cisco

Official Cert Guide

Learn, prepare, and practice for exam success

CCNA Collaboration

CICD 210-060

ciscopress.com

MICHAEL VALENTINE

CCNA Collaboration
CICD 210-060

Official Cert Guide

MIKE VALENTINE

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

CCNA Collaboration CICD 210-060 Official Cert Guide

Mike Valentine

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

Printed in the United States of America

First Printing September 2015

Library of Congress Control Number: 2015943875

ISBN-13: 978-1-58714-443-1

ISBN-10: 1-58714-443-3

Warning and Disclaimer

This book is designed to provide information about the CCNA Collaboration CICD exam (210-060). Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Special Sales

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

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

For questions about sales outside the U.S., please contact international@pearsoned.com.

Feedback Information

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

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

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Business Operation Manager, Cisco Press: Jan Cornelssen

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Senior Development Editor: Christopher Cleveland

Project Editor: Seth Kerney

Copy Editor: Keith Cline

Technical Editors: Jason Ball, Michelle Plumb, Ted Trentler

Editorial Assistant: Vanessa Evans

Book Designer: Mark Shirar

Composition: Trina Wurst

Indexer: Ken Johnson

Proofreader: Megan Wade-Taxter

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

About the Author

Michael Valentine has worked in the IT field since 1996 and became a trainer in 2001. Currently, he is a Cisco trainer with Skyline Advanced Technology Services and specializes in Cisco Unified Communications and CCNA classes. His accessible, humorous, and effective teaching style has demystified Cisco for thousands of students since he began teaching CCNA in 2002. Mike holds a bachelor of arts degree from the University of British Columbia and currently holds CCNA, CCNP, CCDP, CCVP, and CCSI No. 31461 certifications. Mike has developed courseware and labs for Cisco and its training partners. Mike is the coauthor of *CCNA Exam Cram (Exam 640-802)*, Third Edition (Que 2008); authored the *CCNA Voice Quick Reference Guide*, and has served as technical editor and contributor on several Cisco Press titles.

About the Technical Reviewers

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

Michelle Plumb is a full-time Cisco Certified Systems Instructor (CCSI). She has 26+ years of experience in the field as an IT professional and telecommunications specialist. She maintains a high number of Cisco, Microsoft, and CompTIA certifications, including CCNP Voice (now known as CCNP Collaboration), MCSE, CompTIA A+, Network+, Project+, and iNet+. Michelle has been a technical reviewer for numerous books related to the Cisco CCNP Route and Switch, CCNP Voice, and CompTIA course materials. Her main passion is helping others learn these new and exciting technologies. She lives in Phoenix, Arizona, with her husband and two dogs.

Dedication

For my mother, Mary Hayes Valentine

Acknowledgments

Writing a book like this is basically awful. Other than the lifestyle of a Cisco Press author—the constant glamour, the fast cars, the celebrity parties in exotic places, and of course, the literal piles of cash that royalties haul in—there's not much fun about parking your butt in a chair and hammering out chapters when there are many other urgent and interesting things needing your time. But it's the thing I take the most pride in as an accomplishment in my career, and it's something that I really feel needs to be good, so that people can use it, learn from it, and actually enjoy doing so.

This book simply wouldn't happen without the involvement of many individuals who variously supported, cajoled, threatened, motivated, reminded, negotiated, introduced, cooked, hugged, reality-checked, edited, coordinated, illustrated, and emailed—and most of them I don't even know and sadly will never meet. If you worked on this book, contributed or in any way helped make it happen, or just make it better, thank you. I hope I can meet you and shake your hand to thank you in person someday.

Brett Bartow: For your professionalism when certain others lost theirs, and most especially for your uncommon kindness and caring. Thank you, sir.

Chris Cleveland: In my mind, you are some kind of mastermind, with the patience of stone and the unfailing ability to catch every single detail that I missed. All of them. Every time. Thanks. I don't know how you do it.

Jeremy Cioara: For passing the torch.

Brian Morgan: I can't thank you enough. Your assistance made this one happen; I will buy the beer when we finally meet in person.

Toby Sauer: A dedicated and competent professional; an honorable man; a good friend and an unfailing supporter who will never hesitate to tell me what I did right, or when I messed up, and exactly how in either case. I value this.

Ed Misely: A good friend and terrifyingly capable technical resource, for his assistance with my labs.

Marshall Bradley: For your time and your help, and for having excellent taste in bass guitars and amps.

Indie and Marvin, the Cattle Dog odd couple: For keeping my feet warm and for always reminding me that Frisbee is more important than anything.

My family: Thank you, again, for your support, your patience, your love, and your belief in me. I can come upstairs now.

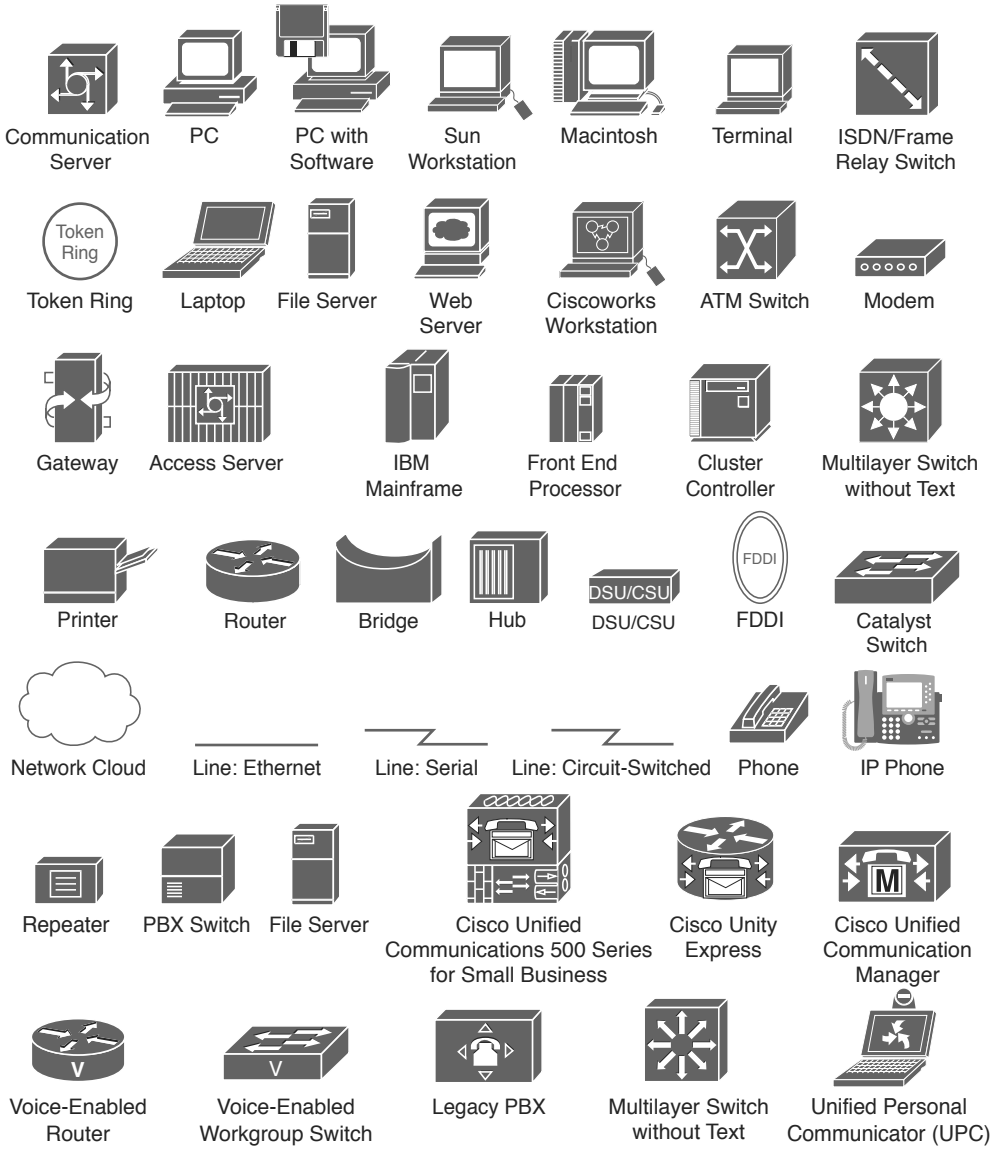
Contents at a Glance

Part VI Appendixes

CD-Only Appendixes

Contents

Icons Used in This Book



Command Syntax Conventions

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

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

Introduction

Welcome to CCNA Collaboration! As the evolution of Voice over IP continues, Cisco has taken deliberate initiatives to further integrate and adapt communications technologies to change how we work, or create products to adapt to how we want to work. First with comprehensive support for video telephony, and now with an equally focused commitment to rich-media collaboration, CCNA Collaboration now represents a more complex set of hardware and software and consequently a larger and more challenging curriculum.

In June 2008, Cisco announced new CCNA specialties, including CCNA Security, CCNA Wireless, and CCNA Voice. These certifications, released 10 years after the initial CCNA, represented Cisco's growth into new and emerging industries. Certification candidates can now specialize in specific areas of study, including Route/Switch; Wireless; Security; Service Provider; Cloud; Industrial; Data Center; and of course, Collaboration, the subject of this book and the companion volume by Brian Morgan and Jason Ball, *CCNA Collaboration CIVND 210-065 Official Cert Guide*.

Achieving your CCNA Collaboration requires that you pass two exams:

- 210-060 CICD
- 210-065 CIVND

There are no prerequisites for CCNA Collaboration; a CCENT or CCNA Route/Switch is no longer a requirement (but might be good knowledge to have anyway).

The official Cisco training "Implementing Cisco Collaboration Devices (CICD)" (the subject of this book) and "Implementing Cisco Video Network Devices, Part 1 (CIVND1)" and "Implementing Cisco Video Network Devices, Part 2(CIVND2)" are the courses associated with these two exams.

Goals and Methods

The most important goal of this book is to help you pass the Implementing Cisco Collaboration Devices (CICD) exam (210-060). In fact, if the primary objective of this book were different, the book's title would be misleading. The methods used in this book help you pass the CICD 210-060 exam and make you much more knowledgeable about how to do your job.

This book uses several key methodologies to help you discover the exam topics that you need to review in more depth, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass by memorization, but helps you truly learn and understand the topics. The CCNA Collaboration CICD exam is the foundation for many of the Cisco professional certifications, and it would be a disservice to you if this book did not help you truly learn the material. Therefore, this book helps you pass the CCNA Collaboration CICD exam by using the following methods:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the CD-ROM

In addition, this book uses a different style from typical certification-preparation books. The newer Cisco certification exams have adopted a style of testing that essentially says, "If you don't know how to do it, you won't pass this exam." This means that most of the questions on the certification exam require you to deduce the answer through reasoning or configuration rather than just memorizing facts, figures, or syntax from a book. To accommodate this newer testing style, the author has written this book as a real-world explanation of Cisco Collaboration topics. Most concepts are explained using real-world examples rather than showing tables full of syntax options and explanations, which are freely available on Cisco.com. As you read this book, you definitely get a feeling of, "This is how I can do this," which is exactly what you need for the newer Cisco exams.

Who Should Read This Book?

The purpose of this book is twofold. The primary purpose is to greatly improve your chances of passing the CCNA Collaboration certification exam. The secondary purpose is to provide the information necessary to manage a VoIP solution using Cisco Unified Communication Manager Express (CME), Cisco Unified Communications Manager (CUCM), Cisco Unity Connection, and Cisco Communications Manager IM and Presence. Cisco's new exam approach provides an avenue to write the book with both a real-world and certification-study approach at the same time. As you read this book and study the configuration examples and exam tips, you have a true sense of understanding how you could deploy a VoIP system, while at the same time feeling equipped to pass the CCNA Collaboration CICD certification exam.

Strategies for Exam Preparation

Strategies for exam preparation will vary depending on your existing skills, knowledge, and equipment available. Of course, the ideal exam preparation would consist of building a small voice lab with a Cisco Integrated Services Router, virtualized lab versions of CUCM, Unity Connection, and CM-IM and Presence servers, a switch, and a few IP Phones, which you could then use to work through the configurations as you read this book. However, not everyone has access to this equipment, so the next best step you can take is to read the chapters and jot down notes with key concepts or configurations on a separate notepad. Each chapter begins with a "Do I Know This Already?" quiz, which is designed to give you a good idea of the chapter's content and your current understanding of it. In some cases, you might already know most of or all the information covered in a given chapter.

After you read the book, look at the current exam objectives for the CCNA Collaboration CICD exam listed on Cisco.com (http://www.cisco.com/web/learning/certifications/associate/ccna_collaboration/index.html). If there are any areas shown in the certification exam outline that you would still like to study, find those sections in the book and review them.

When you feel confident in your skills, attempt the practice exam included on the CD with this book. As you work through the practice exam, note the areas where you lack confidence and review those concepts or configurations in the book. After you have reviewed the areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions will become, so the practice exam will become a less accurate judge of your skills.

After you work through the practice exam a second time and feel confident with your skills, schedule the real CICD (210-060) exam through Vue (http://www.vue.com). You should typically take the exam within a week from when you consider yourself ready to take the exam, so that the information is fresh in your mind.

Keep in mind that Cisco exams are very difficult. Even if you have a solid grasp of the information, many other factors play into the testing environment (stress, time constraints, and so on). If you pass the exam on the first attempt, fantastic! If not, know that this commonly happens. The next time you attempt the exam, you will have a major advantage: You already experienced the exam first-hand. Although future exams may have different questions, the topics and general "feel" of the exam remain the same. Take some time to study areas from the book where you felt weak on the exam. Retaking the exam the same or following day from your first attempt is a little aggressive; instead, schedule to retake it within a week, while you are still familiar with the content.

210-060 CICD Exam Topics

Table I-1 lists the exam topics for the 210-060 CICD exam. This table also lists the book parts in which each exam topic is covered.

Table I-1 210-060 CICD Exam Topics

CICD 210-060 Exam Topic	Chapter(s) in Which Topic Is Covered
1.0 Describe the Characteristics of a Cisco Unified Communications Solution	
1.1 Describe the Cisco Unified Communications components and their functions	Chapter 2
1.2 Describe call signaling and media flows	Chapter 3
1.3 Describe quality implications of a VoIP network	Chapter 3
2.0 Provision End Users and Associated Devices	
2.1 Describe user creation options for Cisco Unified Communications Manager and Cisco Unified Communications Manager Express	Chapters 4, 5, 9
2.2 Create or modify user accounts for Cisco Unified Communications Manager	Chapter 9
2.3 Create or modify user accounts for Cisco Unified Communications Manager Express using the GUI	Chapter 5
2.4 Create or modify endpoints for Cisco Unified Communications Manager	Chapter 9
2.5 Create or modify endpoints for Cisco Unified Communications Manager Express using the GUI	Chapter 5
2.6 Describe how calling privileges function and how calling privileges impact system features	Chapters 6 and 10
2.7 Create or modify directory numbers	Chapter 9
2.8 Enable user features and related calling privileges for extension mobility, call coverage, intercom, native presence, and unified mobility remote destination configuration	Chapters 11 and 12
2.9 Enable end users for Cisco Unified IM and Presence	Chapter 14
2.10 Verify user features are operational	Chapters 11 and 12
3.0 Configure Voice Messaging and Presence	
3.1 Describe user creation options for voice messaging	Chapter 13
3.2 Create or modify user accounts for Cisco Unity Connection	Chapter 13
3.3 Describe Cisco Unified IM and Presence	Chapter 14
3.4 Configure Cisco Unified IM and Presence	Chapter 14
4.0 Maintain Cisco Unified Communications System	
4.1 Generate CDR and CMR reports	Chapter 16
4.2 Generate capacity reports	Chapter 16
4.3 Generate usage reports	Chapter 16

4.4 Generate RTMT reports to monitor system activities	Chapter 16
4.5 Monitor voicemail usage	Chapter 17
4.6 Remove unassigned directory numbers	Chapter 10
4.7 Perform manual system backup	Chapter 16
5.0 Provide End User Support	
5.1 Verify PSTN connectivity	Chapters 6 and 10
5.2 Define fault domains using information gathered from end user	Chapter 16
5.3 Troubleshoot endpoint issues	Chapter 16
5.4 Identify voicemail issues and resolve issues related to user mailboxes	Chapter 17
5.5 Describe causes and symptoms of call quality issues	Chapters 3 and 16
5.6 Reset single devices	Chapters 5 and 9
5.7 Describe how to use phone applications	Chapter 11

CCNA Collaboration CICD 210-060 Official Certification Guide

The objective of this book is to help you pass the CCNA Collaboration CICD exam (210-060). While you are learning about topics that can help you pass the CICD exam, you will also become more knowledgeable about how to do your job. Although this book and the accompanying CD have many exam preparation tasks and sample test questions, the method in which they are used is not to simply make you memorize as many questions and answers as you possibly can.

The methodology of this book helps you discover the exam topics about which you need more review, fully understand and remember exam topic details, and prove to yourself that you have retained your knowledge of those topics. So, this book helps you pass not by memorization, but by helping you truly learn and understand the topics. The CICD exam is just one of the foundation topics in the CCNA Collaboration certification, and the knowledge contained within is vitally important to consider yourself a truly skilled Cisco Collaboration engineer or specialist.

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

Book Features and Exam Preparation Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics.

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

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

  Key Topic

  - **Key Topics Review:** The Key Topic icon is shown next to the most important items in the "Foundation Topics" section of the chapter. The Key Topics Review activity lists the key topics from the chapter and page number. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic. Review these topics carefully.
  - **Memory Tables:** To help you exercise your memory and memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the CD. This document lists only partial information, allowing you to complete the table or list. CD-only Appendix D holds the incomplete tables, and Appendix E includes the completed tables from which you can check your work.
  - **Definition of Key Terms:** Although Cisco exams might be unlikely to ask a question such as "Define this term," the CICD exam requires that you learn and know a lot of networking terminology. This section lists some of the most important terms from the chapter, asking you to write a short definition and compare your answer to the Glossary at the end of the book.
- **CD-based practice exam:** The companion CD contains an exam engine, including a bank of multiple-choice questions. You can use the practice exams to get a feel for the actual exam content and to gauge your knowledge of switching topics.

How This Book Is Organized

Although this book could be read cover-to-cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. If you do intend to read all the chapters, the order in the book is an excellent sequence to use.

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

- **Chapter 1, "Traditional Voice Versus Unified Voice."** This chapter discusses what would be known as the traditional telephony world. It begins where the telephone system originally started: analog connectivity. It then moves into the realm of digital connections and considerations and concludes the traditional voice discussion with the primary pieces that you need to know from the public switched telephone network (PSTN). Chapter 1 then moves into the unified voice realm, discussing the benefits of Voice over IP (VoIP), the process of coding and decoding audio, digital signal processors (DSPs), and the core VoIP protocols.
- **Chapter 2, "Understanding the Components of Cisco Unified Communications."** This chapter primarily focuses on the components of a Cisco VoIP network. By breaking down the voice infrastructure into four distinct areas, each component can be categorized and described. These components include endpoints, call processing agents, applications, and network infrastructure devices.
- **Chapter 3, "Understanding Cisco IP Phones."** This chapter discusses the preparation and base configuration of the LAN infrastructure to support VoIP devices. This preparation includes support for Power over Ethernet (PoE), voice VLANs, a properly configured DHCP scope for VoIP devices, and the Network Time Protocol (NTP).
- **Chapter 4, "Getting Familiar with CME Administration."** This chapter familiarizes you with Cisco Unified Communication Manager Express (CME) administration by unpacking the two primary administrative interfaces of CME: the command line and the Cisco Configuration Professional (CCP) graphical user interface (GUI).
- **Chapter 5, "Managing Endpoints and End Users in CME."** This chapter focuses on the process to create and assign directory numbers (DNs) and user accounts to Cisco IP Phones. The chapter walks through these configurations in both the command-line and CCP interfaces.
- **Chapter 6, "Understanding the CME Dial Plan."** Now that the internal VoIP network is operational through the CME configuration, this chapter examines connections to the outside world through the PSTN or over an IP network. Concepts covered in this chapter include the configuration of physical voice port characteristics, dial peers, digit manipulation, class of restriction (COR), and quality of service (QoS).
- **Chapter 7, "Enabling Telephony Features with CME."** This chapter examines feature after feature supported by the CME router. By the time you finish this chapter, you will understand how to configure features such as intercom, paging, call park and pickup, and many others.
- **Chapter 8, "Administrator and End-User Interfaces."** This chapter introduces the administration interfaces for CUCM, CUC, and CUP. From the administrative GUI for each application to the common Unified Serviceability interface, disaster recovery, and command-line interface (CLI), the fundamentals of navigation and configuration are laid out in a clear and logical sequence.
- **Chapter 9, "Managing Endpoints and End Users in CUCM."** The configuration and management of users and phones is covered in this chapter, including integration with Lightweight Directory Access Protocol (LDAP).

- **Chapter 10, "Understanding CUCM Dial Plan Elements and Interactions."** The guts of the call-routing system in CUCM are explained with simplicity and clarity. Call flows in different deployments and under different conditions of use and failure (including Call Admission Control [CAC] and Automated Alternate Routing [AAR]) are demonstrated and compared, and the great mystery of partitions and calling search spaces (CSS) is revealed for the simple truth it really is.
- **Chapter 11, "Enabling Telephony and Mobility Features with CUCM."** A sample of the many features available in CUCM, including extension mobility and call coverage, is provided.
- **Chapter 12, "Enabling Mobility Features in CUCM."** A step-by-step guide to enabling some of the most popular and powerful features in CUCM: Mobile Connect and Mobile Voice Access.
- **Chapter 13, "Voice Messaging Integration with Cisco Unity Connection."** The power, stability, and wealth of features available in CUC are examined, followed by a look at the configuration of user accounts and their mail boxes.
- **Chapter 14, "Enabling CM IM and Presence Support."** The capabilities, features, and basic configuration of the CUP server and clients are covered, giving an introduction to one of the most powerful additions to the Unified Communications capabilities of any business.
- **Chapter 15, "Common CME Management and Troubleshooting Issues."** This chapter takes the CME concepts you learned and builds them into troubleshooting scenarios. The chapter begins by discussing a general troubleshooting process you can employ for any technical troubleshooting situation, then walks through many common CME troubleshooting situations dealing with IP phone registration. The chapter concludes by discussing dial plan and QoS troubleshooting methods.
- **Chapter 16, "CUCM Monitoring, Maintenance, and Troubleshooting."** This chapter reviews the tools available to administrators to assist in the care and feeding of their CUCM servers. From the myriad of built-in reporting tools to the power of the Real-Time Monitoring Tool (RTMT), the administrator is introduced to his arsenal of tools to monitor the health and performance of the system.
- **Chapter 17, "Monitoring Cisco Unity Connection."** The wealth of built-in reporting and monitoring tools for CUC are reviewed in this chapter.

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

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

- **Appendix D, "Memory Tables":** This appendix holds the key tables and lists from each chapter with some of the content removed. You can print this appendix, and as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exams.

- **Appendix E, "Memory Table Answer Key":** This appendix contains the answer key for the exercises in Appendix D.
- **Appendix F, "Study Planner":** This is a spreadsheet with major study milestones, where you can track your progress through your study

For More Information

If you have any comments about the book, you can submit those via http://www.ciscopress.com. Just go to the website, select Contact Us, and type in your message.

Cisco might make changes that affect the CICD exam from time to time. You should always check http://www.cisco.com/web/learning/certifications/associate/index.html for the latest details.

This page intentionally left blank

This chapter covers the following topics:

- **Implementing IP Phones in CUCM:** This section reviews the required network services and systems configurations to support IP phones; details the startup and registration processes; and reviews manual, automatic, and bulk administration tasks for adding phones.
- **Describe End Users in CUCM:** This section describes the characteristics of end-user configuration in CUCM.
- **Implementing End Users in CUCM:** This section reviews the methods by which end users may be added to CUCM, including manual addition, bulk administration, and LDAP synchronization and authentication.

CHAPTER 9

Managing Endpoints and End Users in CUCM

IP phones and end users are important parts of a Unified Communications deployment; after all, without phones or people to use them, what is the point of having the system? This chapter reviews the configuration of endpoints and users in Cisco Unified Communications Manager (CUCM), including setting up basic network services, registering phones, configuration, and bulk administration.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter or simply jump to the "Exam Preparation Tasks" section for review. If you are in doubt, read the entire chapter. Table 9-1 outlines the major headings in this chapter and the corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers Appendix."

Table 9-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions Covered in This Section
Implementing IP Phones in CUCM	1–6
Describe End Users in CUCM	7
Implementing End Users in CUCM	8–10

1. Which of the following protocols is critical for IP phone operation?
   a. DNS
   b. DHCP
   c. NTP
   d. TFTP
2. What file does an IP phone first request from TFTP during its startup and registration process?
   a. SEP<mac_address>.cnf.xml
   b. None. The phone receives all information via SCCP signaling.
   c. SEP<mac_address>.xml
   d. XMLDefault.cnf.xml

3. Which of the following statements is true?
   a. SCCP phone configuration files contain all settings, including date/time and softkey assignments.
   b. SIP phone configuration files are larger than SCCP phone configuration files.
   c. SCCP phone configuration files are exactly the same as SIP phone configuration files.
   d. SIP phone configuration files are much smaller than SCCP configurations files because of the limited feature set of SIP phones.
4. Which of the following is true of DHCP in CUCM?
   a. The DHCP server capability is no longer available as of CUCM v8.x.
   b. The DHCP service is a basic capability intended for supporting up to 1000 IP phones.
   c. DHCP is mandatory for IP phones.
   d. CUCM supports a proprietary IP address assignment protocol called LLDP.
5. Which of the following is not a device pool setting?
   a. Cisco Unified Communications Manager Group
   b. Local Route Group
   c. Region
   d. Common Phone Profile
6. Bob asks you to provide a third DN button and a BLF speed dial for the Auto Parts desk's 12 7965 IP phones. Which of the following is the best choice?
   a. Modify the standard user softkey template.
   b. Copy the standard user softkey template, name it PartsDesk, and add the requested features.
   c. Copy the standard 7965 SCCP Phone Button template, name it PartsDesk, and add the requested features.
   d. It is not possible to add a third DN and a BLF speed dial to a 7965 IP phone.
7. Pete recently learned that he can add his own speed dials, subscribe to phone services, and do other useful things via his Self-Care Portal web page. He comes to you complaining that he cannot do any of these things. Why can't Pete modify his own phone?
   a. The Active Directory GPO is limiting Pete's permissions.
   b. Pete's account needs to be associated with his phone in the Device Associations settings in his User Configuration page.
   c. Additional licensing is required to support User Web Page functionality.
   d. Pete must be part of the CCM super users group to make these changes.

8. Angie changes her Windows domain login password but notices that her password for her Self-Care Portal in CUCM has not changed. Which of the following is true?
   a. LDAP synchronization has not been configured.
   b. Cisco Unified Services for Windows domains has not been configured.
   c. Angie must wait 24 hours for the password to synchronize.
   d. LDAP authentication has not been configured.
9. Which of the following is not true of LDAP synchronization in CUCM v10.x?
   a. Application user accounts must be configured in LDAP before they can be replicated to CUCM.
   b. End-user accounts that exist in CUCM and which do not exist in LDAP are maintained as local accounts in CUCM.
   c. LDAP checks the user accounts in CUCM and syncs those that also exist in LDAP.
   d. End-user accounts that exist in LDAP are synced to CUCM unless the LDAP sn attribute is blank.
10. Which is true of LDAP synchronization agreements?
   a. The User Search Base defines the point in the tree where CUCM begins searching. CUCM can search all branches below that point.
   b. The User Search Base defines the point in the tree where CUCM begins searching. CUCM can search all branches above and below that point.
   c. The User Search Base must specify the root of the domain; LDAP Custom Filters must be used to limit the search returns.
   d. All synchronization agreements must run on a regular scheduled basis.
   e. Only one synchronization agreement can be made with a single LDAP system.

Foundation Topics

Implementing IP Phones in CUCM

The implementation of IP phones is remarkably simple, considering the myriad of services, protocols, and processes going on in the background to make the system work well. This section reviews these "hidden" processes and details some of the administrative tasks required to easily and reliably run IP phones in CUCM.

Special Functions and Services Used by IP Phones

A variety of standards-based and proprietary protocols and services support IP phones in CUCM. In no particular order, they include the following:

- Network Time Protocol (NTP)
- Cisco Discovery Protocol (CDP)
- Dynamic Host Configuration Protocol (DHCP)
- Power over Ethernet (PoE)
- Trivial File Transfer Protocol (TFTP)
- Domain Name System (DNS)

The next section describes each of these services, how IP phones use them, and how to configure them in CUCM (or other systems as appropriate).

NTP

NTP is an IP standard that provides network-based time synchronization. There are many good reasons to use NTP beyond the convenience and consistency of having the same time on all devices. Call detail records (CDRs) and call management records (CMRs) are time stamped, as are log files. Comparing sequential events across multiple platforms is much simpler and easier to understand if the relative time is exactly the same on all those devices. Some functions and features can also be time (calendar) based, so time synchronization is important for those functions to operate properly.

In a typical NTP implementation, a corporate router synchronizes its clock with an Internet time server (such as an atomic clock or a GPS clock). Other devices in the corporate network then sync to the router.

The CUCM Publisher is one such device; during installation, CUCM asks for the IP address of an NTP server. (Alternatively, it can use its internal clock, which is not recommended because of its inaccuracy compared to NTP.) The Subscriber servers then sync their clocks to the Publisher, and the IP phones get their time from their subscribers via Skinny Client Control Protocol (SCCP) messages. Session Initiation Protocol (SIP) phones need an NTP reference (detailed later), but in the absence of one, they can get the time from the time stamp in the SIP OK response from the Subscriber server.

CDP

CDP is a Cisco proprietary Layer 2 protocol that provides network mapping information to directly connected Cisco devices. (You learned about CDP in your CCNA studies, so we do not detail it here.) Cisco IP phones generate CDP messages and use CDP to learn the voice VLAN ID from the Cisco switch to which they are connected. The IP phone then tags the voice frames it is transmitting with that VLAN ID in the 802.1Q/P frame header.

DHCP

DHCP is a widely used IP standard that can provide the following information to IP phones:

- IP address
- Subnet mask
- Default gateway
- DNS servers
- TFTP servers

Although it is possible to statically configure IP phones with all that information, it would be time-consuming and error-prone. DHCP is faster, easier, more scalable, and a widely accepted practice. DHCP can be provided by an existing DHCP server (because most deployments already have one), a local router, or even by CUCM itself (although this is not generally recommended for large deployments). Later sections review the configuration of DHCP services in CUCM and router IOS.

PoE

PoE is a standards-based feature that delivers DC power supply over Ethernet cabling. IP phones can use this feature, and doing so means less cabling to clutter the desk, no power supplies to buy for the phones, and potential cost savings. PoE is generally assumed to be provided by the switch that the phones connect to, but it may also be provided by a powered patch panel or inline power injector.

TFTP

TFTP is a critical service for IP phones. The phones use TFTP to download their config files, firmware, and other data. Without TFTP, the phones simply do not function properly. When you make a configuration change to a device, CUCM creates or modifies a config file for the device and uploads it to the TFTP servers. TFTP services must therefore be provided by one (or more in large deployments) of the CUCM servers in the cluster; a generic TFTP server will not have the integrated capability that a CUCM TFTP server does and will not correctly fulfill the role.

DNS

DNS provides hostname-to-IP address resolution. DNS services are not critical to IP phones. (In fact, in most deployments, it is recommended to eliminate DNS reliance from the IP phones [see Chapter 10, “Understanding CUCM Dial Plan Elements and Interactions”].) But in some circumstances, it is desirable. A DNS server must be external to the CUCM cluster; DNS is not a service that CUCM can offer.

IP Phone Registration Process

Key Topic

The steps that each phone goes through as it registers and becomes operational are more complex than you might think. The following section reviews these steps:

Step 1. The phone obtains power (PoE or AC adapter).

Step 2. The phone loads its locally stored firmware image.

Step 3. The phone learns the voice VLAN ID via CDP from the switch.

Step 4. The phone uses DHCP to learn its IP address, subnet mask, default gateway, and TFTP server address. (Other items may be learned also.)

Step 5. The phone contacts the TFTP server and requests its configuration file. (Each phone has a customized configuration file named SEP<mac_address>.cnf.xml created by CUCM and uploaded to TFTP when the administrator creates or modifies the phone.)

Step 6. The phone registers with the primary CUCM server listed in its configuration file. CUCM then sends the softkey template to the phone using SCCP messages.

Note What is in that SEP<mac_address.cnf.xml file?

The file contains a list of CUCM server, in order, that the phone should register with. It lists the TCP ports it should use for SCCP communication. It also lists the firmware version for each device model and the service URLs that each device should be using.

The CUCM server sends other configurations, such as DNs, softkeys, and speed dials, via SCCP messages in the last phase of the registration process. The configuration files for SIP phones are generally larger than the equivalent files for SCCP phones. This is because SIP phones have no equivalent mechanism for configuring items that are set by SCCP messages on SCCP phones; these items must be included in the configuration file downloaded from TFTP.

SIP Phone Registration Process

SIP phones use a different set of steps to achieve the same goal. Steps 1 to 4 are the same as SCCP phones. The following are the rest of the steps:

Step 1. The phone contacts the TFTP server and requests the Certificate Trust List file (only if the cluster is secured).

Step 2. The phone contacts the TFTP server and requests its SEP<mac_address>.cnf.xml configuration file.

Step 3. The phone downloads the SIP Dial Rules (if any) configured for that phone.

Step 4. The phone registers with the primary CUCM server listed in its configuration file.

Step 5. The phone downloads the appropriate localization files from TFTP.

Step 6. The phone downloads softkey configurations from TFTP.

Step 7. The phone downloads custom ringtones (if any) from TFTP.

Preparing CUCM to Support Phones

Before we add phones, a certain amount of work should be done on the CUCM servers. Doing this setup work makes adding phones easier, more consistent, and more scalable, assuming that we follow our design plan.

The tasks we review in this section are as follows:

- **Configure and Verify Network Services:** Set up NTP, DHCP, and TFTP.
- **Configure Enterprise Parameters:** Modify and verify cluster-wide default settings.
- **Configure Service Parameters:** Tune application settings and behavior.

Service Activation

Many required services are deactivated by default on CUCM. Using the Unified Serviceability admin page, you must activate the one you need. For our purposes, we activate the Cisco CallManager, Cisco TFTP, and Cisco DHCP Monitor services. Figure 9-1 shows the Unified Serviceability Service Activation page with those services activated.

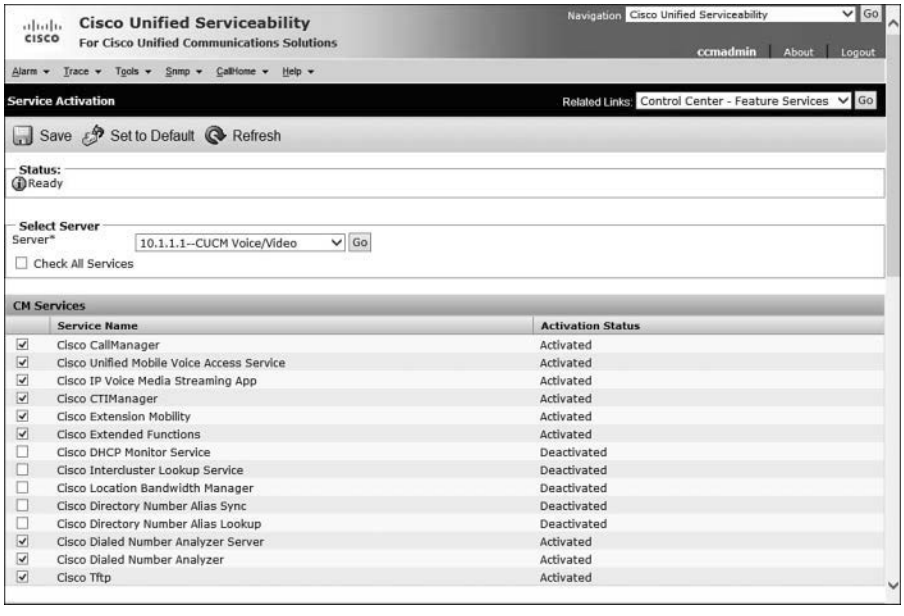


Figure 9-1 *Activating Required Services*

DHCP Server Configuration

CUCM includes a basic DHCP server capability. It is intended to support only IP phones, and not very many of them: only up to 1000 phones. (This is the maximum recommended due to heavy CPU load.) There is no native capability for DHCP server redundancy and only one DHCP server is supported per cluster. Multiple subnets (scopes) can be configured on the server.

If you decide that you want to use CUCM for DHCP, setting up the DHCP service is straightforward. We already activated the DHCP Monitor Service, so now we follow these basic steps:

Step 1. Navigate to **System > DHCP > DHCP Server**.

Step 2. Click **Add New**.

Step 3. Select the server running the DHCP Monitor Service from the pull-down.

Step 4. Configure the desired settings.

The settings that can be configured on the Server page include the following (among others):

- Primary DNS Server IPv4 Address
- Primary TFTP Server IPv4 Address
- IP Address Lease Time

Any settings you configure on the server page are inherited by the subnet configuration (shown next); however, any setting you change on the subnet page overrides the Server setting. Figure 9-2 shows the DHCP Server Configuration page.

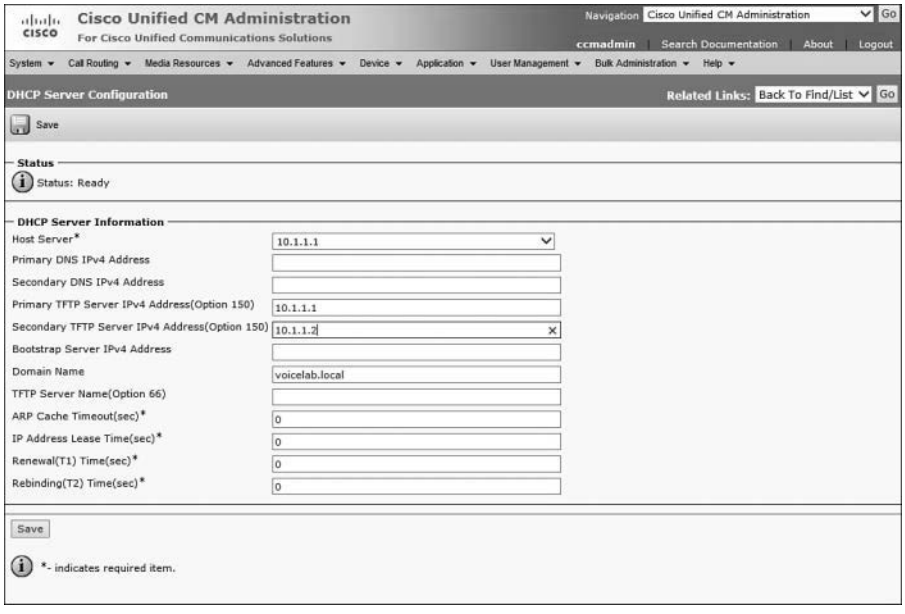


Figure 9-2 *DHCP Server Configuration*

Configuring DHCP subnets requires some understanding of IP subnetting and assumes that you have an IP addressing plan in place. Because these topics are covered in the CCNA prerequisite, we assume you have a grasp of these fundamentals. To configure DHCP subnets, navigate to **System > DHCP > DHCP Subnet**. Click **Add New** to create subnets; you can create multiple subnets as needed for your environment design. On the Subnet Configuration page, select the server from the DHCP Server drop-down list. You can then configure the following (some other settings are not listed):

- Subnet address
- Primary range start IP

- Primary range end IP
- Primary router IP address (default gateway)
- Subnet mask
- Primary DNS server IP address
- TFTP server IP address

Remember that settings in the subnet configuration override the same settings in the server configuration. Figure 9-3 shows the DHCP Subnet Configuration page.

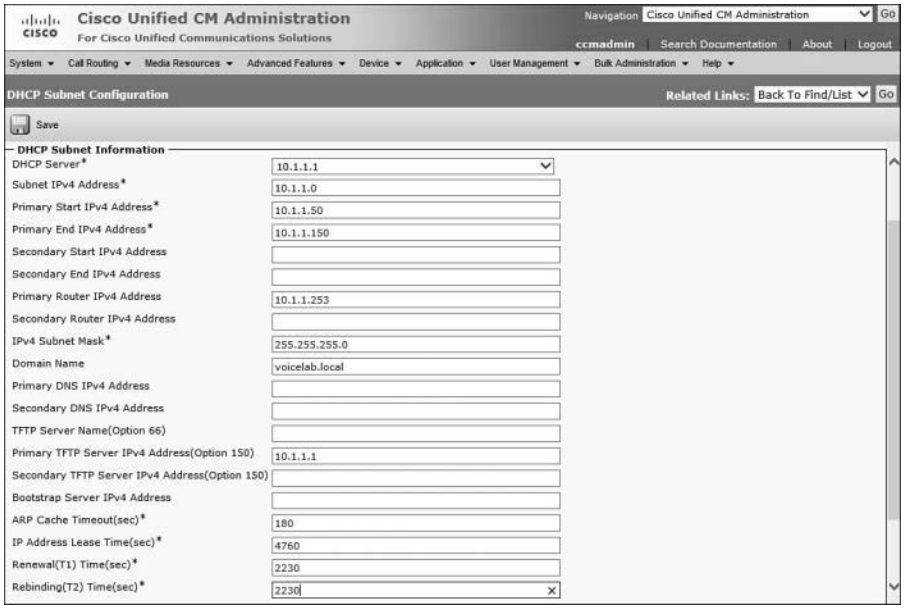


Figure 9-3 *DHCP Subnet Configuration*

Configuring DHCP in Router IOS

Cisco routers support basic DHCP server functionality, and this capability is commonly used in small office environments where a dedicated DHCP server is not needed or available. Example 9-1 shows a typical DHCP configuration, with commands annotated for reference:

Example 9-1 *DHCP Configuration*

```
service dhcp
! Enables the DHCP service
!
ip dhcp excluded-address 10.1.1.1 10.1.1.10
! Specifies a start / end range of addresses that DHCP will NOT assign
ip dhcp pool name IP_PH0NES
! Creates a pool of addresses (case-sensitive name) and enters DHCP configuration mode
!
network 10.1.1.0 255.255.255.0
! Defines the subnet address for the pool
```

```
default-router address 10.1.1.1
! Defines the default gateway
dns-server address 192.168.1.10 192.168.1.11
! Identifies the DNS server IP address(es) - up to 8 IPs
!
option 150 ip 192.168.1.2
! Identifies the TFTP server IP. Multiple IPs may be included, separated by spaces.
```

Multiple DHCP pools can be created, so DHCP services can be provided for PCs in a small office by the same router. For some third-party SIP phones, it may be necessary to specify Option 66 (the TFTP server DNS name).

IP Phone Configuration Requirements in CUCM

CUCM has several configuration elements for IP phones. We briefly look at the following basic required elements:

- Device pool
- Cisco Unified CM group
- Region
- Location
- Date/time group
- Phone NTP reference
- Device defaults
- Softkey template
- Phone button template
- SIP profile
- Phone security profile
- Common phone profile

Device Pool

Device pools provide a set of common configurations to a group of devices; think of a device pool as a template to apply several different settings all at once, quickly and accurately. You can create as many device pools as you need, typically one per location, but they can also be applied per function. (For example, all the phones in the call center may use a different device pool from the rest of the phones in the administration offices, although they are all at the same location.) There are several settings within the device pool; some of the ones relevant to us are as follows:

- **Cisco Unified CM group:** A CM group defines a top-down ordered list of redundant call-processing servers to which the phones can register. The list can include a maximum of three servers (plus an optional Survivable Remote Site Telephony [SRST] reference). The first server in the list is the primary subscriber, the second is the backup, and the third is the tertiary. In normal operation, phones send primary registration messages to

the primary, backup registration messages to the backup, and nothing to the tertiary. If the primary server fails or otherwise becomes unavailable, the phone sends a primary registration message to the backup server (and registers with it) and begins sending backup registration messages to the tertiary.

The number of CM groups created depends on the number of subscribers in the cluster; the goal is to provide server redundancy to the phones while distributing phone registrations evenly as planned in the system design. A server may be listed in more than one CM group to provide an overlapping depth of coverage, as long as its performance capacity will not be exceeded in any foreseeable failure circumstance. This is simply another requirement of a good design.

- **Region:** A region is a virtual assignment that allows the system designer to control the bit rate for calls. For example, if we define two regions, called Vancouver_HQ_REG and Ottawa_BR_REG, we can set the bit rate for calls within the Vancouver region to 256 kbps, within the Ottawa region to 64 kbps, and between the two regions to 16 kbps.

  We are in effect selecting (or at least influencing) the codec to be used for these calls; the codec in turn generates a known bit rate, which in turn uses a predictable amount of bandwidth and provides a predictable voice quality. In general, it is assumed that WAN bandwidth is limited; selecting a lower bit rate reduces the amount of bandwidth per call at the expense of call quality.

- **Location:** As you just saw, we can select the appropriate bit rate for calls and, therefore, the bandwidth used by each call. Given that WAN bandwidth is assumed to be limited, we need to be able to limit the amount of bandwidth used by calls to a particular location. Location defines a maximum amount of bandwidth used by calls to a particular location; each call is tracked, and the bandwidth it uses is deducted from the total for that location. When the bandwidth remaining is not enough to support another call at a given bit rate, that call is dropped by default (but may be rerouted over the PSTN if AAR is correctly configured). This is one mechanism for Call Admission Control (CAC), which is described later in this book.

- **Date/time group:** As discussed earlier, it is recommended to use NTP for time synchronization of all devices. The problem is that NTP references Greenwich mean time, which makes the time displayed on devices "wrong" if they are not in the GMT time zone. Date/time groups allow us to offset the correct time learned via NTP to match the local time zone of the device. Date/Time Groups also allow us to display the time and date in the desired format, which can vary from place to place.

- **Phone NTP reference:** SIP phones need an NTP server address from which they can obtain the time using NTP. (This is not required for SCCP phones, which are configured to the correct time using SCCP signaling.) It is preferred that the NTP reference be local to the phones that need it.

It is common to have groups of phones with similar configurations. Using a device pool for each group simplifies and speeds up administrative tasks, while making them less error-prone in the bargain. Figure 9-4 shows part of a Device Pool Configuration page.

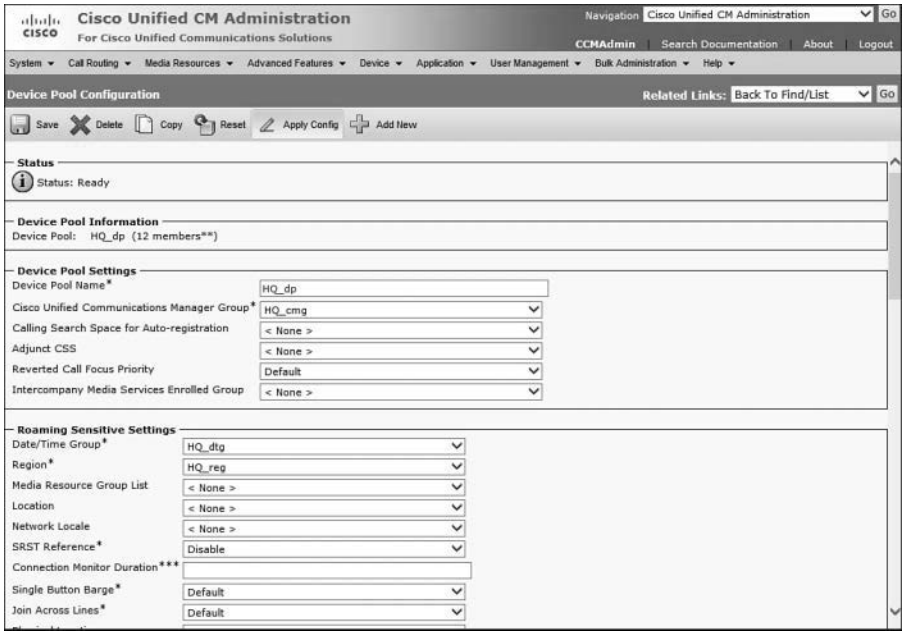


Figure 9-4 *Device Pool*

Device Defaults

The Device Defaults page lists all the supported endpoints (with separate entries for SCCP and SIP as necessary), and the firmware load, device pool, and phone button template each endpoint uses by default. This allows an administrator to set useful system-wide defaults for any newly registered device of each type.

Softkey Template and Phone Button Template

The softkey template controls what softkey button functions are available to the user; these are typically used for feature access (conference, transfer, park, Extension Mobility, and so on). Seven softkey templates are available by default, and you can create as many more as your design requires.

The Phone Button template defines the behavior of the buttons to the right of the phone screen (for most models). Eighty (or more) are defined by default because there are unique templates for each supported phone type—and for most phones, a separate template for SCCP and SIP. The default templates typically provide two lines and as many speed dials as there are remaining buttons on a particular phone model; you can add and customize the templates to assign each button one of many different functions.

Profiles

Profiles allow for a one-time configuration of repetitive tasks; several types of profiles exist, and you can create many versions of each type to be applied to phones as needed.

Phone Security Profile

A default phone security profile exists for each type of phone/protocol. These default profiles have security disabled; you can choose to configure the device as secured, set encrypted TFTP configuration files, and modify Certificate Authority Proxy settings.

Common Phone Profile

The common phone profile includes settings that control the behavior of the phone, including the following:

- DND settings
- Phone personalization capabilities
- VPN settings
- USB port behavior
- Video capabilities
- Power-save options

Adding Phones in CUCM

Phones can be added to CUCM in several ways:

- **Manual configuration:** The administrator creates a new phone, configuring all settings in real time on the Phone Configuration page.
- **Auto-registration:** The administrator configures CUCM to dynamically configure and add to the database any new IP phone that connects to the network.
- **Bulk Administration Tool (BAT):** Using templates configured for the purpose by the administrator in CUCM, the administrator creates CSV files that contain all the required information to create multiple phones in one operation.
- **Auto Register Phone Tool (TAPS):** An Interactive Voice Response (IVR) server enhances the auto-register and BAT functionality, providing an automated method of adding potentially thousands of phones at a time.
- **Self-provisioning:** Operating in a manner similar to TAPS, self-provisioning is a new capability for CUCM 10.x. The IVR and CTI capabilities are now integral to the CUCM application, and no external server is required; the required administrative steps are detailed later in this section.

The following sections provide more detail on each of these operations.

Manual Configuration of IP Phones

The basic steps for manually adding an IP phone are as follows:

Step 1. Navigate to **Device > Phone**, and then click **Add New**.

Step 2. Choose the IP phone model from the drop-down list.

Step 3. Choose the device protocol (either SCCP or SIP; some phones will support only one protocol, and this step will be skipped).

Step 4. Select, or enter, the required specific information for the phone. The five required settings that do not have default values (must be manually configured) include the following:

- **MAC Address:** The MAC address is the unique identifier that links the IP phone hardware to the software configuration in CUCM. If you are building a phone for Bob, you must obtain the MAC address of the phone that will end up on Bob's desk; otherwise, Bob will not see the correct settings, DN, and so forth.
- **Device Pool:** The device pool (as described earlier in this chapter) applies many common settings to the phone that are relevant to its physical location and desired behavior.
- **Phone Button Template:** The Phone Button template (also detailed earlier in this chapter) defines what functions are assigned to the buttons on the phone (DNs, speed dials, services, and so on).
- **Owner User ID:** Associates or assigns the phone to a user account for license calculation purposes. This setting should not be confused with the user configuration page setting for device association, which is used for features such as the Self-Care Portal and Extension Mobility.
- **Device Security Profile:** Applies a set of security-related configurations, as described previously in this chapter.

Step 5. Click **Save**.

When the page reloads, a new pane labeled Association Information appears on the left, in which you can configure the phone buttons functions. The base functionality (line, speed dial, intercom, service, and so on) is defined by the Phone Button template specified previously; here is where you specify what the DN number on the lines will be, what service is accessed, or which Intercom DN is dialed. Figure 9-5 shows the Phone Configuration page, including the Association Information pane.

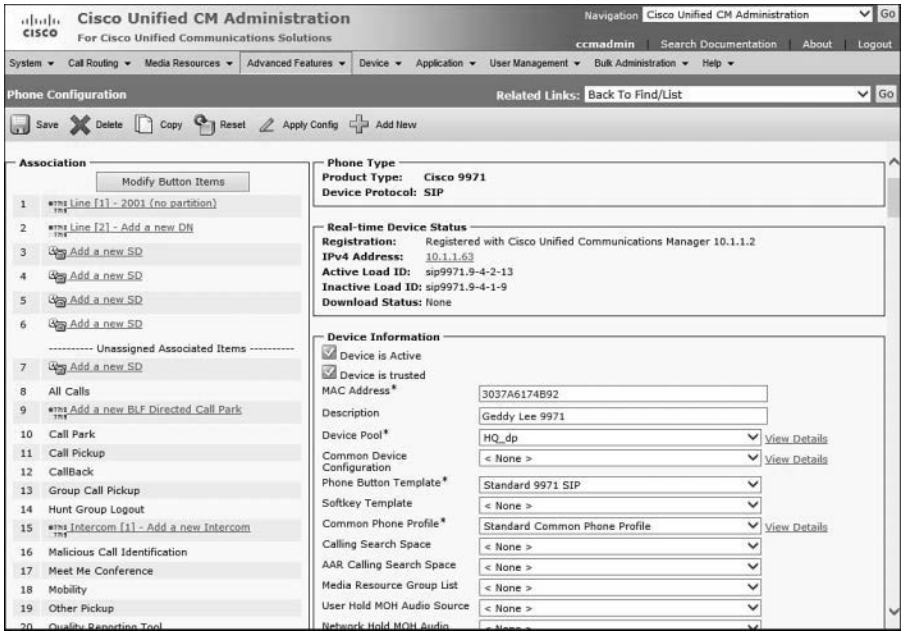


Figure 9-5 *The Phone Configuration Page*

In the Association Information pane, continue the basic phone configuration steps, as follows:

Step 6. Click **Line [1] - Add New DN**. The Directory Number Information page opens, in which you must enter a directory number, and optionally set the partition and other optional configurations. The following points highlight a few of the settings found on the Directory Number Configuration page:

- **Route Partition:** As discussed in Chapter 10, the partition is part of the calling privileges system or class of control.
- **Alerting Name:** This is the name to display on the caller's phone when this phone is ringing. Some public switched telephone network (PSTN) connections might not support this functionality.

- **Call Forward and Call Pickup Settings:** This is where the administrator can determine how to forward a call if the DN is busy or does not answer, or for Call Forward All. The user can set Call Forward All at the phone itself using the CallFwdAll softkey or on their user web page; other call forward settings (such as Busy and No Answer) are available to the user only on the user's user web page and not on the phone.
- **Display:** The text entered in the Display field serves as an internal caller ID. When this DN calls another IP phone, the display text replaces the calling DN number. In other words, if Bob's DN is 5309 and the Display field is blank, when Bob calls Ethan, Ethan's phone shows that 5309 is calling. If the Display field on Bob's phone has Bob Loblaw as the entry, Ethan's phone displays the caller as Bob Loblaw.
- **Line Text Label:** This is the text that displays on the phone to describe the line; for example, if the second button on the phone is the shared DN for the Parts Desk, the line text label for line 2 might read "Parts Line."
- **External Phone Number Mask:** If this phone makes an off-net call (typically to the PSTN), this field can change the calling line ID (CLID) to present a full PSTN number instead of the internal DN.

Step 7. Click **Save** twice.

Tip The "Save twice" instruction is a recent one, and one that will trouble a lot of admins who are familiar with versions of CUCM prior to 9.x. Watch for the message at the top of the DN Configuration page when you click Save the first time: "Directory Number Configuration has refreshed due to a directory number change. Please click Save button to save the configuration." If you do not Save again, your changes are not preserved (but this should only happen if you change the DN).

Step 8. In the Related Links drop-down, select **Configure Device** (<*Phone*>), and then click **Go**.

Step 9. You are now back at the Phone Configuration page for the new phone. At this point, if you need to continue making config changes you can do so, or you can click **Save** again to commit the changes so far. The page prompts you to "Click on the Apply Config button to have the changes take effect." This happens because in order for the phone to adopt the changes, it has to reload with its new config. This requires either a restart or a reset, depending on what was changed.

Note There is a great deal of confusion about Restart, Reset, and Apply Config. The differences are explained in the following points:

- A reset reboots both the firmware and the configuration of the phone. Some information such as firmware version, locale changes, SRST, or Communications Manager Group changes require a full reset so that the phone will pull a new file from the TFTP server. A reset can be triggered

from the Administration web page, or from the phone itself by entering **Settings >** **#** (using the keypad).

- A restart unregisters the phone, and then the phone comes right back and registers again. Because Communications Manager reads the database for this device when it registers, it is a good way to refresh information that is not passed through the configuration file. Button changes, names, and forwarding would only require a restart. A restart is faster than a reset because the firmware is not rebooted as well.
- The confusion between Restart and Reset was such that in CUCM 8.x, a new function called Apply Config was introduced. This button intelligently triggers either a reset or a restart as appropriate, depending on what changes were made to the device. In all cases, the phone has to be registered for the reset or restart to be sent to the phone.

It is common, especially if advanced features such as Extension Mobility or Cisco Unified Personal Communicator are in use, to associate a user with a particular device (IP phone). It is required to associate the user with the device if you want users to be able to use the user web pages to customize their phones. The end user is associated with the device (IP phone), and the device is associated with one or more DNs. This allows the user not only to access the user web pages to configure this phone, but for other applications and processes to interact with the user through the phone system.

So, what happens if you delete an end user who is associated with a device that is associated with a DN? Nothing. Although the association exists and is important and useful, the three database entities of user, device, and DN are independent of each other. The device and the DN do not go away if the user is deleted, and the same result applies if the device or DN are deleted (although a phone without a DN, or a DN without a phone, cannot make calls).

Auto-Registration of IP Phones

CUCM includes the auto-registration feature, which dynamically adds new phones to the database and allows them to register, including issuing each new phone a DN so that it can place and receive calls. Auto-registration is supported by all Cisco IP phones.

To enable auto-registration, perform the following steps:

Step 1. Verify your auto-registration phone protocol. Access this setting under **System > Enterprise Parameters**; choose either **SCCP** (default) or **SIP**. Phones that do not support the chosen protocol will still auto-register using their native protocol.

Step 2. Verify that at least one CM Group has auto-registration enabled (by selecting the check box for Auto-Registration Cisco Unified Communications Manager Group).

Step 3. Enable and configure auto-registration on one or more CUCM servers within the CM group enabled for auto-registration:

- Enable auto-registration by deselecting the **Auto-Registration Disabled on this Cisco Unified Communications Manager** check box; it is disabled by default, so unchecking the box enables it.
- Configure the range of DNs that will be dynamically and sequentially issued to auto-registering phones. The default starting directory number is 1000; if you change the ending directory number to anything higher than 1000, Auto-registration is automatically enabled. If you set the starting and ending DNs to the same value, auto-registration is automatically disabled. (Auto-registration is disabled by default because both the starting and ending directory numbers are set to 1000.) You want to choose a range of DNs that fits in well with your dial plan to avoid overlap and confusion.
- Select a (previously configured) universal device template (UDT) and universal line template (ULT). UDTs and ULTs are introduced and explained in the following note.
- Set the Partition that will be assigned to the auto-registered DNs. This is optional, but it is one good way to limit and control auto-registered phones.
- Verify that the Auto-Registration Disabled on this Cisco Unified Communications Manager check box is unchecked, and then click **Save**.

A simple way to test auto-registration is to plug in a new phone; if it receives a DN in the range you specified (or a DN in the range of 1000 to 1999 if you left it at the defaults), auto-registration is working.

Some administrators see auto-registration as a security weakness because any IP phone will be dynamically added to the database and potentially begin making calls, perhaps even to the PSTN if it is not restricted. It is common to enable auto-registration only when it is needed to prevent the registration of "rogue phones."

Figure 9-6 shows the Auto-Registration Information section of the Unified CM Configuration page.

Note UDTs and ULTs were introduced in CUCM v9.0 as a way to simplify and accelerate the administrative process of adding new phones and users. In essence, they are simply ordinary templates that you create (as many as you need) and set up with common settings for each of the different groups of phones you identify. What makes universal templates interesting is that they utilize variables so that as you create a phone, the UDT/ULT can be set up to create a description as "User's first name followed by user's last name," for example, and have the actual names inserted when the associated user is identified. The other cool part of the universal templates is the interface, which is modern and interactive.

Figure 9-7 shows a UDT under construction. In the UDT configuration screen, clicking the little pencil icon next to the Device Description field opens the Build Input for Device Description dialog box shown in the callout bubble. In this dialog, clicking the various icons labeled with First Name, Last Name, and so forth builds a string of variables (for example, #FirstName##LastName#) as shown in the Device Description field. Those variables are

replaced by the actual first and last names of the user when the phone is associated to the user during self-provisioning. You can do this any time the pencil icon is available next to a field. It is not always applicable, of course. Most of the fields do not use data for which variables are necessary; for those, simply enter or select the appropriate data.

UDTs and ULTs are a cool and useful tool in the day-to-day move/add/change routine of CM administration.

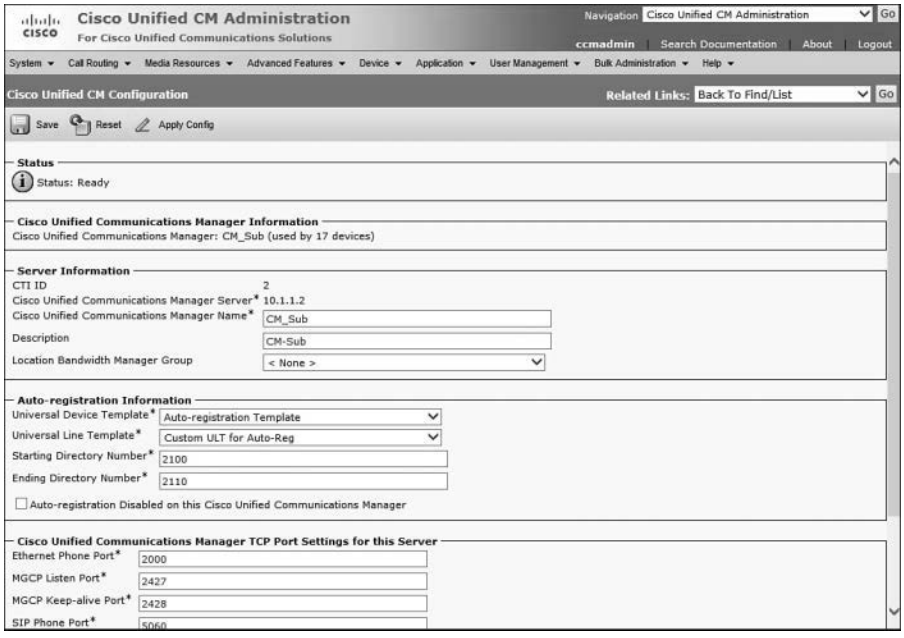


Figure 9-6 *Auto-Registration Configuration*

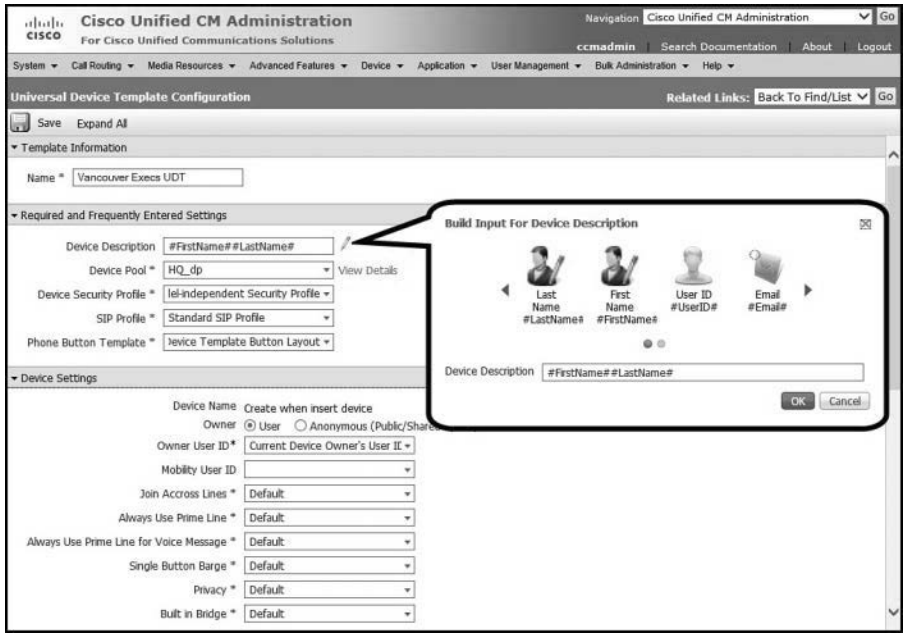


Figure 9-7 *Building a Universal Device Template*

Bulk Administration Tool

The Bulk Administration Tool (BAT) enables administrators to perform database inserts, modifications, or deletions in bulk. This makes it feasible to add a great many phones, users, or other elements more quickly and with fewer errors; it also allows the administrator to schedule the operation to happen automatically and unattended.

The BAT Export feature enables the administrator to pull selected records from the database and export them. The administrator can then modify the records and re-import them into the database, making bulk changes faster and more accurate.

BAT can be used to add, modify, or delete almost any component in CUCM, including phones, users, forced authorization codes and client matter codes, user device profiles, the region matrix, gateway devices, and many others.

The components of BAT include an Excel template that provides the required fields and formatting for the new unique data server-side templates that configure the common data and a set of web page interfaces for preparing and executing the many operations that BAT supports.

The Excel template is downloaded from the CUCM server. The administrator then customizes the templates for the needs of this BAT operation, populates the required fields with the correct data, and uploads the resulting CSV file to the server.

Using the BAT interface appropriate for the operation (insert phones, insert users, create call routing components, and so on), the administrator may need to create a server-side BAT Template for adding new devices, or in some cases simply select the uploaded CSV file for

processing. If templates are required (as they would be if adding phones, for example), the template specifies all the settings that all the phones have in common, whereas the CSV file specifies all of the unique settings for each phone, such as DN, line text label, and so forth.

The only trick to adding phones with the BAT tool is that the MAC address of each phone must be specified. Using a barcode scanner to scan the MAC barcode label on the phone into the CSV file makes things faster and more accurate, but there is another challenge waiting for you: You create a detailed config for the phone, including DNs and other user-specific settings, and you specify the MAC address of the new phone. Now you must make sure that the physical phone with that MAC gets to the user it was built for; this is no easy task if several hundred phones are being deployed at once.

A couple of alternative strategies are available to make BAT deployments easier. One is to use auto-registration to get all the phones working and then use the BAT tool to modify the phones' configurations after the fact. This approach still has some weaknesses, notably that you must still be positive of the MAC address of the physical phone that sits on the desk and match it to the database entry that BAT changes.

Auto Register Phone Tool

A more sophisticated (but much more complex) strategy involves the use of the Auto Register Phone Tool (formerly known as the Tool for Auto Registered Phone Support, but which is still known as TAPS because it is a better acronym than ARPT). TAPS goes one step further in the automation of new IP phone deployments, as summarized in the following steps:

Step 1. An IP-IVR server is built and configured to support TAPS, and the CUCM server is integrated with the IP-IVR server. The IP-IVR functionality is supported by several Cisco applications, including Unified Contact Center Express.

Step 2. The administrator prepares a BAT job, specifying a device template for all the common phone settings and a detailed CSV file with all the unique phone settings. The administrator runs the BAT job, substituting fake "dummy" MAC addresses for the as-yet-unknown real ones. (A simple check box in the BAT interface does this substitution automatically.)

Step 3. The new phones are auto-registered and receive a DN. They can now place calls.

Step 4. Using Bob's phone as an example: Bob (or perhaps an administrator if Bob feels uncomfortable doing so) picks up his new auto-registered phone that currently has DN 1024 (from the default auto-registration range) and dials the specially configured IP-IVR pilot number.

Step 5. The IP-IVR may prompt Bob to authenticate. (This is an optional but more secure approach.) When Bob has authenticated successfully, the IP-IVR prompts Bob to enter the extension his phone should have; in a new deployment, this may be provided to Bob on an information sheet, or it may simply be the same extension (let's assume 5309 in this case) that he had on the old phone system that is being migrated to CUCM.

Step 6. When Bob enters the extension, the IP-IVR records his input of 5309 and captures the MAC address of the phone Bob is using. The IP-IVR sends all this information to CUCM.

Step 7. CUCM looks up the extension of 5309 in the database and finds it in the record for one of the newly added BAT job phones; the one that will become Bob's phone. CUCM replaces the dummy MAC address in the BAT record with the real MAC captured and forwarded by the IP-IVR. The database record is now complete and accurate, including the real MAC address of the phone that sits on Bob's desk.

Step 8. CUCM restarts Bob's phone, and when it comes back online, it is fully configured with all the specific details from the BAT record for Bob's phone.

This is a powerful way to deploy thousands of IP phones. With some minor tweaks and some training of the users, it requires minimal administrator involvement in the phone deployment. The downside is that it requires the IP-IVR hardware and software and a capable administrator to configure it and still involves either training users to set up their own phones or using administrators to perform repetitive simple tasks, which are not cost-effective uses of their time.

Self-Provisioning

Self-provisioning is conceptually almost exactly the same as TAPS, with the very significant difference being that all of the IVR capability has been integrated into the CUCM application. This means that we no longer need to go to the trouble and expense of building and configuring an external IVR; we just configure CM to do it for us. Self-provisioning utilizes UDTs and ULTs, giving us even better customization with much less effort because we can leverage the variables definitions in the UDT and ULT.

Describe End Users in CUCM

It is technically true that a phone system does not need end users. If a person sits in front of a phone and starts using it, it does not really matter who the person is as long as the phone does what that person needs it to do. But a Unified Communications system provides much more than just phone functionality; it has a massive array of features that can be provided to and customized by individual users. Converged networks are increasingly complex, and end users expect an increasing simplicity of use. The configuration of end users is an integral part of a full-featured system, or as one of my friends put it: "All the fun stuff needs user accounts."

End Users Versus Application Users

CUCM makes a clear distinction between end users and application users. The distinction is simple: End Users are typically people who type a username and password into a login screen (usually a web page) to access features or controls. An application user is typically an application that sends authentication information inline with a request to read or write information to a system (perhaps a third-party billing application accessing the CDR/CAR database, for example). Table 9-2 lists some of the characteristics and limitations of end users versus application users.

Table 9-2 End Users Versus Application Users

End Users	Application Users
Associated with an actual person	Associated with an application
For individual use in interactive logins	For noninteractive logins
Used to assign user features and administrative rights	Used for application authorization
Included in the user directory	Not included in the user directory
Can be provisioned and authenticated using Lightweight Directory Access Protocol (LDAP)	Must be provisioned locally (no LDAP)

Credential Policy

The credential policy defines preset passwords, end-user PINs, and application-user passwords. The default credential policy applies the application password specified at install to all application users.

Administrators can define additional policies that can specify the allowed number of failed login attempts, minimum password length, minimum time between password changes, number of previous passwords stored, and the lifetime of the password. The policy can also check for weak passwords. A strong password

- Contains three of the four characteristics: uppercase, lowercase, numbers, and symbols
- Cannot use the same number or character more than three times consecutively
- Cannot include the alias, username, or extension
- Cannot include consecutive numbers or characters

Similar rules exist for phone PINs:

- Cannot use any number more than two times consecutively
- Cannot include the user mailbox or extension, nor the reverse of them
- Must contain at least three different numbers (for example, 121212 is invalid)
- Cannot be the dial-by-name version of the user name (such as Mike = 6453)
- Cannot contain repeated digit patterns, nor any patterns that are dialed in a straight line on the phone keypad (for example, 2580 or 357)

Features Interacting with User Accounts

The following features use the end-user account login process, with either the username/password or PIN as the authentication:

- Unified CM Administration web pages
- User web pages (Self-Care Portal)
- Serviceability
- OS administration
- Disaster recovery system

- Cisco Extension Mobility
- Cisco Unified Communications Manager Assistant
- Directories
- IP phone services
- Data associated with user accounts

User account information is divided into three categories, with fields for specific data in each category:

1. **Personal and Organizational Settings:**
   - UserID
   - First, Middle, Last Name
   - Manager UserID
   - Department
   - Phone Number, Mail ID
2. **Password Information:** Password
3. **CUCM Configuration Settings:**
   - PIN
   - SIP Digest Credentials
   - User Groups and Roles
   - Associated PCs, controlled devices, and DNs
   - Application and feature parameters (Extension Mobility, Presence Group, CAPF)

Application user accounts use a subset of the previous attributes.

User Locale

User locales allow different languages to be displayed on the IP phone and the user web pages. Additional locales are installed on the CUCM server; then specific locale files are downloaded to the phone via TFTP. This allows for the customization of the primary interfaces for users in a wide range of available locales/languages.

Device Association

For users to be able to control their own devices (using the Self-Care Portal to up their own speed dials, services, and ring preferences, for example), the end-user account must be associated with the device. In CUCM, end users can be associated with IP phones, Cisco IP Communicator (CIPC), and Cisco Extension Mobility profiles.

Because the end-user account must have a unique user attribute name in the CUCM database, it is possible to dial a user by name. Cisco Unified Presence Server (CUPS) tracks the availability status of a user and his communication capabilities (such as voice, video, and chat).

Implementing End Users in CUCM

End users can be added to the CUCM database via three main methods:

- Manual, one-at-a-time entry
- Bulk import using the Bulk Administration Tool
- LDAP synchronization (and optional authentication)

This section reviews each of these methods.

Manual Entry

The CUCM database includes fields for comprehensive user information. Only some of these fields are required, including the following:

- User ID
- Last Name
- Presence Group (defaults to Shared Presence Group)
- Remote Destination Limit (defaults to 4)

Given that the last two required fields are populated by default, it is clear that CUCM does not require much information to create a new user. The user ID must be unique, which implies that you should have a naming convention that accommodates many users with similar names.

There are many optional fields on the End User Configuration page, including Password, PIN, First Name, Telephone Number, and Device Association. The more users you have, the more likely it is that these optional fields will be populated to implement features, improve searching and reporting, or improve security. Figure 9-8 shows part of the End User Configuration page.

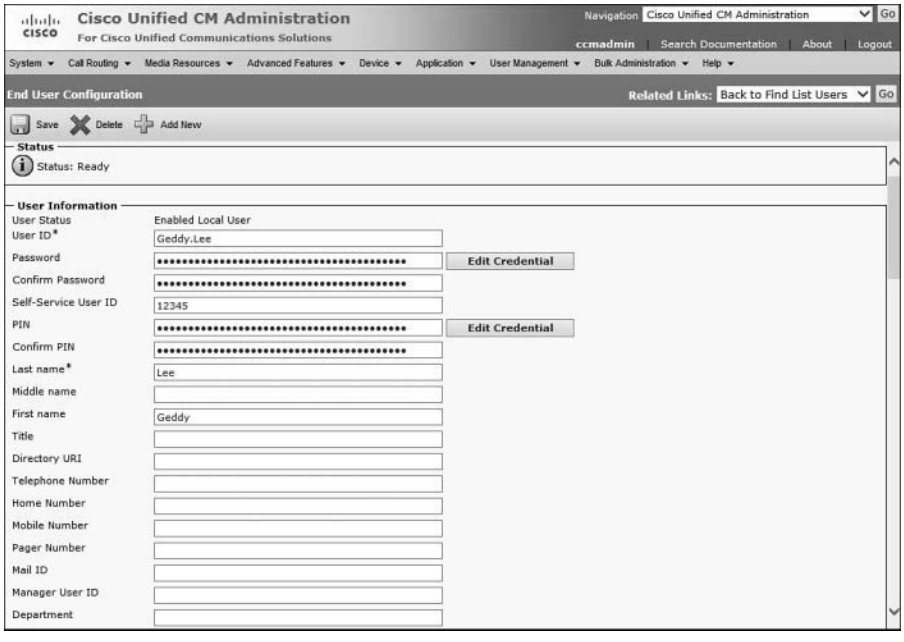


Figure 9-8 *End User Configuration Page*

Bulk Import Using BAT

Instead of adding potentially hundreds or thousands of users one at a time, the administrator can add users in bulk using the Bulk Administration Tool. BAT allows the administrator to create and upload a CSV file with all the users' information populated and insert the data into the database in an automated way. BAT is a fast way to add, remove, or modify database entries for many fields in the CUCM database.

LDAP Integration

Key Topic

CUCM supports integration with Lightweight Directory Access Protocol (LDAP). LDAP is a standards-based system that allows an organization to create a single, centralized directory information store. LDAP holds information about user accounts, passwords, and user privileges. The information centralized in LDAP is available to other applications, so that separate directories do not need to be maintained for each application. Using LDAP simplifies user administration, and makes using systems slightly easier for users because they only need to maintain their information and passwords in one place.

Note Only end users are replicated by LDAP sync. Application users are always and only maintained as local entries in the CUCM database.

CUCM supports LDAP integration with several widely used LDAP systems, including the following:

- Microsoft Active Directory 2000, 2003 and 2008 (support for AD 2012 only in CUCM 10.x and later)
- Microsoft Active Directory Application Mode 2003
- Microsoft Lightweight Directory Services 2008
- iPlanet Directory Server 5.1
- Sun ONE Directory Server (5.2, 6.x)
- Open LDAP (2.3.39, 2.4)

CUCM can interact with LDAP in two ways: LDAP Synchronization populates the CUCM database with user attributes from LDAP, and (as an optional additional configuration) LDAP authentication redirects password authentication to the LDAP system. Typically, synchronization and authentication are enabled together. In either case, some information that now comes from LDAP is no longer configurable in CUCM; the fields actually become read-only in CUCM, because the information can only be edited in LDAP. The following sections review LDAP synchronization and authentication in more detail.

LDAP Synchronization

Implementing LDAP synchronization (LDAP sync) means that some user data (but not all) for LDAP-sourced end user accounts is maintained in LDAP and replicated to the CUCM database. When LDAP sync is enabled, LDAP-sourced user accounts must be created and maintained in LDAP and cannot be created or deleted in CUCM; the user attributes that LDAP holds become read-only in CUCM. However, some user attributes are not held in

LDAP and are still configured in CUCM because those attributes exist only in the CUCM database. As of CUCM v9.x, local CUCM user accounts can coexist with LDAP-sourced accounts; in this case, CUCM maintains read-write access to all the attributes of local accounts, but LDAP-sourced accounts still have attributes that are read-only in CUCM and which must be managed in the LDAP system.

It is important to understand that when using LDAP sync without LDAP authentication, the user passwords are still managed in the CUCM database. This means that, although a user account in LDAP is replicated to the CUCM database, the user password must be maintained separately in both the LDAP system and in CUCM.

CUCM uses the DirSync service to perform LDAP sync. The synchronization can be configured to run just once, on demand, or on a regular schedule. The choice depends on the system environment and the frequency of changes to LDAP content; the need for up-to-date information must be balanced against the load on the servers and network if the sync is frequent or takes place during busy times.

Note If LDAP authentication is enabled and LDAP fails or is inaccessible, only local end-user accounts will be able to log in to the CUCM (in addition to any application user accounts including the primary Administrator account defined at install). This may cause drastic unified communications service interruption, depending on how users normally interact with the system. Of course, if LDAP has failed, it is likely to be a serious issue already, causing many applications to cease functioning.

LDAP Authentication

LDAP authentication redirects password authentication requests from CUCM to the LDAP system. End-user account passwords are maintained in the LDAP system and are not configured, stored, or replicated to CUCM. Because one of the benefits (particularly to the end user) of LDAP is a centralized password system (making single sign-on possible), it is typical and desirable to implement LDAP authentication with LDAP sync.

LDAP Integration Considerations

A common misconception regarding CUCM LDAP integration is that all user data resides in LDAP. This is absolutely false. With LDAP sync, certain LDAP user attributes are held in the LDAP directory and are replicated to the CUCM database as read-only attributes. The balance of the user attributes in the CUCM database (fields such as associated devices, PINs, Extension Mobility profile, and so on) are still held and managed only in the CUCM database.

There is a similar misconception with LDAP authentication: Remember that the LDAP password is not replicated to the CUCM database; rather, the authentication process is redirected to the LDAP system. When an LDAP authentication-enabled user logs in to CUCM, the username and password are sent to the LDAP system (the password in sent as an MD5 hash). The LDAP system compares the submitted hash with its own hash of the correct password, and if they match, then the LDAP system indicates to the CUCM that the user is successfully authenticated (and, obviously, if the hashes do not match, the authentication fails).

The interaction of CUCM with LDAP varies with the type of LDAP implementation. The primary concern is how much data is replicated with each synchronization event. For example, Microsoft Active Directory performs a full sync of all records contained in the configuration every time; this can mean a very large amount of data is being synchronized, potentially causing network congestion and server performance issues. For this reason, sync intervals and scheduling should be carefully considered to minimize the performance impact.

Synchronization with all other supported LDAP systems is incremental (for example, only the new or changed information is replicated), which typically greatly reduces the amount of data being replicated, thereby reducing the impact on the network and servers.

LDAP Attribute Mapping

The user attribute field names that LDAP uses are most likely different from the equivalent attribute field names in the CUCM database. Therefore, the various LDAP attributes must be mapped to the appropriate CUCM database attribute. Creating an LDAP sync agreement involves identifying the one LDAP user attribute that will map to the CUCM user ID attribute. In a Microsoft Active Directory integration, for example, the LDAP attribute that will become the CUCM user ID can be any one of the following:

- sAMAccountName
- uid
- mail
- TelephoneNumber

It does not matter which one is chosen, but for consistency and ease of use, the attribute that the users are already using to log in to other applications should be used.

After the initial user ID mapping is selected, some other LDAP attributes should be manually mapped to CUCM database fields. Table 9-3 lists the fields in the CUCM database that map to the possible equivalent attribute in each type of supported LDAP database.

Table 9-3 LDAP User Attribute Mapping

CUCM	Microsoft AD	Other Supported LDAP
User ID	sAMAccountName	uld
	mail	mail
	employeeNumber	employeeNumber
	telephoneNumber	telephonePhone
	UserPrincipalName	
First Name	givenName	Givenname
Middle Name	middleName	initials
	Initials	
Last Name	sn	sn

CUCM	Microsoft AD	Other Supported LDAP
Manager ID	manager	manager
Department	department	department
Phone Number	telephoneNumber	telephonenumber
	ipPhone	
Mail ID	mail	mail
	sAMAccountName	uld

LDAP Sync Requirements and Behavior

Keep these points in mind when planning and implementing an LDAP sync:

- The data in the LDAP attribute that is mapped to the CUCM User ID field must be unique in the LDAP (and therefore CUCM) database. Some LDAP fields allow duplicate entries, but the CUCM user ID must be unique, so it is necessary to verify that the LDAP data is unique before the sync agreement is built.
- The sn attribute (surname/last name) in LDAP must be populated with data; otherwise, the record will not be replicated to CUCM.
- If the LDAP attribute that maps to the CUCM user ID attribute contains the same data as an existing application user in CUCM, that entry is skipped and not imported into the CUCM database.

LDAP Sync Agreements

An LDAP sync agreement defines what part of the LDAP directory will be searched for user accounts. Many LDAP systems have a highly organized structure, with different containers for different functions, departments, locations, or privileges. The synchronization agreement specifies at which point in the tree the search for user accounts will begin. CUCM has access to the container specified in the agreement, and all levels below that in the tree; it cannot search higher up the tree than the start point, nor can it search across to other branches in the tree that must be accessed by going higher than the starting point then back down.

The agreement can specify the root of the domain, but although this is a simple agreement to create, it causes the entire LDAP structure to be searched, which may return unwanted accounts or simply too many accounts.

CUCM can integrate with only one LDAP system, but within that system version 10.x can support up to 20 synchronization agreements. The total number of LDAP-sourced user accounts should not exceed 160,000. To be more precise

- If the number of users is less than 80,000, up to 20 sync agreements are possible.
- If the number of users is greater than 80,000 (to the maximum recommended 160,000), the number of sync agreements supported is 10.

LDAP Sync Mechanism

The LDAP sync agreement specifies when to begin synchronizing and when to repeat the synchronization (a schedule). It is possible to have a synchronization run only once, although this is somewhat unusual.

LDAP Custom Filters

The default behavior of LDAP sync is to import all user accounts from the start point in the tree on down. This may cause accounts to be imported that are not wanted. Using a custom filter allows an administrator to limit which accounts are imported; for example, a filter could specify that only user accounts in a particular organizational unit (OU) are imported. If the filter is changed, a full LDAP sync must be performed for the change to take effect.

Configure LDAP Sync

Setting up LDAP sync is surprisingly simple. The main difficulty is typically gaining a full understanding of the target LDAP structure, knowing what containers hold the users to be imported, and knowing where to start the LDAP search.

The basics steps to set up LDAP sync are as follows:

Step 1. Activate the Cisco DirSync service.

Step 2. Configure the LDAP system.

Step 3. Configure the LDAP directory.

Step 4. Configure LDAP custom filters.

For CUCM to be able to access and search LDAP, an account must be created in LDAP for CUCM. Configurations may vary between LDAP systems, but the account must essentially have read permissions on everything in the search base.

Activate DirSync

Using the Unified Serviceability application, navigate to **Tools > Service Activation**. From the Server drop-down list, choose the **Publisher**. Find the Cisco DirSync service, check the box next to it, and click **Save**.

Configure the LDAP System

Follow these steps to enable LDAP sync in CUCM:

Step 1. Using the Unified CM Administration application, navigate to **System > LDAP > LDAP System**.

Step 2. Check the **Enable Synchronizing from LDAP Server** box.

Step 3. From the LDAP Server Type drop-down, choose the type of LDAP system with which CUCM will synchronize.

Step 4. From the LDAP Attribute for User ID drop-down, select which LDAP attribute will map to the CUCM User ID attribute.

Step 5. Click **Save**.

Figure 9-9 shows the LDAP System Configuration page.

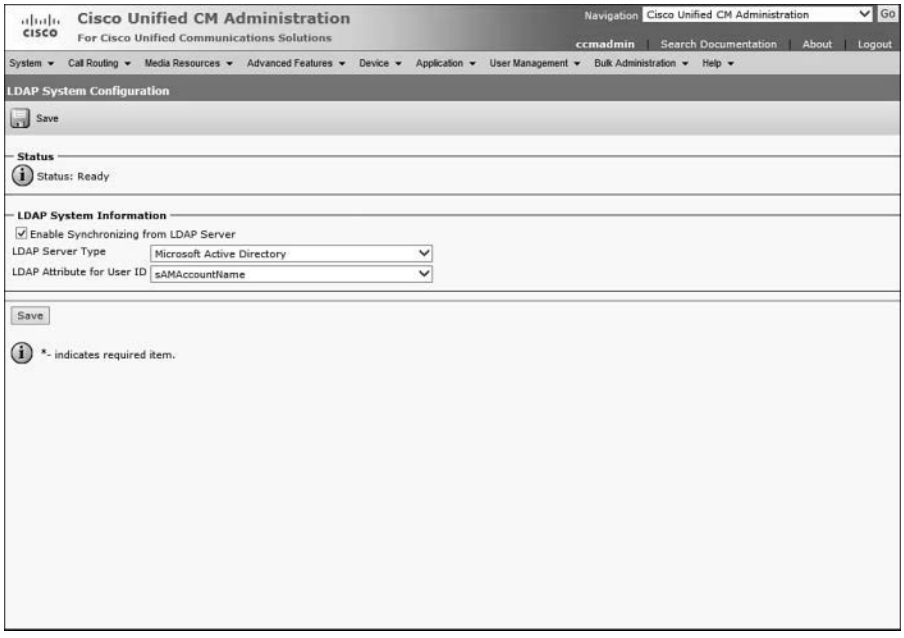


Figure 9-9 *LDAP System Configuration*

Configure the LDAP Directory

To configure the LDAP directory, follow these steps:

Step 1. Using the Unified CM Administration application, navigate to **System > LDAP > LDAP Directory**.

Step 2. Specify a name for this LDAP Sync agreement in the LDAP Configuration Name field.

Step 3. Add the account name and password that CUCM will use to access LDAP.

Step 4. Define the User Search Base. This will be the full LDAP path syntax (for example, ou=Users,dc=Pod1,dc=com).

Step 5. Set the synchronization schedule.

Step 6. Specify the LDAP user fields to be synchronized (mapping CUCM fields to LDAP fields).

Step 7. Specify at least one (up to three for redundancy) LDAP server IP address. Specify SSL to secure the LDAP sync process (requires similar configuration on the LDAP system).

Note There are several new and interesting capabilities in the LDAP integration system that are beyond the scope for CICD. Things such as the ability to add users to specified groups as you import them and to associate or even create directory numbers based on the LDAP information or specified settings, are good news for ease of user administration, but not CICD exam material.

Figure 9-10 shows the LDAP Directory configuration page.

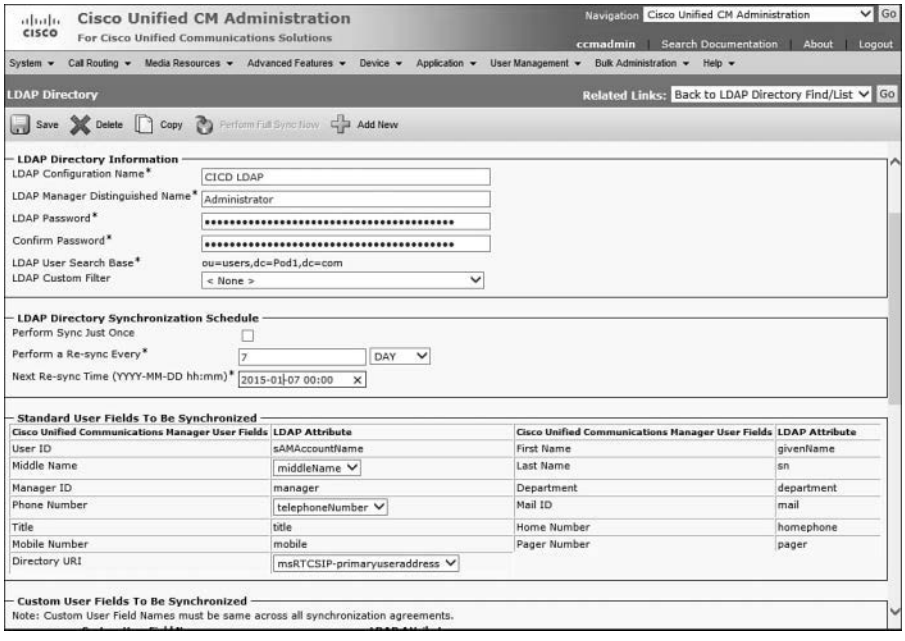


Figure 9-10 *LDAP Directory Configuration Page*

Verify LDAP Sync

The simplest way to verify that LDAP sync is working is to do a quick search of the end users on the CUCM. In the column under LDAP Sync Status, the LDAP-sourced users' status will be listed as Active LDAP Synchronized User. Users that are locally maintained in the CUCM database will be listed as Enabled Local User.

When you open the configuration page for an LDAP-synced user, you see that the User ID, Last Name, Middle Name, First Name, Telephone Number, Mail ID, Manager User ID, Department and a few other fields are not editable; this is because they are synced with LDAP and can only be edited in the LDAP system.

Configuring LDAP Authentication

Configuring CUCM to redirect authentication to the LDAP system is normally done as part of an LDAP integration. It is not typical to sync all the users but still make them maintain a separate password in CUCM.

To set up LDAP authentication, follow these steps:

Step 1. Navigate to **System > LDAP > LDAP Authentication**.

Step 2. Check the box next to **Use LDAP Authentication for End Users**.

Step 3. Specify the account and password CUCM will use to access the LDAP system.

Step 4. Specify the LDAP User Search Base.

Step 5. Specify the LDAP server IP address (up to three for redundancy).

Step 6. Click **Save**.

Verify LDAP Authentication

Verifying LDAP authentication can be achieved by opening a user configuration page and observing that the Password field is gone; this is because the password is maintained in LDAP, not locally in the CUCM database. A user can test the LDAP authentication by changing her password in LDAP and observing that CUCM requires the new password to log in.

Note that the user PIN is always locally maintained in the CUCM database, as are all the other CUCM-specific attributes.

Create LDAP Custom Filters

Create LDAP custom filters by navigating to **System > LDAP > LDAP Custom Filter**. Click **Add New**. In the Filter Configuration page, specify a name for the filter.

In the Filter field, type the filter statement. The statement must be in parentheses: ( ). Some sample filter statements follow; for more detail, see RFC 4515, *LDAP: String Representation of Search Filters*:

- (cn=Milton Macpherson)
- (!(cn=Milton Macpherson))
- (&(objectClass=Person)(|(sn=Macpherson)(cn=Milton M*)))
- (sn=M*)

Exam Preparation Tasks

Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 9-4 describes these key topics and identifies the page number on which each is found.

Key Topic

Table 9-4 Key Topics for Chapter 9

Key Topic Element	Description	Page Number
Section	IP phone registration process	236
Section	IP phone configuration requirements in CUCM	240
Section	End users versus application users	252
Section	LDAP integration	256

Definitions of Key Terms

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

device pool, Unified CM group, softkey template, phone button template, region, location, date/time group, self-provisioning

This page intentionally left blank

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K - L

M

N

O

P

Q

R

S

T

U

V

W

X - Y - Z