gateway The oldest Cisco router type that can operate as a Local Gateway for a Webex Calling deployment. Branch Gateways include the ISR1100 and the ISR4000 series routers.

BRI Basic Rate Interface; an ISDN configuration intended primarily for use in subscriber lines similar to those that have long been used for voice-grade telephony services. This allows BRI connections to use existing telephony infrastructure at businesses. BRI ISDN contains two Bearer channels, or B-channels, and one Delta channel, or D-channel. BRI Bearer channels support 64 kbps bandwidth and are used to carry audio data. The BRI Delta channel supports 16 Kbps and is used to send all the control signaling, such as call setup messaging, call teardown messaging, and timing for TMD.

BRI NT port An NT port found on the BRI Network Termination box. An NT port always connects to a TE port and vice versa.

BRI TE port A TE port found on BRI ISDN Terminals, such as ISDN phones or PBX trunk ports. A TE port always connects to an NT port and vice versa.

C

C8000v The Catalyst 8000v is a continuation of the CSR1000v. The C8000v is a software-based virtual router that combines the functionalities of Cisco Cloud Services Router (Cisco CSR1000V) and Cisco Integrated Services Virtual Router (Cisco ISRv) into a single image that is intended for deployment in cloud and virtual data centers. It is supported in ESXi, KVM, and NFVIS hypervisors. Further, you can deploy this router on public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba Cloud.

CA Certificate authority; the certificate server that issues and verifies the authenticity of certificates.

CAC Call Admission Control; a feature on the CUCM that allows the systems in place to control various aspects of voice and video calls over IP, such as bandwidth consumption and QoS across an enterprise network.

Call Forwarding A user-configurable feature that allows you to forward calls to another number when you are away from your main line.

call handler A messaging system that allows calls to be routed to specific destinations based on the caller's input.

Call Notify A user configurable feature that allows you to receive an email notification when a call or voicemail is received.

Call on Webex Call on Webex is simply the ability for users to call using SIP over IP. This can be achieved through the Webex App, unified IP phones or Webex endpoints without a Webex Calling subscription.

Call Park Direct Allows users to park a call against a specific user's extension or Call Park Extension.

Call Park Group A feature that allows a defined group of users known as "members" to automatically park calls against available park destinations configured in a call park group. Park destinations can be either members' extensions or Call Park Extensions.

call pickup Users that are added to a call pickup can answer calls when another member of the call pickup is busy.

Call Queue An answering service for customers' calls that can't be answered. The Call Queue will provide them with an automated answer, comfort messages, and music on hold until someone can answer their call.

call queuing A feature that allows hunt pilot callers to be held in a queue while they wait for an agent to become available. Call queuing is based on the existing call distribution capabilities that are provided by hunt lists and hunt pilots. It enables calls to a hunt pilot to be redirected to a queue if all agents that are associated with the hunt pilot are busy, logged out, unregistered, or do not answer.

call routing A method the CUC employs to handle calls from users in the system, as well as undefined callers from outside the organization.

Call Setup mode An H.323 setting configured on an endpoint that can be set to either Direct or Gatekeeper. If Call Setup mode is set to Direct, the endpoint will never attempt to register to a gatekeeper and will only be able to dial by IP address. When Gatekeeper mode is used, the endpoint is completely subservient to a gatekeeper and will perform no function until it has registered.

Call Waiting A user-configurable feature that allows you to place an ongoing call on hold to answer a new, incoming call at your discretion. Should you choose to disregard the incoming call, it will be transferred to your voicemail or another predetermined destination.

CAMA Centralized Automated Message Accounting; a system developed so that billing data can be recorded at a centralized crossbar tandem office for message unit and toll calls originated by telephone customers served by a large number of local dial central offices.

CAPF Certificate Authority Proxy Function; a level of security that performs several tasks depending on your configuration. It can be used to authenticate via an existing manufacturing installed certificate (MIC), locally significant certificate (LSC), randomly generated authentication string, or optional less secure "null" authentication. It issues locally significant certificates to supported Cisco Unified IP phones. It upgrades existing locally significant certificates on the phones. CAPF also retrieves phone certificates for viewing and troubleshooting.

CAPWAP Control and Provisioning of Wireless Access Points; a protocol that enables an access controller to manage a collection of wireless termination points.

CAR Committed access rate; a service that limits the input or output transmission rate on an interface or subinterface based on a flexible set of criteria. Another tool is known as DCAR, or Distributed CAR.

CAR Tool CDR Analysis and Reporting Tool; a tool that uses CDR and CMR data to provide system-generated reports to users, managers, and administrators. These reports can help monitor QoS issues, device utilization, or call statistics.

cardioid mic A directional mic with a pickup pattern shaped like a heart. The mic's effective pickup area is primarily focused on the area in front and to the sides of the microphone.

CAS Channel Associated Signaling; a form of signaling that is part of the PRI T1 format for ISDN communications.

CAST Cisco Audio Session Tunnel; a proprietary protocol used to split the audio and video media streams between Cisco Jabber and a VoIP phone when using CTI for desk phone control from Jabber.

Catalyst 8000 Edge Platforms These routers are the replacement solutions for the Branch Gateways and will support the Local Gateway function. These cloud edge platforms are designed for accelerated services, multilayer security, cloud-native agility, and edge intelligence to accelerate the customer journey to cloud.

CBWFQ Class-Based Weighted Fair Queuing; an algorithm that provides class bandwidth guarantees for user-defined traffic classes. It provides flow-based WFQ support for non-user-defined traffic classes.

CCD Charged-couples device; an image sensor that detects variable attenuation of light waves and converts them into electrical current.

CCMCIP Cisco CallManager Cisco IP Phone service; Cisco Jabber requires you to configure a Cisco Unified Communications Manager IP Phone service profile on Cisco Unified Communications Manager to retrieve settings and information about devices that are associated for each user.

CCP Cloud Connected PSTN is one of three options an administrator can choose in Webex Control Hub to leverage for PSTN connections when setting up Webex Calling. Choose this option if you're looking for a cloud solution that doesn't require deployment of local hardware, and then select a CCP provider of choice.

CCUC Cloud Connected Unified Communications is a set of services in the Webex cloud that provides enhanced business and operational insights with the aim of improving administrative workflow productivity. It allows customers to leverage the benefits of the Webex cloud while keeping your critical calling workload on-premises.

CDP Cisco Discovery Protocol; a proprietary protocol used at Layer 2 of the network for device and information discovery across a network.

CDR Call detail records; data records that contain information about each call that was processed by CallManager.

CDR Agent service A service that transfers CDR and CMR files that CUCM generates from the local host to the CDR Repository node, where the CDR Repository Manager service runs over an SFTP connection.

CDR Repository Manager service A service that maintains the CDR and CMR files, allocates the amount of disk space for use by CMRs and CDRs, sends the files to up to three configured destinations, and tracks the delivery result for each destination.

CDR Repository node CUCM node where CDR and CMR files are stored.

CE Collaboration Endpoint; software that comes preloaded onto DX, MX, SX, and WebEx endpoints. This software is based on the legacy TC software.

CEC Consumer Electronics Control; a feature used to set the screen in standby when an endpoint itself enters standby. Likewise, the system will wake up the screen when the system itself wakes up from standby.

cell boundary overlap The primary mechanism for providing RF high availability. In general, a cell boundary overlap of 20 to 30 percent on nonadjacent channels is recommended to provide high availability in the wireless network.

CER Cisco Emergency Responder; a database server that enhances the existing emergency 9-1-1 functionality of the Cisco Unified Communications Manager by ensuring it will send emergency calls to the appropriate Public Safety Answering Point (PSAP) for the caller's location and that the PSAP can identify the caller's location and return the call if necessary.

Certificate-based Local Gateway The certificate-based method of connecting a Local Gateway uses Mutual TLS as the connection type. This method also uses four bidirectional connections rather than a single one-way connection as with the registration-based connection. This connection type requires CA-signed certificates in the Local Gateway. The engineer also needs to add the Webex Calling trust bundle into the Local Gateway so that the SBC trusts the certificates of Webex Calling.

chrominance A measurement of the color spectrum in light.

CIF Common intermediate format; a video format designed by the ITU as a compromise between NTSC and PAL resolutions for digital video transmission, particularly regarding video communication.

Cisco Precision Video Engine Technology embedded into the Cisco Jabber soft client that uses specialized compression algorithms to offer higher-quality video over lower bandwidth. This technology is what makes HD call capability possible in the Jabber client.

Cisco PSTN One of three options an administrator can choose in Webex Control Hub to leverage for PSTN connections when setting up Webex Calling. Choose this option if you'd like a bundled solution that allows you to order new PSTN numbers and port existing numbers to Cisco.

Cisco UBE Cisco Unified Border Element is a Unified Communications border element, or edge service, providing voice and video connectivity between the enterprise IP network and a service provider network. The service provide will make the conversion from IP to ISDN, and vice versa.

Cisco UBE HA Cisco Unified Border Element High Availability uses Layer 2 box-to-box redundancy through the Redundancy Group Infrastructure Protocol to offer failover between two Cisco UBE routers using an active/standby pair.

Cisco Unified Serviceability A service and reporting tool available on the Cisco Unified Communications Manager, Cisco Unified IM and Presence server, and Cisco Unity Connection.

Cisco Unity Connection Serviceability A reporting tool available only through the Cisco Unity Connection server that allows for 20 different reports to be generated.

Cisco Webex Calling A service in Webex that allows users to call out across the PSTN using the Webex App or a unified IP phone.

Claim Domain This option allows an administrator to claim a domain to automatically associate any users within that domain to the organization. If the domain isn't claimed, users who sign up for a Webex account will need to be claimed manually by an administrator.

Claim Users Claiming users is a process performed by administrators within the Webex Control Hub. This option allows users who already signed up for a free Webex account to be claimed and moved into a subscription account.

classification pulse A "first detection" pulse sent from a PSE to a device to determine whether the device is powered or not.

CleanAir A Cisco technology used to increase the WLAN reliability by detecting radio frequency interference in real time and providing a self-healing and self-optimizing wireless network.

ClearPath technology Special algorithms applied at the codec to incoming video that clarifies the video quality by adding pixels to the image. There is no extra bandwidth cost to using ClearPath technology, but the image quality is greatly improved.

CLI Command-line interface; a text-based command structure that allows an administrator to interact with a system. CLI can be used over an IP connection or through a console connection.

clipping A form of distortion that occurs when a signal exceeds the maximum dynamic range of an audio channel.

Cloud Connected UC Cloud Connected Unified Communications is a service Cisco developed in the Webex Control Hub to support hybrid integrations between an on-premises UC solution and Webex in the cloud. Cloud Connected UC also supports full migration from the premises to the cloud.

cluster-level backup A backup of all servers in a cluster collected in a central location and archived to a physical storage device.

cluster group Connected UC on-premises servers are organized in Control Hub using cluster groups. Cluster groups can represent geolocations, release environments, and so on.

CMA Cisco Meeting Application; a softphone application based on the WebRTC protocol that works with Cisco Meeting Server.

CMC Client Matter Codes; a feature that forces the user to enter a code to specify that a call relates to a specific client matter. You can assign client matter codes to customers, students, or other populations for call accounting and billing purposes.

CME Communications Manager Express; a Cisco Unified application that provides call processing to Cisco Unified IP phones for distributed enterprise branch-office environments. Cisco Unified CME delivers on this need by providing localized call control, mobility, and conferencing alongside data applications on Cisco ISRs.

CMOS Complementary metal-oxide-semiconductor; an image sensor that detects variable attenuation of light waves and converts them into electrical current.

CMR Call management records; data records that contain quality of service or diagnostic information about the call. Also referred to as *diagnostic records*.

CMS Cisco Meeting Server; an on-premises conferencing server used for rich media multipoint conferencing between three or more participants.

CN Common Name; a subcategory in an LDAP hierarchical tree used to categorize users or devices within an organization.

COBRAS Consolidated Object Backup and Restore Application Suite; a tool used to migrate the legacy Cisco Unity server settings into the Cisco Unity Connection server platform.

codec A conjunction of the words *coding* and *decoding*; the hardware or software that codes and decodes audio and video data. Codec also refers to the standards that outline how the coding and decoding operates.

codec preference list A list that allows the router to act as a demarcation point on a VoIP network and allows a dial peer to be established only if the desired codec criteria are satisfied. Preferences can be used to determine which codecs will be selected over others.

coherent late reflections Sound wave reflections from surfaces that stand out from normal reverberation levels; they are the ones we typically identify as echoes. In this case, the arrival of the late reflection sound waves passes a certain millisecond tolerance and is perceived as a second sound rather than the prolonging of the first sound.

Common Identity A term used to describe a state that must exist before certain Webex cloud services can be utilized. When a user exists in Webex Control Hub and Cisco Unified Communications Manager, the user's email address must match in both locations to create a "Common Identity."

compliance A function of Cisco IMP that allows the storing of instant messages on an external server or database for archiving.

component video A video signal split into two or more component channels.

composite video Video information combined into a single line level.

compression One of the link efficiency mechanisms that work in conjunction with queuing and traffic shaping to manage existing bandwidth more efficiently and predictably. There are two types of compression available. See also *stacker* and *cRTP*.

condenser mic A type of mic that operates on electrostatic principles in which two conductive plates in close proximity to each other exchange a charge as the plates vibrate. This operation requires that an external power source be used to supply the charging voltage to element, usually in the form of phantom power.

conferencing Mixing multiple streams (three or more) to create one output stream.

congestion avoidance An effect achieved through packet dropping. Congestion avoidance mechanisms monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks.

congestion management The use of markings on a packet to determine in which queue to place it. Different queues are given different treatment by the queueing algorithm that is based on the class of packets in the queue. Generally, queues with high-priority packets receive preferential treatment.

corporate directory A phonebook that an endpoint subscribes to when an entry needs to be looked up. These directories do not live on the endpoint itself; rather, they exist solely on the system designed to deliver the aliases when requested.

CoS Class of service; a Layer 2 QoS mechanism that operates on the 802.1q VLAN. CoS is used to mark packets at the Layer 2 switch port and create trust boundaries so that phones and other trusted devices can mark their own QoS packets.

CoS (on CUC) Class of service; in this context, the term describes which features the Cisco Unity Connection users have permission to use.

COS Cost of service; a mechanism in the CUCM that is used to control telephony charges by blocking costly service numbers and international calls for some users. COS is also used to protect the privacy of some users, such as to disallow direct calls to managers except through their assistants.

CQ Custom queuing; a function that guarantees some level of service to all traffic because you can allocate bandwidth to all classes of traffic. You can define the size of a queue by determining its configured packet-count capacity, thereby controlling bandwidth access.

critical distance The distance between a person who is speaking and a microphone as it relates to other active mics. A good rule of thumb is a 1:3 ratio. If the person speaking is 3 feet from the target mic, the next closest mic should be no closer than 9 feet.

CRT Cathode Ray Tube; the old analog style of monitor, which is no longer in use.

cRTP Compressed RTP; a link efficiency compression algorithm that can compress the IP, UDP, and RTP headers down from 40 bytes to 2–4 bytes.

CSF Cisco Unified Client Services Framework is the option to select to create a CSF device for Webex App for Mac or Webex App for Windows.

CSR Certificate signing request; a template used to submit information to a CA so that a certificate can be signed.

CSR1000v The Cloud Services Router 1000v is a virtual IOS-XE router that can run in VMware ESXi, Citrix XenServer, Microsoft Hyper-V, SuSE KVM, and Red Hat KVM virtual environments. The CSR1000v can also be deployed in Microsoft Azure, Amazon EC2, and Google Cloud Platform. The CSR1000v can support up to IOS-XE version 17.3 software. After that version, the branding and licensing was changed to reflect the new product name, Catalyst 8000v.

CSS Calling search spaces; a classification that defines which partitions are accessible to a particular device within the CUCM.

CSV Comma-separated values; a simple file format used to store tabular data, such as a spreadsheet or database. Files in the CSV format can be imported to and exported from programs that store data in tables, such as Microsoft Excel or OpenOffice Calc.

CTI Computer Telephony Integration; a technology that enables computer and telephone systems to interact together.

CTI port A virtual port that is analogous to a trunk line in a traditional ACD or PBX setting.

CTI route point A virtual device that can receive multiple simultaneous calls for the purpose of application-controlled redirection.

CTIQBE Computer Telephony Interface Quick Buffer Encoding; a protocol used by TAPI and other Cisco services to communicate with the CUCM.

CTL Certificate trust list; a certificate file sent from a CUCM to an endpoint to establish a trust between that device and the CUCM for secure communication. The CTL file contains a server certificate, public key, serial number, signature, issuer name, subject name, server function, DNS name, and IP address for each server.

CUC Cisco Unity Connections; a unified messaging and voicemail solution within Cisco's Collaboration suite of products.

CUCL Cisco User Connect Licensing; per-user based licensing for individual Cisco Unified Communications applications, including the applications server software, user licensing, and a soft client. User Connect Licensing is available in Essential, Basic, Enhanced, and Enhanced Plus versions.

CUCM Cisco Unified Communications Manager; a platform that provides reliable, secure, scalable, and manageable call control and session management.

CUCSF Cisco Unified Client Services Framework; the framework used to support the Cisco Jabber soft client application.

CUE Cisco Unity Express; a tool that offers industry-leading integrated messaging, voicemail, fax, automated attendant, interactive voice response, time-card management, and a rich set of other messaging features on the Cisco Integrated Services Router platform.

current logging A list of current available logs on a CE software-based endpoint since the last reboot of the endpoint.

CUWL Cisco Unified Workspace Licensing; a communications and video solution that provides the most popular Cisco Collaboration applications and services in a cost-effective, simple package. Two Cisco Unified Workspace Licensing offers are available, depending on your needs: Professional Edition and Standard Edition. Professional Edition includes comprehensive, unlimited participant video conferencing with Personal Multiparty video at no additional cost.

D

data compression A reduction in the amount of bandwidth consumed from the total transmission capacity. Compression involves utilizing encoding algorithms to reduce the size of digital data.

data VLAN A VLAN partition used for grouping common data usage, such as emails and web searching.

DC Domain controller; the main domain under which all categories in an LDAP hierarchical tree reside for an organization.

DECT Digital Enhanced Cordless Telecommunications. Cisco DECT phone systems are cordless phones that can all operate out of a single base station within their range of communication.

depth of field A camera effect that refers to the objects, from nearest to farthest, that are in sharp focus of a camera's lens. The size of the depth of field is a function of focal length and Iris. On cameras equipped with an iris, the depth of field can be extended by decreasing the aperture.

DER encoded format Distinguished Encoding Rules encoded format; a binary format used with certificates.

Desk Phone mode A mode in which the Cisco Jabber client controls the Cisco IP phone of the user. For an IP phone without a camera, the video input and output are processed on the Cisco Jabber client platform but the voice input and output are processed on the IP phone. This split media is performed using CAST.

DHCP Dynamic Host Configuration Protocol; an open-source protocol used by network devices to automatically discover network addressing information so that communication across the network is possible. The DHCP process is a four-step process that involves discovery, offer, request, and acknowledgment.

DI Deployment Insights uses telemetry modules through microservices to collect user and device information from the Cisco Unified Communications Manager. Because DI is capable of collecting user information, you must agree to the terms of service before saving these changes.

dial peer A concept that Cisco IOS XE routers use to route calls. Every call that traverses through the router has to match an inbound dial peer and an outbound dial peer.

dial plan A carefully planned design for reaching devices and services in a Collaboration network and in the PSTN.

DID Direct inward dialing; a service that maps PSTN E.164 numbers directly to an IP phone behind a PBX.

Diffie-Hellman Key Exchange A method of securely exchanging cryptographic keys over a public channel; it was one of the first public-key protocols.

DiffServ A QoS network design model that operates on classes that require special QoS treatment.

diffusion The process of dispersing radiated energy so that it is less direct or coherent. It is caused by sound waves reflecting off many complex surfaces.

digital signal A continuous quantity of samples that is a representation of a sequence of discrete values that can take on only one of a finite number of values.

digit-by-digit analysis A method of addressing used exclusively by SCCP phones. When the phone goes "off hook," a message is sent to the Cisco Unified Communications Manager. The CUCM will analyze every keypress or action of the SCCP phone until a successful match is found.

direct sound The first and primary sound waves that hit your ears.

directional mic A microphone with a polar pickup pattern intended for pointing at a more selective group of audio sources.

directory A centralized enterprise-wide datastore used for the storage of information about individuals within an enterprise.

Directory Connector An essential tool for synchronizing your on-premises AD with the backend Webex cloud directory that allows your users to use cloud services such as Webex Meetings and Webex App services.

directory schema A plan that defines the type of information stored, its container (or attribute), and its relationship to users and resources.

Directory URI A unique Uniform Resource Identifier on the CUCM, similar in nature to a standard URI, that takes the form of User@domain or User@IP. The Domain part of the Directory URI is also referred to as the Host part of the URI.

DirSync A service on the CUCM that is used to enable the Directory Synchronization function.

Discovery mode A mode in which an endpoint will locate the gatekeeper to which it will attempt to register. Discovery mode can be configured to either Automatic or Manual.

distance factor The ability of a microphone to pick up sound from a distance as related to two different types of microphones, such as a handheld microphone and an omnidirectional mic.

distribution list (CUC) A list in CUC that is used to send voice messages to multiple users. The users who are members of a system distribution list are typically those who need the same information on a regular basis, such as employees in a department or members of a team.

DMVPN Dynamic Multipoint Virtual Private Network; a solution that provides an alternative to the complicated administrative setup and maintenance that comes with establishing a mesh network. Initially, the DMVPN is set up as a hub-and-spoke network. After communication is established between the spokes and the hub, each spoke will dynamically discover each of the other spokes and establish a tunnel between one another.

DMZ Demilitarized zone; a perimeter network or screened subnet security solution. It is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet.

DN Directory number; a unique number assigned to a phone from the CUCM that can be used to call into that phone. DNs are similar in nature to an E.164 address.

DNA Dialed Number Analyzer; a tool on the CUCM that allows the administrator to analyze call flows through the CUCM by simulating call attempts.

DND Do Not Disturb is a user-configurable feature that prevents incoming calls and messages from alerting you when you need to concentrate.

DNIS Dialed Number Identification Service; a service offered to companies by PSTN carriers that identifies the originally dialed telephone number of an inbound call. Companies may use this information for call routing to internal destinations or activation of special call handling.

DNS Domain Name System; a type of service that allows URL addresses to be used in place of IP addresses. DNS will resolve the URLs to their IP address mapping.

dp Density-independent pixels is a unit of length for screen size, typically used in mobile software to scale an app display to different screen sizes.

DPC Desk Phone Control is a Cisco proprietary protocol that allows a soft client, such as Cisco Jabber or Webex App, to control a desk phone. Calls can be initiated or answered on the phone through the soft client application. DCP uses CTI to take control of the phone.

DS0 A signal introduced to carry a single digitized voice call. For a typical phone call, the audio sound is digitized at an 8 kHz sample rate using 8-bit pulse-code modulation for each of the 8000 samples per second. This results in a data rate of 64 kbps.

DS1 A signal in which 24 DS0s are multiplexed. To limit the number of wires required between two destinations that need to host multiple calls simultaneously, a system was built in which multiple DS0s are multiplexed together on higher-capacity circuits.

DS3 A signal in which 28 DS1s are multiplexed. To limit the number of wires required between two destinations that need to host multiple calls simultaneously, a system was built in which multiple DS0s are multiplexed together on higher-capacity circuits.

DSCP Differentiated services code point; a Layer 3 QoS classification for marking packets.

DSP Digital signal processor; a card used in Cisco routers to provide software- and hardware-based media resources.

DTMF Dual-tone Multifrequency signaling; an in-band communications system that has been used for many years by telephone companies, which allows end users to communicate by pressing keys on their phone.

DuoVideo A Tandberg proprietary protocol for content sharing.

DV certificate Domain validation certificate; a type of certificate in which the CA only checks the right of the applicant to use a specific domain name. No company identity information is vetted, and no information is displayed other than encryption information within the Secure Site Seal.

DX Desktop Experience; a branding type for Cisco Telepresence endpoints that offers a personal Telepresence desktop endpoint for customers.

dynamic range A range of amplitudes that can be accurately captured by the microphone. This is usually represented in decibels at a certain frequency, typically 1 kHz.

E

E&M Receive and Transmit, also referred to as Ear and Mouth; ports for an analog trunk connection to a legacy PBX system.

E.164 Alias Numeric-only values containing 1–15 digits that are assigned to an endpoint. They work in the same manner as any phone number would in a typical telephony environment.

early reflections Sound waves that bounce off but arrive at your ears at almost precisely the same time as the direct sound coming from the sound source.

EIGRP Enhanced Interior Gateway Routing Protocol; an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers.

electronic filters Filters used to help remove unwanted frequency, or noise, from an analog signal.

EMR Electromagnetic radiation; different spectrums of light.

en bloc A type of dialing in which the whole dialed string is sent in a single SIP INVITE message.

end users Users who are associated with a physical person and an interactive login. This category includes all IP telephony users as well as Cisco Unified Communications Manager administrators when using the user groups and roles configurations.

endpoint An audio-only or audio- and video-capable device used for communication.

Enterprise firmware The software that must be installed on a Cisco Unified IP Phone before it can register to the Cisco Unified Communications Manager.

enterprise parameters Factors used to define cluster-wide system settings; these parameters apply to all devices and services across all nodes within the entire cluster.

Enterprise software Software used on Cisco phones that need to register to the Cisco Unified Communications Manager.

Euroblock European-style terminal block; a low-voltage connector and terminal block combination commonly used for microphone- and line-level audio signals and for control signals such as RS-232. It is also known as the Phoenix connector from one of the manufacturers, though many manufacturers make compatible products. The Euroblock is a solderless connector that uses screw terminals to clamp connecting wires. After the wires are installed, the entire assembly is plugged into a matching socket in the electronic device. Euroblocks are more convenient than the terminal strips they replace because the signal cables can be quickly disconnected from or connected to the electronic device so that you don't have to unscrew and re-screw each wire individually.

EV certificates Extended validation certificates; certificates that the certificate authority uses to check the right of an applicant to use a specific domain name; in addition, it conducts a thorough vetting of the organization.

eventlog A folder, also included in the current folder, that contains a directory of log files that offer more verbose information.

Extended Logging A setting on CE software-based endpoints that sets a higher level of debug on the system in order to capture deeper log traces from endpoint activity. There are three levels to extended logging. Start Extended Logging enables debugs, including SIP Tracing, and lasts for 10 minutes. Include Limited Packet Capture enables the same as above, plus a packet capture of the signaling during call setup and teardown but no media, and will last for 10 minutes. Include Full Packet Capture includes all the above plus media packet capture but lasts for only 3 minutes.

F

FAC Feature Access Code is a code users can enter on a phone to trigger features such as call park. The call park direct FAC is *68 and must be entered followed by the extension the call will be parked for the caller to be placed on hold. The call park group FAC is #58. Use *88 plus the extension of the parked call to retrieve a call using either method.

FCM Firebase Cloud Messaging is a cross-platform messaging solution. This solution allows you to notify the client app when new data is available to sync. FCM is generally used with Android devices.

FECC Far-end camera control; the ability of an endpoint's camera to be controlled using PTZ from a far-end endpoint while in a call.

field of view The width and height of an image captured by a camera.

FIFO First-in, first-out; a method that performs no prioritization of data packets on user data traffic. It entails no concept of priority or classes of traffic. When FIFO is used, ill-behaved sources can consume available bandwidth, bursty sources can cause delays in time-sensitive or important traffic, and important traffic may be dropped because less important traffic fills the queue.

firewall A system that exists to protect the inside of a corporate network from outside attack. The purpose of a firewall is to control IP traffic entering your network. Firewalls generally block unsolicited incoming requests, meaning that any communication originating from outside your network will be prevented. However, firewalls can be configured to allow outgoing requests to certain trusted destinations, and to allow responses from those destinations. Allowing traffic in both directions prevents the firewall from doing its job.

Flex Cisco Collaboration Flex Plan; a subscription-based offer that entitles people to use Cisco's industry-leading collaboration tools. It helps with transitions to the cloud and investment protection by including cloud, premises, hosted and hybrid deployments, with the flexibility to use them all.

Foveon X3 sensors Sensors that use a method similar to how color film for photography works. An array of layered pixel sensors separates light via the inherent wavelength-dependent absorption property of silicon, such that every location senses all three color channels.

FQDN Fully qualified domain name; a domain that has been qualified against an authority, such as the Cisco Expressway or a publicly registered DNS address.

frame A still image. Each still image in a series, known as a reel, is a separate frame.

frame rate The number of frames that are shown per second, or fps.

frequency The rate of air pressure fluctuation produced by an acoustic energy wave.

frequency response The range of frequencies accurately captured.

frequency spectrum The complete range of frequencies audible to the ear.

FRTS Frame Relay Traffic Shaping; a QoS shaping tool used on output interfaces to help smooth out mismatches in the network and limit transmission rates.

FTP File Transfer Protocol; a protocol used to transfer large files between a server and a client. A secure transmission can also be established using SFTP.

FXO Foreign eXchange Office; an interface that receives POTS service, typically from a central office of the public switched telephone network.

FXS Foreign eXchange Subscriber; an interface that delivers POTS service from the local phone company and must be connected to subscriber equipment.

G

gain The ability of a system to adjust the power or amplitude of a signal between the input and the output of a given circuit. Gain can be in the form of amplification or attenuation in either a digital or analog process; no change in the signal as it passes through is called unity gain or simply unity.

gatekeeper A call control device used with H.323. Gatekeepers provide registration, security, and call control in an otherwise unsecure and uncontrolled environment.

gaze angle Based on the position of a camera to the display, an angle that allows a participant in a room to look a far-end participant in the eye, or at the display, and still maintain eye contact with the far-end participant on the display.

GLBP Gateway Load Balancing Protocol; a Cisco proprietary protocol that offers gateway redundancy. This protocol was designed to overcome the limitations with HSRP and VRRP. It protects data traffic from a failed router or circuit, while also allowing packet load sharing between a group of redundant routers.

global directory A phone book that originates on a server outside of the endpoint itself that is pushed out to the endpoint, so the directory entries live on the endpoint just as the local directory entries live on the endpoint.

good levels A modifier that identifies an audio signal that is significantly higher than the noise floor (good S/NR) but not so strong as to cause clipping and may also indicate leaving appropriate headroom.

group A prioritized list of one or more call-processing servers within Cisco Unified Communications Manager. Cisco Unified Communications Manager Groups are used to collect servers within a cluster that run the Cisco CallManager service in order to provide call-processing redundancy.

Group Call Management An advanced call queue capability that makes it easy and affordable to support high call volume and team call handling services as a core part of Webex Calling. It adds key features that provide supervisor capabilities, enhanced queue policies to determine call routing based on business hours, skill-based routing, callback capabilities for customers, and reports and analytics for administrators.

Group Call Pickup This feature enables a user to answer any ringing line within their pickup group. A pickup group is an administrator-defined set of users within a site to which the Call Pickup feature applies.

GRQ Gatekeeper Request; a RAS broadcast message initiated by an endpoint and used to locate a gatekeeper within the broadcast domain. The gatekeeper to respond will send a GCF, or Gatekeeper Confirm.

GTS Generic Traffic Shaping; a QoS shaping tool used on output interfaces to help smooth out mismatches in the network and limit transmission rates.

GUI Graphical user interface; in this context, a method of visually checking a voice mailbox through the Cisco Unity Connection server.

H

H.224 The standard for far-end camera control.

H.239 The H.320 and H.323 standard for content sharing.

H.245 The process used in H.323 for capability set exchange, master/slave negotiation, and opening logical channels, or ports. H.245 is also responsible for closing logical channels at the end of the call.

H.261 The minimum standard that must be used and was the first of the ITU video codecs. This codec will support QCIF and CIF formats; it uses 64 kbps to 2 Mbps of bandwidth to transmit and receive video. This standard is usually utilized only by legacy devices.

H.263 The standard that came out after H.261 and offers superior advantages. H.263 has better compression, especially in the lower bitrate range, and uses basically the same bandwidth. H.263 also offers support for SQCIF 4CIF and 16CIF at a little less than 30 fps, hence a crisper image.

H.264 The standard sometimes called MPEG-4; it came out at a time when HD communication was being more readily used. This standard was created by the ITU in cooperation with the International Organization for Standardization (ISO) and the International Electrotechnical Commission. It currently is most often used for high-definition video. It is based off MPEG-4 and delivers video that is at the same quality as H.263. The reason it is so favored currently is its capability to deliver video at half the bandwidth usage as H.263.

H.265 HEVC A high-efficiency video codec; it is a draft compression standard ratified in 2013. It's a logical successor to H.264 AVC, aimed at reducing bitrate significantly due to the complexity of mathematical calculations; and it leverages new compression and prediction techniques.

H.320 An ITU umbrella standard that encompasses many other standards for circuit-switched communication.

H.323 An ITU umbrella standard for packet-switched communication.

H.323 ID An alias that can use any combination of numbers, letters, and/or special characters, but spaces are not allowed. Because of this capability, an H.323 ID can be in the form of a URI. However, an H.323 ID is not a URI because it is not dependent on the domain being a fully qualified domain name.

H.460.17 An H.323 firewall and NAT traversal standard that performs firewall traversal by carrying the media over TCP ports instead of UDP.

H.460.18 An H.323 firewall and NAT traversal standard that works just like Assent, except it requires demultiplexed ports 50000 to 52400 to be opened on the firewall.

H.460.19 An H.323 firewall and NAT traversal standard that works as a layer on H.460.18 to allow multiplexing the media ports so that only two ports need to be opened for RTP and RTCP media streams.

HCS Hosted Collaboration Solution; a cloud offering for Cisco Collaboration through service providers.

HDMI High-Definition Multimedia Interface; an audio and video interface for transmitting uncompressed video data and compressed or uncompressed digital audio data from an HDMI-compliant source device to a compatible display. HDMI is a digital replacement for analog video standards.

HD-SDI High-Definition Serial Digital Interface; an interface that consists of a pair of SMPTE 292M links. It provides a nominal 2.970 Gbps interface used in applications that require greater fidelity and resolution than standard HDTV can provide.

headroom A safety zone for unintended peaks in a signal. It becomes particularly important when a signal may go through several opportunities for gain adjustment within a given system. Microphones, mixers, and amplifiers should be adjusted to always allow adequate headroom to avoid clipping.

historical log A compressed folder containing all the current logs on a CE software-based endpoint designed to send to a Cisco TAC agent over email or file share. Historical logs are created each time the endpoint is rebooted.

HSRP Hot Standby Router Protocol; a Cisco proprietary protocol that provides a fault-tolerant default gateway in the event the primary default gateway should fail.

HTTP Hypertext Transfer Protocol; the underlying protocol used by the World Wide Web. This protocol defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.

HTTPS Secure Hypertext Transfer Protocol; an extension of the Hypertext Transfer Protocol. It is used for secure communication over a computer network and is widely used on the Internet.

HTTPS Reverse Proxy Cisco MRA settings that provide a mechanism to support visual voicemail access, contact photo retrieval, Cisco Jabber custom tabs, and other data applications.

Hub_None A sample location that typically serves as a hub linking two or more locations. It is configured by default with the Unlimited intralocation bandwidth allocations for audio, video, and immersive bandwidth, but you can specify bandwidth allocations for each of these. By default, devices not assigned to other locations are assigned to Hub_None automatically.

hunt exhaustion A status in the CUCM that occurs after hunting has tried the last line-group member and there were no other line-group members or other line groups to be used.

hunt group Hunt groups route incoming calls to specific employees in a predetermined pattern. This is done by assigning a phone number to a group of employees and then setting rules that define how the call is answered, how long the call remains on hold, and who to forward the call to.

hunting The capability to route or reroute a call to a group of users within the CUCM so that calls are not just dropped when the originally intended target is not reached.

hypercardioid mic A directional mic that has a narrow focal range, so a larger lobe at the rear of the mic develops.

I

ICANN Internet Corporation for Assigned Names and Numbers; an organization that has been managing IP addresses and domains since 1998.

ICE Interactive Connectivity Establishment; a framework that pulls together a number of different techniques such as TURN and STUN; it provides a mechanism for SIP client NAT traversal. It allows clients residing behind NAT devices to discover paths through which they can pass media, verify peer-to-peer connectivity via each of these paths, and then select the optimum media connection path. The available paths typically depend on any inbound and outbound connection restrictions that have been configured on the NAT device.

IDD International Direct Dialing; a trunk prefix, also called an international call prefix or dial-out code, used to select an international telephone circuit for placing an international call.

Identity Management A system that involves the management of individuals and the authentication and authorization of these individuals.

IDS Informix Dynamics Server; an IBM-based database management system.

IEEE Institute of Electrical and Electronics Engineers; an association that controls communication using packet-switched technology.

IETF Internet Engineering Task Force; an open standards organization that develops Internet standards.

IM Instant messaging; a text-based communications tool that allows real-time text messages to be sent over the Internet.

IM forking A process by which an end user sends an instant message to a contact who is signed into multiple IM clients, and Cisco IMP Service delivers the instant message to each client. Cisco IMP Service continues to fork instant messages to each client until the contact replies. After the contact replies, Cisco IMP Service only delivers instant messages to the client on which the contact replied.

IMAP Internet Message Access Protocol; an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection. IMAP is defined by RFC 3501.

IME Intercompany Media Engine; a Cisco network management application that provides system health, events, and collaboration monitoring in addition to reporting and configuration for up to 10 sensors. IME monitors sensor health using customizable dashboards and provides security alerts through RSS feed integration from Cisco Security Center.

IMP IM and Presence; the Cisco Unified Communications Manager IM and Presence Service that provides native standards-based, dual-protocol, enterprise instant messaging, and network-based presence as part of Cisco Unified Communications.

IMS Identity Management System; an internal library inside the CUCM that is used to challenge both end user and application user authentication when services try to log in.

inductive loop An electromagnetic communication or detection system that uses a moving magnet or an alternating current to induce an electric current in a nearby wire. Induction loops are used for transmission and reception of communication signals, or for detection of metal objects in metal detectors or vehicle presence indicators.

Intelligent Proximity for Content Sharing A Cisco proprietary protocol, also referred to as simply Intelligent Proximity, that uses an ultrasonic audio tone, unheard by the human ear, that pairs the endpoint with the Intelligent Proximity application. This application can be installed on a smartphone, tablet, Mac computer, or Windows computer. Once paired, the application will use a Wi-Fi signal, which must be on the same network as the endpoint, to establish communication. Then the Intelligent Proximity app can be used to view and select participants to call from the directories on the endpoint, launch calls, answer incoming calls, and view content being shared during a call. You can scroll back and view previously shared information even when the presenter is sharing something different, and you can take snapshots of the content to peruse after the call ends. When using Intelligent Proximity from a Mac or Windows computer, you can also share content through the application.

Intelligent Proximity MV Intelligent Proximity for Mobile Voice; a service in some Cisco IP phones that brings the worlds of desk phone and mobile phone together. You can move the audio path over to the Cisco IP Phone 8851 during active mobile calls to take advantage of its superior audio acoustics. You also can share contact information from a mobile phone to the desk phone for ease of call placement. Intelligent Proximity MV uses Bluetooth technology for audio and contact sharing.

interlaced scanning A scanning process by which pixels are populated within a frame working from top to bottom, left to right. Odd lines and even lines are populated separately on alternating frames.

intersite routing A type of call-routing that occurs between multiple sites. A translation pattern is used for both centralized and distributed call-processing deployment models.

IntServ A QoS network design model that uses RSVP to guarantee predictable behavior on the network for applications that have specific bandwidth and delay requirements.

IOS XE Internetworking Operating System XE; a combination of a Linux kernel and a monolithic application that runs on top of this kernel. IOS is a monolithic operating system that runs directly on the hardware itself.

IP VMS IP Voice Media Streaming Service; a Cisco Unified Communications Manager service that provides software-based media resources.

IPP IP Precedence; a Layer 3 QoS classification for marking packets.

IPsec V3PN IP Security Virtual Private Network; a network that integrates three core Cisco technologies: IP Telephony, QoS, and IPsec VPN. The result is an end-to-end VPN service that can guarantee the delivery of latency-sensitive voice and video communications.

ISDN Integrated Services Digital Network; a network that is similar to POTS, but the original analog signal is converted to digital format before it is sent across a wire. That digital signal must be converted back to analog at the receiving phone. ISDN uses time-division multiplexing to send the digital signals across the copper wire.

ISR Integrated Services Router; a Layer 3 Cisco router that provides many other services than a typical Layer 3 router.

ITL Identity Trust List; a certificate of authentication that allows the phone to verify that the configuration file came from a trusted source. ITLs by themselves use asymmetric cryptography to authenticate the identity of the server.

ITU International Telecommunication Union; a specialized agency of the United Nations that is responsible for standardizing communication technologies.

ITU BT.709 A standard that defines the color space, resolutions, and frame rates of widescreen high-definition television using the 16:9 aspect ratio.

ITU-R BT.601 A standard that defines the color space, resolutions, and frame rates for encoding interlaced analog video signals into digital video form. A signal that conforms to the BT.601 standard can be regarded as if it is a digitally encoded analog component video signal.

IVR Interactive Voice Response; an auto attendant of sorts that allows a caller to enter the destination alias of the intended target after an initial number has been dialed.

IX Immersive Experience; a branding type for Cisco Telepresence endpoints that offers an in-room immersive endpoint for premium quality collaboration. This is the only Cisco Telepresence endpoint that does not run the CE software. Rather, it runs an older version of CTS software.

J

Jabber A soft client tool that includes the most commonly used Cisco UC tools in a single software package.

Java MIDlets Applications on Cisco IP phones that allow more sophisticated application capabilities such as animated graphics, custom user interface objects, advanced network connectivity, and persistent local storage.

jitter A delay that is similar to latency; however, jitter is a variable of the latency that occurs over a period of time.

JSON JavaScript Object Notation; a lightweight data-interchange format or text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and many others. These properties make JSON an ideal data-interchange language.

K–L

KEM Key Expansion Module; a side card that attaches to supported phones and increases the number of lines supported on that phone.

KPML Key Press Markup Language; an XML notation that allows digits to be sent one by one, similar to digit-by-digit analysis. Unlike NTE, which is an in-band method of sending DTMF, KPML uses the signaling channel (out-of-band, or OOB) to send SIP messages containing the DTMF digits. KPML procedures use a SIP SUBSCRIBE message to register for DTMF digits. The digits themselves are delivered in NOTIFY messages containing an XML-encoded body.

LAN Local area network; a network within a single confined area.

latency The delay packets experience when traversing across many different network devices.

LCD Liquid crystal display.

LDAP Lightweight Directory Access Protocol; a search protocol used most commonly for extracting user information from a corporate directory.

LDAP authentication A process that enables the IMS library to authenticate user credentials of LDAP-synchronized end users against a corporate LDAP directory using the LDAP standard Simple_Bind operation.

LDAP Manager Distinguished Name An LDAP setting in the CUCM where an LDAP manager account from the LDAP database should be specified. To import the data into the Cisco Unified Communications Manager database, the system performs a bind to the LDAP directory using the account specified in the configuration as the LDAP Manager Distinguished Name and reading of the database is done with this account.

LDAP synchronization A process that uses an internal tool called Cisco Directory Synchronization, or DirSync, on the Cisco Unified Communications Manager to synchronize a number of user attributes from a corporate LDAP directory.

LED Light-emitting diode; a semiconductor light source that emits light when current flows through it.

LFI Link Fragmentation and Interleaving; a tool that can reduce delay and jitter on slower-speed links by breaking up large data packets and interleaving low-delay traffic packets with the resulting smaller packets. LFI is typically used on slow WAN links to ensure minimal delay for voice and video traffic.

line level The output of any device with an internal pre-amplifier.

link efficiency Methods used to reduce the overhead that is associated with voice and video transportation. These bandwidth-saving mechanisms, such as compression, link fragmentation, and interleaving, help support large amounts of traffic over a slower link.

LLDP-MED Link Layer Discovery Protocol-Media Endpoint Discovery is an open-source protocol that can be used cross-vendor at Layer 2 of the network for device and information discovery across a network.

LLQ Low-Latency Queueing; a congestion management mechanism developed by Cisco to bring strict priority queuing to Class-Based Weighted Fair Queuing. LLQ allows delay-sensitive data, such as voice and video, to be given preferential treatment over other traffic by letting this data be dequeued and sent first.

Local Agent A service that runs backup and restore scripts on the server. In a cluster, the Local Agent runs backup and restore scripts on each node in the cluster.

local directory A collection of aliases that have been saved directly on the endpoint itself.

Local Gateway A trunk created between a Cisco router (typically located at the customer site) and Webex Control Hub. The Local Gateway is used to route calls from Webex to the PSTN connection as well as from the PSTN connection to Webex. Cisco recommends using Cisco UBE for the PSTN connection.

local route group A group within a route plan that can decouple the location of a PSTN gateway from the route patterns that are used to access the gateway.

location The aspect of CAC on the CUCM that determines the amount of total bandwidth available for all calls within a particular site, or between sites. When a call is set up, the regional value for that call must be subtracted from the total bandwidth allowed for that site.

Locations Locations are settings configured in the Webex Control Hub for Webex Calling that allow users and devices using the calling feature that have the same dialing behaviors based on their location to be grouped together. This can be configured based on any location that will have a Local Gateway assigned to it.

lossless A compression algorithm that searches content for statistically redundant information that can be represented in a compressed state without losing any original information.

lossy A compression algorithm that searches for nonessential content that can be deleted to conserve storage space.

luminance A measurement of the brightness of light.

LWAP Lightweight Access Point; a wireless access point device that can be controlled by a wireless controller using LWAPP.

LWAPP Lightweight Access Point Protocol; a protocol that allows multiple Wi-Fi wireless access points, called LWAPs, to be controlled all at once from a single management device, called a wireless controller, including configuring, monitoring, or troubleshooting.

M

macroblock A division of units that are a collection of pixels generally 16×16 in size but can be divided into 8×8 and 4×4 sizes as well.

manual backup A backup that is initiated by an administrator and starts immediately.

Master Agent A service that stores systemwide component registration information, maintains a complete set of scheduled tasks in an XML file, and updates this file when it receives updates of schedules from the user interface. The Master Agent sends executable tasks to the applicable Local Agents, as scheduled. The Local Agents execute immediate backup tasks without delay. The Master Agent stores backup data on a local attached drive or at a remote network location.

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

mic level The level of voltage that comes out of a microphone when someone speaks into it is known as the microphone level signal, or mic level (–60dBV to –40dBV). Because mics are self-contained, they produce a much smaller signal than amplifiers, which needs to be treated differently by the device that receives its signal. This is why devices, such as endpoints, have mic level settings and line level settings.

Migration Insights Migration Insights is a tool designed to help you to plan your Jabber migration from an on-premises deployment to cloud deployment. It allows you to gather the required information about the user's existing on-premises deployment services, such as third-party integration, endpoint types and configurations, and the type of services used by the end users.

millibar 100 pascals.

MIMO Multiple Input and Multiple Output; a method for multiplying the capacity of a radio link using multiple transmission and receiving antennas to exploit multipath propagation. MIMO has become an essential element of wireless communication standards including IEEE 802.11n, 802.11ac, HSPA+ (3G), WiMAX (4G), and Long Term Evolution (4G LTE). More recently, MIMO has been applied to power-line communication for three-wire installations as part of ITU G.hn standard and HomePlug AV2 specification.

MOH Music On Hold; streaming music to callers on hold.

mono The audio signal played when only one channel is used for both left and right speakers.

MPLS Multiprotocol Label Switching; a transport protocol that uses labels to route traffic rather than network addresses. Packets are forwarded based on the content of the label, so deciphering between voice, video, and data is simple. It is protocol agnostic, so it will function in circuit-switched or packet-switched networks.

MPP Multiplatform Phone firmware is the software that must be installed on an IP Phone before it can register to the Webex Control Hub.

MRA Mobile and Remote Access; a Cisco feature that uses the Expressway series devices to proxy registrations to the CUCM from endpoints outside the corporate network without the use of a VPN.

MRGL Media Resource Group List; a prioritized list of Media Resource Groups.

MTLS Mutual TLS, also referred to as *TLS Verify*; a process in which both parties authenticate each other by verifying the provided digital certificate so that both parties are assured of the other's identity.

MTP Media Termination Point; a media resource that allows the passing of a stream from one noncontiguous connection to another.

multipoint An industrywide term used to describe any call that involves three or more participants.

multisite The option key available on CE software-based endpoints that enable the endpoints to host a multipoint call.

multiway Call escalation from a point-to-point call to a multipoint call hosted on a Multipoint Conferencing Unit. Multiway is a function used by the Cisco VCS through a setting called Conference Factory. It can be used only in conjunction with Cisco Telepresence MCUs, which are end-of-life products.

Mutual TLS See *MTLS* and *TLS Verify*.

MWI Message Waiting Indicator.

MX Multipurpose Experience; a branding type for Cisco Telepresence endpoints that offers a plug-and-play meeting room endpoint for customers that's ready to use out of the box.

N

NANP North American Numbering Plan; a standardized national dial plan that assigns individual or blocks of telephone numbers, which are called E.164 addresses, to physical lines or circuits.

NAT Network Address Translation; a process of masquerading private IP addresses with public IP addresses.

network services Services that enable network-related capabilities in the CUCM and cannot be enabled or disabled by an administrator. However, they can be stopped, started, and restarted.

Newton The standard international unit for force. It is equal to the amount of net force required to accelerate a mass of one kilogram at a rate of one meter per second squared.

NR No Radio; a prefix signifying that all features that depend on a radio variant have been removed from certain Cisco phone models.

NRC rating Noise Reduction Coefficient rating; a measurement that informs the degree a substance absorbs sound energy, usually applied to building materials.

NTE Named Telephony Events; a method of sending DTMF from one endpoint to another after the call media has been established. The tones are sent as packet data using the already-established RTP stream and are distinguished from the audio by the RTP payload type field.

NTP Network Time Protocol; a protocol for synchronizing computer system clocks over IP networks. NTP has a hierarchical organization that is based on clock strata. Stratum 0 is an extremely precise clock source, such as an atomic clock or radio clock. A stratum 1 server is directly connected to a stratum 0 clock and can provide time information to other (stratum 2) devices, which in turn serve stratum 3 devices.

Numbers A list of phone numbers, sorted by location, that can be used for Webex Calling. Numbers can be assigned to the main number of the organization, to a workspace, or to a user. Some services can also have a number assigned to them, such as a group voicemail.

O

OAM Operation, administration, and maintenance; the processes that allow the Ethernet interfaces on devices to support the IEEE 802.3ah standard for operation, administration, and maintenance of Ethernet in access networks. The standard defines OAM link fault management.

OBTP One-Button-to-Push; a Cisco technology that allows participants to press a single button to join a scheduled meeting.

offline IM Instant messages stored for users who are currently offline.

off-net A setting that applies a marker to calls on the CUCM that leave the IP network and traverse the PSTN circuit-switched network. Applying this marker allows other call behavior settings to be applied.

omnidirectional mic A microphone with a polar pickup area intended to be at the center of a group of audio sources with a 360-degree pickup area.

on-net A setting that applies a marker to calls on the CUCM that remain on the IP network, even when they leave the corporate network. Applying this marker allows other call behavior settings to be applied.

Option 66 An industrywide protocol created by the IETF that allows TFTP server address information to be discovered during DHCP negotiation.

Option 150 A Cisco proprietary protocol that allows TFTP server address information to be discovered during DHCP negotiation.

OS Operating system.

OSD Onscreen display.

OSPF Open Shortest Path First; a Layer 3 routing protocol that uses a link-state routing algorithm and falls into the group of Interior Gateway Protocols, operating within a single autonomous system.

OU Organizational unit; a subcategory in an LDAP hierarchical tree used to categorize users or devices within an organization.

OV certificates Organization validation certificates; certificates for which the CA checks the right of the applicant to use a specific domain name and conducts some vetting of the organization. Additional vetted company information is displayed to customers when clicking on the Secure Site Seal, giving enhanced visibility in who is behind the site and associated enhanced trust.

overlap sending and receiving A function that allows digits to be sent or received one by one over an ISDN PRI.

over-sampling Sampling an analog input signal at a rate much higher than the minimum frequency required by the Nyquist-Shannon theorem.

P

packet loss The dropping of packets by the router due to congestion on a link.

paging group Group Paging allows a user to place a one-way call or group page to up to 75 target users and workspaces by dialing a number or extension assigned to a specific paging group. You can create a paging group so that users can send an audio message to a person, a department, or a team.

partition A group of dialable patterns within the CUCM that share identical accessibility.

Pascal A measurement of one newton of pressure per square meter.

PAT Port Address Translation; an alternative to NAT but works in a similar fashion.

PBX Private branch exchange; a system that operates in a similar fashion to the automatic telephone exchange, except that the purpose of a PBX is to route calls within a business exclusively. PBXs can also connect to the outside world over the public telephone network, but they operate on the same circuit-switched network using POTS or ISDN.

PCM Pulse-code modulation; a technique in which the amplitude of an analog signal is converted to a binary value represented as a series of pulses.

PD Powered device; an IEEE term used to describe a device that receives power from another device using PoE.

PDL Plasma display panel; a type of flat-panel display that uses small cells containing plasma, which is ionized gas that responds to electric fields.

People+Content A proprietary protocol for content sharing that was originally designed by PictureTel and later developed by Polycom.

Perfmon counters Performance counters on RTMT that contain information on the CUCM, CUC, and IMP systems, as well as devices on these systems.

Personal Contacts Directory entries that can be saved on any phone or device for faster calling. Personal Contacts are another type of user in Webex and can include any of the previously mentioned user types as entries.

Personal Rooms Webex meeting rooms that are assigned to and used by specific users.

Phantom A location that specifies unlimited bandwidth for audio, video, and immersive calls. You specify this location to allow successful call admission control for calls across intercluster trunks that use the H.323 or SIP trunks to certain destinations that support the earlier location CAC feature.

PHB Per hop behavior; a Layer 3 QoS classification for marking packets.

PIMG PBX IP Media Gateway; a Cisco device used to integrate Cisco Unity Connection with the circuit-switched network.

PIP Picture-in-picture; a video screen layout in which a smaller video pane can exist within a larger video pane.

pixel A contraction of the words *picture* and *element*; it generally is used to describe the smallest component of a digital image.

pixel saturation The total number of pixels that make up a frame. Multiplying the two numbers in a resolution will provide the pixel saturation.

PKI Public key infrastructure; a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

PMP Personal Multiparty Plus; a product for which licenses can be purchased as Basic or Advanced. PMP Basic provides one PMP license per user that will support host meetings on the Cisco Meeting Server for up to four participants in each meeting. PMP Advanced provides one PMP license per user that will support host meetings on the Cisco Meeting Server for an undefined number of participants in each meeting. The number of participants for PMP Advanced licenses is limited only by the infrastructure that has been installed.

PoE Power over Ethernet; any of several standard or ad hoc systems that pass electric power along with data on twisted-pair Ethernet cabling. This allows a single cable to provide both data connection and electric power to devices such as wireless access points, IP cameras, and VoIP phones.

PoE Power Budget The total power a switch can supply down Ethernet cables.

polar pattern The directionality pattern of highest sensitivity for the microphone element.

policing Conditioning traffic before transmitting or receiving it through the network. Policing controls traffic bursts by marking or dropping packets when predefined limits are reached. Policing mechanisms can drop traffic classes that have lower QoS priority markings. Policing tools include class-based policing and committed access rate (CAR).

POTS Plain old telephone service; the means of audible communication using analog signals transmitted over wire.

Power Save A power-saving mode on Cisco IP phones where the backlight or screen turns off when the phone is inactive for a set interval. The backlight can be managed.

Power Save Plus A power-saving mode on Cisco IP phones where the phone screen turns on and off at times that are based on the employee's work schedule. If work hours or work days change, an administrator can reconfigure that employee's phone.

PQ Priority queue; a congestion management technique that guarantees strict priority in that it ensures one type of traffic will be sent, possibly at the expense of all others. For PQ, a low priority queue can be detrimentally affected, and, in the worst case, never allowed to send its packets if a limited amount of bandwidth is available or if the transmission rate of critical traffic is high.

Precision Camera A PTZ camera designed by Cisco but loosely based on the PrecisionHD camera. There are two models in this camera line. The Precision 40 camera supports an 8x zoom with an optical zoom of 4x. The Precision 60 supports up to 20x zoom capability.

Precision MIC 20 An omnidirectional Cisco tabletop microphone that uses a mini-jack and comes with a built-in mute button.

PrecisionHD Camera A PTZ camera originally designed by Tandberg, which was later acquired by Cisco. These cameras come in 4x, 8x, or 12x zoom capabilities.

prediction blocks Multiple variable-sized partitions into which a macroblock can be split. In an interpredicted macroblock, a separate motion vector is specified for each partition.

prefix A feature of H.323 dial plan architecture that allows easy access to services such as MCUs and gateways.

premises-based PSTN Premises-based PSTN (formerly Local Gateway) is one of three options an administrator can choose in Webex Control Hub to leverage for PSTN connections when setting up Webex Calling. Choose this option if you want to keep your current PSTN provider. Trunks for premises-based PSTN through Local Gateway can also be used to connect to on-premises PBXs. You can retain existing Local Gateway functionality without making any configuration changes. Locations using Local Gateway are set to Premises-based PSTN, and the Local Gateways become trunks.

presence An indicator light that identifies if a user is online, offline, away, or busy.

Prestandard PoE A Cisco proprietary protocol that supplies power to IP phones over an Ethernet cable. Prestandard PoE supports up to 7W of power.

PRI Primary Rate Interface; a telecommunications interface standard used on an Integrated Services Digital Network (ISDN) to carry multiple DS0 voice and data transmissions between the network and a user. PRI is the standard for providing telecommunication services to enterprises and offices.

Priority Alert A user-configurable feature that allows users to set up unique ringtones based on predefined criteria.

progressive scanning A scanning process by which pixels are populated within a frame working from top to bottom, left to right, and all lines are populated for each frame.

PSE Power sourcing equipment; an IEEE term used to describe any device capable of supplying power to another device using PoE.

PSTN Public switched telephone network; the world's collection of interconnected circuit-switched public telephone networks.

PSTN routing A type of call routing that occurs between a site and the PSTN.

PTR Reverse Pointer Record; a setting that maps an IP address to a domain name, while a record maps the domain name to an IP address.

PTZ Pan, Tilt, Zoom; a description used for cameras that have the automated capability to be repositioned within a room.

PVC Permanent virtual circuit.

Q–R

Q.931 A standard based on the ISDN H.320 standard; it contains the source and destination IP address, in hexadecimal format, and any crypto-hash token if a call is to be encrypted. Q.931 is also responsible for the Alerting and Connect messages sent from the destination endpoint.

QoS Quality of service; a Layer 3 management tool used to allow or drop packets traversing through a router based on priority.

quantization The act of sampling an analog signal for the purpose of reducing it to a smaller set of manageable digital values. Also known as *quantizing*.

quantization error The difference between the resulting digital representation of an original analog signal and the actual value of the original analog signal.

RAS Registration, Admission, and Status; an ITU-created communication protocol that identifies all messaging schemes between any device and a gatekeeper using H.323.

RBG Red, Blue, Green; a component signal that breaks out a separate channel for luminance (Y), chrominance red (R), chrominance blue (B), and chrominance green (G).

RCA An analog audio and video cable for composite analog video. The name was taken from the company called Radio Corporation of America.

Receptionist Client A web-based tool that combines your desk phone with a desktop interface and enables you to process calls to users within your organization. You can screen incoming calls, manage calls and contacts, and monitor calls in a queue.

reflection An effect caused when an object of obstruction causes sound waves to bounce, or reflect, into another direction. The law of reflection is the angle of incidence equals the angle of reflection.

registration-based Local Gateway With a registration-based connection, you create the connection in Control Hub, and you are provided with credentials to allow your Local Gateway to create a TCP connection to the cloud. This is a one-way connection from the Local Gateway to the cloud. The connection does not require CA-signed certificates; however, the link has a lower call capacity and is not as durable if there are any network issues, such as high latency or packet loss.

regions Sites where the bandwidth of audio and video calls can be set on a per-call basis. The audio limit on a region can result in filtering out codecs with higher bit rates. However, for video calls, the video limit constrains the quality (resolution and transmission rate) of the video. Regions control per-call bandwidth within a site and between sites.

remote browse A feature on RTMT that allows administrators to view traces on the server without downloading the trace files. Remote Browse can also be used to download these trace files.

rendezvous conferencing An always-on conference space that can be joined at any time.

resolution The number of pixels within a digital frame.

Restore Wizard A tool embedded in the backup and restore system. It is used if a recovery from a server failure is needed.

reverb time The amount of time a sound takes to eventually lose enough energy and drop below the level of perception.

reverberations The prolonging of a sound caused by the reception of multiple reflections off walls and ceilings within a few milliseconds of each other, also known as late reflections.

RF Radio frequency; In general terms, RF is any electromagnetic wave frequency that oscillates in the range of 3 kHz and 300 GHz. The Wi-Fi channel coverage provided by AP radios operates in the 2.4 GHz and 5 GHz frequency bands.

RFC Request for Comments; a type of publication from the IETF that describes methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.

RGBQuantizationRange A video output setting on Cisco CE software-based endpoints. Devices connected to an HDMI output should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately, some devices do not follow the standard and this configuration on CE endpoints may be used to override the settings to get a perfect image with any display. Most HDMI displays expect full quantization range.

RIP Request In Progress; a RAS message sent by a gatekeeper that informs the H.323 endpoint that a request is being processed.

RIS Real-Time Information server; a server that maintains real-time information such as device registration status, performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as the IM and Presence Real-Time Monitoring Tool (RTMT), SOAP applications, and so on, to retrieve the information that is stored in all RIS nodes in the cluster.

RMS Root mean squared; a method used to calculate a comparable measure of power efficiency.

RMS Rich Media Session; a type of license that can be installed on the Expressway Core and Expressway Edge servers. These licenses allow for B2B calling and SIP-to-Microsoft interworking capabilities.

RNAR Ring No Answer Revision; a ring duration timer used with hunting on the CUCM. When a device rings to the full duration of the RNAR, the hunt will continue on to the next participant.

root CA The certificate authority server that generates, signs, and authenticates certificates used for authentication. This is the authority for all certificates signed by it.

root CA certificate A certificate that establishes a trusted chain beginning at the root CA, through the root CA certificate, and ending at the certificate that was signed.

route filter A filter that restricts certain numbers that are otherwise allowed by the route pattern.

route group Available paths; the route group distributes calls to gateways and trunks.

route list A prioritized list of the available paths for a call.

route pattern A pattern that matches an external dialed string and uses it to select a gateway or a corresponding route list.

routing prefix A type of prefix that is configured on a gateway or bridge and registers to an H.323 gatekeeper. It is used to route all calls to that server regardless of the following digits.

RRQ Registration Request; a RAS message initiated by an endpoint to attempt to register to a gatekeeper. The gatekeeper will respond with either RCF (Registration Confirm) or RRJ (Registration Reject).

RSA Rivest-Shamir-Adleman; a public-key cryptographic system used for secure data transmission.

RTMT Real-Time Monitoring Tool; a service that runs as a client application and uses HTTPS and TCP to monitor system performance, device status, device discovery, CTI applications, and voice-messaging ports.

RTP Real-time Transport Protocol; a protocol used over UDP to carry real-time media traffic.

S

sample Measurement of an analog signal that must be taken at precise points.

SBC A Session Border Controller is an edge service that provides voice and video connectivity between the enterprise IP network and a service provider network. The service provider will make the conversion from IP to ISDN, and vice versa. Cisco UBE is a SBC.

SCCP Skinny Call Control Protocol; a Cisco proprietary protocol used for voice communication over IP.

Scheduler A Disaster Recovery tool in the CUCM that allows the administrator to perform automatic backups in specific time frames.

SCIM The System for Cross-domain Identity Management API is an open standard for automating the exchange of user identity information between identity domains and IT systems. SCIM is designed to make it easier to manage user identities in cloud-based applications and services. SCIM uses a standardized API through REST.

SDP Session Description Protocol; a protocol used during SIP call setup to exchange capabilities and identify UDP ports to be used.

Selective Calling A user-configurable feature that allows a user to choose which calls to accept, reject, or forward based on the phone number, who's calling, and/or the time and day of the call.

self-provisioning A feature that allows phones to be provisioned across the network by enabling end users to provision their own phones without contacting an administrator.

Sequential Ring A user-configurable feature that allows the user to create a list of up to five additional numbers to ring, in a specific order, when receiving incoming calls following the schedules they create.

Server Report A Cisco Unified Serviceability Report generated on the CUC that contains statistics on the server performance for the day.

service A set of parameters that encapsulate a specific feature or function within the Cisco Unified Communications Manager.

Service Number A Service Number that is a machine account for a feature such a hunt group, paging, or conference device is another type of user in Webex.

service parameter A factor used to define settings for a specific feature service on an individual server. Unlike enterprise parameters, service parameters are defined separately for each server in the cluster and for each feature service enabled on each server.

Service Profile A configuration menu on the Cisco Unified Communications Manager that allows UC Services to be grouped together. A service profile can then be applied to an end user to use with their assigned phones.

servlet A Java class that receives an HTTP or HTTPS request and generates a response that is based on that request.

shadow A system location created for inter-cluster Enhanced Location CAC. To pass locations across clusters, the SIP inter-cluster trunk (ICT) must be assigned to the system location Shadow.

shaping mechanisms Mechanisms used on output interfaces to help smooth out mismatches in the network and limit transmission rates. Although these mechanisms are typically used to limit the flow from a high-speed link to a low-speed link, shaping could also be used to manage the flow of traffic at a point in the network where multiple flows are aggregated.

shotgun mic A directional mic with a narrow pickup range, but it can also pick up sound from the greatest distances.

SIF Source input format; a format defined by the ISO as part of MPEG-1. Often referred to as a “Constrained parameters bit stream,” SIF defines the minimum specifications any decoder should be able to handle to provide a decent balance between quality and transmission performance.

SIMPLE Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions; an instant messaging and presence protocol suite based on Session Initiation Protocol.

Simultaneous Ring A user-configurable feature that rings the user’s office phone and other phones of their choice at the same time. The user can also set up schedules to ring these phones during certain times of the day and/or days of the week.

sine wave A mathematical curve indicating that all the signal energy is concentrated at one frequency.

Single number reach (office anywhere) A user-configurable feature that enables the user to make, receive, and move calls to or from any device without interruption.

SIP Session Initiation Protocol; an IETF signaling protocol used for real-time sessions, such as voice, video, and instant messaging.

SIP proxy A function of the SIP server used to connect devices in voice or video calls.

SIP registrar A function of the SIP server used to map SIP URI addresses to IP addresses for SIP endpoints when they register.

SIP server The call control device for SIP voice and video systems.

SIPS A term used to define a secure layer over SIP; Secure SIP, or Secure Session Initiation Protocol.

SLDAP Secure Lightweight Directory Access Protocol; a protocol that enables LDAP to be sent over a Secure Sockets Layer connection and can be enabled by adding the LDAP server into the Tomcat trust store within the Unified CM Platform Administration.

SMP Shares Multiparty Plus; an application that allows licenses to be added to the Cisco Meeting Server so that any user can create and join a meeting using this license.

SNMP Simple Network Management Protocol; an Internet standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

SNR Single Number Reach.

SOAP Simple Object Access Protocol; a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks. Its purpose is to provide extensibility, neutrality, and independence.

Soft Phone mode A user mode in which the Cisco Jabber client behaves like an IP phone and originates and terminates all audio and video communication interactions on the software endpoint itself.

sound pressure The disruption of the normal atmospheric pressure caused by a sound wave. Half of a sound wave is made up of the compression of the medium, and the other half is the decompression or rarefaction of the medium. Sound pressure is measured in pascals or millibars.

SP Service Provider is the name Cisco uses to describe partners who host Cisco equipment within their own data centers and then sell those services to customers directly.

Speaker Track 60 A dual-camera system that enhances the user experience by each camera zooming in on an individual participant in a meeting based on who's speaking. If one camera is zoomed in on one participant in a room and another participant starts speaking, the second camera will zoom in on that participant before the camera switches to the new participant view.

SPID Service profile identifier.

SRST Survivable Remote Site Telephony; a redundancy feature available on Cisco IOS routers that allows Cisco Unified IP phones registered to the Cisco Unified Communications Manager from remote office locations to register to their local router during WAN network failure events.

SRTP Secure Real-time Transport Protocol; a secure protocol over TLS used over UDP to carry real-time media traffic.

SRV record A location service within DNS that can be used to identify protocols, port numbers, and host names of servers for particular services.

SSID Service Set Identifier; the name assigned to a wireless broadcast signal so that users can easily select the Wi-Fi network to which they need to connect.

SSL Secure Sockets Layer; a legacy cryptographic protocol that provides communications security over a computer network for TCP and UDP traffic. SSL has been replaced by the more secure TLS.

SSO Single sign-on; a form of identity management that allows users to sign into one application, such as a computer, and access all other associated applications.

stacker A link efficiency compression algorithm that compresses the payload of Layer 2 frames. Also referred to as a *predictor* algorithm.

stereo An audio signal that has two channels, one for left speakers and one for right speakers.

STP Spanning Tree Protocol; a Layer 2 protocol that runs on switches and is specified by the IEEE standard 802.1d. The purpose of STP is to prevent loops when configuring redundant paths within the network. Different flavors of STP can be used, and each one requires different timing for convergence. Therefore, it is recommended that the same version of STP is used within a single environment. Some of the other Spanning Tree Protocols that exist include IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Instance Spanning Tree Protocol (MISTP).

stratum A hierarchical organization within NTP that is based on clock strata. Stratum 0 is an extremely precise clock source, such as an atomic clock or radio clock. A stratum 1 server is directly connected to a stratum 0 clock and can provide time information to other (stratum 2) devices, which in turn serve stratum 3 devices, and so on.

STUN Session Traversal Utilities for NAT; a set of methods that requires a STUN client, which could be a phone or some other device that sends packets to a STUN server on the Internet. The STUN server replies with information about the IP address and ports from which the packets were received and detects the type of NAT device through which the packets were sent. The STUN client can then use the public IP and assigned port in constructing its headers so that external contacts can reach the client without the need for any other device or technique. After the STUN server assigns a port, it is no longer involved in the line of communication.

supercardioid mic A directional mic that has a narrower range of focus. As a result of this narrowing, a small lobe develops behind the mic and may require consideration.

S-Video Separate video, or Y/C; a composite video for analog video signals. S-Video separates the luminance (Y) from the chrominance (C). Although S-Video offers better quality video than other composite video components, it cannot compare to the quality of video from component video.

SX Solutions Experience; a branding type for Cisco Telepresence endpoints that offers integrator options for customers.

symmetric cryptography A process of negotiating between a server and client that details which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. Identification is usually in the form of digital “certificates” that contain the server name, the trusted certificate authority, and the server’s public encryption key.

synchronization agreement A type of agreement that specifies a search base that is a position in the LDAP tree where the Cisco Unified Communications Manager will begin its search for user accounts to import.

T

T.150 An early ITU substandard of the H.320 umbrella standard that allows content sharing between devices; Terminal Equipment and Protocols for Telematic Services, otherwise known as the Telewriting Terminal Equipment.

T302 Timer A setting that specifies the interdigit timer for variable-length numbers. Reducing the default value will speed up dialing (shorter post-dial delay).

TAB Cisco Jabber for Tablet is the option to select to create a TAB device for Webex App on an iPad, Android tablet, or Google Chromebook.

TC Telepresence Collaboration; legacy software that came preloaded on Cisco Telepresence endpoints. It has since been replaced by CE software.

TCP Transmission Control Protocol; a routing protocol that ensures communication by use of acknowledgments. If an acknowledgment is not received, the packet will be retransmitted.

TCP/IP Transmission Control Protocol over Internet Protocol; a standard used to control how information is transmitted and received over the Internet.

TCT Cisco Dual Mode for iPhone is the option to select to create a TCT device for Webex App on iPhones.

TDM Time-division multiplexing; a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line so that each signal appears on the line only a fraction of time in an alternating pattern.

TDoS Telephony denial of service; a security mechanism used to prevent attacks.

TEI Terminal endpoint identifier; a number between 0 and 127, where 0–63 are used for static TEI assignment, 64–126 are used for dynamic assignment, and 127 is used for group assignments. These numbers are used exclusively within an ISDN environment.

telepresence An industry term used to identify systems capable of high-quality video and audio communications.

text conferencing Ad hoc group chat or persistent group chat; it is supported as part of the Jabber XCP feature set.

TFTP Trivial File Transfer Protocol; a protocol that builds configuration files and serves embedded component executables, ringer files, and device configuration files.

TIMG T1 IP Media Gateway; a Cisco device used to integrate Cisco Unity Connection with the circuit-switched network.

TIP Telepresence Interoperability Protocol; an open standard that allows RTP and RTCP streams to be multiplexed together.

TLS Transport Layer Security; a secure layer of the TCP protocol that uses encryption to scramble data being shared between nodes.

TLS Verify A process in which both client and server present and authenticate each other by verifying each other's provided digital certificate so that both parties are assured of the other's identity. This process occurs before communication can be established. Also known as *Mutual TLS*.

TMS Telepresence Management Suite; a management solution for Cisco Collaboration that runs on a Microsoft Windows Server.

ToD Time of day; a routing component of call privileges that controls when routing is allowed to occur.

TON Type of number; a record sent with each telephony transaction through the PSTN. There are two components of a TON: the number type of a called number and the numbering plan. Basically, four different types of numbers can be used. They are Cisco CallManager, National, International, or Unknown, which is the default. Different plans can be used as well, such as Cisco CallManager, ISDN, National Standard, Private, or Unknown. Each type and plan can be used to determine when and how a translation rule should be applied.

ToS Type of service; a Layer 3 QoS classification for marking packets.

Touch 10 A 10-inch multitouch capacitive control pad that is used to control a Telepresence endpoint.

transcoding Converting the data stream from one compression type to another.

transform block A processing unit that serves as input to a linear block transform. In the YCbCr color space, each single 16×16 macroblock consists of 16×16 luma (Y) samples and 8×8 chroma (Cb and Cr) samples. These samples are split into four Y blocks, one Cb block, and one Cr block.

translation pattern A pattern that when matched provides an entry to the call-routing table. If a dialed number matches the pattern, another number, which is the translated number that is configured at the translation pattern, is looked up in the call-routing table.

TRAP Telephone Record and Playback.

traversal chaining A more secure means of traversing firewalls when one Expressway is placed within a DMZ. As well as acting as a traversal server, an Expressway-E can act as a traversal client to another Expressway-E. If you chain two Expressway-Es, the first Expressway-E is a traversal server for the Expressway-C. That first Expressway-E is also a traversal client of the second Expressway-E. The second Expressway-E is a traversal server for the first Expressway-E.

traversal client zone The zone created on the traversal client, which is the Expressway Core in a typical Cisco Collaboration environment, used to establish communication with the traversal server. Some Cisco endpoints can also be traversal clients, as well as the Expressway Edge. Also, the legacy Cisco VCS Control and VCS Expressway can support the role of traversal client.

traversal server zone The zone created on the traversal server, which is the Expressway Edge in a typical Cisco Collaboration environment, used to proxy communication messages to the internal network through the traversal client. The legacy Cisco VCS Expressway can also support the role of traversal server.

traversal zone A zone that is used for communication through a firewall. An Expressway Core and an Expressway Edge are required to set up a traversal communication through a firewall. The Expressway Core needs to be located inside the firewall, whereas the Expressway Edge needs to be located outside the firewall or in a DMZ.

TRC Telepresence Remote Control.

TSPEC Traffic Specification; Cisco APs and wireless Unified Communications clients now use Traffic Specification instead of the QoS Basic Service Set for call admission control.

TTS Text-to-Speech.

TUI Telephone user interface; an interactive means of accessing the Cisco Unity Connection server using the DTMF touch tones on a telephone.

TURN Traversals Using Relays around NAT; a protocol that connects clients behind a NAT to a single peer. Its purpose is to provide the same protection as that created by symmetric NATs and firewalls. Symmetric NATs use dynamic ports that often change. Therefore, the TURN server acts as a relay so that any data received is forwarded on to the client, and port allocation can be updated on the fly. The client on the inside can also be on the receiving end, rather than the sending end, of a connection that is requested by a client on the outside.

TVS Trust Verification Service; a remote trust store on the CUCM that can be used by phones with limited storage so that a full certificate trust store does not have to be placed on each IP phone.

two-stage dialing A type of connectivity in which all endpoints share a single PSTN number.

U

UC Unified Communications; a set of products that provide a consistent unified user interface and experience across multiple devices and media types.

UC Services A configuration menu on the Cisco Unified Communications Manager that allows various services to be configured. These services include Voicemail, Mailstore, Conferencing, Directory, IM and Presence Service, CTI, Video Conference Scheduling Service, and Cisco Jabber Client Configuration.

UCCE Unified Contact Center Enterprise; a service that helps companies deliver proactive and personalized customer experiences for contact centers with up to 24,000 agents. Fault tolerance helps ensure uninterrupted operation. Comprehensive reporting gives you the business intelligence needed to optimize your contact center’s performance.

UCCX Unified Contact Center Express; a complete “Contact Center in a Box.” It delivers call routing, management, and administration features, and is designed for businesses ranging from very small to enterprise branch offices with up to 400 agents.

UDP User Datagram Protocol; an alternative communications protocol to Transmission Control Protocol used primarily for establishing low-latency and loss-tolerating connections between applications on the Internet.

UltraHD Also called UHD or Ultra High-Definition. This resolution defines the latest 4K resolutions available at 3840×2160.

UN Unsolicited Notify; a DTMF relay method used primarily by Cisco IOS SIP gateways to transport DTMF digits using SIP NOTIFY messages. Unlike KPML, these NOTIFY messages are unsolicited, and there is no prior registration to receive these messages using a SIP SUBSCRIBE message. Also, unlike KPML, which has an XML-encoded body, the message body in these NOTIFY messages has a 10-character encoded digit, volume, and duration, describing the DTMF event. Similar to KPML, UN messages are OOB.

unbalanced audio cable A type of cable that has two wires: one to carry the positive (+) side of a signal, and the other wire shares both the negative () side of the signal and the grounding shield. Inside the cable itself, the signal wire is typically in the center of the cable with the ground wire surrounding it. The ground wire serves two functions. It carries part of the audio signal and serves to shield the main signal wire to some degree from outside interference from noise. It does help reject some noise, but the wire itself also acts like an antenna and picks up noise.

under-sampling Sampling an analog input signal at a rate much lower than the minimum frequency required by the Nyquist-Shannon theorem.

Unified Communications Traversal Zone A special type of traversal zone on Expressway servers that are used for MRA deployments. This type of traversal zone requires that TLS Verify be used for the highest security in communications.

Unified CVP Unified Customer Voice Portal; a system that combines open-standards support for speech with intelligent application development and industry-leading call control to deliver personalized self-service to callers.

UPN User Principal Name; the name of a system user in an email address format. The username is followed by the at sign (@) followed by the name of the Internet domain with which the user is associated.

URI Uniform Resource Identifier; a string of characters that identifies a particular resource. URIs typically take the form of User@FQDN.

URL Uniform Resource Locator; a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. URLs typically take the form of User.FQDN.

USB Universal Serial Bus; an industry standard that establishes specifications for cables and connectors and protocols for connection, communication, and power supply between computers, peripheral devices, and other computers.

User (in Webex) A person who has a phone or soft client associated with the user account.

V

VAR Value-added reseller is a name Cisco uses to describe a partner who resells Cisco products and solutions to customers but does not typically host the equipment itself.

VCS Video Communications Server; a Cisco (formerly Tandberg) call control device designed specifically for video Telepresence endpoints and devices. The base code of the Cisco VCS is used with the Cisco Expressway servers as well.

Verify Domain Verifying your domain is a process in Webex Control Hub used to prove to Webex that you own that domain. Verifying your domain allows you to claim users into your organization if they're signed up in a different organization. Administrations can click the **Verify Domain** button to begin this process.

VGA Video graphics array; a graphics standard for an analog composite video display controller. The cable that connects to the VGA controller is called a VGA connector.

Virtual Extensions A feature that allows you to assign extensions to external phone numbers that users frequently call.

VISCA A professional camera control protocol that was originally designed by Sony. This protocol provides pan, tilt, and zoom capabilities to the camera from a remote.

visible spectrum A small area of the EMR spectrum that is perceivable to the human eye in the form of color.

VLAN Virtual local area network; virtual partitions at Layer 2 of the network used to decouple traffic and logically group data packets being sent across the network. VLANs can be used for QoS.

VNC Virtual network computing; a graphical desktop-sharing system that uses the Remote Frame Buffer protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical-screen updates back in the other direction, over a network.

Voice VLAN The virtual partition in the Layer 2 part of the network allocated specifically for voice and video network traffic.

Voicemail Group A feature that allows you to manage a shared voicemail and inbound fax box for Webex Calling. You can create a shared voicemail box and inbound fax box to assign to users or call routing features like an Auto Attendant, call queue, or hunt group. With the Voicemail Group feature, you can set up new message notifications, choose where you want the messages stored, and customize the voicemail box greeting.

voicemail port An entity that requests a call that the Cisco Unified Communications Manager is routing. When a call is sent to a voicemail system, that system can request that the call be transferred to another directory number, to a PSTN destination, such as the cell phone of a user, or to an assistant.

VoIP Voice over IP; an audio technology that allows voice communication to be translated into a binary format and encapsulated into packets and sent across an IP network.

VPN Virtual private network; a protocol used to connect two autonomous networks across a WAN.

VRRP Virtual Router Redundancy Protocol; an IETF protocol based on RFC 5798 that offers default gateway redundancy similar to HSRP. However, these two protocols are mutually exclusive and cannot operate in tandem with one another.

VSS Virtual Switching System; a method that ensures redundancy on Cisco Catalyst switches.

VUI Voice user interface; an interactive means of accessing the Cisco Unity Connection server using audio prompts and communication.

VVID Voice VLAN ID; the numeric value associated with the voice VLAN.

W

WAN Wide area network; a telecommunications network that extends over a large geographical area for the primary purpose of computer networking.

WAP Wireless access point; the wireless router that wireless devices connect to.

watt The rate of transfer of energy in one second, or one joule per second. A joule is equal to the energy expended in applying a force of one newton through a distance of one meter.

wavelength The distance to complete one cycle in an audio wave.

WebDAV Web Distributed Authoring and Versioning; an extension of the Hypertext Transfer Protocol that allows clients to perform remote web content authoring operations. WebDAV is defined in RFC 4918 by a working group of the Internet Engineering Task Force.

Webex App A soft client that Cisco originally developed as a fully cloud-based application that supports messaging, meeting, and calling. Cisco now supports Webex App registration to the Cisco Unified Communications Manager for on-premises calling.

Webex App Hub A website used to deliver pre-built solutions with third-party applications from vendors such as Microsoft, Google Cloud, Miro, Salesforce, and more to deliver a complete collaboration experience.

Webex Calling DI Dedicated Instance leverages existing CCP partner peering with Webex Calling for this feature. To enable this feature for DI, Webex Calling introduces a new call routing construct called Route Lists.

Webex Calling Route Lists Route Lists in Webex Calling are lists of numbers reachable through a Route Group. Each Route List is exclusively assigned to a Location that supplies up to 40,000 unassigned numbers from the hosted pool. Only customers with DI entitlements can see or configure Route Lists in Control Hub.

Webex Control Hub A full cloud-based call control service that manages all aspects of messaging, meeting, and calling.

Webex endpoints Cisco Telepresence endpoint products based on the CE endpoint software that offer both integrator solutions and plug-and-play options ready to use out of the box.

Webex Events The end-to-end event platform that powers continuous engagement to drive better results for virtual, in-person, and hybrid events.

Webex Meeting A virtual space hosted in the cloud that anyone can join from any device anywhere they have an Internet connection.

Webex Meeting App A meeting application that allows users to join or start Webex meetings. This app can also be used to share content during a meeting hosted in the Webex cloud.

Webex Messaging Allows users to send someone a direct message or bring everyone together easily and quickly into a Webex Space. This feature enables everyone to see and share all the information they need to work together productively in real time by sending messages, sharing files, and creating or editing whiteboards.

Webex Teams app A messaging application that allows users to share content and instant messages with other users point-to-point or as a group in a Teams Space. The app can also be used to join Webex meetings or share content during a meeting hosted in the Webex cloud.

Webex Webinars Another meeting platform designed for larger townhall-style meetings. Webinars support the same basic features Personal Rooms supports, plus many extra features tailored to larger groups, with a much larger capacity of participant support.

WebRTC A free, open project that provides browsers and mobile applications with Real-Time Communications capabilities via simple APIs.

WebSocket A bidirectional persistent connection between a client and a server where information can flow back and forth without the overhead of initiating a new TCP connection or authentication for every request.

WFQ Weighted Fair Queuing; an algorithm that does not require configuration of access lists to determine the preferred traffic on a serial interface. Rather, the fair queue algorithm dynamically sorts traffic into messages that are part of a conversation.

white balance A setting used in cameras to set the reference value for white so that color anomalies caused by color temperature can be corrected.

WLAN Wireless local area network, also known as Wi-Fi. Instituted, monitored, and managed by the IEEE, WLAN standards include 802.11a/b/g/n/ac and 802.11ax, also known as Wireless 6.

WLC Wireless LAN Controller; a device used to manage wireless access points.

WMM TSPEC Wi-Fi Multimedia Traffic Specification; the QoS mechanism that enables WLAN clients to provide an indication of their bandwidth and QoS requirements so that APs can react to those requirements.

Workspaces Workspaces, such as conference rooms, lobby phones, and areas, with a device or machine account from the calling environment are another type of user in Webex.

WRED Weighted Random Early Detection; an early detection congestion avoidance mechanism that ensures high-precedence traffic has lower loss rates than other traffic during times of congestion.

X–Z

xAPI Experience API; a new specification for learning technology that makes it possible to collect data about the wide range of experiences a person has (online and offline). This API captures data in a consistent format about a person or group's activities from many technologies. Very different systems are able to securely communicate by capturing and sharing this stream of activities using xAPI's simple vocabulary.

XCP Extensible Communications Platform; a highly programmable presence and messaging platform that supports the exchange of information between applications in real time.

XML application A tool that lets you create interactive service applications with XML objects that are defined for Cisco Unified IP Phones.

XMPP Extensible Messaging and Presence Protocol; a set of open technologies for instant messaging, presence, multiparty chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of XML data.

YCbCr A color representation model used with digital video signals. Y is the luminance signal, Cb is the chroma blue signal, and Cr is the chroma red signal. Green is deduced from the three signals using an algorithm.

YPrPb A color representation model used with analog signals. Y is the luminance signal, Pr is the primary red signal, and Pb is the primary blue signal. Green is deduced from the three signals using an algorithm.

YUV A component video process, where Y represents the luminance component, and UV represents the chrominance components. The term is used for a specific analog encoding of color information in television systems.

Zoom The adjustability of a lens that creates the illusion of bringing objects closer, or increasing magnification.

This page intentionally left blank

Index

This page intentionally left blank

This part covers the following topics:

- **Appendix B, Memory Tables (Website only):** Available on the book's companion website, this exercise will provide you with the opportunity to test your knowledge of some key exam topics.
- **Appendix C, Memory Tables Answer Key (Website only):** Available on the book's companion website, this document will provide an answer key to the Memory Tables exercise.
- **Appendix D, Study Planner (Website only):** Available on the book's companion website, this spreadsheet will provide a planning sheet to prepare to take the exam.

Part XII

Online Appendices

Appendix B: Memory Tables

Appendix C: Memory Tables Answer Key

Appendix D: Study Planner

APPENDIX B

Memory Tables

Chapter 2

Table 2-2 Speed of Sound Through Four Common Mediums

Medium	Speed (Meters per Second)	Speed (Feet per Second)	Speed Factor
	344	1130	
	1480	4854	
	3400	11,152	
	6600	22,305	

Table 2-3 Audio Codecs Commonly Used by Cisco

Codec and Bit Rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Bandwidth MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G.711 (64 Kbps)	80	10	4.1	160		
G.729 (8 Kbps)	10	10	3.92	20		
G.723.1 (6.3 Kbps)	24	30	3.9	24		
G.723.1 (5.3 Kbps)	20	30	3.8	20		
G.726 (32 Kbps)	20	5	3.85	80		
G.726 (24 Kbps)	15	5		60		
G.728 (16 Kbps)	10	5	3.61	60		
G.722_64k (64 Kbps)	80	10	4.13	160		
iLBC_Mode_20 (15.2 Kbps)	38	20	4.14	38		
iLBC_Mode_30 (13.33 Kbps)	50	30	4.14	50		

Chapter 3

Table 3-2 Common Encoding Techniques Used in Digital Video Communication

CIF (Common Intermediate Format)	SIF (Source Input Format)
SQCIF = 128 × 96	N/A
QCIF = ___ × ___	QSIF = 176 × 140
SCIF – 256 × 192	SIF (NTSC/525) = ___ × ___

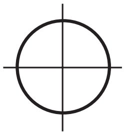
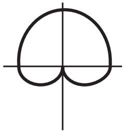
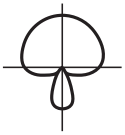
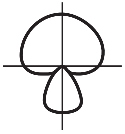
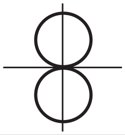
CIF (Common Intermediate Format)	SIF (Source Input Format)
CIF = ___ × ___	SIF (PAL/625) = ___ × ___
DCIF = 528 × 384	N/A
2CIF = 704 × 288	N/A
N/A	4SIF (NTSC/525) = 704 × 480
4CIF = ___ × ___	4SIF (PAL/625) = 704 × 576
16CIF = ___ × ___	16SIF = ___ × ___

Table 3-3 H.264 AVC Compared to H.265 HEVC

	H.264 AVC	H.265 HEVC
Name	MPEG 4 Part 10, AVC	MPEG-H Part 2 HEVC
Approved date	2003	2013
Progression	Successor to MPEG-2 Part	Successor to _________
Key improvement	■ ________ bit rate reduction compared with MPEG-2 Part ■ Available to deliver HD sources for Broadcast and Online	■ _________ bit rate reduction compared with H.264 at the same visual quality ■ It is likely to implement Ultra HD, 2K, 4K for Broadcast and Online (OTT)
Highest Resolution Supported		
Highest Frame Rate Supported		

Chapter 4

Table 4-2 Microphone Pickup Patterns

Polar Pattern Name	Omnidirectional	Cardioid	Supercardioid	Hypercardioid	Bidirectional
Polar Pattern					
Angle of Coverage					
Null Angle (Angle of Maximum Rejection)	N/A	180	120	108	90

Polar Pattern Name	Omnidirectional	Cardioid	Supercardioid	Hypercardioid	Bidirectional
Rear Rejection	0	23 dB	14 dB	7 dB	0
Ambient Sensitivity					
Distance Factor (in Meters)					

Chapter 5

Table 5-2 Minimum Standards for H.320 Compliance

Capability	Codec
Audio	
Video	
Data Sharing	
Control	

Table 5-3 Configurable Options for TURN on the Cisco Expressway

Field	Description	Usage Tips
TURN Services	Determines whether the Expressway offers TURN Services to traversal clients.	
TURN Requests Port	The listening port for TURN requests. The default is ____. On large VM deployments, you can configure a range of TURN request listening ports. The default range is _______.	To allow endpoints to discover TURN Services, you need to set up DNS SRV records for _turn._udp. and _turn._tcp. (either for the single port or a range of ports as appropriate). If you need to change the TURN requests port (or range, for large systems) while the TURN Services are already On, do the following: **1.** **2.** **3.** The reason is that changes to the port numbers do not take effect until the TURN Services are restarted.

Field	Description	Usage Tips
	This is the realm sent by the server in its authentication challenges.	Ensure that the client's credentials are stored in the local authentication database.
	The lower and upper port in the range used for the allocation of TURN relays. The default TURN relay media port range is _____.	

Chapter 6

Table 6-2 Cisco Telepresence Endpoint Product Portfolio

Webex Desk	Webex Room	Webex Room Kit	Webex Board

Table 6-3 Comparison of the Cisco Expressway and the Cisco VCS

Feature	Cisco Expressway	Cisco VCS
Server Components		
Registration Licensing		
Call Licensing		
Microsoft Interop License	Requires RMS licenses	Requires Option Key

Feature	Cisco Expressway	Cisco VCS
FindMe License	Available	Requires Option Key
Device Provisioning License	Requires Option Key (Free)	Requires Option Key (Free)
Clustering Capabilities	Up to 6 servers	Up to 6 servers

Table 6-4 CUWL and CUCL Licensing Model

	CUCL Essentials	CUCL Basic	CUCL Enhanced	CUWL Standard	CUWL Professional
Number of Devices Supported					Multiple
Cisco Prime Collaboration					
Jabber/IMP	Included				
Jabber UC					
Expressway Firewall Traversal					
Unity Connection			Optional		
Webex Conferencing					
PMP Basic					
PMP Advanced		N/A			

Chapter 7

Table 7-2 Cisco IP 7800 Series Phone Models and Features

Feature	7811	7821	7832	7841	7861
Screen	3.28”	3.5”	3.4”	3.5”	3.5”
Ethernet Switch	10/100	10/100	10/100	10/100/1000	10/100/1000
Line Keys					
Backlit	No	Yes	Yes	Yes	Yes
Wideband Audio	Optional	Yes	Yes	Yes	Yes
Field-Replaceable bezel	No	Yes	No	Yes	Yes
PoE					
Cloud Ready					
Power Save Plus					

Table 7-3 8800 Series Phone Models and Features

Feature	8811	8841	8851	8851NR	8861	8845	8865	8865NR
Screen	Grayscale		Color					
HD Video 720p	No							
Bluetooth	No		Yes					
Cisco Intelligent Proximity (MV)	No							
USB Ports	0	0				0		
KEM	0	0				0		
Wi-Fi	No	No						

Table 7-4 MPP Firmware Feature Support

Security	Applications	Call Control and Audio Features	Directory	Management
				Configuration: Browser Phone Auto Provision
Media encryption via SRTP		Call forwarding		
		Call hold	Intelligent search	Encrypted HTTP data in plain HTTP transmissions
Encrypted configuration files			Call history	
			Reverse address lookup in all directories	Remote generation and upload of PRT data
Password login		Call transfer		Configuration report to provisioning server
HTTPs secure provisioning		Call waiting		

Security	Applications	Call Control and Audio Features	Directory	Management
Mandatory/ Optional Secure Call		Intercom Music on Hold		

Chapter 8

Table 8-2 DX70 and DX80 Feature Differences

	DX70	DX80
Screen Resolution	____ 1920×1080	_____ 1920×1080
Multisite		
Contrast Ratio		
Wi-Fi Capable	802.11a, b, g, n	802.11a, b, g, n
EoS	August 16, 2018	January 30, 2021

Table 8-3 SX Endpoint Feature Differences

	SX10	SX20	SX80
Video Resolution			
Protocol Support			
Multisite			
Video Codec			
Display Support			
Bandwidth Support			
EoS	January 28, 2020	October 29, 2019	October 29, 2019

Table 8-4 Cisco Telepresence MX Series Feature Differences

	MX200G2	MX300G2	MX700	MX800 (Single or Dual)
Display Size	____ 1920×1080 with 1300 contrast ratio	____ 1920×1080 with 4000:1 contrast ratio	_____ 1920×1080 with 4000:1 contrast ratio	____ 1920×1080 with 4000:1 contrast ratio

	MX200G2	MX300G2	MX700	MX800 (Single or Dual)
Mounting Options	Floor stand, wheel base, table stand, wall mount			
Multisite		2+1 at 720p30 3+1 at 576p30		
Video Codec			H.265HEVC	
Camera	2.5× optical zoom (5× with digital)			
Bandwidth Support	6Mbps point-to-point or multipoint	6Mbps point-to-point or multipoint	6Mbps point-to-point 10Mbps multipoint	6Mbps point-to-point 10Mbps multipoint
EoS	May 2, 2018	May 2, 2018	April 1, 2019	April 1, 2019

Table 8-5 Webex Room Kit USB and Room Kit Mini Features

Feature	Webex Room Kit USB	Webex Room Kit Mini
Bandwidth		
Resolution		
Audio features	High-quality 20 kHz audio Automatic gain control Automatic noise reduction Active lip synchronization	
Content sharing	One HDMI input supports formats up to a maximum 4K (3840×2160) at 30 fps, including HD1080p60	H.239 and BFCP up to 3840×2160p5
Wireless sharing		
Multipoint support		
Protocols	SIP, H.323, and Webex	SIP, H.323, and Webex
Camera	_______________, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity	4K UltraHD 2× zoom, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity

Table 8-6 Webex Room Kit Features

Feature	Description
Bandwidth	
Resolution	
Audio features	High-quality 20 kHz audio Subwoofer line out Automatic gain control Automatic noise reduction Active lip synchronization
Content sharing	H.239 and BFCP up to 3840×2160p5 or 1080p30
Wireless sharing	
Multipoint support	
Protocols	SIP, H.323, and Webex
Camera	_______________, 15.1 MP image sensor, 1/1.7 CMOS, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity

Table 8-7 Webex Room Kit Plus Features

Feature	Description
Bandwidth	
Resolution	
Audio features	High-quality 20 kHz audio Subwoofer line out Prepared for inductive loop (line out) Automatic gain control Automatic noise reduction Active lip synchronization
Content sharing	H.239 and BFCP up to 3840×2160p5 or 1080p30
Wireless sharing	
Multipoint support	

Feature	Description
Protocols	SIP, H.323, and Webex
Camera	____________, 15.1 MP image sensor, 1/1.7 CMOS, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity

Table 8-8 Webex Room Kit Pro Features

Feature	Description
Bandwidth	Up to _____ point-to-point up to _____ multisite
Resolution	Up to 4K video input and output at 30 fps or 1080p60
Video inputs	__ HDMI up to 1080p60 __ HDMI up to 3840×2160p30 1 _____________ up to 1080p60
Video outputs	__ HDMI up to 3840×2160p60 __ HDMI up to 3840×2160p30
Audio features	High-quality 20 kHz audio 8 separate acoustic echo cancellers 8-port audio mixer 8 assignable equalizers Automatic gain control Automatic noise reduction Active lip synchronization
Audio inputs	___ microphones, 48V phantom powered, Euroblock connector, mic level or balanced line level 3 _____ outputs
Audio outputs	6 __________, Euroblock connector ___ HDMI outputs HDMI Input #1 supports Audio Return Channel (ARC) audio output to Cisco Webex Quad Camera 1 Line out for ________ (Cisco Webex Quad Camera)
Multipoint support	_____ up to 1080p30 _____ up to 720p30 _____ up to 720p30

Feature	Description
Network interfaces	__ Ethernet 10/100/1000 for LAN __ Ethernet 10/100/1000 for direct pairing with camera __ Ethernet 10/100/1000 with PoE, 1 dedicated for direct pairing with Touch 10

Table 8-9 Cisco Webex Board Features

	Webex Board 55s	Webex Board 70s	Webex Board 85
Display	___ LED LCD 4K	___ LED LCD 4K	___ LED LCD 4K
Camera	Fixed lens Infinite focus _____ resolution _____ horizontal field of view _____ vertical field of view	Fixed lens Infinite focus _____ resolution _____ horizontal field of view _____ vertical field of view	Fixed lens Infinite focus _____ resolution _____ horizontal field of view _____ vertical field of view
Participants	Up to ____ people	Up to ___ people	Up to ___ people
Dimensions (H×W×D)	36.2×55.7×7.5 in (919×1416×191 mm)	47.5×73.8×9.6 in (1207×1875×245 mm)	48.1×77.4×3 in (1221×1966×76 mm)
Audio Features	High-quality 20 kHz audio Acoustic echo cancellation Automatic gain control Autonoise reduction Active lip synchronization Mic array with voice tracking	High-quality 20 kHz audio Acoustic echo cancellation Automatic gain control Autonoise reduction Active lip synchronization Mic array with voice tracking	High-quality 20 kHz audio Acoustic echo cancellation Automatic gain control Autonoise reduction Active lip synchronization Mic array with voice tracking

Table 8-10 Webex Desk Series Endpoints Features

Feature	Webex Desk Mini	Webex Desk	Webex Desk Pro
Display	15-inch	24-inch	27-inch
Camera	64° horizontal field of view, 50° vertical field of view 8MP image sensor, supports up to 30 fps	64° horizontal field of view, 50° vertical field of view 8MP image sensor, supports up to 30 fps	4K Ultra HD camera 71° horizontal field of view, 59° vertical field of view 12 MP image sensor, supports up to 30 fps
Multisite	No	3-way resolution up to 1080p30 + content up to 1080p15 4-way resolution up to 720p30 + content up to 1080p15	Adaptive SIP/H.323 MultiSite: 3-way, resolution up to 1080 at 30 fps, plus content up to 4K at 15 fps 4-way, resolution up to 720 at 30 fps, plus content up to 4K at 15 fps 5-way, resolution up to 720 at 30 fps, plus content up to 4K at 10 fps
Dimensions (H×W×D)	Width: 14.6 in (37.1 cm) Height: 16.25 in (41.3 cm) Depth: 5.3 in (13.5 cm) Weight: 8.5 lb (3.9 kg)	Width: 22.2 in (56.5 cm) Height: 18.7 in (47.4 cm) Depth: 2.8 in (7.0 cm) Weight: 19.2 lb (8.7 kg)	Width: 24.8 in (63 cm) Height: 20.1 in (51 cm) Depth: 3 in (7.5 cm) without desk stand, 7.1 in (18 cm) with desk stand attached Weight: 24.4 lb (11.6 kg)
Audio features	Acoustic Echo Cancellation (AEC) Active Lip Synchronization Automatic Gain Control (AGC) Focused sound pickup	High-quality full-band audio Automatic Gain Control (AGC) AI-powered noise removal	High-quality 20 kHz audio Automatic gain control Automatic noise reduction Active lip synchronization Keyclick suppression

Feature	Webex Desk Mini	Webex Desk	Webex Desk Pro
	De-reverberation Full duplex Full-band audio Music mode Noise reduction Noise removal Optimize for my voice Self-hear Third-party integration Ultrasound technology	Active lip synchronization Focused microphone pickup Music mode	

Chapter 9

Table 9-2 Meraki Switch PoE Classifications

Class	Usage	Classification Current [mA]	Power Range [watt]	Class Description
0	Default	0–4	0.44–12.94	Classification unimplemented
		9–12	0.44–3.84	Very low power
		17–20	3.84–6.49	Low power
		26–30		
		36–44		

Table 9-3 Three PoE Types Supported on Cisco Switches

Prestandard Inline PoE	802.3af PoE	802.3at PoE+
		Backward compatible with 802.3af; PoE+ just adds an additional class of power to the 802.3af standard
		30W per port
		Relatively new; currently only Cisco is shipping PoE+ phones
Incompatible with all non-Cisco devices that accept Power over Ethernet	PoE devices are not compatible with Cisco prestandard PoE; the power negotiation process is completely different	

Prestandard Inline PoE	802.3af PoE	802.3at PoE+
	Cisco PoE switches are backward compatible with prestandard PoE	
	Enough power for most IP phones and wireless access points from all manufacturers	

Chapter 12

Table 12-2 PoE Types and Supported Power

PoE Type	PoE Power Capabilities	Example Switches
	___ Watts power	3550-24 or 48 ports
	___ Watts power (______)	3560-24 ports or 3670-48 ports
	___ Watts power (______)	2960-24 is Type 1 or Type 2
	___ Watts power (______)	4500 supports all types of PoE
	___ Watts power (______)	9000 supports all types of PoE

Table 12-3 ISR and ASR Routers and Software Options

Router Model	Software Version	Sizing Limitations (SRTP/ RTP Sessions)
ASR 900		
ASR 1000 Series		
ASR 9000 Series		
ISRv		
ISR 1000		
ISR 4000 Series		
CSR 1000v		
ISR 800 Series		
ISR 900 Series		
ISR 2900 Series	Classic IOS	Up to 200

Table 12-4 800 Series ISRs

Model	Deployment Recommendation	Top WAN Speed with Services On
860		10 Mbps
880		15 Mbps
810		15 Mbps

Model	Deployment Recommendation	Top WAN Speed with Services On
890		>20 Mbps
800M	Microbranches, industrial, Internet of Things/IoT (modular platform)	Various Cellular Data Rates

Chapter 13

Table 13-2 Traffic Classification Map

Application	Layer 3 Classification			Layer 2 Classification
	ToS/IPP	PHB	DSCP	CoS
Routing	6	CS6	48	6
Voice Only				
Voice/Video				
Telepresence Video				
Streaming Video	3	CS4	32	3
Call Signaling				
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Scavenger	1	CS1	8	1
Best Effort				

Table 13-3 QoS Value Comparison with 802.11e

Traffic Type	DSCP (PHB)	802.1p UP	802.11e UP
Voice	46 (EF)	5	
Video	34 (AF41)	4	
Voice and Video Signaling	24 (CS3)	3	

Table 13-4 Four Criterion Matches for Packet Classification

MQC Command	Description
Router(config-cmap)# **match access-group** *access-group-name*	____________________ against whose contents packets are checked to determine if they belong to the class.
Router(config-cmap)# **match input-interface** *interface-name*	____________________ as a match criterion against which packets are checked to determine if they belong to the class.
Router(config-cmap)# **match protocol** *protocol*	____________________ as a match criterion against which packets are checked to determine if they belong to the class.
Router(config-cmap)# **match fr-dlci** *dlci-number*	____________________ as a match criterion against which packets are checked to determine if they belong to the class.

Table 13-5 IOS Router Show Commands for QoS

Command	Description
Router# **show policy-map**	Displays all configured policy maps.
Router# **show policy-map** *policy-map* **class** *class-name*	Displays the configuration for the specified class of the specified policy map. Enter the policy map name and the class name.
Router# **show frame-relay pvc dlci**	
Router# **show policy-map interface** *interface-name*	When LLQ is configured, displays the configuration of classes for all policy maps.
Router# **show policy-map interface** *interface-name* **dlci**	When LLQ is configured, displays the configuration of classes for the policy map on the specified DLCI.
Router# **show policy-map interface** *interface-name*	Displays traffic statistics of all classes configured for all service policies on the specified interface, subinterface, or PVC on the interface. When a policy map has multiple instances of the same class, and this policy map is attached to an interface, the following command returns only the first instance: **show policy-map interface** *interface_name* **output class** *class-name*

Chapter 14

Table 14-2 SRV Records Needed for SIP, H.323, CUCM, and IMP

_service.	_protocol.	FQDN.	TTL	Priority	Weight	Port	Target
		cisco.com.	7200	10	10		exp1.cisco.com
		cisco.com.	7200	10	10		exp1.cisco.com
		cisco.com.	7200	10	10		exp1.cisco.com
		cisco.com.	7200	10	10		exp1.cisco.com
		cisco.com.	7200	10	10		exp1.cisco.com
		cisco.com.	7200	10	10		ucm.cisco.com
		cisco.com.	7200	10	10		imp.cisco.com

Chapter 15

Table 15-2 Average Bandwidth Consumption per Video Codec

Codec	H.261	H.263	H.264	H.265 HEVC
Bandwidth rate at 480p30				
Bandwidth rate at 720p30	N/A			
Bandwidth rate at 1080p30	N/A			

Codec	H.261	H.263	H.264	H.265 HEVC
Bandwidth rate at 1080p60	N/A	N/A		
Bandwidth rate at 4Kp60	N/A	N/A	N/A	

Chapter 16

Table 16-2 Default Application Users in the CUCM

Application User	Used by
CCMAdministrator	
CCMQRTSecureSysUser	
CCMQRTSysUser	
CCMSysUser	
IPMASecureSysUser	
IPMASysUser	
WDSecureSysUser	
WDSysUser	

Table 16-3 LDAP Directory Attribute Map

CUCM User Field	Microsoft AD	ADAM or AD LDS	Oracle DSEE and SUN	OpenLDAP and Other LDAPv3 Types
User ID	One of:	One of:	One of:	One of:
	________	________	________	________
	mail	mail	mail	mail
	employeeNumber	employeeNumber	employee-Number	employeeNumber
	telephoneNumber	telephoneNumber	telephone-Number	telephoneNumber
	userPrincipalName	userPrincipal-Name	userPrincipal-Name	userPrincipal-Name
First Name	givenName	givenName	givenName	givenName
Middle Name	One of:	One of:	initials	initials
	middleName	middleName		
	initials	initials		
Last Name	sn	sn	sn	sn
Manager ID	manager	manager	manager	manager

CUCM User Field	Microsoft AD	ADAM or AD LDS	Oracle DSEE and SUN	OpenLDAP and Other LDAPv3 Types
Mail ID	One of:	One of:	One of:	One of:
	mail	mail	mail	mail
	sAMAccountName	uid	uid	uid
objectGUID	objectGUID	objectGUID	N/A	N/A
Title	title	title	Title	title
Home Phone Number	homePhone	homePhone	Homephone	homeTelephone Number
Mobile Phone Number	mobile	mobile	Mobile	mobileTelephone Number
Directory URI	One of:	One of:	One of:	One of:
	msRTCSIP-PrimaryUserAddress	mail	mail	mail
	mail	none	none	none
	none			
Display Name	displayName	displayName	displayName	displayName

Table 16-4 Directory Number Creation Using Masks with LDAP Integration

Number in LDAP	Mask	Result
14085551234		
14085551234	+XXXXXXXXXX	
14085551234	+XXXXXXXXXXXXXXXXX	
14085551234	XXXX	
+14085551234		
+14085551234	+XXXXXXXXXXXXXXXXX	
+490100123	+XXXXXXXXXXXXXXXXX	

Chapter 18

Table 18-2 Comparison of Dial Plan Configuration Elements

Dial Plan Component	Cisco Unified Communications Manager	Cisco IOS Gateway	Cisco Expressway Series
Endpoint Addressing			

Dial Plan Component	Cisco Unified Communications Manager	Cisco IOS Gateway	Cisco Expressway Series
Call Routing and Path Selection			
Digit Manipulation			
Call Privileges			
Call Coverage			

Table 18-3 Directory URI Characters Supported

	User Portion	Domain (Host) Portion
Letters		
Special Characters		
Numbers		

Table 18-4 PSTN Calling Privilege Class Map

Calling Privilege Class (COS)	Allowed Destinations
Internal	
Local	
Long Distance	
International	

Chapter 19

Table 19-2 Call-Routing Source and Target Components

Routing Component	Description	Call-Routing Source, Target, or Both
IP Phones		
Trunks		
Gateways	A call request received from a gateway is looked up in the call-routing table.	
Translation Patterns		Both
Voicemail Ports		
Directory Numbers		
Directory URIs		
Route Patterns, SIP Route Patterns		
Call Park Numbers		

Table 19-3 Addressing Methods for Destination Numbers

Device Type	Signaling Protocol(s)	Addressing Method
IP Phones		
Gateways		
Trunks		

Table 19-4 Wildcards and Special Characters in Route Patterns

Character	Description
@	
X	
!	
?	The question mark (?) wildcard matches zero or more occurrences of the preceding digit or wildcard value.
+	
[ ]	The square bracket ([ ]) characters enclose a range of values. Only one value in the range can represent a dialed character.
-	The hyphen (-) character, used with the square brackets, denotes a range of values.
^	The circumflex (^) character, used with the square brackets, negates a range of values. Ensure that it is the first character following the opening bracket ([). Each route pattern can have only one ^ character.
.	The dot (.) character, used as a delimiter, separates the Cisco Unified Communications Manager access code from the directory number. Use this special character, with the discard digits instructions, to strip off the Cisco Unified Communications Manager access code before sending the number to an adjacent system. Each route pattern can have only one dot (.) character.
*	
#	
\+	

Chapter 20

Table 20-2 Licensing on the Cisco VCS Compared to the Expressway Series

	VCS Control	VCS Expressway	Expressway Core	Expressway Edge
Registration Licenses				

	VCS Control	VCS Expressway	Expressway Core	Expressway Edge
Calling Licenses				
FindMe	FindMe Option Key	FindMe Option Key	FindMe Option Key	FindMe Option Key
Microsoft Interop	Microsoft Interop Option Key	Microsoft Interop Option Key		
Device Provisioning	Device Provisioning Option Key	Device Provisioning Option Key	Device Provisioning Option Key	Device Provisioning Option Key
Cloud Call Connectors	Installed from Webex Cloud Management Portal	Installed from Webex Cloud Management Portal	Installed from Webex Cloud Management Portal	Installed from Webex Cloud Management Portal

Chapter 21

Table 21-2 Public DNS SRV Records for Expressway-E Cluster

Service	Protocol	Domains	Priority	Weight	Port	Target
		Cisco.com	10	10		Exp-e1.cisco.com
		Cisco.com	10	10		Exp-e2.cisco.com
		Cisco.com	10	10		Exp-e1.cisco.com
		Cisco.com	10	10		Exp-e2.cisco.com

Table 21-3 Private DNS SRV Records for CUCM and CUCM IMP Clusters

Service	Protocol	Domains	Priority	Weight	Port	Target
		Cisco.com	10	10		cucm1.cisco.com
		Cisco.com	10	10		cucm2.cisco.com
		Cisco.com	10	10		imp1.cisco.com
		Cisco.com	10	10		imp2.cisco.com

Table 21-4 Certificate Pairs Used in an MRA Deployment

Certificate Type	Core	Edge	Required
Public or enterprise CA certificate chain used to sign Expressway Core certificate			
Public or enterprise CA certificate chain used to sign Expressway Edge certificate			

Certificate Type	Core	Edge	Required
CUCM Tomcat certificates or CA chain			
CUCM CallManager certificates or CA chain			
IMP Tomcat certificate or CA chain			
CUCM CAPF certificates			

Table 21-5 Classes of Certificates on Cisco Collaboration Servers

Options	Types			Support Info
	DV	OV	EV	
Single Host/Domain	Yes			Supported on all Cisco Collaboration servers
UCC/Multiple SAN/Cert		Yes		
Multiple Subdomain Wildcard Cert				

Chapter 23

Table 23-2 Cisco Unified IP Phones Supported in Webex Control Hub

Phone Model	Phone Type	Cisco Unified Communications Manager Registration	Webex Control Hub Registration
6821, 6825, 6841, 6851, 6861, 6871	VoIP Phones	No	Yes
7811, 7821, 7841, 7861	VoIP Phones	Yes	Yes
8811, 8841, 8861	VoIP Phones	Yes	Yes
8845, 8865, 8865NR, 8875	Video Phones	Yes	Yes
7832, 8832, Webex Room Phone	Conference Phones	Yes	Yes
8821-EX, Cisco Wireless Phone 840, Cisco Wireless Phone 860	Wireless Phones	Yes	Yes

Chapter 26

Table 26-2 Firewall and NAT Traversal Port, IP Addresses, and Protocols

Purpose	Source IP	Source Ports	Protocol	Destination IP	Destination Ports
SIP Signaling	Webex Calling facing interface of Local Gateway	8000–65535	TCP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25	8934

Purpose	Source IP	Source Ports	Protocol	Destination IP	Destination Ports
RTP Media	Webex Calling facing interface of Local Gateway	8000–48000	UDP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25	19560–65535

Table 26-4 Cisco IOS XE Commands for Local Gateway Registration

Task	Command Syntax
This command will download a signed CA root bundle to create a trust point using TLS version 1.2 in the router.	`crypto pki trustpool import clean url`

These commands establish communication with Webex Control Hub for registration of the local gateway.	`voice class Tenant 200`
	`registrar dns:XXXXXX scheme sips expires 240 refresh-ratio 50 tcp tls`
	`credentials number XXXXXX username XXXXXX password 0 XXXXXX realm BroadWorks`
	`authentication username XXXXXX password 0 XXXXXX realm BroadWorks`
	`authentication username XXXXXX password 0 XXXXXX realm XXXXXX`
	`no remote-party-id  sip-server dns:XXXXXX  connection-reuse`
	`srtp-crypto 200  session transport tcp tls  url sips  error-passthru asserted-id pai`
	`bind control source-interface GigabitEthernet1`
	`bind media source-interface GigabitEthernet1`
	`no pass-thru content custom-sdp`
	`sip-profiles 200`
	`outbound-proxy dns:XXXXXX  privacy-policy passthru`

Task	Command Syntax

Configure the following SIP profile required to convert SIPS URIs back to SIP, as Webex Calling does not support SIPS URIs in the request/response messages (but needs them for SRV query; for example, **_sips._tcp.<outbound-proxy>**).
rule 20 modifies the From header to include the **Trunk Group OTG/DTG** parameter from Control Hub to uniquely identify a LGW site within an enterprise. Make sure you replace that with your **Trunk Group OTG/DTG** information.
	`voice class sip profiles 200`
	`rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"`
	`  rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"`
	`  rule 11 request ANY sip-header From modify "<sips:" "<sip:\1"`
	`  rule 12 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"`
	`  rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"`
	`  rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"`
	`  rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"`
	`  rule 20 request ANY sip-header From modify ">" ";otg=XXXXXX>”`
	`  rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"`

Table 26-5 Cisco IOS XE Commands for Inbound Calls from Cisco UBE

Task	Command Syntax

These commands are needed to route calls from Cisco UBE to Cisco Unified Communications Manager destined for Webex Control Hub registered devices.	`voice class uri 100 sip`
	` host <PSTN IP address>`
	
	`dial-peer voice 100 voip`
	` description Inbound dialpeer from PSTN`
	` incoming uri via 100`
	` destination dpg 302`
	
	`voice class dpg 302`
	` dial-peer 305 preference 1`
	` dial-peer 307 preference 1`

Task	Command Syntax
	voice class server-group 305 ipv4 <cucm-node-1> ipv4 <cucm-node-5> voice class server-group 307 ipv4 <cucm-node-6> ipv4 <cucm-node-7> dial-peer voice 305 voip description Outgoing dial-peer to CUCM for inbound from PSTN – 1st 5 destination-pattern .T session server-group 305 dial-peer voice 307 voip description Outgoing dial-peer to CUCM for inbound from PSTN– 2nd 5 destination-pattern .T **session server-group 307**

Table 26-6 Cisco IOS XE Commands for Inbound Calls to Local Gateway

Task	Command Syntax
These are the commands Local Gateway will use to route calls from Cisco Unified Communications Manager to Webex Control Hub.	voice class uri 300 sip pattern <cucm-nodes-ip-address and port-regex-for-dcloud> ex: pattern 10\.1\.2\..*:5065 matches 10.1.2.X:5065 range

Task	Command Syntax
	dial-peer voice 300 voip description Incoming dial-peer from CUCM for dcloud incoming uri via 300 destination dpg 200 voice class dpg 200 dial-peer 201 preference 1 dial-peer voice 201 voip description Outgoing dial-peer to BroadCloud destination-pattern .T **session-target sip-server**

Table 26-7 Cisco IOS XE Commands for Outbound Calls from Local Gateway

Task	Command Syntax
These are the commands Local Gateway will use to route calls from Webex Control Hub to Cisco Unified Communications Manager.	voice class uri 200 sip pattern :8934 dial-peer voice 200 voip description Incoming dial-peer from Webex incoming uri via 200 destination dpg 300 voice class dpg 300 dial-peer 301 preference 1 dial-peer 303 preference 1 voice class server-group 301 ipv4 <cucm-node-1> port 5065 ipv4 <cucm-node-5> port 5065

Task	Command Syntax

	`voice class server-group 303`
	`ipv4 <cucm-node-6> port 5065`
	`ipv4 <cucm-node-7> port 5065`
	
	`dial-peer voice 301 voip`
	`description Outgoing dial-peer to CUCM for inbound from`
	`Webex – 1st 5`
	`destination-pattern .T`
	`session server-group 301`
	
	`dial-peer voice 303 voip`
	`description Outgoing dial-peer to CUCM for inbound from`
	`Webex – 2nd 5`
	`destination-pattern .T`
	`session server-group 303`

Table 26-8 Cisco IOS XE Commands for Outbound Calls to Cisco UBE

Task	Command Syntax

These commands are used to route calls from Cisco Unified Communications Manager to Cisco UBE destined for the PSTN.	`voice class uri 302 sip`
	`pattern <cucm-nodes-ip-address and port-regex-for-pstn>`
	`ex:  pattern 10\.1\.2\..*:5060 matches 10.1.2.X:5060`
	`range`
	
	`dial-peer voice 302 voip`
	`description Incoming dial-peer from CUCM for pstn`
	`incoming uri via 302`
	`destination dpg 100`

Task	Command Syntax

	`voice class dpg 100`
	` dial-peer 101 preference 1`
	
	`dial-peer voice 101 voip`
	` description Outgoing dial-peer to PSTN`
	` destination-pattern .T`
	` session target ipv4:<pstn ip address>`

Chapter 29

Table 29-2 Comparison of Calls Through Cisco Unified Communications Manager and Calls/Meetings Through the Cloud

Calls Through Cisco Unified Communications Manager Environment	Calls and Meetings Through Webex Cloud
Calls initiated directly from a 1:1 space or from a contact card in the Webex App.	Ad hoc meetings from a group space in the Webex App.
Searching and then calling a user in the Webex App.	Using the Join button in the Webex App to join an ad hoc or scheduled meeting.
Dialing directory numbers or PSTN numbers from the Call button in the Webex App.	Dialing on-premises Directory URIs from the Call button in the Webex App. (Depends on the Cisco Unified Communications Manager SIP Address Routing setting in Control Hub.)
Desk phone control (DPC) calls. (For outgoing calls, dial a directory or PSTN number in the Webex App and take the call on the Cisco Unified Communications Manager device; for incoming calls, answer the call in Webex App and take the call on the device.)	Joining a meeting while paired through Room, Desk, or Board devices.
	One-to-one calls that are placed directly in the Webex App to a free user in the consumer organization, to a user in another organization, or to a user in the same organization who doesn't have a directory number. (Numbers are not shared across organizations, so they don't appear in contact cards.) These are classified as a call on Webex App.

Table 29-3 Device Name Format for Soft Phone Devices

Device Type	Required Format
Cisco Unified Client Services Framework	Valid characters: a–z, A–Z, 0–9. 15-character limit.
Cisco Dual Mode for iPhone	The device name must begin with *TCT*. For example, if you create a TCT device for the user Tanya Adams, whose username is tadams, enter **TCTTADAMS**. Must be uppercase. Valid characters: A–Z, 0–9, period (.), underscore (_), and hyphen (-). 15-character limit.
Cisco Jabber for Tablet	The device name must begin with *TAB*. For example, if you create a TAB device for the user Tanya Adams, whose username is tadams, enter **TABTADAMS**. Must be uppercase. Valid characters: A–Z, 0–9, period (.), underscore (_), and hyphen (-). 15-character limit. For Android, Webex App identifies devices with displays that are 600dp or greater as a tablet.
Cisco Dual Mode for Android	The device name must begin with *BOT*. For example, if you create a BOT device for the user Tanya Adams, whose username is tadams, enter **BOTTADAMS**. Must be uppercase. Valid characters: A–Z, 0–9, period (.), underscore (_), and hyphen (-). 15-character limit. For Android, Webex App identifies devices with displays that are less than 600dp as a phone.

Chapter 30

Table 30-2 Common Endpoint Call Setup Issues and Probable Causes

Call Setup Issue	Probable Causes
Reorder tone during and at the end of dialing	
No ring-back tone	
Unexpected second dial tone	
Video is not set up, only audio	
Dead air is heard	
One-way audio or video	
Call is dropped after dialed	
Call is dropped in the middle of the call	

Table 30-3 Major Elements Influencing Media Quality in a Cisco Collaboration Solution

Element	Description
Input video peripherals	
Video codec	
Output video peripherals	
Amount of video information	
Network QoS	
Correct bandwidth provisioned	
CPU utilization	

Table 30-4 Common Call Setup Issues on Cisco Jabber

Issue	Possible Causes
No calls possible	
No audio (softphone mode)	
One-way audio or video (softphone mode)	
Poor audio quality	
Incoming video is black (permanent)	
Incoming video is black (transient)	

Chapter 31

Table 31-2 CDR and CMR Service Parameters on the CUCM

Service Parameter	Description
	This parameter determines whether CDRs are generated. Valid values specify True (CDRs are generated) or False (CDRs are not generated). For this required field, the default value specifies False. Enable this parameter on all servers.
	This parameter enables or disables the logging of CDRs for calls that never connected or that lasted less than one second. Cisco CallManager logs unsuccessful calls (calls that result in reorder, such as might occur due to a forwarding directive failure or calls that attempt to go through a busy trunk) regardless of this flag. This is a required field with a default value of False.
	Three settings can be configured under this menu option: ■ ________________________________: Generates CMRs only when the CDR Enabled Flag service parameter is set to True. ■ ________________________________: Generates CMRs without regard to the setting in the CDR Enabled Flag service parameter. This parameter represents a required field. ■ The default value specifies __________, which will not generate CMRs.

Service Parameter	Description
	This parameter determines whether the forced authorization codes (FAC) associated with the call display in the CDR. Valid values specify True (display authorization code in CDRs) or False (do not display authorization code in CDRs) for this required field. The default value specifies False.
	This parameter determines whether the finalCalledPartyNumber field in the CDRs shows the directory number of the line group member who answers the call or the hunt pilot directory number. Valid values specify True (the finalCalledPartyNumber in CDRs will show the directory number of the phone that answered the call) or False (the finalCalledPartyNumber in CDRs will show the hunt pilot directory number). This parameter applies only to basic calls that are routed through a hunt list without future interactions, such as transfers, conference, and call park. If a feature is involved in the call, the hunt pilot directory number will show in the finalCalledPartyNumber field regardless of the setting in this parameter. The default value for this required field specifies False.
	This parameter determines whether CUCM adds the incoming prefix (as specified in the National Number Prefix, International Number Prefix, Subscriber Number Prefix, and Unknown Number Prefix Service Parameters) to the calling party number in the CDRs for that call. If the prefix is applied on the inbound side of the call, it is always added to the calling party number in the CDRs for that call. This occurs even if this parameter is set to False. If the prefix is applied on the outbound side, the prefix is added to the calling party number in the CDR or CDRs for that call, only if the parameter is set to True. If the Destination of the call is a gateway, CUCM will not add the prefix to the CDRs even if this parameter is enabled. This parameter is applied on a clusterwide basis. The default value for this required field specifies False.

Table 31-3 User Reports on the CUCM

User Report	Method of Application	User Access Allowed
Bills	Individual	
Top N		

User Report	Method of Application	User Access Allowed
Cisco Unified Communications Manager Assistant (IPMA)		
		Administrators
Cisco IP Phone Service		

Table 31-4 System Reports on the CUCM

System Report	Method of Application	User Access Allowed
QoS	Detail	Administrators
		Managers and Administrators
		Administrators
		Administrators
Traffic		Administrators
		Administrators
Forced Authorization Code/Client Matter Code (FAC/CMC)		Administrators
		Administrators
		Administrators
Malicious Call Details		Administrators
Precedence Call Summary		Administrators
System Overview		Administrators
CDR Error		Administrators

Table 31-5 Device Reports on the CUCM

Device Report	Method of Application	User Access Allowed
Gateway		Administrator
		Administrator
		Administrator

Device Report	Method of Application	User Access Allowed
Route Pattern/Hunt Pilot		Administrator
		Administrator
		Administrator
		Administrator
		Administrator
Conference Bridge		Administrator
		Administrator
Voice Messaging Utilization		Administrator

Chapter 33

Table 33-2 Disaster Recovery System Components

Cisco Unified Communications Manager	Cisco IM and Presence Server	Cisco Unity Connection
Platform	Platform	Platform
Cisco License Manager	Cisco License Manager	Cisco License Manager
Trace Collection Tool	Trace Collection Tool	Trace Collection Tool
Syslog	Syslog	Syslog

Chapter 34

Table 34-2 Reports Available Through Cisco Unity Connection Serviceability

Report Name	Description of Output
	Includes the following information for every failed attempt to sign into Unity Connection by phone: ■ Name of user, alias, caller ID, and extension of user who failed to sign in ■ Date and time the failed login occurred ■ Whether the maximum number of failed sign-ins has been reached for the user

Report Name	Description of Output
	Includes the following information for each user: ■ Last name, first name, and alias ■ Information that identifies the Unity Connection or Cisco Business Edition server associated with the user ■ Billing ID, class of service, and extension ■ Whether the account is locked ■ Whether the user has enabled personal call transfer rules Includes totals for the following traffic categories: Voice Fax Email Nondelivery receipt (NDR) Delivery receipt Read receipt Hourly totals Daily totals
	Includes the following information for voice-messaging ports: ■ Name ■ Number of inbound calls handled ■ Number of outbound MWI calls handled
	■ Number of outbound AMIS calls handled ■ Number of outbound notification calls handled ■ Number of outbound TRAP calls handled ■ Total number of calls handled
	Includes the following information about the specified mailbox stores: ■ Mail database name ■ Display name ■ Server name ■ Whether access is enabled ■ Mailbox store size ■ Last error ■ Status ■ Whether the mail database can be deleted

Report Name	Description of Output
	Includes a list of the search spaces configured on the Unity Connection or Cisco Business Edition server, with an ordered list of partitions assigned to each search space. If the server is part of a digital network, also lists the search spaces and associated partition membership on every other Unity Connection location on the network.
	Includes a list of all users and their extensions in the specified partition that is configured in the Unity Connection directory. If a partition is not specified, lists all users and their extensions for all partitions that are configured in the directory.
	Includes the following information about phone logins, MWI activity, and message notifications to phone devices per user: ■ Name, extension, and class of service ■ Date and time for each activity ■ The source of each activity ■ Action completed (for example, Login, MWI On or Off, and Phone Dialout) ■ Dialout number and results (applicable only for message notifications to phone devices) ■ The number of new messages for a user at time of login
	Includes the following information about messages sent and received, per user: ■ Name, extension, and class of service ■ Date and time for each message ■ Type of message ■ Action completed (for example, new message or message saved) ■ Information on the message sender
	Includes the following information: ■ Name and display name of the list ■ Date and time the list was created (date and time are given in Greenwich Mean Time) ■ A count of the number of users included in the list ■ If the Included List Members check box is checked, includes a listing of the alias of each user who is a member of the list
	Includes user alias, number of failed login attempts for the user, credential type (a result of 4 indicates a login attempt from the Unity Connection conversation; a result of 3 indicates a login attempt from a web application), and the date and time that the account was locked. (Date and time are given in Greenwich Mean Time.)

Report Name	Description of Output
	Includes user alias and display name, and the date and time that the user account was created. (Date and time are given in Greenwich Mean Time.)
	Includes the following information for each call: ■ Name, extension, and billing ID of the user ■ Date and time that the call occurred ■ The phone number dialed ■ The result of transfer (connected, ring-no-answer (RNA), busy, or unknown)
	Includes the following information, arranged by day and by the extension of the user who placed the call: ■ Name, extension, and billing ID ■ Date and time the call was placed ■ The phone number called ■ The result of the call (connected, ring-no-answer [RNA], busy, or unknown) ■ The duration of the call in seconds
	Arranged by date and according to the name, extension, and billing ID of the user who placed the call, and includes a listing of the 24 hours of the day, with a dialout time in seconds specified for each hour span.
	Includes the following information for each call handler and use for each hour of a day: ■ Total number of calls ■ Number of times each key on the phone keypad was pressed ■ Extension ■ Invalid extension ■ Number of times the After Greeting action occurred ■ Number of times the caller hung up
	Includes detailed information about all aspects of the configuration of the Unity Connection system.
	Includes the total number of transcribed messages, failed transcriptions, and truncated transcriptions for a given user during a given time period. If the report is run for all users, then the output is broken out by user.
	Includes the total number of transcribed messages, failed transcriptions, and truncated transcriptions for the entire system during a given time period. When a message is sent to multiple recipients, the message is transcribed only once, so the transcription activity is counted only once.

Report Name	Description of Output
	(Applicable only for HTTPS Networking) Includes the following information associated with the directory objects that do not synchronize during directory synchronization: ■ Creation Date ■ Failed ObjectID ■ USN ■ Object Type ■ Location Display Name ■ HTTP(S) Link ■ Error Message

This page intentionally left blank

APPENDIX C

Memory Tables Answer Key

Chapter 2

Table 2-2 Speed of Sound Through Four Common Mediums

Medium	Speed (Meters per Second)	Speed (Feet per Second)	Speed Factor
Air	344	1130	1
Water	1480	4854	4.3
Concrete	3400	11,152	9.8
Gypsum Board	6600	22,305	19.6

Table 2-3 Audio Codecs Commonly Used by Cisco

Codec and Bit Rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Bandwidth MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G.711 (64 Kbps)	80	10	4.1	160	82.8	87.2
G.729 (8 Kbps)	10	10	3.92	20	26.8	31.2
G.723.1 (6.3 Kbps)	24	30	3.9	24	18.9	21.9
G.723.1 (5.3 Kbps)	20	30	3.8	20	17.9	20.8
G.726 (32 Kbps)	20	5	3.85	80	50.8	55.2
G.726 (24 Kbps)	15	5		60	42.8	47.2
G.728 (16 Kbps)	10	5	3.61	60	28.5	31.5
G.722_64k (64 Kbps)	80	10	4.13	160	82.8	87.2
iLBC_Mode_20 (15.2 Kbps)	38	20	4.14	38	34.0	38.4
iLBC_Mode_30 (13.33 Kbps)	50	30	4.14	50	25.867	28.8

Chapter 3

Table 3-2 Common Encoding Techniques Used in Digital Video Communication

CIF (Common Intermediate Format)	SIF (Source Input Format)
SQCIF = 128 × 96	N/A
QCIF = 176 × 144	QSIF = 176 × 140
SCIF – 256 × 192	SIF (NTSC/525) = 352 × 240

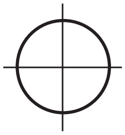
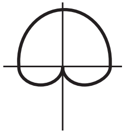
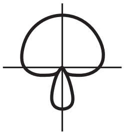
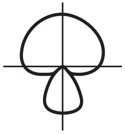
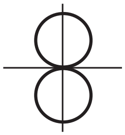
CIF (Common Intermediate Format)	SIF (Source Input Format)
CIF = 352 × 288	SIF (PAL/625) = 704 × 480
DCIF = 528 × 384	N/A
2CIF = 704 × 288	N/A
N/A	4SIF (NTSC/525) = 704 × 480
4CIF = 704 × 576	4SIF (PAL/625) = 704 × 576
16CIF = 1408 × 1152	16SIF = 1408 × 960

Table 3-3 H.264 AVC Compared to H.265 HEVC

	H.264 AVC	H.265 HEVC
Name	MPEG 4 Part 10, AVC	MPEG-H Part 2 HEVC
Approved date	2003	2013
Progression Key improvement	Successor to MPEG-2 Part ■ 40%–50% bit rate reduction compared with MPEG-2 Part ■ Available to deliver HD sources for Broadcast and Online	Successor to H.264/AVC ■ 25%–50% bit rate reduction compared with H.264 at the same visual quality ■ It is likely to implement Ultra HD, 2K, 4K for Broadcast and Online (OTT)
Highest Resolution Supported	Supports up to 4K	Supports up to 8K
Highest Frame Rate Supported	Support up to 59.94 fps only	Supports up to 300 fps

Chapter 4

Table 4-2 Microphone Pickup Patterns

Polar Pattern Name	Omnidirectional	Cardioid	Supercardioid	Hypercardioid	Bidirectional
Polar Pattern					
Angle of Coverage	360	130	112	103	90
Null Angle (Angle of Maximum Rejection)	N/A	180	120	108	90

Polar Pattern Name	Omnidirectional	Cardioid	Supercardioid	Hypercardioid	Bidirectional
Rear Rejection	0	23 dB	14 dB	7 dB	0
Ambient Sensitivity	100%	32%	26%	24%	32%
Distance Factor (in Meters)	1	1.8	1.9	2.1	1.6

Chapter 5

Table 5-2 Minimum Standards for H.320 Compliance

Capability	Codec
Audio	G.711
Video	H.261
Data Sharing	T.120
Control	H.221

Table 5-3 Configurable Options for TURN on the Cisco Expressway

Field	Description	Usage Tips
TURN Services	Determines whether the Expressway offers TURN Services to traversal clients.	
TURN Requests Port	The listening port for TURN requests. The default is 3478. On large VM deployments, you can configure a range of TURN request listening ports. The default range is 3478–3483.	To allow endpoints to discover TURN Services, you need to set up DNS SRV records for _turn._udp. and _turn._tcp. (either for the single port or a range of ports as appropriate). If you need to change the TURN requests port (or range, for large systems) while the TURN Services are already On, do the following: **1.** Change TURN Services to Off and click Save. **2.** Edit the port number/range. **3.** Change TURN Services to On and click Save. The reason is that changes to the port numbers do not take effect until the TURN Services are restarted.

Field	Description	Usage Tips
Authentication Realm	This is the realm sent by the server in its authentication challenges.	Ensure that the client's credentials are stored in the local authentication database.
Media Port Range Start/End	The lower and upper port in the range used for the allocation of TURN relays. The default TURN relay media port range is 24000–29999.	

Chapter 6

Table 6-2 Cisco Telepresence Endpoint Product Portfolio

Webex Desk	Webex Room	Webex Room Kit	Webex Board
Webex Desk Mini	Webex Room 55 Single	Webex Room Kit USB	Webex Board 55
Webex Desk	Webex Room 55 Dual	Webex Room Kit Mini	Webex Board 70
Webex Desk Pro	Webex Room 70 Single G2	Webex Room Kit	Webex Board 85
Webex Desk Camera	Webex Room 70 Dual G2	Webex Room Kit Plus	Webex Board Pro
Webex Desk Hub	Webex Room Panorama	Webex Room Kit Plus P60	
		Webex Room Kit Pro	
		Webex Room Kit Pro P60	

Table 6-3 Comparison of the Cisco Expressway and the Cisco VCS

Feature	Cisco Expressway	Cisco VCS
Server Components	Expressway Core Expressway Edge	VCS Control VCS Expressway
Registration Licensing	Included with CUCL and CUWL user licenses (Registration supported on X8.9 or later)	Device Registration Licenses required (2500 max per server)
Call Licensing	Internal and mobile calling included Rich Media Session (RMS) Licenses required for B2B and B2C calling	Nontraversal Call Licenses required Traversal Call Licenses required
Microsoft Interop License	Requires RMS licenses	Requires Option Key

Feature	Cisco Expressway	Cisco VCS
FindMe License	Available	Requires Option Key
Device Provisioning License	Requires Option Key (Free)	Requires Option Key (Free)
Clustering Capabilities	Up to 6 servers	Up to 6 servers

Table 6-4 CUWL and CUCL Licensing Model

	CUCL Essentials	CUCL Basic	CUCL Enhanced	CUWL Standard	CUWL Professional
Number of Devices Supported	One	One	One or Two	Multiple	Multiple
Cisco Prime Collaboration	Included	Included	Included	Included	Included
Jabber/IMP	Included	Included	Included	Included	Included
Jabber UC	N/A	N/A	Included	Included	Included
Expressway Firewall Traversal	N/A	N/A	Included	Included	Included
Unity Connection	Optional	Optional	Optional	Included	Included
Webex Conferencing	Optional	Optional	Optional	Optional	Included
PMP Basic	N/A	N/A	Optional	Optional	Included
PMP Advanced	N/A	N/A	Optional	Optional	Optional

Chapter 7

Table 7-2 Cisco IP 7800 Series Phone Models and Features

Feature	7811	7821	7832	7841	7861
Screen	3.28”	3.5”	3.4”	3.5”	3.5”
Ethernet Switch	10/100	10/100	10/100	10/100/1000	10/100/1000
Line Keys	1	2	1	4	16
Backlit	No	Yes	Yes	Yes	Yes
Wideband Audio	Optional	Yes	Yes	Yes	Yes
Field-Replaceable bezel	No	Yes	No	Yes	Yes
PoE	Class 1	Class 1	Class 2	Class 1	Class 1
Cloud Ready	Yes	Yes	Yes	Yes	Yes
Power Save Plus	No	Yes	No	Yes	Yes

Table 7-3 8800 Series Phone Models and Features

Feature	8811	8841	8851	8851NR	8861	8845	8865	8865NR
Screen	Grayscale	Color	Color	Color	Color	Color	Color	Color
HD Video 720p	No	No	No	No	No	Yes	Yes	Yes
Bluetooth	No	No	Yes	No	Yes	Yes	Yes	No
Cisco Intelligent Proximity (MV)	No	No	Yes	No	Yes	Yes	Yes	No
USB Ports	0	0	1	1	2	0	2	2
KEM	0	0	2	2	3	0	3	3
Wi-Fi	No	No	No	No	Yes	No	Yes	No

Table 7-4 MPP Firmware Feature Support

Security	Applications	Call Control and Audio Features	Directory	Management
802.1x authentication	Cisco XML Services Interface (XSI)	Busy Lamp Field (BLF)	Local phonebook	Configuration: Browser Phone Auto Provision
Media encryption via SRTP	UC-One Presences	Call forwarding	XML/LDAP remote directory	Auto Provision via TFTP/HTTP/HTTPs for mass deployment
Transport Layer Security (TLS)		Call hold	Intelligent search	Encrypted HTTP data in plain HTTP transmissions
Encrypted configuration files		Call pickup	Call history	Packet Capture, Problem Reporting Tool (PRT), and upload of PRT
Digest authentication		Call park	Reverse address lookup in all directories	Remote generation and upload of PRT data
Password login		Call transfer	Intelligent Proximity MV	Configuration report to provisioning server
HTTPs secure provisioning		Call waiting		

Security	Applications	Call Control and Audio Features	Directory	Management
Mandatory/ Optional Secure Call		Do Not Disturb (DND) Extension Mobility/Hot Desking Intercom Music on Hold		

Chapter 8

Table 8-2 DX70 and DX80 Feature Differences

	DX70	DX80
Screen Resolution	14″ 1920×1080	23″ 1920×1080
Multisite	No	2+1
Contrast Ratio	700:1	1000:1
Wi-Fi Capable	802.11a, b, g, n	802.11a, b, g, n
EoS	August 16, 2018	January 30, 2021

Table 8-3 SX Endpoint Feature Differences

	SX10	SX20	SX80
Video Resolution	1080p30	1080p60	1080p60
Protocol Support	SIP	SIP/H.323	SIP/H.323
Multisite	N/A	2+1 at 720p30 3+1 at 576p30	4+1 at 720p30 3+1 at 1080p30
Video Codec	H.264AVC	H.264AVC	H.265HEVC
Display Support	1	2	3
Bandwidth Support	3Mbps point-to-point	6Mbps point-to-point or multipoint	6Mbps point-to-point 10Mbps multipoint
EoS	January 28, 2020	October 29, 2019	October 29, 2019

Table 8-4 Cisco Telepresence MX Series Feature Differences

	MX200G2	MX300G2	MX700	MX800 (Single or Dual)
Display Size	42″ 1920×1080 with 1300 contrast ratio	55″ 1920×1080 with 4000:1 contrast ratio	55″ 1920×1080 with 4000:1 contrast ratio	70″ 1920×1080 with 4000:1 contrast ratio

	MX200G2	MX300G2	MX700	MX800 (Single or Dual)
Mounting Options	Floor stand, wheel base, table stand, wall mount	Floor stand, wheel base, table stand, wall mount	Floor stand, wall mount	Floor stand, wall mount
Multisite	2+1 at 720p30 3+1 at 576p30	2+1 at 720p30 3+1 at 576p30	4+1 at 720p30 3+1 at 1080p30	4+1 at 720p30 3+1 at 1080p30
Video Codec	H.264AVC	H.264AVC	H.265HEVC	H.265HEVC
Camera	2.5× optical zoom (5× with digital)	4× optical zoom (8× with digital)	20× total zoom (10× optical, 2× digital)	20× total zoom (10× optical, 2× digital)
Bandwidth Support	6Mbps point-to-point or multipoint	6Mbps point-to-point or multipoint	6Mbps point-to-point 10Mbps multipoint	6Mbps point-to-point 10Mbps multipoint
EoS	May 2, 2018	May 2, 2018	April 1, 2019	April 1, 2019

Table 8-5 Webex Room Kit USB and Room Kit Mini Features

Feature	Webex Room Kit USB	Webex Room Kit Mini
Bandwidth	Up to 6Mbps point-to-point	Up to 6Mbps point-to-point
Resolution	Live video resolutions (encode and decode) up to 1920×1080p30 and p60 (HD1080p)	Up to 4K video input and output at 30 fps or 1080p60
Audio features	High-quality 20 kHz audio Automatic gain control Automatic noise reduction Active lip synchronization	High-quality 20 kHz audio Automatic gain control Automatic noise reduction Active lip synchronization
Content sharing	One HDMI input supports formats up to a maximum 4K (3840×2160) at 30 fps, including HD1080p60	H.239 and BFCP up to 3840×2160p5
Wireless sharing	Webex app Intelligent Proximity	Webex app Intelligent Proximity
Multipoint support	No	2+1 up to 1080p30 3+1 up to 720p30
Protocols	SIP, H.323, and Webex	SIP, H.323, and Webex
Camera	4K UltraHD 2× zoom, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity	4K UltraHD 2× zoom, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity

Table 8-6 Webex Room Kit Features

Feature	Description
Bandwidth	Up to 6Mbps point-to-point
Resolution	Up to 4K video input and output at 30 fps or 1080p60
Audio features	High-quality 20 kHz audio Subwoofer line out Automatic gain control Automatic noise reduction Active lip synchronization
Content sharing	H.239 and BFCP up to 3840×2160p5 or 1080p30
Wireless sharing	Webex Teams app Webex Meetings app Intelligent Proximity
Multipoint support	2+1 up to 1080p30 3+1 up to 720p30
Protocols	SIP, H.323, and Webex
Camera	5K UltraHD 3× zoom, 15.1 MP image sensor, 1/1.7 CMOS, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity

Table 8-7 Webex Room Kit Plus Features

Feature	Description
Bandwidth	Up to 6Mbps point-to-point
Resolution	Up to 4K video input and output at 30 fps or 1080p60
Audio features	High-quality 20 kHz audio Subwoofer line out Prepared for inductive loop (line out) Automatic gain control Automatic noise reduction Active lip synchronization
Content sharing	H.239 and BFCP up to 3840×2160p5 or 1080p30
Wireless sharing	Webex Teams app Webex Meetings app Intelligent Proximity
Multipoint support	2+1 up to 1080p30 3+1 up to 720p30

Feature	Description
Protocols	SIP, H.323, and Webex
Camera	5K UltraHD 5× zoom, 15.1 MP image sensor, 1/1.7 CMOS, autoframing, autobrightness and white balance, and focus distance from 1 m to infinity

Table 8-8 Webex Room Kit Pro Features

Feature	Description
Bandwidth	Up to 6Mbps point-to-point up to 15Mbps multisite
Resolution	Up to 4K video input and output at 30 fps or 1080p60
Video inputs	2 HDMI up to 1080p60 3 HDMI up to 3840×2160p30 1 3G-SDI/HD-SDI up to 1080p60
Video outputs	2 HDMI up to 3840×2160p60 1 HDMI up to 3840×2160p30
Audio features	High-quality 20 kHz audio 8 separate acoustic echo cancellers 8-port audio mixer 8 assignable equalizers Automatic gain control Automatic noise reduction Active lip synchronization
Audio inputs	8 microphones, 48V phantom powered, Euroblock connector, mic level or balanced line level 3 HDMI outputs
Audio outputs	6 balanced line-level outputs, Euroblock connector 3 HDMI outputs HDMI Input #1 supports Audio Return Channel (ARC) audio output to Cisco Webex Quad Camera 1 Line out for Subwoofer (Cisco Webex Quad Camera)
Multipoint support	2+1 up to 1080p30 3+1 up to 720p30 4+1 up to 720p30

Feature	Description
Network interfaces	1 Ethernet 10/100/1000 for LAN 2 Ethernet 10/100/1000 for direct pairing with camera 2 Ethernet 10/100/1000 with PoE, 1 dedicated for direct pairing with Touch 10 Wi-Fi 802.11a/b/g/n/ac 2.4 GHz and 5 GHz for LAN 2×2 Multiple Input and Multiple Output (MIMO) Bluetooth 4.0 LE

Table 8-9 Cisco Webex Board Features

	Webex Board 55s	Webex Board 70s	Webex Board 85
Display	55″ LED LCD 4K	70″ LED LCD 4K	85″ LED LCD 4K
Camera	Fixed lens Infinite focus 4kp60 resolution 83° horizontal field of view 55° vertical field of view	Fixed lens Infinite focus 4kp60 resolution 83° horizontal field of view 55° vertical field of view	Fixed lens Infinite focus 4kp60 resolution 83° horizontal field of view 55° vertical field of view
Participants	Up to 5 people	Up to 7 people	Up to 14 people
Dimensions (H×W×D)	36.2×55.7×7.5 in (919×1416×191 mm)	47.5×73.8×9.6 in (1207×1875×245 mm)	48.1×77.4×3 in (1221×1966×76 mm)
Audio Features	High-quality 20 kHz audio Acoustic echo cancellation Automatic gain control Autonoise reduction Active lip synchronization Mic array with voice tracking	High-quality 20 kHz audio Acoustic echo cancellation Automatic gain control Autonoise reduction Active lip synchronization Mic array with voice tracking	High-quality 20 kHz audio Acoustic echo cancellation Automatic gain control Autonoise reduction Active lip synchronization Mic array with voice tracking

Table 8-10 Webex Desk Series Endpoints Features

Feature	Webex Desk Mini	Webex Desk	Webex Desk Pro
Display	15-inch	24-inch	27-inch
Camera	64° horizontal field of view, 50° vertical field of view 8MP image sensor, supports up to 30 fps	64° horizontal field of view, 50° vertical field of view 8MP image sensor, supports up to 30 fps	4K Ultra HD camera 71° horizontal field of view, 59° vertical field of view 12 MP image sensor, supports up to 30 fps
Multisite	No	3-way resolution up to 1080p30 + content up to 1080p15 4-way resolution up to 720p30 + content up to 1080p15	Adaptive SIP/H.323 MultiSite: 3-way, resolution up to 1080 at 30 fps, plus content up to 4K at 15 fps 4-way, resolution up to 720 at 30 fps, plus content up to 4K at 15 fps 5-way, resolution up to 720 at 30 fps, plus content up to 4K at 10 fps
Dimensions (H×W×D)	Width: 14.6 in (37.1 cm) Height: 16.25 in (41.3 cm) Depth: 5.3 in (13.5 cm) Weight: 8.5 lb (3.9 kg)	Width: 22.2 in (56.5 cm) Height: 18.7 in (47.4 cm) Depth: 2.8 in (7.0 cm) Weight: 19.2 lb (8.7 kg)	Width: 24.8 in (63 cm) Height: 20.1 in (51 cm) Depth: 3 in (7.5 cm) without desk stand, 7.1 in (18 cm) with desk stand attached Weight: 24.4 lb (11.6 kg)
Audio features	Acoustic Echo Cancellation (AEC) Active Lip Synchronization Automatic Gain Control (AGC) Focused sound pickup	High-quality full-band audio Automatic Gain Control (AGC) AI-powered noise removal	High-quality 20 kHz audio Automatic gain control Automatic noise reduction Active lip synchronization Keyclick suppression

Feature	Webex Desk Mini	Webex Desk	Webex Desk Pro
	De-reverberation Full duplex Full-band audio Music mode Noise reduction Noise removal Optimize for my voice Self-hear Third-party integration Ultrasound technology	Active lip synchronization Focused microphone pickup Music mode	

Chapter 9

Table 9-2 Meraki Switch PoE Classifications

Class	Usage	Classification Current [mA]	Power Range [watt]	Class Description
0	Default	0–4	0.44–12.94	Classification unimplemented
1	Optional	9–12	0.44–3.84	Very low power
2	Optional	17–20	3.84–6.49	Low power
3	Optional	26–30	6.49–12.95	Mid power
4	Valid for 802.3at (Type 2) devices, not allowed for 802.3af devices	36–44	12.95–25.50	High power

Table 9-3 Three PoE Types Supported on Cisco Switches

Prestandard Inline PoE	802.3af PoE	802.3at PoE+
Cisco Proprietary	IEEE standard	Backward compatible with 802.3af; PoE+ just adds an additional class of power to the 802.3af standard
10/100 only	15.4W per port	30W per port
7W per port	Compatible with Gigabit Ethernet	Relatively new; currently only Cisco is shipping PoE+ phones
Incompatible with all non-Cisco devices that accept Power over Ethernet	PoE devices are not compatible with Cisco prestandard PoE; the power negotiation process is completely different	

Prestandard Inline PoE	802.3af PoE	802.3at PoE+
	Cisco PoE switches are backward compatible with prestandard PoE	
	Enough power for most IP phones and wireless access points from all manufacturers	

Chapter 12

Table 12-2 PoE Types and Supported Power

PoE Type	PoE Power Capabilities	Example Switches
Pre-Standard Inline Power	6.3 Watts power	3550-24 or 48 ports
802.3af PoE	15.4 Watts power (Type 1)	3560-24 ports or 3670-48 ports
802.3at PoE	30 Watts power (Type 2)	2960-24 is Type 1 or Type 2
	60 Watts power (Type 3)	4500 supports all types of PoE
	100 Watts power (Type 4)	9000 supports all types of PoE

Table 12-3 ISR and ASR Routers and Software Options

Router Model	Software Version	Sizing Limitations (SRTP/RTP Sessions)
ASR 900	IOS XE	Unknown
ASR 1000 Series	IOS XE	Unknown
ASR 9000 Series	IOS XR	Unknown
ISRv	IOS XE	Up to 1000
ISR 1000	IOS XE	75 to 100
ISR 4000 Series	IOS XE	40 to 1500
CSR 1000v	IOS XE	225 to 800 (1 or 4 vCPU)
ISR 800 Series	Classic IOS	20
ISR 900 Series	Classic IOS	50
ISR 2900 Series	Classic IOS	Up to 200

Table 12-4 800 Series ISRs

Model	Deployment Recommendation	Top WAN Speed with Services On
860	Home or small offices with up to 10 users	10 Mbps
880	Remote workers, small offices, and branch locations with up to 20 users	15 Mbps
810	Machine-to-machine and device-to-device deployments such as ATMs, point-of-sale, kiosks, vending machines (fixed platform)	15 Mbps

Model	Deployment Recommendation	Top WAN Speed with Services On
890	Enterprise remote offices with up to 50 users	>20 Mbps
800M	Microbranches, industrial, Internet of Things/IoT (modular platform)	Various Cellular Data Rates

Chapter 13

Table 13-2 Traffic Classification Map

Application	Layer 3 Classification			Layer 2 Classification
	ToS/IPP	PHB	DSCP	CoS
Routing	6	CS6	48	6
Voice Only	5	EF	46	5
Voice/Video	4	AF41	34	4
Telepresence Video	4	CS4	32	4
Streaming Video	3	CS4	32	3
Call Signaling	3	CS3	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Scavenger	1	CS1	8	1
Best Effort	0	0	0	0

Table 13-3 QoS Value Comparison with 802.11e

Traffic Type	DSCP (PHB)	802.1p UP	802.11e UP
Voice	46 (EF)	5	6
Video	34 (AF41)	4	5
Voice and Video Signaling	24 (CS3)	3	4

Table 13-4 Four Criterion Matches for Packet Classification

MQC Command	Description
Router(config-cmap)# **match access-group** *access-group-name*	Specifies the name of the access control list (ACL) against whose contents packets are checked to determine if they belong to the class.
Router(config-cmap)# **match input-interface** *interface-name*	Specifies the name of the input interface used as a match criterion against which packets are checked to determine if they belong to the class.
Router(config-cmap)# **match protocol** *protocol*	Specifies the name of the protocol used as a match criterion against which packets are checked to determine if they belong to the class.
Router(config-cmap)# **match fr-dlci** *dlci-number*	Specifies the Frame Relay DLCI number as a match criterion against which packets are checked to determine if they belong to the class.

Table 13-5 IOS Router Show Commands for QoS

Command	Description
Router# **show policy-map**	Displays all configured policy maps.
Router# **show policy-map** *policy-map* **class** *class-name*	Displays the configuration for the specified class of the specified policy map. Enter the policy map name and the class name.
Router# **show frame-relay pvc dlci**	Displays statistics about the PVC and the configuration of classes for the policy map on the specified data-link connection identifier (DLCI).
Router# **show policy-map interface** *interface-name*	When LLQ is configured, displays the configuration of classes for all policy maps.
Router# **show policy-map interface** *interface-name* **dlci**	When LLQ is configured, displays the configuration of classes for the policy map on the specified DLCI.
Router# **show policy-map interface** *interface-name*	Displays traffic statistics of all classes configured for all service policies on the specified interface, subinterface, or PVC on the interface. When a policy map has multiple instances of the same class, and this policy map is attached to an interface, the following command returns only the first instance: **show policy-map interface** *interface_name* **output class** *class-name*

Chapter 14

Table 14-2 SRV Records Needed for SIP, H.323, CUCM, and IMP

_service.	_protocol.	FQDN.	TTL	Priority	Weight	Port	Target
_sips.	_tcp.	cisco.com.	7200	10	10	5061	exp1.cisco.com
_sip.	_tcp.	cisco.com.	7200	10	10	5060	exp1.cisco.com
_sip.	_udp.	cisco.com.	7200	10	10	5060	exp1.cisco.com
_h323ls.	_udp.	cisco.com.	7200	10	10	1719	exp1.cisco.com
_h323cs.	_tcp.	cisco.com.	7200	10	10	1720	exp1.cisco.com
_cisco-uds.	_tcp.	cisco.com.	7200	10	10	8443	ucm.cisco.com
_cuplogin.	_tcp.	cisco.com.	7200	10	10	8443	imp.cisco.com

Chapter 15

Table 15-2 Average Bandwidth Consumption per Video Codec

Codec	H.261	H.263	H.264	H.265 HEVC
Bandwidth rate at 480p30	512 kbps	384 kbps	256 kbps	128 kbps
Bandwidth rate at 720p30	N/A	1024 kbps	768 kbps	384 kbps
Bandwidth rate at 1080p30	N/A	1536 kbps	1024 kbps	512 kbps

Codec	H.261	H.263	H.264	H.265 HEVC
Bandwidth rate at 1080p60	N/A	N/A	2048 kbps	1024 kbps
Bandwidth rate at 4Kp60	N/A	N/A	N/A	2048 kbps

Chapter 16

Table 16-2 Default Application Users in the CUCM

Application User	Used by
CCMAdministrator	Unified CM Administration (default "super user")
CCMQRTSecureSysUser	Cisco Quality Reporting Tool
CCMQRTSysUser	Cisco Quality Reporting Tool
CCMSysUser	Cisco Extension Mobility
IPMASecureSysUser	Cisco Unified Communications Manager Assistant
IPMASysUser	Cisco Unified Communications Manager Assistant
WDSecureSysUser	Cisco WebDialer
WDSysUser	Cisco WebDialer

Table 16-3 LDAP Directory Attribute Map

CUCM User Field	Microsoft AD	ADAM or AD LDS	Oracle DSEE and SUN	OpenLDAP and Other LDAPv3 Types
User ID	One of:	One of:	One of:	One of:
	sAMAccountName	uid	uid	uid
	mail	mail	mail	mail
	employeeNumber	employeeNumber	employeeNumber	employeeNumber
	telephoneNumber	telephoneNumber	telephoneNumber	telephoneNumber
	userPrincipalName	userPrincipal-Name	userPrincipal-Name	userPrincipal-Name
First Name	givenName	givenName	givenName	givenName
Middle Name	One of:	One of:	initials	initials
	middleName	middleName		
	initials	initials		
Last Name	sn	sn	sn	sn
Manager ID	manager	manager	manager	manager

CUCM User Field	Microsoft AD	ADAM or AD LDS	Oracle DSEE and SUN	OpenLDAP and Other LDAPv3 Types
Mail ID	One of:	One of:	One of:	One of:
	mail	mail	mail	mail
	sAMAccountName	uid	uid	uid
objectGUID	objectGUID	objectGUID	N/A	N/A
Title	title	title	Title	title
Home Phone Number	homePhone	homePhone	Homephone	homeTelephone Number
Mobile Phone Number	mobile	mobile	Mobile	mobileTelephone Number
Directory URI	One of:	One of:	One of:	One of:
	msRTCSIP-PrimaryUserAddress	mail	mail	mail
	mail	none	none	none
	none			
Display Name	displayName	displayName	displayName	displayName

Table 16-4 Directory Number Creation Using Masks with LDAP Integration

Number in LDAP	Mask	Result
14085551234		14085551234
14085551234	+XXXXXXXXXX	+14085551234
14085551234	+XXXXXXXXXXXXXXXXX	+14085551234
14085551234	XXXX	1234
+14085551234		+14085551234
+14085551234	+XXXXXXXXXXXXXXXXX	+14085551234
+490100123	+XXXXXXXXXXXXXXXXX	+490100123

Chapter 18

Table 18-2 Comparison of Dial Plan Configuration Elements

Dial Plan Component	Cisco Unified Communications Manager	Cisco IOS Gateway	Cisco Expressway Series
Endpoint Addressing	Directory Number, Directory URI	ephone-dn, voice register pool	IP Address, H.323 ID, E.164 Alias, Directory URI, Service Prefix

Dial Plan Component	Cisco Unified Communications Manager	Cisco IOS Gateway	Cisco Expressway Series
Call Routing and Path Selection	Route Patterns, SIP Route Patterns, Route Groups, Route Lists, Trunks	Dial Peers	Search Rules, Zones
Digit Manipulation	Translation Patterns, Transformation Patterns, Route Patterns	Voice Translation Profiles and Rules, Dial Peer Settings	Transforms, Call Policy, FindMe
Call Privileges	Partitions, Calling Search Spaces, ToD	COR	Call Policy
Call Coverage	Hunt Pilots, Line Groups, Hunt Lists, Shared Lines, Call Forward settings	Dial Peers, Hunt Groups, Call Applications	FindMe

Table 18-3 Directory URI Characters Supported

	User Portion	Domain (Host) Portion
Letters	a–z, A–Z	a–z, A–Z
Special Characters	! $ % & * _ + ~ - = \ ? ’ , . /	- .
Numbers	0–9	0–9

Table 18-4 PSTN Calling Privilege Class Map

Calling Privilege Class (COS)	Allowed Destinations
Internal	Internal Emergency
Local	Internal Emergency Local PSTN
Long Distance	Internal Emergency Local PSTN Long-Distance PSTN
International	Internal Emergency Local PSTN Long-Distance PSTN International PSTN

Chapter 19

Table 19-2 Call-Routing Source and Target Components

Routing Component	Description	Call-Routing Source, Target, or Both
IP Phones	A number dialed by an IP phone is looked up in the call-routing table.	Source
Trunks	A call request received through a trunk is looked up in the call-routing table.	Source
Gateways	A call request received from a gateway is looked up in the call-routing table.	Source
Translation Patterns	After a translation pattern is best matched (as a target of a call-routing table lookup), the transformed number is looked up again in the call-routing table. The entry that generates this lookup is the translation pattern.	Both
Voicemail Ports	A voicemail system can be configured to allow calling of other extensions or PSTN numbers (such as the mobile phone of an employee). In these cases, the call-routing request is received from the voicemail port of the CUCM.	Both
Directory Numbers	Assigned to endpoints.	Target
Directory URIs	Assigned to directory numbers.	Target
Route Patterns, SIP Route Patterns	Used to route calls to off-net destinations (via a gateway) or to other CUCM clusters via a trunk.	Target
Call Park Numbers	Allows a call on hold to be sent to a number and retrieved from another phone by dialing that number.	Target

Table 19-3 Addressing Methods for Destination Numbers

Device Type	Signaling Protocol(s)	Addressing Method
IP Phones	SCCP	Digit-by-digit analysis
		En bloc (not on type-A phones)
	SIP	En bloc
		KPML (not on type-A phones)
		SIP dial rules
Gateways	MGCP, SIP, H.323	En bloc
		Overlap sending and receiving
Trunks	SIP, H.323	En bloc
		Overlap sending and receiving

Table 19-4 Wildcards and Special Characters in Route Patterns

Character	Description
@	The at symbol (@) wildcard matches all National Numbering Plan numbers. Each route pattern can have only one @ wildcard.
X	The X wildcard matches any single digit in the range 0 through 9.
!	The exclamation point (!) wildcard matches one or more digits in the range 0 through 9.
?	The question mark (?) wildcard matches zero or more occurrences of the preceding digit or wildcard value.
+	The plus sign (+) wildcard matches one or more occurrences of the preceding digit or wildcard value.
[ ]	The square bracket ([ ]) characters enclose a range of values. Only one value in the range can represent a dialed character.
-	The hyphen (-) character, used with the square brackets, denotes a range of values.
^	The circumflex (^) character, used with the square brackets, negates a range of values. Ensure that it is the first character following the opening bracket ([). Each route pattern can have only one ^ character.
.	The dot (.) character, used as a delimiter, separates the Cisco Unified Communications Manager access code from the directory number. Use this special character, with the discard digits instructions, to strip off the Cisco Unified Communications Manager access code before sending the number to an adjacent system. Each route pattern can have only one dot (.) character.
*	The asterisk (*) character can provide an extra digit for special dialed numbers.
#	The octothorpe (#) character, often called the pound sign, generally identifies the end of the dialing sequence. Ensure the # character is the last character in the pattern.
\+	A plus sign preceded by a backslash, that is, \+, indicates that you want to configure the international escape character +. Using \+ means that the international escape character + is used as a dialable digit, not as a wildcard.

Chapter 20

Table 20-2 Licensing on the Cisco VCS Compared to the Expressway Series

	VCS Control	VCS Expressway	Expressway Core	Expressway Edge
Registration Licenses	SIP/H.323 Registration	SIP/H.323 Registration	SIP.H.323 Device Registration Room Registration	SIP.H.323 Device Registration Room Registration SIP Proxy Registration Only

	VCS Control	VCS Expressway	Expressway Core	Expressway Edge
Calling Licenses	Non-Traversal Call Licenses	Non-Traversal Call Licenses	Local Call Licenses Included	Local Call Licenses Included
	Traversal Call Licenses	Traversal Call Licenses	RMS Licenses for B2B and B2C Calls	RMS Licenses for B2B and B2C Calls
FindMe	FindMe Option Key	FindMe Option Key	FindMe Option Key	FindMe Option Key
Microsoft Interop	Microsoft Interop Option Key	Microsoft Interop Option Key	Microsoft Interop Included with RMS	Microsoft Interop Included with RMS
Device Provisioning	Device Provisioning Option Key	Device Provisioning Option Key	Device Provisioning Option Key	Device Provisioning Option Key
Cloud Call Connectors	Installed from Webex Cloud Management Portal	Installed from Webex Cloud Management Portal	Installed from Webex Cloud Management Portal	Installed from Webex Cloud Management Portal

Chapter 21

Table 21-2 Public DNS SRV Records for Expressway-E Cluster

Service	Protocol	Domains	Priority	Weight	Port	Target
_Collab-edge.	_tls.	Cisco.com	10	10	8443	Exp-e1.cisco.com
_Collab-edge.	_tls.	Cisco.com	10	10	8443	Exp-e2.cisco.com
_sips.	_tcp.	Cisco.com	10	10	5061	Exp-e1.cisco.com
_sips.	_tcp.	Cisco.com	10	10	5061	Exp-e2.cisco.com

Table 21-3 Private DNS SRV Records for CUCM and CUCM IMP Clusters

Service	Protocol	Domains	Priority	Weight	Port	Target
_cisco-uds.	_tcp.	Cisco.com	10	10	8443	cucm1.cisco.com
_cisco-uds.	_tcp.	Cisco.com	10	10	8443	cucm2.cisco.com
_cuplogin.	_tcp.	Cisco.com	10	10	5061	imp1.cisco.com
_cuplogin.	_tcp.	Cisco.com	10	10	5061	imp2.cisco.com

Table 21-4 Certificate Pairs Used in an MRA Deployment

Certificate Type	Core	Edge	Required
Public or enterprise CA certificate chain used to sign Expressway Core certificate	Yes	Yes	Yes
Public or enterprise CA certificate chain used to sign Expressway Edge certificate	Yes	Yes	Yes

Certificate Type	Core	Edge	Required
CUCM Tomcat certificates or CA chain	Yes	No	No
CUCM CallManager certificates or CA chain	Yes	No	No
IMP Tomcat certificate or CA chain	Yes	No	No
CUCM CAPF certificates	No	Yes	No

Table 21-5 Classes of Certificates on Cisco Collaboration Servers

Options	Types			Support Info
	DV	OV	EV	
Single Host/Domain	Yes	Yes	Yes	Supported on all Cisco Collaboration servers
UCC/Multiple SAN/Cert	Yes	Yes	Yes	Supported on all Cisco Collaboration servers
Multiple Subdomain Wildcard Cert	Yes	Yes	No	Not supported at all on Cisco Expressways

Chapter 23

Table 23-2 Cisco Unified IP Phones Supported in Webex Control Hub

Phone Model	Phone Type	Cisco Unified Communications Manager Registration	Webex Control Hub Registration
6821, 6825, 6841, 6851, 6861, 6871	VoIP Phones	No	Yes
7811, 7821, 7841, 7861	VoIP Phones	Yes	Yes
8811, 8841, 8861	VoIP Phones	Yes	Yes
8845, 8865, 8865NR, 8875	Video Phones	Yes	Yes
7832, 8832, Webex Room Phone	Conference Phones	Yes	Yes
8821-EX, Cisco Wireless Phone 840, Cisco Wireless Phone 860	Wireless Phones	Yes	Yes

Chapter 26

Table 26-2 Firewall and NAT Traversal Port, IP Addresses, and Protocols

Purpose	Source IP	Source Ports	Protocol	Destination IP	Destination Ports
SIP Signaling	Webex Calling facing interface of Local Gateway	8000–65535	TCP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25	8934

Purpose	Source IP	Source Ports	Protocol	Destination IP	Destination Ports
RTP Media	Webex Calling facing interface of Local Gateway	8000–48000	UDP	199.59.65.0/25 199.59.66.0/25 199.59.70.0/25 199.59.71.0/25	19560–65535

Table 26-4 Cisco IOS XE Commands for Local Gateway Registration

Task	Command Syntax
This command will download a signed CA root bundle to create a trust point using TLS version 1.2 in the router.	`crypto pki trustpool import clean url`

These commands establish communication with Webex Control Hub for registration of the local gateway.	`voice class Tenant 200`
	`  registrar dns:XXXXXX scheme sips expires 240 refresh-ratio 50 tcp tls`
	`  credentials number XXXXXX username XXXXXX password 0 XXXXXX realm BroadWorks`
	`  authentication username XXXXXX password 0 XXXXXX realm BroadWorks`
	`  authentication username XXXXXX password 0 XXXXXX realm XXXXXX`
	`  no remote-party-id  sip-server dns:XXXXXX  connection-reuse`
	`  srtp-crypto 200  session transport tcp tls  url sips  error-passthru asserted-id pai`
	`  bind control source-interface GigabitEthernet1`
	`  bind media source-interface GigabitEthernet1`
	`  no pass-thru content custom-sdp`
	`sip-profiles 200`
	`  outbound-proxy dns:XXXXXX  privacy-policy passthru`

Task	Command Syntax
Configure the following SIP profile required to convert SIPS URIs back to SIP, as Webex Calling does not support SIPS URIs in the request/response messages (but needs them for SRV query; for example, **_sips._tcp.<outbound-proxy>**). **rule 20** modifies the From header to include the **Trunk Group OTG/DTG** parameter from Control Hub to uniquely identify a LGW site within an enterprise. Make sure you replace that with your **Trunk Group OTG/DTG** information.	voice class sip profiles 200 rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1" rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1" rule 11 request ANY sip-header From modify "<sips:" "<sip:\1" rule 12 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>" rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1" rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1" rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1" rule 20 request ANY sip-header From modify ">" ";otg=XXXXXX>” rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"

Table 26-5 Cisco IOS XE Commands for Inbound Calls from Cisco UBE

Task	Command Syntax
These commands are needed to route calls from Cisco UBE to Cisco Unified Communications Manager destined for Webex Control Hub registered devices.	voice class uri 100 sip host <PSTN IP address> dial-peer voice 100 voip description Inbound dialpeer from PSTN incoming uri via 100 destination dpg 302 voice class dpg 302 dial-peer 305 preference 1 dial-peer 307 preference 1

Task	Command Syntax
	voice class server-group 305 ipv4 <cucm-node-1> ipv4 <cucm-node-5> voice class server-group 307 ipv4 <cucm-node-6> ipv4 <cucm-node-7> dial-peer voice 305 voip description Outgoing dial-peer to CUCM for inbound from PSTN – 1st 5 destination-pattern .T session server-group 305 dial-peer voice 307 voip description Outgoing dial-peer to CUCM for inbound from PSTN– 2nd 5 destination-pattern .T **session server-group 307**

Table 26-6 Cisco IOS XE Commands for Inbound Calls to Local Gateway

Task	Command Syntax
These are the commands Local Gateway will use to route calls from Cisco Unified Communications Manager to Webex Control Hub.	voice class uri 300 sip pattern <cucm-nodes-ip-address and port-regex-for-dcloud> ex: pattern 10\.1\.2\..*:5065 matches 10.1.2.X:5065 range

Task	Command Syntax
	dial-peer voice 300 voip description Incoming dial-peer from CUCM for dcloud incoming uri via 300 destination dpg 200 voice class dpg 200 dial-peer 201 preference 1 dial-peer voice 201 voip description Outgoing dial-peer to BroadCloud destination-pattern .T **session-target sip-server**

Table 26-7 Cisco IOS XE Commands for Outbound Calls from Local Gateway

Task	Command Syntax
These are the commands Local Gateway will use to route calls from Webex Control Hub to Cisco Unified Communications Manager.	voice class uri 200 sip pattern :8934 dial-peer voice 200 voip description Incoming dial-peer from Webex incoming uri via 200 destination dpg 300 voice class dpg 300 dial-peer 301 preference 1 dial-peer 303 preference 1 voice class server-group 301 ipv4 <cucm-node-1> port 5065 ipv4 <cucm-node-5> port 5065

Task	Command Syntax
	voice class server-group 303 ipv4 <cucm-node-6> port 5065 ipv4 <cucm-node-7> port 5065 dial-peer voice 301 voip description Outgoing dial-peer to CUCM for inbound from Webex - 1st 5 destination-pattern .T session server-group 301 dial-peer voice 303 voip description Outgoing dial-peer to CUCM for inbound from Webex - 2nd 5 destination-pattern .T **session server-group 303**

Table 26-8 Cisco IOS XE Commands for Outbound Calls to Cisco UBE

Task	Command Syntax
These commands are used to route calls from Cisco Unified Communications Manager to Cisco UBE destined for the PSTN.	voice class uri 302 sip pattern <cucm-nodes-ip-address and port-regex-for-pstn> ex: pattern 10\.1\.2\..*:5060 matches 10.1.2.X:5060 range dial-peer voice 302 voip description Incoming dial-peer from CUCM for pstn incoming uri via 302 destination dpg 100

Task	Command Syntax

	`voice class dpg 100`
	` dial-peer 101 preference 1`
	
	`dial-peer voice 101 voip`
	` description Outgoing dial-peer to PSTN`
	` destination-pattern .T`
	` session target ipv4:<pstn ip address>`

Chapter 29

Table 29-2 Comparison of Calls Through Cisco Unified Communications Manager and Calls/Meetings Through the Cloud

Calls Through Cisco Unified Communications Manager Environment	Calls and Meetings Through Webex Cloud
Calls initiated directly from a 1:1 space or from a contact card in the Webex App.	Ad hoc meetings from a group space in the Webex App.
Searching and then calling a user in the Webex App.	Using the Join button in the Webex App to join an ad hoc or scheduled meeting.
Dialing directory numbers or PSTN numbers from the Call button in the Webex App.	Dialing on-premises Directory URIs from the Call button in the Webex App. (Depends on the Cisco Unified Communications Manager SIP Address Routing setting in Control Hub.)
Desk phone control (DPC) calls. (For outgoing calls, dial a directory or PSTN number in the Webex App and take the call on the Cisco Unified Communications Manager device; for incoming calls, answer the call in Webex App and take the call on the device.)	Joining a meeting while paired through Room, Desk, or Board devices.
	One-to-one calls that are placed directly in the Webex App to a free user in the consumer organization, to a user in another organization, or to a user in the same organization who doesn't have a directory number. (Numbers are not shared across organizations, so they don't appear in contact cards.) These are classified as a call on Webex App.

Table 29-3 Device Name Format for Soft Phone Devices

Device Type	Required Format
Cisco Unified Client Services Framework	Valid characters: a–z, A–Z, 0–9. 15-character limit.
Cisco Dual Mode for iPhone	The device name must begin with *TCT*. For example, if you create a TCT device for the user Tanya Adams, whose username is tadams, enter **TCTTADAMS**. Must be uppercase. Valid characters: A–Z, 0–9, period (.), underscore (_), and hyphen (-). 15-character limit.
Cisco Jabber for Tablet	The device name must begin with *TAB*. For example, if you create a TAB device for the user Tanya Adams, whose username is tadams, enter **TABTADAMS**. Must be uppercase. Valid characters: A–Z, 0–9, period (.), underscore (_), and hyphen (-). 15-character limit. For Android, Webex App identifies devices with displays that are 600dp or greater as a tablet.
Cisco Dual Mode for Android	The device name must begin with *BOT*. For example, if you create a BOT device for the user Tanya Adams, whose username is tadams, enter **BOTTADAMS**. Must be uppercase. Valid characters: A–Z, 0–9, period (.), underscore (_), and hyphen (-). 15-character limit. For Android, Webex App identifies devices with displays that are less than 600dp as a phone.

Chapter 30

Table 30-2 Common Endpoint Call Setup Issues and Probable Causes

Call Setup Issue	Probable Causes
Reorder tone during and at the end of dialing	Misconfigured CUCM Components: ■ Misconfigured dial plan ■ Insufficient calling privileges ■ Misconfigured digit manipulation
	CAC can also cause this issue
No ring-back tone	IP reachability issues to CUCM
	Gateway may block or drop audio
	ISDN may not provide ring-back tone
Unexpected second dial tone	Misconfigured dial plan
Video is not set up, only audio	Video codec mismatch
	CAC (such as RSVP Video Desired Mode)
	Regions
Dead air is heard	Firewall or ACL blocking media
One-way audio or video	Firewall or ACL blocking media in one direction, or CAC
Call is dropped after dialed	Audio or video codec mismatch
Call is dropped in the middle of the call	Repeatable issues are usually due to network connectivity events, but could also be caused by CAC or permission on the CUCM

Table 30-3 Major Elements Influencing Media Quality in a Cisco Collaboration Solution

Element	Description
Input video peripherals	Video input peripheral quality, lens, exposure range, focus capabilities, lighting conditions
Video codec	Selection of video codec, performance, and capabilities of video codec
Output video peripherals	Video output peripheral quality: screen, image-enhancing capabilities
Amount of video information	Video resolution, frames per second, object-moving behavior, background complexity, resulting video bit rate
Network QoS	Network, packet loss, jitter and delay characteristics, CAC, differentiated services in converged network
Correct bandwidth provisioned	Bandwidth overhead calculation and provisioning
CPU utilization	Computer hosting Cisco Jabber running many applications

Table 30-4 Common Call Setup Issues on Cisco Jabber

Issue	Possible Causes
No calls possible	Softphone is not registered, or deskphone CTI control does not work. Network connectivity issues or misconfigured servers exist.
No audio (softphone mode)	Required network ports are not open on the computer that hosts the application.
One-way audio or video (softphone mode)	Computer audio or video device on either side does not work. If connected over a Cisco VPN client (for Windows), ensure that the stateful firewall is disabled.
Poor audio quality	If echo or feedback is heard, be sure to use a proper headset and not computer speakers.
Incoming video is black (permanent)	Required network ports are not open on the computer that hosts the application.
Incoming video is black (transient)	Local or far-end computer experiences lack resources to encode or decode the video signal. Camera could be muted.

Chapter 31

Table 31-2 CDR and CMR Service Parameters on the CUCM

Service Parameter	Description
CDR Enabled Flag	This parameter determines whether CDRs are generated. Valid values specify True (CDRs are generated) or False (CDRs are not generated). For this required field, the default value specifies False. Enable this parameter on all servers.
CDR Log Calls with Zero Duration Flag	This parameter enables or disables the logging of CDRs for calls that never connected or that lasted less than one second. Cisco CallManager logs unsuccessful calls (calls that result in reorder, such as might occur due to a forwarding directive failure or calls that attempt to go through a busy trunk) regardless of this flag. This is a required field with a default value of False.
Call Diagnostics Enabled	Three settings can be configured under this menu option: ■ **Enabled Only When CDR Enable Flag is True:** Generates CMRs only when the CDR Enabled Flag service parameter is set to True. ■ **Enabled Regardless of CDR Enabled Flag:** Generates CMRs without regard to the setting in the CDR Enabled Flag service parameter. This parameter represents a required field. ■ The default value specifies **Disabled**, which will not generate CMRs.

Service Parameter	Description
Display FAC in CDR	This parameter determines whether the forced authorization codes (FAC) associated with the call display in the CDR. Valid values specify True (display authorization code in CDRs) or False (do not display authorization code in CDRs) for this required field. The default value specifies False.
Show Line Group Member DN in finalCalledPartyNumber CDR Field	This parameter determines whether the finalCalledPartyNumber field in the CDRs shows the directory number of the line group member who answers the call or the hunt pilot directory number. Valid values specify True (the finalCalledPartyNumber in CDRs will show the directory number of the phone that answered the call) or False (the finalCalledPartyNumber in CDRs will show the hunt pilot directory number). This parameter applies only to basic calls that are routed through a hunt list without future interactions, such as transfers, conference, and call park. If a feature is involved in the call, the hunt pilot directory number will show in the finalCalledPartyNumber field regardless of the setting in this parameter. The default value for this required field specifies False.
Add Incoming Number Prefix to CRD	This parameter determines whether CUCM adds the incoming prefix (as specified in the National Number Prefix, International Number Prefix, Subscriber Number Prefix, and Unknown Number Prefix Service Parameters) to the calling party number in the CDRs for that call. If the prefix is applied on the inbound side of the call, it is always added to the calling party number in the CDRs for that call. This occurs even if this parameter is set to False. If the prefix is applied on the outbound side, the prefix is added to the calling party number in the CDR or CDRs for that call, only if the parameter is set to True. If the Destination of the call is a gateway, CUCM will not add the prefix to the CDRs even if this parameter is enabled. This parameter is applied on a clusterwide basis. The default value for this required field specifies False.

Table 31-3 User Reports on the CUCM

User Report	Method of Application	User Access Allowed
Bills	Individual	Users, Managers, or Administrators
	Department	Managers or Administrators
Top N	By Charge	Managers or Administrators
	Duration	Managers or Administrators
	By Number of Calls	Managers or Administrators

User Report	Method of Application	User Access Allowed
Cisco Unified Communications Manager Assistant (IPMA)	Manager Call Usage	Administrators
	Assistant Call Usage	Administrators
Cisco IP Phone Service	Shows Cisco IP Phone Services, the number of users who are subscribed to each of the selected services, and the utilization percentage for each of the selected services	Administrators

Table 31-4 System Reports on the CUCM

System Report	Method of Application	User Access Allowed
QoS	Detail	Administrators
	Summary	Managers and Administrators
	By Gateway	Administrators
	By Call Types	Administrators
Traffic	Summary	Administrators
	Summary by Extension	Administrators
Forced Authorization Code/Client Matter Code (FAC/CMC)	Client Matter Code	Administrators
	Authorization Code Name	Administrators
	Authorization Level	Administrators
Malicious Call Details	CUCM MCID service	Administrators
Precedence Call Summary	CUCM Call Precedence service	Administrators
System Overview	High-level picture of the CUCM network	Administrators
CDR Error	Error records in the CAR Billing_ Air table	Administrators

Table 31-5 Device Reports on the CUCM

Device Report	Method of Application	User Access Allowed
Gateway	Detail	Administrator
	Summary	Administrator
	Utilization	Administrator

Device Report	Method of Application	User Access Allowed
Route Pattern/Hunt Pilot	Route and Line Group Utilization	Administrator
	Route/Hunt List Utilization	Administrator
	Route Pattern/Hunt Pilot Utilization	Administrator
	Hunt Pilot Summary	Administrator
	Hunt Pilot Detail	Administrator
Conference Bridge	Conference Call Details	Administrator
	Conference Bridge Utilization	Administrator
Voice Messaging Utilization	Utilization percentage of the voice-messaging devices	Administrator

Chapter 33

Table 33-2 Disaster Recovery System Components

Cisco Unified Communications Manager	Cisco IM and Presence Server	Cisco Unity Connection
Platform	Platform	Platform
Cisco License Manager	Cisco License Manager	Cisco License Manager
Trace Collection Tool	Trace Collection Tool	Trace Collection Tool
Syslog	Syslog	Syslog
Cisco Unified CM DB	Cisco Unified Communications Manager IM and Presence Service DB	Cisco Unity Connection DB
TFTP/MOH Files	XCP Data	Mailbox Store
CDR/CAR Data	CUP Data	Greetings

Chapter 34

Table 34-2 Reports Available Through Cisco Unity Connection Serviceability

Report Name	Description of Output
Phone Interface Failed Logon	Includes the following information for every failed attempt to sign into Unity Connection by phone: ■ Name of user, alias, caller ID, and extension of user who failed to sign in ■ Date and time the failed login occurred ■ Whether the maximum number of failed sign-ins has been reached for the user

Report Name	Description of Output
Users	Includes the following information for each user: ■ Last name, first name, and alias ■ Information that identifies the Unity Connection or Cisco Business Edition server associated with the user ■ Billing ID, class of service, and extension ■ Whether the account is locked ■ Whether the user has enabled personal call transfer rules
Message Traffic	Includes totals for the following traffic categories: Voice Fax Email Nondelivery receipt (NDR) Delivery receipt Read receipt Hourly totals Daily totals
Port Activity	Includes the following information for voice-messaging ports: ■ Name ■ Number of inbound calls handled ■ Number of outbound MWI calls handled
	■ Number of outbound AMIS calls handled ■ Number of outbound notification calls handled ■ Number of outbound TRAP calls handled ■ Total number of calls handled
Mailbox Store	Includes the following information about the specified mailbox stores: ■ Mail database name ■ Display name ■ Server name ■ Whether access is enabled ■ Mailbox store size ■ Last error ■ Status ■ Whether the mail database can be deleted

Report Name	Description of Output
Dial Plan	Includes a list of the search spaces configured on the Unity Connection or Cisco Business Edition server, with an ordered list of partitions assigned to each search space. If the server is part of a digital network, also lists the search spaces and associated partition membership on every other Unity Connection location on the network.
Dial Search Scope	Includes a list of all users and their extensions in the specified partition that is configured in the Unity Connection directory. If a partition is not specified, lists all users and their extensions for all partitions that are configured in the directory.
User Phone Login and MWI	Includes the following information about phone logins, MWI activity, and message notifications to phone devices per user: ■ Name, extension, and class of service ■ Date and time for each activity ■ The source of each activity ■ Action completed (for example, Login, MWI On or Off, and Phone Dialout) ■ Dialout number and results (applicable only for message notifications to phone devices) ■ The number of new messages for a user at time of login
User MessageActivity	Includes the following information about messages sent and received, per user: ■ Name, extension, and class of service ■ Date and time for each message ■ Type of message ■ Action completed (for example, new message or message saved) ■ Information on the message sender
Distribution Lists	Includes the following information: ■ Name and display name of the list ■ Date and time the list was created (date and time are given in Greenwich Mean Time) ■ A count of the number of users included in the list ■ If the Included List Members check box is checked, includes a listing of the alias of each user who is a member of the list
User Lockout	Includes user alias, number of failed login attempts for the user, credential type (a result of 4 indicates a login attempt from the Unity Connection conversation; a result of 3 indicates a login attempt from a web application), and the date and time that the account was locked. (Date and time are given in Greenwich Mean Time.)

Report Name	Description of Output
Unused Voicemail Accounts	Includes user alias and display name, and the date and time that the user account was created. (Date and time are given in Greenwich Mean Time.)
Transfer Call Billing	Includes the following information for each call: ■ Name, extension, and billing ID of the user ■ Date and time that the call occurred ■ The phone number dialed ■ The result of transfer (connected, ring-no-answer (RNA), busy, or unknown)
Outcall BillingDetail	Includes the following information, arranged by day and by the extension of the user who placed the call: ■ Name, extension, and billing ID ■ Date and time the call was placed ■ The phone number called ■ The result of the call (connected, ring-no-answer [RNA], busy, or unknown) ■ The duration of the call in seconds
Outcall BillingSummary	Arranged by date and according to the name, extension, and billing ID of the user who placed the call, and includes a listing of the 24 hours of the day, with a dialout time in seconds specified for each hour span.
Call Handler Traffic	Includes the following information for each call handler and use for each hour of a day: ■ Total number of calls ■ Number of times each key on the phone keypad was pressed ■ Extension ■ Invalid extension ■ Number of times the After Greeting action occurred ■ Number of times the caller hung up
System Configuration	Includes detailed information about all aspects of the configuration of the Unity Connection system.
SpeechView Activity Report By User	Includes the total number of transcribed messages, failed transcriptions, and truncated transcriptions for a given user during a given time period. If the report is run for all users, then the output is broken out by user.
SpeechView Activity Summary Report	Includes the total number of transcribed messages, failed transcriptions, and truncated transcriptions for the entire system during a given time period. When a message is sent to multiple recipients, the message is transcribed only once, so the transcription activity is counted only once.

Report Name	Description of Output
HTTPS Networking Sync Error Report	(Applicable only for HTTPS Networking) Includes the following information associated with the directory objects that do not synchronize during directory synchronization: ■ Creation Date ■ Failed ObjectID ■ USN ■ Object Type ■ Location Display Name ■ HTTP(S) Link ■ Error Message

This page intentionally left blank

Appendix D

Study Planner

Practice Test	Reading	Task

Element	Task	Goal Date	First Date Completed	Second Date Completed (Optional)	Notes
Introduction	Read Introduction				
1. Introduction to Collaboration	Read Foundation Topics				
1. Introduction to Collaboration	Review Key Topics using the book or companion website				
1. Introduction to Collaboration	Define Key Terms using the book or companion website				
1. Introduction to Collaboration	Repeat DIKTA questions using the book or PTP exam engine				
1. Introduction to Collaboration	Complete the Q&A section				
Practice Test	Take practice test in study mode in practice test software for this chapter				
2. Audio Basics	Read Foundation Topics				
2. Audio Basics	Review Key Topics using the book or companion website				

2. Audio Basics	Define Key Terms using the book or companion website				
2. Audio Basics	Repeat DIKTA questions using the book or PTP exam engine				
2. Audio Basics	Complete the Q&A section				
2. Audio Basics	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
3. Video Basics	Read Foundation Topics				
3. Video Basics	Review Key Topics using the book or companion website				
3. Video Basics	Define Key Terms using the book or companion website				
3. Video Basics	Repeat DIKTA questions using the book or PTP exam engine				
3. Video Basics	Complete the Q&A section				
3. Video Basics	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
4. Collaboration Endpoint Components and Environment	Read Foundation Topics				
4. Collaboration Endpoint Components and Environment	Review Key Topics using the book or companion website				
4. Collaboration Endpoint Components and Environment	Define Key Terms using the book or companion website				

4. Collaboration Endpoint Components and Environment	Repeat DIKTA questions using the book or PTP exam engine				
4. Collaboration Endpoint Components and Environment	Complete the Q&A section				
4. Collaboration Endpoint Components and Environment	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
5. Communication Protocols	Read Foundation Topics				
5. Communication Protocols	Review Key Topics using the book or companion website				
5. Communication Protocols	Define Key Terms using the book or companion website				
5. Communication Protocols	Repeat DIKTA questions using the book or PTP exam engine				
5. Communication Protocols	Complete the Q&A section				
5. Communication Protocols	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
6. Cisco Solution for Converged Collaboration	Read Foundation Topics				
6. Cisco Solution for Converged Collaboration	Review Key Topics using the book or companion website				

6. Cisco Solution for Converged Collaboration	Define Key Terms using the book or companion website				
6. Cisco Solution for Converged Collaboration	Repeat DIKTA questions using the book or PTP exam engine				
6. Cisco Solution for Converged Collaboration	Complete the Q&A section				
6. Cisco Solution for Converged Collaboration	Review command tables for this chapter				
6. Cisco Solution for Converged Collaboration	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
Part I. AV Fundamentals	Take practice test in study mode using Part Review exam in practice test software for this part				
7. Cisco Unified Communications Phones	Read Foundation Topics				
7. Cisco Unified Communications Phones	Review Key Topics using the book or companion website				
7. Cisco Unified Communications Phones	Define Key Terms using the book or companion website				
7. Cisco Unified Communications Phones	Repeat DIKTA questions using the book or PTP exam engine				
7. Cisco Unified Communications Phones	Complete the Q&A section				
7. Cisco Unified Communications Phones	Review command tables for this chapter				

7. Cisco Unified Communications Phones	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
8. Cisco Telepresence Endpoints	Read Foundation Topics				
8. Cisco Telepresence Endpoints	Review Key Topics using the book or companion website				
8. Cisco Telepresence Endpoints	Define Key Terms using the book or companion website				
8. Cisco Telepresence Endpoints	Repeat DIKTA questions using the book or PTP exam engine				
8. Cisco Telepresence Endpoints	Complete the Q&A section				
8. Cisco Telepresence Endpoints	Review command tables for this chapter				
8. Cisco Telepresence Endpoints	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
9. Endpoint Registration	Read Foundation Topics				
9. Endpoint Registration	Review Key Topics using the book or companion website				
9. Endpoint Registration	Define Key Terms using the book or companion website				

9. Endpoint Registration	Repeat DIKTA questions using the book or PTP exam engine				
9. Endpoint Registration	Complete the Q&A section				
9. Endpoint Registration	Review command tables for this chapter				
9. Endpoint Registration	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
10. Call Settings on Cisco CE Software-Based Endpoints	Read Foundation Topics				
10. Call Settings on Cisco CE Software-Based Endpoints	Review Key Topics using the book or companion website				
10. Call Settings on Cisco CE Software-Based Endpoints	Define Key Terms using the book or companion website				
10. Call Settings on Cisco CE Software-Based Endpoints	Repeat DIKTA questions using the book or PTP exam engine				
10. Call Settings on Cisco CE Software-Based Endpoints	Complete the Q&A section				
Practice Test	Take practice test in study mode in practice test software for this chapter				
11. Maintaining Cisco Endpoints	Read Foundation Topics				
11. Maintaining Cisco Endpoints	Review Key Topics using the book or companion website				
11. Maintaining Cisco Endpoints	Define Key Terms using the book or companion website				

11. Maintaining Cisco Endpoints	Repeat DIKTA questions using the book or PTP exam engine				
Practice Test	Take practice test in study mode in practice test software for this chapter				
Practice Test	Take practice test in study mode using Part Review exam in practice test software for this part				
12. Cisco Core Network Components	Read Foundation Topics				
12. Cisco Core Network Components	Review Key Topics using the book or companion website				
12. Cisco Core Network Components	Define Key Terms using the book or companion website				
12. Cisco Core Network Components	Repeat DIKTA questions using the book or PTP exam engine				
12. Cisco Core Network Components	Complete the Q&A section				
12. Cisco Core Network Components	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
13. Layer 2 and Layer 3 QoS Parameters	Read Foundation Topics				
13. Layer 2 and Layer 3 QoS Parameters	Review Key Topics using the book or companion website				
13. Layer 2 and Layer 3 QoS Parameters	Define Key Terms using the book or companion website				

13. Layer 2 and Layer 3 QoS Parameters	Repeat DIKTA questions using the book or PTP exam engine				
13. Layer 2 and Layer 3 QoS Parameters	Complete the Q&A section				
13. Layer 2 and Layer 3 QoS Parameters	Review command tables for this chapter				
13. Layer 2 and Layer 3 QoS Parameters	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
14. DNS, NTP, and SNMP	Read Foundation Topics				
14. DNS, NTP, and SNMP	Review Key Topics using the book or companion website				
14. DNS, NTP, and SNMP	Define Key Terms using the book or companion website				
14. DNS, NTP, and SNMP	Repeat DIKTA questions using the book or PTP exam engine				
14. DNS, NTP, and SNMP	Complete the Q&A section				
14. DNS, NTP, and SNMP	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
Practice Test	Take practice test in study mode using Part Review exam in practice test software for this part				

15. Cisco Unified Communications Manager Setup	Read Foundation Topics				
15. Cisco Unified Communications Manager Setup	Review Key Topics using the book or companion website				
15. Cisco Unified Communications Manager Setup	Define Key Terms using the book or companion website				
15. Cisco Unified Communications Manager Setup	Repeat DIKTA questions using the book or PTP exam engine				
15. Cisco Unified Communications Manager Setup	Complete the Q&A section				
15. Cisco Unified Communications Manager Setup	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
16. LDAP Integration with Cisco Unified Communications Manager	Read Foundation Topics				
16. LDAP Integration with Cisco Unified Communications Manager	Review Key Topics using the book or companion website				
16. LDAP Integration with Cisco Unified Communications Manager	Define Key Terms using the book or companion website				
16. LDAP Integration with Cisco Unified Communications Manager	Repeat DIKTA questions using the book or PTP exam engine				
16. LDAP Integration with Cisco Unified Communications Manager	Complete the Q&A section				
16. LDAP Integration with Cisco Unified Communications Manager	Complete all memory tables in this chapter using the companion website				

Practice Test	Take practice test in study mode in practice test software for this chapter				
17. Registering SIP Endpoints to the Cisco Unified Communications Manager	Read Foundation Topics				
17. Registering SIP Endpoints to the Cisco Unified Communications Manager	Review Key Topics using the book or companion website				
17. Registering SIP Endpoints to the Cisco Unified Communications Manager	Define Key Terms using the book or companion website				
17. Registering SIP Endpoints to the Cisco Unified Communications Manager	Repeat DIKTA questions using the book or PTP exam engine				
17. Registering SIP Endpoints to the Cisco Unified Communications Manager	Complete the Q&A section				
Practice Test	Take practice test in study mode in practice test software for this chapter				
18. Cisco Unified Communications Manager Call Admission Control (CAC)	Read Foundation Topics				
18. Cisco Unified Communications Manager Call Admission Control (CAC)	Review Key Topics using the book or companion website				
18. Cisco Unified Communications Manager Call Admission Control (CAC)	Define Key Terms using the book or companion website				
18. Cisco Unified Communications Manager Call Admission Control (CAC)	Repeat DIKTA questions using the book or PTP exam engine				
18. Cisco Unified Communications Manager Call Admission Control (CAC)	Complete the Q&A section				
18. Cisco Unified Communications Manager Call Admission Control (CAC)	Complete all memory tables in this chapter using the companion website				

Practice Test	Take practice test in study mode in practice test software for this chapter				
19. Configuring Globalized Call Routing in Cisco Unified Communications Manager	Read Foundation Topics				
19. Configuring Globalized Call Routing in Cisco Unified Communications Manager	Review Key Topics using the book or companion website				
19. Configuring Globalized Call Routing in Cisco Unified Communications Manager	Define Key Terms using the book or companion website				
19. Configuring Globalized Call Routing in Cisco Unified Communications Manager	Repeat DIKTA questions using the book or PTP exam engine				
19. Configuring Globalized Call Routing in Cisco Unified Communications Manager	Complete the Q&A section				
19. Configuring Globalized Call Routing in Cisco Unified Communications Manager	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
Practice Test	Take practice test in study mode using Part Review exam in practice test software for this part				
20. Introduction to Cisco Edge Services	Read Foundation Topics				
20. Introduction to Cisco Edge Services	Review Key Topics using the book or companion website				
20. Introduction to Cisco Edge Services	Define Key Terms using the book or companion website				
20. Introduction to Cisco Edge Services	Repeat DIKTA questions using the book or PTP exam engine				

20. Introduction to Cisco Edge Services	Complete the Q&A section				
20. Introduction to Cisco Edge Services	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
21. Mobile and Remote Access (MRA)	Read Foundation Topics				
21. Mobile and Remote Access (MRA)	Review Key Topics using the book or companion website				
21. Mobile and Remote Access (MRA)	Define Key Terms using the book or companion website				
21. Mobile and Remote Access (MRA)	Repeat DIKTA questions using the book or PTP exam engine				
21. Mobile and Remote Access (MRA)	Complete the Q&A section				
21. Mobile and Remote Access (MRA)	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
Practice Test	Take practice test in study mode using Part Review exam in practice test software for this part				
22. Components of the Webex Solution	Read Foundation Topics				
22. Components of the Webex Solution	Review Key Topics using the book or companion website				

22. Components of the Webex Solution	Define Key Terms using the book or companion website				
22. Components of the Webex Solution	Repeat DIKTA questions using the book or PTP exam engine				
22. Components of the Webex Solution	Complete the Q&A section				
Practice Test	Take practice test in study mode in practice test software for this chapter				
23. Adding Users and Devices In the Webex Control Hub	Read Foundation Topics				
23. Adding Users and Devices In the Webex Control Hub	Review Key Topics using the book or companion website				
23. Adding Users and Devices In the Webex Control Hub	Define Key Terms using the book or companion website				
23. Adding Users and Devices In the Webex Control Hub	Repeat DIKTA questions using the book or PTP exam engine				
23. Adding Users and Devices In the Webex Control Hub	Complete the Q&A section				
23. Adding Users and Devices In the Webex Control Hub	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
24. Webex Calling Options	Read Foundation Topics				
24. Webex Calling Options	Review Key Topics using the book or companion website				
24. Webex Calling Options	Define Key Terms using the book or companion website				

24. Webex Calling Options	Repeat DIKTA questions using the book or PTP exam engine				
24. Webex Calling Options	Complete the Q&A section				
24. Webex Calling Options	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
25. Webex Calling Features	Read Foundation Topics				
25. Webex Calling Features	Review Key Topics using the book or companion website				
25. Webex Calling Features	Define Key Terms using the book or companion website				
25. Webex Calling Features	Repeat DIKTA questions using the book or PTP exam engine				
25. Webex Calling Features	Complete the Q&A section				
Practice Test	Take practice test in study mode in practice test software for this chapter				
26. Webex Calling Using a Local Gateway	Read Foundation Topics				
26. Webex Calling Using a Local Gateway	Review Key Topics using the book or companion website				
26. Webex Calling Using a Local Gateway	Define Key Terms using the book or companion website				

26. Webex Calling Using a Local Gateway	Repeat DIKTA questions using the book or PTP exam engine				
26. Webex Calling Using a Local Gateway	Complete the Q&A section				
26. Webex Calling Using a Local Gateway	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
Practice Test	Take practice test in study mode using Part Review exam in practice test software for this part				
27. Understanding Cisco Unity Connection	Read Foundation Topics				
27. Understanding Cisco Unity Connection	Review Key Topics using the book or companion website				
27. Understanding Cisco Unity Connection	Define Key Terms using the book or companion website				
27. Understanding Cisco Unity Connection	Repeat DIKTA questions using the book or PTP exam engine				
27. Understanding Cisco Unity Connection	Complete the Q&A section				
Practice Test	Take practice test in study mode in practice test software for this chapter				
28. Cisco Unity Connection End-User and Voice Mailbox	Read Foundation Topics				
28. Cisco Unity Connection End-User and Voice Mailbox	Review Key Topics using the book or companion website				

28. Cisco Unity Connection End-User and Voice Mailbox	Define Key Terms using the book or companion website				
28. Cisco Unity Connection End-User and Voice Mailbox	Repeat DIKTA questions using the book or PTP exam engine				
28. Cisco Unity Connection End-User and Voice Mailbox	Complete the Q&A section				
Practice Test	Take practice test in study mode in practice test software for this chapter				
29. Deploying the Webex Application	Read Foundation Topics				
29. Deploying the Webex Application	Review Key Topics using the book or companion website				
29. Deploying the Webex Application	Define Key Terms using the book or companion website				
29. Deploying the Webex Application	Repeat DIKTA questions using the book or PTP exam engine				
29. Deploying the Webex Application	Complete the Q&A section				
Practice Test	Take practice test in study mode in practice test software for this chapter				
Practice Test	Take practice test in study mode using Part Review exam in practice test software for this part				
30. Troubleshooting Endpoints	Read Foundation Topics				
30. Troubleshooting Endpoints	Review Key Topics using the book or companion website				

30. Troubleshooting Endpoints	Define Key Terms using the book or companion website				
30. Troubleshooting Endpoints	Repeat DIKTA questions using the book or PTP exam engine				
30. Troubleshooting Endpoints	Complete the Q&A section				
30. Troubleshooting Endpoints	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
31. Cisco Unified Communications Manager Reports	Read Foundation Topics				
31. Cisco Unified Communications Manager Reports	Review Key Topics using the book or companion website				
31. Cisco Unified Communications Manager Reports	Define Key Terms using the book or companion website				
31. Cisco Unified Communications Manager Reports	Repeat DIKTA questions using the book or PTP exam engine				
31. Cisco Unified Communications Manager Reports	Complete the Q&A section				
31. Cisco Unified Communications Manager Reports	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
32. Real-Time Monitoring Tool (RTMT)	Read Foundation Topics				

32. Real-Time Monitoring Tool (RTMT)	Review Key Topics using the book or companion website				
32. Real-Time Monitoring Tool (RTMT)	Define Key Terms using the book or companion website				
32. Real-Time Monitoring Tool (RTMT)	Repeat DIKTA questions using the book or PTP exam engine				
32. Real-Time Monitoring Tool (RTMT)	Complete the Q&A section				
Practice Test	Take practice test in study mode in practice test software for this chapter				
33. Understanding the Disaster Recovery System	Read Foundation Topics				
33. Understanding the Disaster Recovery System	Review Key Topics using the book or companion website				
33. Understanding the Disaster Recovery System	Define Key Terms using the book or companion website				
33. Understanding the Disaster Recovery System	Repeat DIKTA questions using the book or PTP exam engine				
33. Understanding the Disaster Recovery System	Complete the Q&A section				
Practice Test	Take practice test in study mode in practice test software for this chapter				
34. Monitoring Voicemail in Cisco Unity Connection	Read Foundation Topics				
34. Monitoring Voicemail in Cisco Unity Connection	Review Key Topics using the book or companion website				
34. Monitoring Voicemail in Cisco Unity Connection	Define Key Terms using the book or companion website				

34. Monitoring Voicemail in Cisco Unity Connection	Repeat DIKTA questions using the book or PTP exam engine				
34. Monitoring Voicemail in Cisco Unity Connection	Complete the Q&A section				
34. Monitoring Voicemail in Cisco Unity Connection	Complete all memory tables in this chapter using the companion website				
Practice Test	Take practice test in study mode in practice test software for this chapter				
Practice Test	Take practice test in study mode using Part Review exam in practice test software for this part				
Final Review	Take practice test in study mode for all Book Questions in practice test software				
Final Review	Review all Key Topics in all chapters				
Final Review	Review the Key Term Glossary				
Final Review	Complete all memory tables for all chapters using the companion website				
Final Review	Take practice test in practice exam mode using Exam Bank #1 questions for all chapters				
Final Review	Take practice test in practice exam mode using Exam Bank #2 questions for all chapters				