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

Copyright© 2016 Cisco Systems, Inc.

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

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

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.**

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

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 I Voice Perspectives

Chapter 1 Traditional Voice Versus Unified Voice 3

Chapter 2 Understanding the Components of Cisco Unified Communications 29

Chapter 3 Understanding Cisco IP Phones 51

Part II Cisco Unified Communications Manager Express

Chapter 4 Getting Familiar with CME Administration 85

Chapter 5 Managing Endpoints and End Users in CME 97

Chapter 6 Understanding the CME Dial Plan 113

Chapter 7 Enabling Telephony Features with CME 165

Part III Cisco Unified Communications Manager

Chapter 8 Administrator and End-User Interfaces 211

Chapter 9 Managing Endpoints and End Users in CUCM 231

Chapter 10 Understanding CUCM Dial Plan Elements and Interactions 267

Chapter 11 Enabling Telephony and Mobility Features with CUCM 287

Chapter 12 Enabling Mobility Features in CUCM 323

Part IV Voicemail and Presence Solutions

Chapter 13 Voice Messaging Integration with Cisco Unity Connection 343

Chapter 14 Enabling CM IM and Presence Support 379

Part V Voice Network Management and Troubleshooting

Chapter 15 Common CME Management and Troubleshooting Issues 399

Chapter 16 CUCM Monitoring, Maintenance, and Troubleshooting 417

Chapter 17 Monitoring Cisco Unity Connection 449

Chapter 18 Final Preparation 467

Part VI Appendixes

Appendix A Answers Appendix 473

Appendix B Exam Updates 477

Appendix C Managing CME Using the Command Line 479

Glossary 493

Index 507

CD-Only Appendixes

Appendix D Memory Tables

Appendix E Memory Table Answer Key

Appendix F Study Planner

Contents

Introduction xxiii

Part I Voice Perspectives

Chapter 1 Traditional Voice Versus Unified Voice 3

"Do I Know This Already?" Quiz 3

Analog Connections 6

Digital Connections 9

Moving from Analog to Digital 9

Channel Associated Signaling 11

Common Channel Signaling 12

Understanding the PSTN 12

Components of the PSTN 12

Understanding PBX and Key Systems 13

Connections To and Within the PSTN 14

PSTN Numbering Plans 15

The Emergence of VoIP 16

VoIP: Why It Is a Big Deal for Businesses 16

The Process of Converting Voice to Packets 17

The Role of Digital Signal Processors 21

Understanding RTP and RTCP 23

Review All the Key Topics 25

Complete the Tables from Memory 25

Definitions of Key Terms 26

Chapter 2 Understanding the Components of Cisco Unified Communications 29

"Do I Know This Already?" Quiz 29

Unified Collaboration 32

Understanding Cisco Unified Communications Manager Express 33

CME Key Features 34

CME Interaction with Cisco IP Phones 35

Understanding Cisco Unified Communications Manager 37

CUCM Key Features 37

CUCM Database Replication and Interacting with Cisco IP Phones 38

Understanding Cisco Unity Connection 41

Cisco Unity Connection Key Features 42

Cisco Unity Connection and CUCM Interaction 43

Understanding Cisco Unified CM IM and Presence 44

Cisco Jabber 45

Understanding Video Communication Server and TelePresence Management Suite 46
Cisco VCS Control and VCS Expressway 46
TelePresence Management Suite 47
Review All the Key Topics 48
Complete the Tables from Memory 48
Definitions of Key Terms 49

Chapter 3 Understanding Cisco IP Phones 51
"Do I Know This Already?" Quiz 51
Connecting and Powering Cisco IP Phones 54
Cisco Catalyst Switch PoE 56
Powering the IP Phone Using a Power Patch Panel or Coupler 56
Powering the IP Phone with a Power Brick 57
VLAN Concepts and Configuration 57
VLAN Review 57
VLAN Trunking/Tagging 58
Understanding Voice VLANs 60
VLAN Configuration 61
Understanding the Cisco IP Phone Boot Process 63
Configuring a Router-Based DHCP Server 64
Setting the Clock of a Cisco Device with NTP 65
IP Phone Registration 67
Quality of Service 68
Understanding the Enemy 69
Requirements for Voice, Video, and Data Traffic 70
Network Requirements for Voice and Video 70
Network Requirements for Data 70
QoS Mechanisms 71
Link Efficiency Mechanisms 72
Queuing Algorithms 73
Applying QoS 74
Using Cisco AutoQoS 74
Review All the Key Topics 82
Complete the Tables from Memory 82
Definitions of Key Terms 83

Part II Cisco Unified Communications Manager Express

Chapter 4 Getting Familiar with CME Administration 85
"Do I Know This Already?" Quiz 85
Preparing the CME Router for Cisco Configuration Professional 88

Managing CME Using CCP 89
CME Integrated GUI 89
Cisco Configuration Professional 90
Review All the Key Topics 94
Complete the Tables from Memory 94

Chapter 5 Managing Endpoints and End Users in CME 97
"Do I Know This Already?" Quiz 97
Describe End Users in CME 100
User Access Levels in CME 100
Creating Users in CME 100
Creating Users with the CME GUI 101
Enabling the CME Built-In GUI 101
Using the CME Built-In GUI to Create the Customer Admin 103
Create or Modify End Users and Endpoints in CME Using the CCP GUI 105
General Capabilities of CCP 105
CCP Unified Communications Configuration 106
Implementing End Users and Endpoints in CME 107
Review All Key Topics 111
Complete the Tables from Memory 111
Define Key Terms 111

Chapter 6 Understanding the CME Dial Plan 113
"Do I Know This Already?" Quiz 113
Configuring Physical Voice Port Characteristics 116
Configuring Analog Voice Ports 116
FXS Ports 116
FXO Ports 119
Configuring Digital Voice Ports 120
Understanding and Configuring Dial Peers 125
Voice Call Legs 126
Configuring POTS Dial Peers 127
Configuring VoIP Dial Peers 131
Using Dial Peer Wildcards 133
Private Line Automatic Ringdown 136
Understanding Router Call Processing and Digit Manipulation 137
Matching Inbound and Outbound Dial Peers 139
Using Digit Manipulation 142
Practical Scenario 1: PSTN Failover Using the prefix Command 143
Practical Scenario 2: Directing Operator Calls to the Receptionist 145
Practical Scenario 3: Specific POTS Lines for Emergency Calls 146

Practical Scenario 4: Using Translation Profiles 148
Using CCP to Configure a CME Dial Plan 151
Understanding and Implementing CME Class of Restriction 153
Using CCP to Implement COR 159
Review All the Key Topics 162
Definitions of Key Terms 163

Chapter 7 Enabling Telephony Features with CME 165
"Do I Know This Already?" Quiz 165
Configuring a Voice Network Directory 168
Configuring Call Forwarding 172
Forwarding Calls from the IP Phone 172
Forwarding Calls from the CLI 172
Using the call-forward pattern Command to Support H.450.3 173
Configuring Call Transfer 175
Configuring Call Park 177
Configuring Call Pickup 182
Configuring Intercom 184
Configuring Paging 187
Configuring After-Hours Call Blocking 191
Configuring CDRs and Call Accounting 194
Configuring Music on Hold 198
Configuring Single Number Reach 199
Configuring Ephone Hunt Groups 201
Final Forwarding Options for Hunt Groups 202
Configuring Night Service Using CCP 203
Configuring Shared Ephone-dn Using CCP 206
Describe Extension Mobility in CME 207
Review All the Key Topics 208
Definitions of Key Terms 208

Part III Cisco Unified Communications Manager

Chapter 8 Administrator and End-User Interfaces 211
"Do I Know This Already?" Quiz 211
Describe the CUCM Administration Interfaces 214
Cisco Unified Communications Manager Administration Interface 214
Cisco Unified Serviceability Administration Interface 215
Cisco Unified Operating System Administration Interface 217
Disaster Recovery System Interface 218
Cisco Unified Reporting Interface 218

CLI 218
User Management in CUCM: Roles and Access Control Groups 219
Roles 219
Access Control Groups 220
Describe the CUC Administration Interfaces 221
Cisco Unity Connection Administration 222
Cisco Unity Connection Serviceability 224
Describe the Cisco Unified CM IM and Presence Server Administration Interfaces 224
Cisco CM-IM and Presence Administration Interface 224
Cisco Unified IM and Presence Serviceability 225
Describe the End-User Interface for CUCM 226
Review All the Key Topics 228
Definitions of Key Terms 228

Chapter 9 Managing Endpoints and End Users in CUCM 231
"Do I Know This Already?" Quiz 231
Implementing IP Phones in CUCM 234
Special Functions and Services Used by IP Phones 234
NTP 234
CDP 235
DHCP 235
PoE 235
TFTP 235
DNS 235
IP Phone Registration Process 236
SIP Phone Registration Process 236
Preparing CUCM to Support Phones 237
Service Activation 237
DHCP Server Configuration 237
Configuring DHCP in Router IOS 239
IP Phone Configuration Requirements in CUCM 240
Device Pool 240
Device Defaults 242
Softkey Template and Phone Button Template 242
Profiles 242
Adding Phones in CUCM 243
Manual Configuration of IP Phones 243
Auto-Registration of IP Phones 247
Bulk Administration Tool 250

Auto Register Phone Tool 251
Self-Provisioning 252
Describe End Users in CUCM 252
End Users Versus Application Users 252
Credential Policy 253
Features Interacting with User Accounts 253
User Locale 254
Device Association 254
Implementing End Users in CUCM 255
Manual Entry 255
Bulk Import Using BAT 256
LDAP Integration 256
LDAP Synchronization 256
LDAP Authentication 257
LDAP Integration Considerations 257
LDAP Sync Agreements 259
LDAP Sync Mechanism 260
LDAP Custom Filters 260
Configure LDAP Sync 260
Activate DirSync 260
Configure the LDAP System 260
Configure the LDAP Directory 261
Verify LDAP Sync 262
Configuring LDAP Authentication 262
Verify LDAP Authentication 263
Create LDAP Custom Filters 263
Review All the Key Topics 264
Definitions of Key Terms 264

Chapter 10 Understanding CUCM Dial Plan Elements and Interactions 267
"Do I Know This Already?" Quiz 267
CUCM Call Flows 270
Call Flow in CUCM If DNS Is Used 270
Call Flow in CUCM If DNS Is Not Used 271
Centralized Remote Branch Call Flow 273
Centralized Deployment PSTN Backup Call Flow 274
Centralized Deployment Considerations and Limitations 275
PSTN Backup Using CAC 275
Distributed Deployment Call Flow 276
Call Routing Sources in CUCM 277

Call Routing Destinations in CUCM 277
Call Routing Configuration Elements 278
Route Pattern 278
Route List 279
Route Group 279
Gateways and Trunks 280
Call Routing Behavior 280
Digit Analysis 280
Hunt Groups 281
Class of Control 282
Partition 282
Calling Search Space 282
Interaction of Partitions and Calling Search Spaces 282
Line Device Configuration 283
Review All the Key Topics 284
Definitions of Key Terms 284

Chapter 11 Enabling Telephony and Mobility Features with CUCM 287
"Do I Know This Already?" Quiz 287
Describe Extension Mobility in CUCM 290
Enable EM in CUCM 291
Describe Telephony Features in CUCM 298
Call Coverage 298
Call Forward 298
Shared Lines 299
Barge and Privacy 299
Call Pickup 300
Call Hunting 300
Call Park 301
Intercom 301
CUCM Native Presence 301
Presence Architecture 302
Enable Telephony Features in CUCM 303
Enabling Call Coverage 303
Configuring Shared Lines 303
Configuring Barge 304
Configuring Call Pickup 305
Configuring Call Park and Directed Call Park 308
Configuring Call Hunting 310
Configuring Intercom Features 313

Configure CUCM Native Presence 315
Configuring BLF Speed Dials 315
Configuring Presence-Enabled Call Lists 316
Configuring Custom Presence Groups 317
Review All the Key Topics 321
Definitions of Key Terms 321

Chapter 12 Enabling Mobility Features in CUCM 323
"Do I Know This Already?" Quiz 323
Understanding CUCM Mobility Features 326
Describe Mobile Connect 326
Unified Mobility Architecture 327
Access Lists 327
Time-of-Day Access 327
Mobile Voice Access 328
Implementing Mobility Features in CUCM 328
Configuring Mobile Connect 329
Step 1: Configure Softkey Templates 329
Step 2: Configure User Accounts for Mobility 329
Step 3: Configure the IP Phone to Support Mobility Features 331
Step 4: Create Remote Destination Profiles 331
Step 5: Add Remote Destinations to Remote Destination Profiles 331
Step 6: Configure Ring Schedules for Each Remote Destination 332
Step 7: Configure Access Lists 333
Step 8: Apply Access Lists 334
Step 9: Configure Service Parameters 335
Configuring MVA 336
Step 1: Activate the MVA Service 337
Step 2: Configure Service Parameters 337
Step 3: Enable MVA for Each User 338
Step 4: Configure the MVA Media Resource 339
Step 5: Configure the MVA VXML Application at the IOS Gateway 340
Review All the Key Topics 341
Definitions of Key Terms 341

Part IV Voicemail and Presence Solutions

Chapter 13 Voice Messaging Integration with Cisco Unity Connection 343
"Do I Know This Already?" Quiz 343
Describe Cisco Unity Connection 346
Overview of Cisco Unity Connection 346

Single-Site and Multisite Deployment Considerations 346
CUC Integration Overview 347
CUC Integration with CUCM Using SCCP 347
CUC Integration Using SIP 348
CUC Features 349
System Settings 349
Enterprise Parameters and Service Parameters 350
LDAP 350
Call Handlers 350
Call Routing 351
Direct Routing Rules 351
Forwarded Routing Rules 352
Call Routing Rule Filters 352
Distribution Lists 352
Authentication Rules 352
Dial Plan 353
Describe Cisco Unity Connection Users and Mailboxes 353
User Templates 353
User Template Basics 353
Password Settings 354
Roles 354
Transfer Rules and Greetings 354
Call Actions 355
Message Settings, Message Actions, and Caller Input 355
TUI Settings 355
CUC End Users 355
Extension and Call Forward Options 356
Voice Messaging with SRST and AAR 356
Voicemail Box 356
Private Distribution Lists 356
Notification Devices 356
User Creation Options 356
CUC Voicemail Boxes 357
Message Aging Policy and Mailbox Quotas 357
Implement Cisco Unity Connection Users and Mailboxes 357
Configure End User Templates 357
User Template Basics 358
Password Settings 359
Roles 360
Message Settings 360

Message Actions 361
Phone Menu 362
Playback Message Settings 363
Notification Devices 364
Configure CUC End Users 365
Manual Process 365
Alternate Extensions and Names 366
Private DLs 367
Importing End Users into CUC 368
Importing Users from CUCM 368
Importing Users from LDAP 370
Bulk Administration Import of CUC Users 372
Managing the CUC Message Store 373
Mailbox Stores Membership 374
Message Aging Policy 374
Mailbox Quotas 375
Review All the Key Topics 377
Definitions of Key Terms 377

Chapter 14 Enabling CM IM and Presence Support 379
"Do I Know This Already?" Quiz 379
Describe CM-IMP Features 381
Jabber 381
Jabber Operating Modes 381
Enterprise Instant Messaging 382
Voice Calls 383
Video Calls 383
Integration Support 383
Cisco Unified Client Services Framework 383
Cisco Unified Communications Manager IP Phone Service 384
Describe Cisco Unified Presence Architecture 384
Integration with Microsoft Office Communications Server 385
Integration with LDAP 385
Integration with Cisco Unity Connection 385
Integration with Conferencing Resources 386
Integration with Calendar Resources 386
Architecture and Call Flow: Softphone Mode 386
Architecture and Call Flow: Deskphone Control Mode 386
IM/Chat, Compliance, and Persistent Chat 387
CM-IMP and QoS Considerations 387

Enabling CM-IMP 389
Enabling End Users for Cisco Jabber in CUCM 389
Step 1: Configure End Users in CUCM 389
Step 2: Associate the Directory Numbers with the End Users in CUCM 390
Step 3: Create a Cisco Unified CSF Device 390
Step 4: Associate the CSF Device with the End User in CUCM 390
Enabling End Users for Jabber in CUCM 390
Enabling CUCM Presence Signaling Integration with CM-IMP 393
Enabling End Users for Jabber in CM-IMP 394
Troubleshooting Jabber 394
Review All the Key Topics 396
Definitions of Key Terms 396

Part V Voice Network Management and Troubleshooting

Chapter 15 Common CME Management and Troubleshooting Issues 399
"Do I Know This Already?" Quiz 399
Troubleshooting 402
Troubleshooting Common CME Registration Issues 403
Issue 1: Verifying PoE 405
Issue 2: Voice VLAN Assignment 405
Issue 3: DHCP Server 406
Issue 4: TFTP Server 406
Issue 5: CME Server 407
Troubleshooting Dial Plan and QoS Issues 407
Dial Plan Issues 407
QoS Issues 410
Review All the Key Topics 414
Definitions of Key Terms 414

Chapter 16 CUCM Monitoring, Maintenance, and Troubleshooting 417
"Do I Know This Already?" Quiz 417
Describe How to Provide End-User Support for Connectivity and Voice Quality Issues 421
Troubleshooting 421
Troubleshooting IP Phone Registration Problems 422
Deleting Unassigned Directory Numbers Using the Route Plan Report 424
Describe CUCM Reports and How They Are Generated 425
Generating Reports 425
Analyzing Reports 427
Understanding CUCM CDR Analysis and Reporting Tool Reports 427

Activate CAR-Related Services 428
Configure CDR Service Parameters 428
CAR Tool Users 429
CDR and CMR Architecture 429
CAR System Parameters 429
Exporting CDR and CMR Records 430
Generating CDR Reports 430
Report Generation Example 431
Generating System Reports 433
Generating Device Reports 434
Describe Cisco Unified RTMT 434
RTMT Interface 436
Monitoring CUCM with RTMT 436
Voice and Video Summary 437
Gateway Activity 437
Device Search 438
Database Summary 439
Call Activity 440
Alert Central 442
Remote Browse 443
Syslog 443
Describe the Disaster Recovery System 444
Using the DRS 445
Set Up a Backup Device 445
Create a Scheduled Backup 445
Perform a Restore 446
Review All the Key Topics 447
Definitions of Key Terms 447

Chapter 17 Monitoring Cisco Unity Connection 449
"Do I Know This Already?" Quiz 449
Generating and Accessing Cisco Unity Connection Reports 452
Cisco Unity Connection Serviceability Reports 452
Cisco Unified Serviceability: Serviceability Reports Archive 455
Analyzing Cisco Unity Connection Reports 457
Troubleshooting and Maintenance Operations Using Cisco Unity Connection Reports 459
Reports to Support Routine Maintenance 462
Review All the Key Topics 465
Definitions of Key Terms 465

Chapter 18 Final Preparation 467
Tools for Final Preparation 467
Exam Engine and Questions on the CD 467
Install the Exam Engine 467
Activate and Download the Practice Exam 468
Activating Other Exams 468
Premium Edition 468
The Cisco Learning Network 469
Memory Tables 469
Chapter-Ending Review Tools 469
Study Plan 469
Recall the Facts 470
Practice Configurations 470
Using the Exam Engine 470

Part VI Appendixes

Appendix A Answers Appendix 473

Appendix B Exam Updates 477
Always Get the Latest at the Companion Website 477
Technical Content 477

Appendix C Managing CME Using the Command Line 479

Glossary 493

Index 507

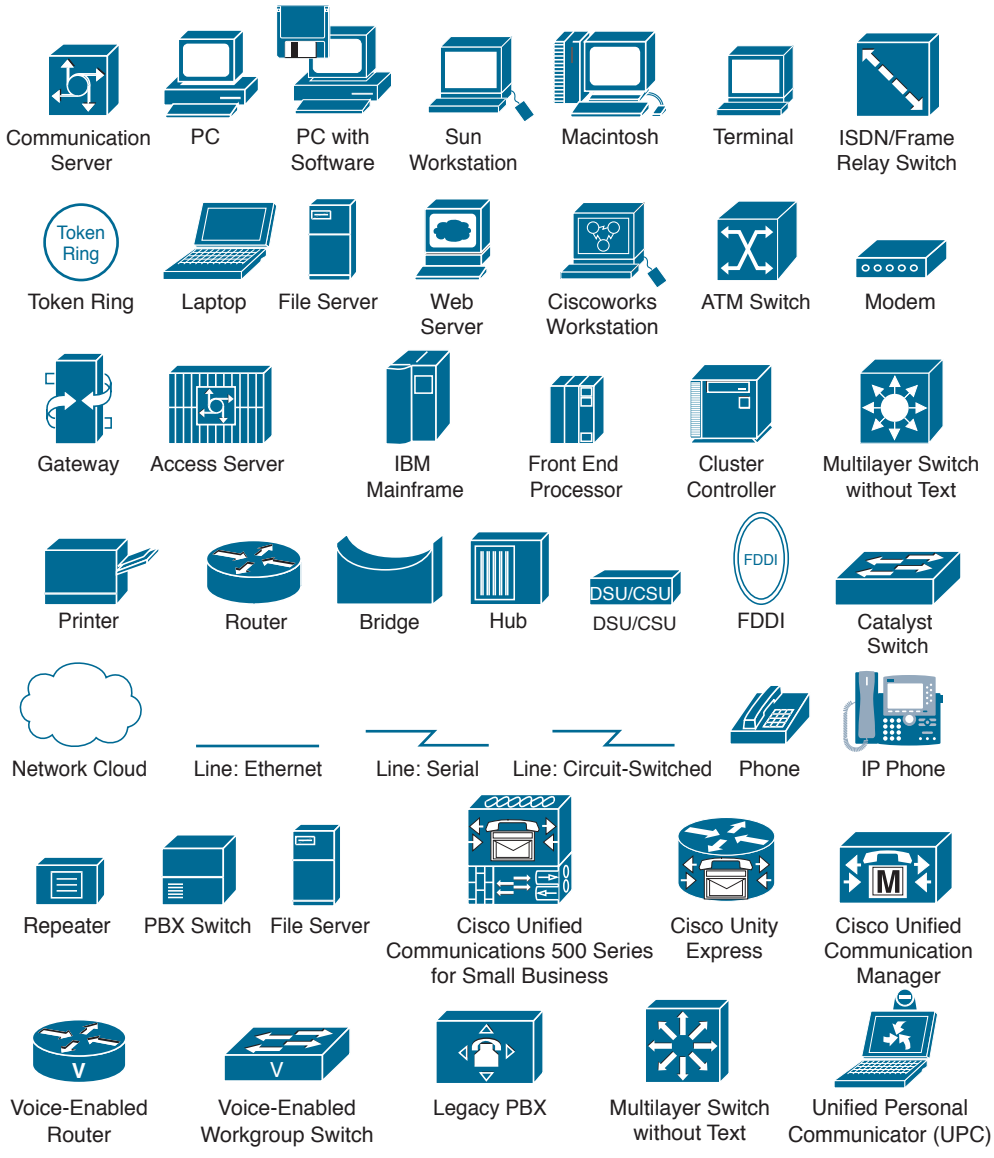
CD-Only Appendixes

Appendix D Memory Tables

Appendix E Memory Table Answer Key

Appendix F Study Planner

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 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 chapter covers the following topics:

- **Analog Connections:** This section discusses the simplest type of modern voice communication: analog connections.
- **Digital Connections:** This section discusses the process of converting analog voice into digital signals and using digital circuits to send multiple calls over a single line.
- **Understanding the PSTN:** This section discusses the components of the PSTN, focusing specifically on PBX and key systems, and the methods used to connect to the PSTN.
- **Understanding VoIP:** Voice has been converted to digital format for decades; however, putting that digital content in a packet is relatively new. This section discusses the core concepts behind VoIP, including the coding/decoding (codec) process, DSPs, and the protocols used to deliver audio.

CHAPTER 1

Traditional Voice Versus Unified Voice

The traditional telephony network has been in place since the early 1900s, and it is not going to disappear overnight. Until it does, new Voice over IP (VoIP) networks must integrate with traditional telephony networks. To perform this integration, you must have a basic understanding of traditional voice telephony. This chapter walks you through the foundations of the public switched telephone network (PSTN), private branch exchange (PBX) systems, and analog and digital circuitry.

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

Foundation Topics Section	Questions Covered in This Section
Analog Connections	1–3
Digital Connections	4–8
Understanding the PSTN	9
Understanding VoIP	10–12

1. Analog phones connected to the PSTN typically use which of the following signal types?
   - **a.** Loop start
   - **b.** Ground start
   - **c.** CAS
   - **d.** CCS
2. Which of the following issues is prevented by using ground start signaling?
   - **a.** Echo
   - **b.** Glare
   - **c.** Reflexive transmissions
   - **d.** Mirrored communication

3. Which of the following signaling types represents supervisory signaling?

   a. Off-hook signal
   b. Dial tone
   c. DTMF
   d. Congestion

4. What are two disadvantages of using analog connectivity?

   a. Conversion complexity
   b. Signal quality
   c. Limited calls per line
   d. Lack of common voice services

5. Which of the following systems allows you to send multiple voice calls over a single digital circuit by dividing the calls into specific time slots?

   a. MUX
   b. DE-MUX
   c. TDM
   d. TCP

6. When using T1 CAS signaling, which bits are used to transmit signaling information within each voice channel?

   a. First bit of each frame
   b. Last bit of each frame
   c. Second and third bits of every third frame
   d. Eighth bit of every sixth frame

7. How large is each T1 frame sent over a digital CAS connection?

   a. 8 bits
   b. 24 bits
   c. 80 bits
   d. 193 bits

8. Which of the following time slots are used for T1 and E1 signaling when using CCS connections? (Choose two.)

   a. Time slot 1
   b. Time slot 16
   c. Time slot 17
   d. Time slot 23
   e. Time slot 24

9. Which of the following standards created by the ITU designates international numbering plans for devices connected to the PSTN?

- **a.** ITU-T
- **b.** E.164
- **c.** ITU-161
- **d.** T-161

10. What frequency range is accurately reproduced by the Nyquist theorem on the PSTN?

- **a.** 200–9000 Hz
- **b.** 300–3400 Hz
- **c.** 300–4000 Hz
- **d.** 20–20,000 Hz

11. What amount of bandwidth is consumed by the audio payload of G.729a?

- **a.** 4.3 kbps
- **b.** 6.3 kbps
- **c.** 8 kbps
- **d.** 16 kbps

12. Which of the following are high-complexity codecs? (Choose two.)

- **a.** G.711 μ-law
- **b.** G.729
- **c.** G.729a
- **d.** iLBC

Foundation Topics

Analog Connections

In 1877, Thomas Edison created a remarkable device known as a phonograph, which is shown in Figure 1-1.

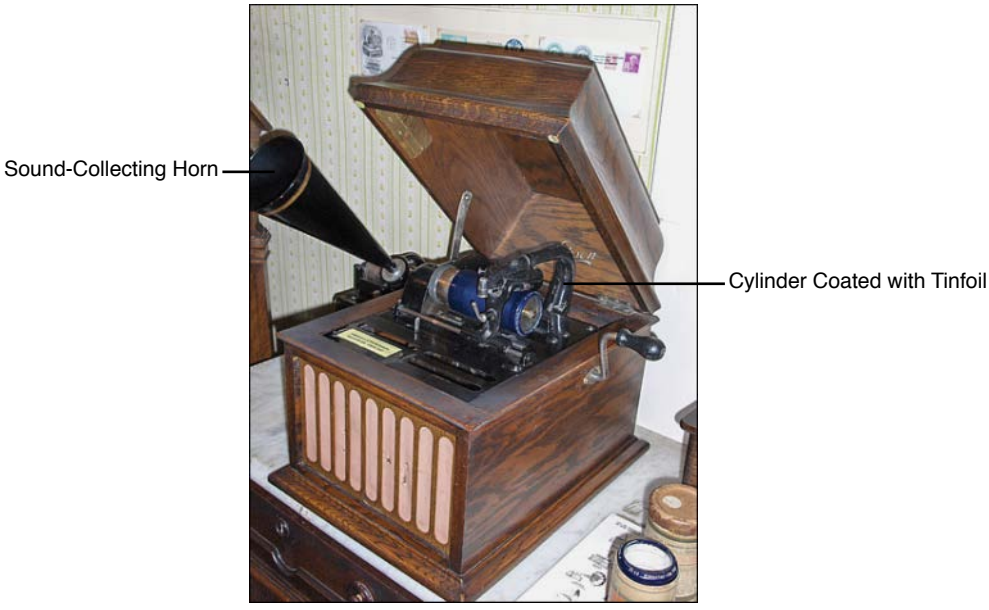


Figure 1-1 *Replica of Edison's Phonograph*

This device was able to record sounds by pressing a needle into a cylinder covered with tinfoil, which made an impression of the vibrations as a person spoke into a sound-collecting horn. The phonograph could then play back this sound by moving the needle at a steady speed back over the indentions made in the tinfoil. This "archaic" form of recording is one representation of an analog signal and is essentially exactly the same technology used by vinyl records today.

An analog signal uses a property of the device that captures the audio signal to convey audio information. In the case of Edison's phonograph, the property was the various indentions in tinfoil. In today's world, where everything is connected through some form of cabling, electric currents are used to send analog signals. When you speak into an analog phone, the sounds that come out of your mouth are converted into electricity. The volume and pitch that you use when speaking result in different variations of electrical current. Electrical voltage, frequency, current, and charge are all used in some combination to convey the properties of your voice. Figure 1-2 illustrates perhaps a more familiar view of using electrical signals to capture the properties of voice.

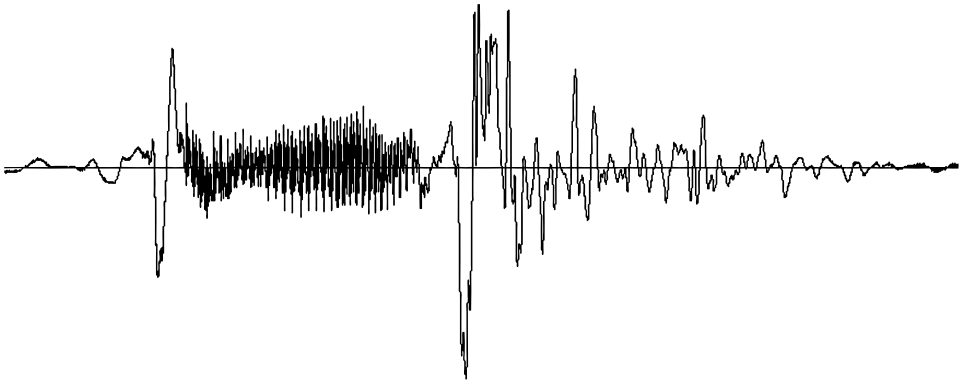


Figure 1-2 *Electrical Analog Waveform of Human Speech*

Note The analog waveform shown in Figure 1-2 is from a person saying "Hello."

Analog phone lines use the properties of electricity to convey changes in voice over cabling. Of course, there is more than just voice to send over the phone lines. The analog phones you use at home must convey signaling, too. Signaling includes messages such as dial tone, dialed digits, busy signals, and so on. These signaling types are discussed in just a moment. For now, let's look at the cabling used to make analog connections function.

Each analog circuit is composed of a pair of wires. One wire is the ground, or positive side of the connection (often called the tip). The other wire is the battery, or negative side of the connection (often called the ring). You'll commonly hear phone technicians talk about these wires as the "tip and ring." These two wires are what power the analog phone and allow it to function, just like the wires that connect your car battery to the car. Figure 1-3 illustrates the connections of the tip and ring wire to your analog phone.

Key Topic

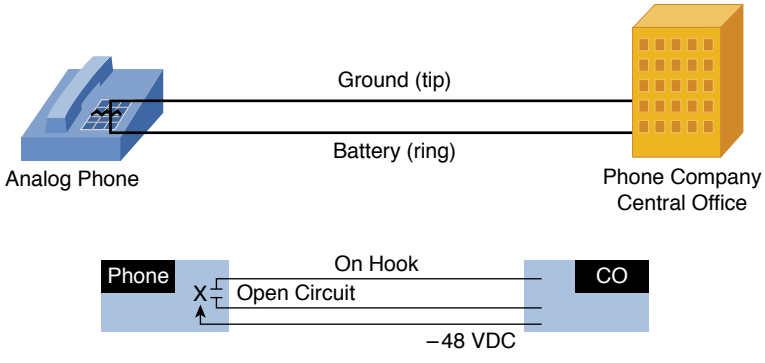


Figure 1-3 *Connections of the Ground and Battery Wires to an Analog Phone*

The jagged line over the wires in the analog phone in Figure 1-3 represents a broken circuit. Whenever the phone is on hook, the phone separates the two wires, preventing electric signal from flowing through the phone. When the phone is lifted off hook, the phone connects the two wires, causing an electrical signal (48V DC voltage) to flow from the phone company central office (CO) into the phone. This is known as loop start signaling.

Loop start signaling is the typical signaling type used in home environments. Loop start signaling is susceptible to a problem known as glare. Glare occurs when you pick up the phone to make an outgoing call at the same time as a call comes in on the phone line before the phone has a chance to ring. This gives you the awkward moment of, "Uh… Oh! Hello, Bob! I'm sorry, I didn't know you were on the phone." In home environments, this is not usually a problem for a couple reasons. First, the chances of having a simultaneous outgoing and incoming call are slim. Second, if you do happen to have an incoming call, it's always meant for your house (unless the caller dialed the wrong number).

In business environments in the past, glare was a significant problem because of the large number of employees and high call volume. For example, a corporation may have a key system (which allows it to run its own, internal phone system) with five analog trunks to the PSTN, as shown in Figure 1-4.

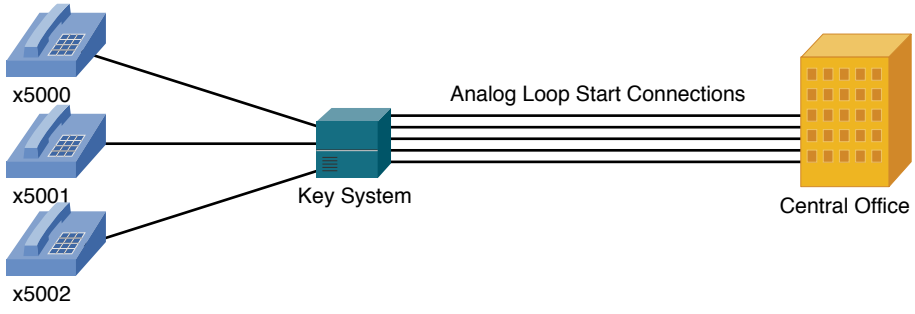


Figure 1-4 *Illustration of Glare*

If a call comes in for x5002 at the same time as x5000 picks up the phone, the key system connects the two signals, causing x5000 to receive the call for x5002. This happens because the loop start signal from x5000 seizes the outgoing PSTN line at the same time as the key system receives the incoming call on the same PSTN line. This is an instance of glare.

Because of glare, most modern PBX systems designed for larger, corporate environments use ground start signaling. Ground start signaling originated from its implementation in pay phone systems. Many years ago, when a person lifted the handset of a pay phone, he did not receive a dial tone until he dropped in a coin. The coin would brush past the tip and ring wires and temporarily ground them. The grounding of the wires signaled the phone company to send a dial tone on the line. Using this type of signaling in PBX systems allows the PBX to separate an answering phone from an incoming phone line, reducing the problem of glare. To receive a dial tone from the CO, the PBX must send a ground signal on the wires. This intentionally signals to the telephone CO that an outgoing call is going to happen, whereas the loop start method of signaling just connects the wires to receive an incoming call or place an outgoing call.

Tip Many other types of signaling exist in the analog world. These include supervisory signaling (on hook, off hook, ringing), informational signaling (dial tone, busy, ringback, and so on), and address signaling (dual-tone multifrequency (DTMF) and pulse). These are discussed in detail as part of the CVOICE certification series. (For more information, see http://www.ciscopress.com/bookstore/product.asp?isbn=1587055546.)

Digital Connections

Analog signaling was almost universally used and very functional, but still posed plenty of problems. First, an analog electrical signal experiences degradation (signal loss) over long distances. To increase the distance the analog signal could travel, the phone company had to install repeaters (shown in Figure 1-5) to regenerate the signal as it became weak.

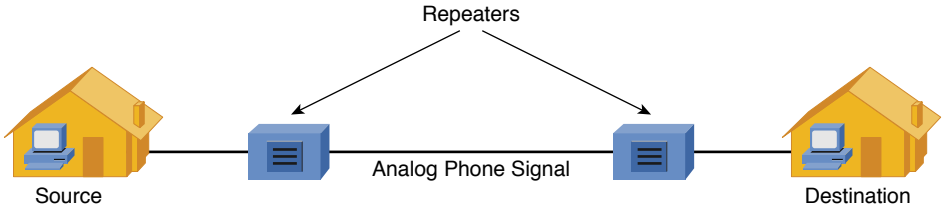


Figure 1-5 *Analog Signal Repeaters*

Unfortunately, as the analog signal was regenerated, the repeater device was unable to differentiate between the voice traveling over the wire and line noise. Each time the repeater regenerated the voice, it also amplified the line noise. So, the more times a phone company regenerated a signal, the more distorted and difficult to understand the signal became.

The second difficulty encountered with analog connections was the sheer number of wires the phone company had to run to support a large geographic area or a business with a large number of phones. Because each phone required two wires, the bundles of wire became massive and difficult to maintain (imagine the hassle of a single pair of wires in the bundle breaking). A solution to send multiple calls over a single wire was needed. A digital connection was that solution.

Moving from Analog to Digital

Simply put, digital signals use binary codes to represent levels of voice instead of a combination of electrical signals. When someone talks about "digitizing voice," they are speaking of the process of changing analog voice signals into a series of numbers (shown in Figure 1-6) that you can use to put the voice back together at the other end of the line.

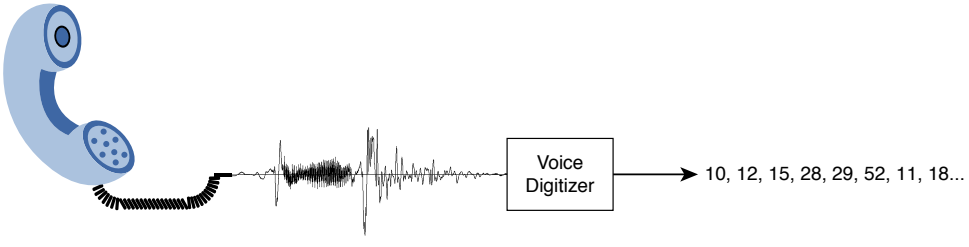


Figure 1-6 *Converting Analog to Digital Signals*

Essentially, each number sent represents a sound that someone made while speaking into a telephone handset. Today's network devices can easily transmit a numeric value over much greater distances with very little degradation or line noise compared to the signal degradation issues faced by analog phone connections. Digital transmission also eliminates the need for the many individual pairs of wires required by multiple analog connections.

Traditional digital voice uses a technology known as time-division multiplexing (TDM). Traditional voice networks use TDM to digitally encode multiple conversations at the same time over a single, four-wire path (in a VoIP system, the equivalent operation is performed by digital signal processors (DSPs), which generate binary data to be loaded into packets). Because the multiple conversations have been digitized, the numeric values are transmitted in specific time slots (thus, the "time division") that differentiate the separate conversations. Figure 1-7 illustrates three separate voice conversations sent over a digital connection.

Key Topic

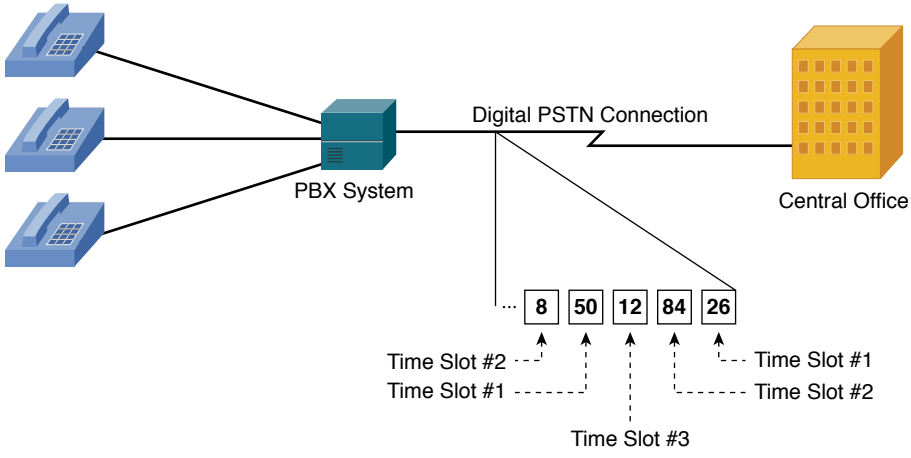


Figure 1-7 *Time-Division Multiplexing Voice Channels*

Observe that each of the voice conversations in Figure 1-7 has been digitized, assigned a numeric value, and transmitted over the digital PSTN connection. Based on the time the voice data was sent, the PSTN carrier is able to distinguish and reassemble the voice conversations.

Note Although the values in each time slot are shown in decimal in Figure 1-7, they are actually transmitted and interpreted in binary.

Corporations using digital voice connections to the PSTN typically implement T1 circuits in the United States, Canada, and Japan. A T1 circuit is 24 separate 64-kbps channels, each of which is called a DS0 (digital signal 0). Each one of these channels is able to support a single voice call. Corporations in areas outside the United States, Canada, and Japan use E1 circuits, which allow you to use up to 30 DS0s (plus 2 D channels) for voice calls.

Although digital technology solves the problems of signal degradation and the "one pair, one call" limitation of analog technology, it creates a new issue: signaling. With analog circuits, supervisory signals were passed by connecting the tip and ring wires together. The phone company generated informational and address signals through specific frequencies of electricity. By solving the problems associated with analog signaling, digital signaling also removed the typical signaling capabilities. To solve this, two primary styles of signaling were created for digital circuits:

Key Topic

- **Channel associated signaling (CAS):** Signaling information is transmitted in the same channel as the voice.

- **Common channel signaling (CCS):** Signaling information is transmitted using a separate, dedicated signaling channel.

The following sections discuss these two styles of signaling.

Channel Associated Signaling

T1 digital connections that use CAS actually "steal" binary bits that would typically have been used to communicate voice information and use them for signaling. Initially, this seems like a bad idea. After all, if you take the binary bits that are used to resynthesize the voice, won't the voice quality drop significantly? Although the voice quality does drop measurably, the number of binary bits stolen for signaling information is small enough that the change in voice quality is not perceptible.

Note Because T1 CAS steals bits from the voice channel to transfer signaling information, it is often called *robbed bit signaling (RBS)*.

The voice device running the T1 line uses the eighth bit on every sixth sample in each T1 channel (DS0). Figure 1-8 illustrates this concept.

As you can see from Figure 1-8, the 24 channels of the digital T1 circuit carry only voice data for the first five frames that they send. On the sixth frame (marked with an *S* in Figure 1-8), the eighth bit (also called the least significant bit) is stolen for the voice devices to transmit signaling information. This process occurs for every sixth frame after this (12th, 18th, 24th, and so on). This stolen bit relays the signaling information for each respective DS0 channel. For example, the bits stolen from the third DS0 channel relay the signaling information only for that channel.

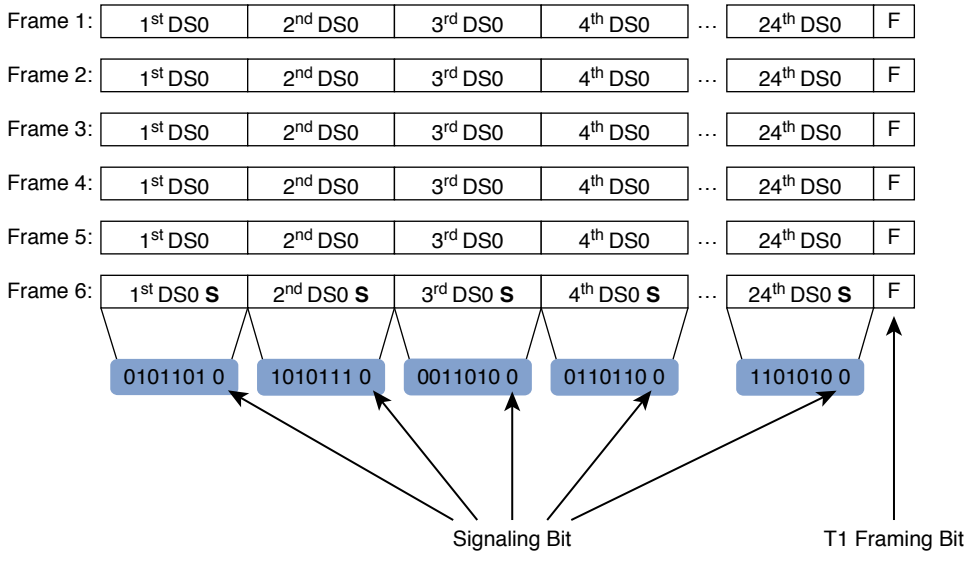


Figure 1-8 *CAS T1 Signaling Bits*

Common Channel Signaling

CCS dedicates one of the DS0 channels from a T1 or E1 link for signaling information. This is often called out-of-band (OOB) signaling because the signaling traffic is sent completely separate from the voice traffic. As a result, a T1 connection using CCS has only 23 usable DS0s for voice. Because CCS dedicates a full channel of the circuit for signaling, the "stolen bit" method of signaling using ABCD bits is no longer necessary. Rather, a separate signaling protocol sends the necessary information for all voice channels. The most commonly used signaling protocol is Q.931, which is the signaling protocol used for ISDN circuits.

CCS is the most common connection between voice systems worldwide because it offers more flexibility with signaling messages, uses all the bandwidth within the voice bearer channels, and provides higher security (because the signaling is not embedded in the voice channel). CCS also allows PBX vendors to communicate proprietary messages (and features) between their PBX systems using ISDN signaling, whereas CAS does not offer any of these capabilities.

Key Topic

Tip When using CCS configurations with T1 lines, the 24th time slot is always the signaling channel. When using CCS configurations with E1 lines, the 17th time slot is always the signaling channel.

Note Although ISDN is the most popular protocol used with CCS configurations, CCS can use other protocols. For example, telephone companies use the Signaling System 7 (SS7) protocol (described later) with CCS configurations to communicate between COs.

Understanding the PSTN

All the signaling standards and communication methods discussed in the previous section typically focus on the connection to one massive voice network, known as the PSTN. If you have ever made a call from a home telephone, you have experienced the results of the traditional telephony network. This network is not unlike many of the data networks of today. Its primary purpose is to establish worldwide pathways to allow people to easily connect, converse, and disconnect.

Components of the PSTN

When the phone system was originally created, individual phones were wired together to allow people to communicate. If you wanted to connect with more than one person, you needed multiple phones. As you can imagine, this solution was short lived as a more scalable system was found. The modern PSTN is now a worldwide network built from the following components, as shown in Figure 1-9:

Key Topic

- **Analog telephone:** Able to connect directly to the PSTN and is the most common device on the PSTN. Converts audio into electrical signals (and vice versa).
- **Local loop:** The link between the customer premises (such as a home or business) and the telecommunications service provider.

- **CO switch:** Provides services to the devices on the local loop. These services include signaling, digit collection, call routing, setup, and teardown.
- **Trunk:** Provides a connection between switches. These switches could be CO or private.
- **Private switch:** Allows a business to operate a "miniature PSTN" inside its company. This provides efficiency and cost savings because each phone in the company does not require a direct connection to the CO switch.
- **Digital telephone:** Typically connects to a PBX system. Converts audio into binary 1s and 0s, which allows more efficient communication than analog.

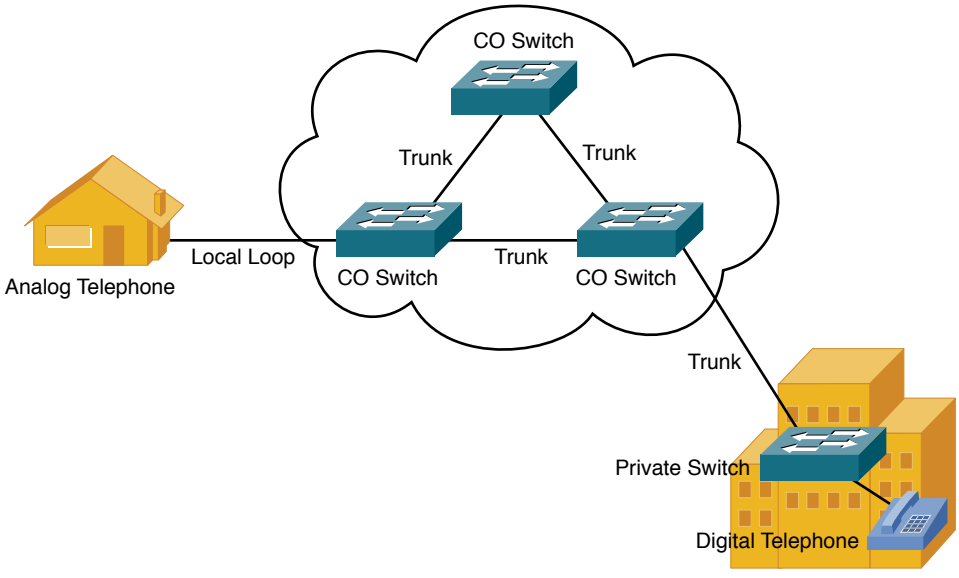


Figure 1-9 *PSTN Components*

Understanding PBX and Key Systems

Many businesses have hundreds or even thousands of phones they support in the organization. If the company purchases a direct PSTN connection for each one of these phones, the cost would be prohibitive, and there would be little or no ability to manage the system. Instead, most organizations choose to use a PBX or key system internally to manage in-house phones. These systems allow internal users to make phone calls inside the office without using any PSTN resources. Calls to the PSTN forward out the company's PSTN trunk link.

When you first look at a PBX system, it looks like a large box full of cards. Each card has a specific function:

- **Line cards:** Provide the connection between telephone handsets and the PBX system
- **Trunk cards:** Provide connections from the PBX system to the PSTN or other PBX systems
- **Control cards:** Provide the intelligence behind the PBX system; all call setup, routing, and management functions are contained in the control complex

If you look at a PBX from a network equipment mindset, "single point of failure" might be one of the first thoughts that jump into your mind. Although this may be true, most PBX systems offer 99.999 percent uptime with a lifespan of 7 to 10 years. That's a hard statistic to beat in just about any industry. In the transition to VoIP, one of our main objectives is to make the VoIP system sound as good as the old PBX did, as often as the old PBX did (which was really good, pretty much all the time). That is a high standard to meet, but current VoIP technology, when properly implemented, can meet and even exceed that standard.

Key systems are geared around small business environments (typically fewer than 50 users). As technology has advanced, the line between key systems and PBXs has begun to blur; however, key systems typically support fewer features and have a "shared line" feel. For example, you might see a key system installed in a small insurance office where users all have four lines assigned to their phone. If Joe were to use line 1, the line would appear busy for all users at the insurance office.

Note Although key systems often have a shared-line feature set, many key systems have numerous features that allow them to operate just like a PBX system but with fewer ports.

Connections To and Within the PSTN

When you want to connect to the PSTN, you have a variety of options. Home users and small offices can connect using analog ports. Each two-wire analog connection has the capability to support a single call. For home users, a single, analog connection to the PSTN may be sufficient. For small offices, the number of incoming analog connections directly relates to the office size and average call volume. As businesses grow, you can consolidate the multiple analog connections into one or more digital T1 or E1 connections, as shown in Figure 1-10.

The PSTN is itself a network of networks, similar to the Internet, which connects the phone switching equipment at the COs of multiple telephony providers together into a massive worldwide network. For all the telephony providers of the world to communicate together, a common signaling protocol must be used, similar to the way TCP/IP operates in the data realm. The voice signaling protocol used around the world is SS7 (Signaling System 7).

SS7 is an out-of-band (CCS-style) signaling method used to communicate call setup, routing, billing, and informational messages between telephone company COs around the world. When a user makes a call, the first CO to receive the call performs an SS7 lookup to locate the number. When the destination is found, SS7 is responsible for routing the call through the voice network to the destination and providing all informational signaling (such as ring back) to the calling device.

Note SS7 is primarily a telephony service provider technology. You do not typically directly interface with the SS7 protocol from a telephony customer perspective.

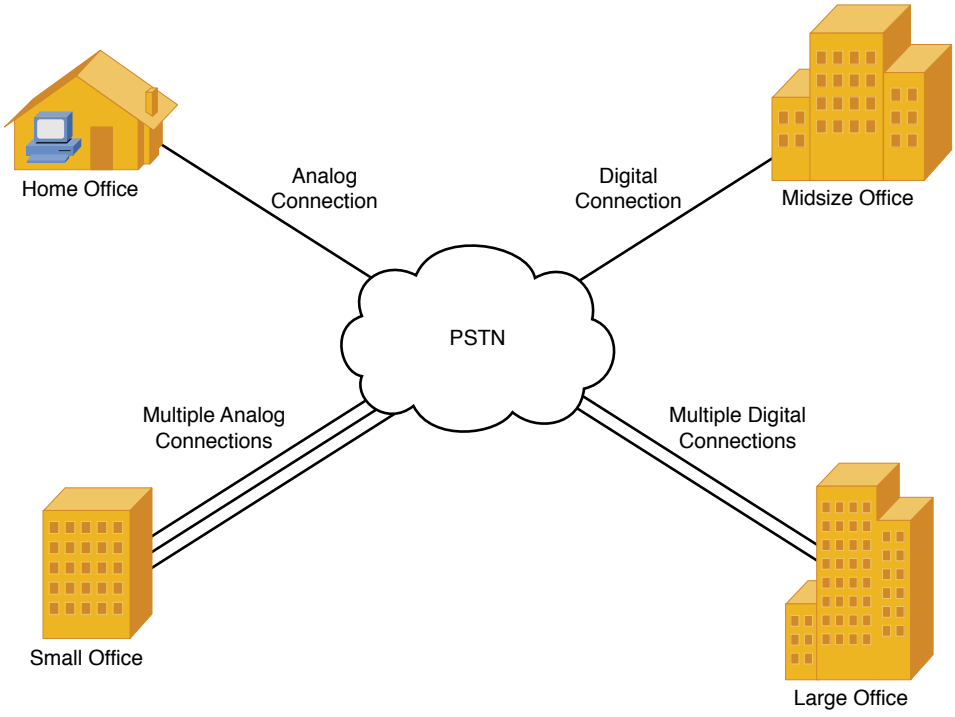


Figure 1-10 *Connections to the PSTN*

PSTN Numbering Plans

Just as data networks use IP addressing to organize and locate resources, voice networks use a numbering plan to organize and locate telephones all around the world. Organizations managing their own internal telephony systems can develop any internal number scheme that best fits the company needs (analogous to private IP addressing). However, when connecting to the PSTN, you must use a valid, E.164 standard address for your telephone system. E.164 is an international numbering plan created by the International Telecommunication Union (ITU). Each number in the E.164 numbering plan contains the following components:

- Country code
- National destination code
- Subscriber number

Note E.164 numbers are limited to a maximum length of 15 digits.

As an example, the North American Numbering Plan (NANP) uses the E.164 standard to break numbers down into the following components:

- Country code
- Area code

- CO or exchange code
- Station code or subscriber number

For example, the NANP number 1-602-555-1212 breaks down as shown in Figure 1-11.

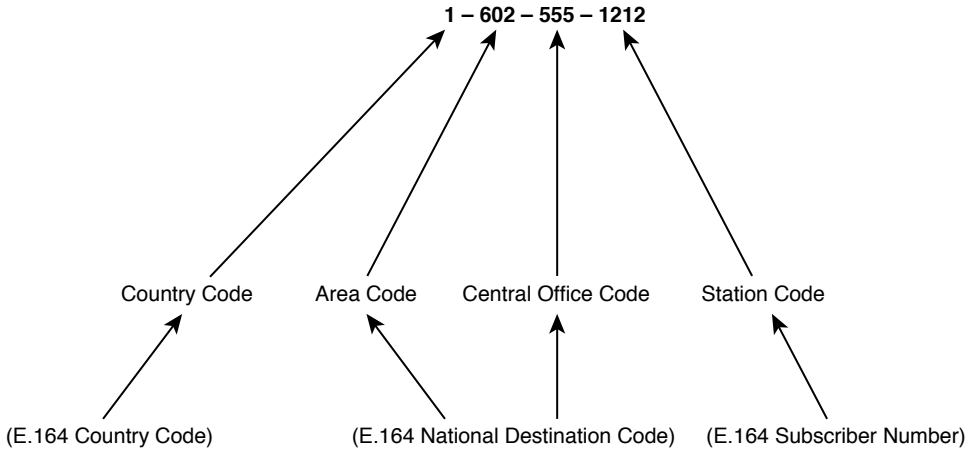


Figure 1-11 *NANP Phone Number Example*

Even though the NANP defines specific categories of numbers that the E.164 standard does not include, the number still falls under the three broad categories, also shown in Figure 1-11.

The Emergence of VoIP

Everything discussed thus far deals with taking spoken voice (as analog signal) and converting it into binary 1s and 0s (digital data). Digitizing voice is "old school." So, what's so new about VoIP? Instead of placing those old school 1s and 0s into a DS0 channel, we now load them into a data packet with IP addressing information in the header. You can then take that VoIP packet and send it across the data network at your office. Sending a packet is just routine for data networks. The real difference, and our biggest concern, is ensuring that the packet gets to its destination intact and rapidly (quality of service [QoS]), choosing the proper coding and decoding (codec) methods, making sure that the VoIP packet is not snooped on (encryption), and a plethora of other concerns. These topics will unfold in due course; for now, take a moment to simply enjoy walking into the world of VoIP.

VoIP: Why It Is a Big Deal for Businesses

One of the biggest benefits of VoIP to businesses is saving cabling and related infrastructure costs, due to the elimination of a completely separate voice cabling implementation. That can be a big deal, but as you dig deeper into the ramifications of running voice over data networks, you begin to uncover many business benefits that were previously untapped.

The business benefits of VoIP include the following:

- **Reduced cost of communications:** Instead of relying on expensive tie lines or toll charges to communicate between offices, VoIP allows you to forward calls over existing WAN (including Internet) connections that are already paid for regardless of utilization.

- **Reduced cost of cabling:** VoIP deployments typically cut cabling costs in half by running a single Ethernet connection instead of both voice and data cables. (This cost savings is only a factor realized in new construction or renovation of offices.)
- **Seamless voice networks:** Because data networks connect offices, mobile workers, and telecommuters, VoIP naturally inherits this property. The voice traffic is crossing "your network" rather than exiting to the PSTN. This also provides centralized control of all voice devices attached to the network and a consistent dial plan. For example, all users could dial each other using four-digit extensions, even though many of them may be scattered around the world.
- **Take your phone with you:** Cost estimates for moves, adds, and changes (MAC) to a traditional PBX system range from $55 to $295 per MAC. With VoIP phone systems, this cost is greatly reduced. In addition, IP phones are becoming increasingly plug-and-play within the local offices, allowing moves with little to no reconfiguration of the voice network. When combined with a VPN configuration, users can even take an IP phone home with them and retain their work extension.
- **IP softphones:** Softphones represent an ideal example of the possibilities when combining voice and data networks. Users can now plug a headset into their laptop or desktop computer or tablet and allow it to act as their phone. Softphones are becoming increasingly more integrated with other applications such as email contact lists, instant messaging, presence, video telephony, and rich-media collaboration tools such as WebEx.
- **Unified email, voicemail, fax:** All messaging can be sent to a user's email inbox. This allows users to get all messages in one place and easily reply to, forward, or archive messages.
- **Increased productivity:** VoIP extensions can forward to ring multiple devices before forwarding to voicemail. This eliminates the "phone tag" game.
- **Feature-rich communications:** Because voice, data, and video networks have combined, users can initiate phone calls that communicate with or invoke other applications from the voice or data network to add additional benefits to a VoIP call. For example, calls flowing into a call center can automatically pull up customer records based on caller ID information or trigger a video stream for one or more of the callers.
- **Open, compatible standards:** In the same way that you can network Apple, Dell, and IBM PCs together, you can now connect devices from different telephony vendors together. Although this capability is still evolving, it will allow businesses to choose the best equipment for their network, regardless of the manufacturer.

The Process of Converting Voice to Packets

In the early 1930s, Dr. Harry Nyquist laid the mathematical foundations for the technology used to this day to convert analog signals (flowing waveforms) into digital format (1s and 0s). It is important to understand this process because it will inform your understanding of VoIP audio sample sizes, DSP resources, and codecs. The process of converting analog to digital consists of three (sometimes four) steps: sampling, quantization, and encoding. (The fourth is compression, which is not always applied.)

The origin of the digital conversion process (which fed many of the developments discussed earlier) takes us back to the 1920s. The Bell Systems Corporation tried to find a way to

deploy more voice circuits with less wire because analog voice technology required one pair of wires for each voice line. For organizations that required many voice circuits, this meant running large bundles of cable. After much research, Nyquist found that he could accurately reconstruct audio streams by taking samples of the analog signal twice as many times per second as the numerical value of the highest frequency used in the audio.

Here is how it breaks down: Audio frequencies vary based on the volume, pitch, and so on that comprise the sound. Here are a few key facts:

- The average human ear is able to hear frequencies from about 20–20,000 Hz.
- Human speech uses frequencies from about 200–9000 Hz.
- Traditional telephone channels typically transmit frequencies from 300–3400 Hz.
- Standard equipment used to digitize human speech reproduces frequencies from 300–4000 Hz.

Now, you might think, "If human speech uses frequencies between 200–9000 Hz and the normal telephone channel only transmits frequencies from 300–400 Hz, how can you understand human conversation over the phone?" That's a good question: Studies have found that telephone equipment can accurately transmit understandable human conversation by sending only a limited range of frequencies. The telephone channel frequency range (300–3400 Hz) gives you enough sound quality to identify the remote caller and sense their mood. The telephone channel frequency range does not send the full spectrum of human voice inflection, and so lowers the actual quality of the audio. For example, when you listen to talk radio, you can always tell the difference in quality between the radio host and the telephone caller, but you can still understand the caller because your brain is very good at filling in the gaps.

Nyquist proved that you can accurately reproduce an audio signal by sampling at twice the highest frequency. Because he was after audio frequencies from 300–4000 Hz, it would mean sampling 8000 times (2 * 4000) every second. So, what's a sample? A sample is a numeric value of the analog waveform, measured at regular intervals. More specifically, in the voice realm, a sample is a numeric value that is encoded by a single byte (8 bits) of information. As Figure 1-12 illustrates, during the process of sampling, the sampling device puts an analog waveform against a Y-axis lined with numeric values.

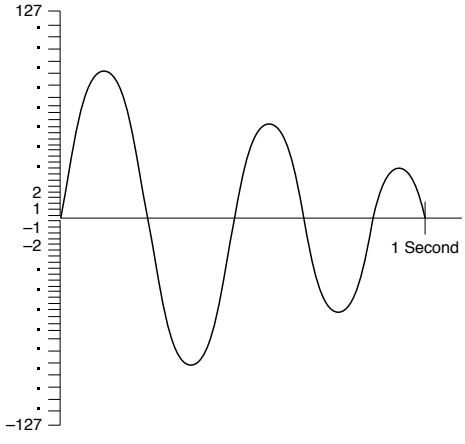


Figure 1-12 *Converting Analog Voice Signals to Digital*

Sampling, therefore, is the measurement of the waveform at regular intervals. This process is inherently inaccurate because an analog waveform is continuous and infinitely precise. By that I mean, if you "zoomed in" on an analog waveform, it would still look like a wave, which by definition has an infinite number of data points on it; keep zooming in, and you just see a closer view of infinity, which is of course still infinite. What we are doing with sampling is taking a "snapshot" that approximates a measurement of the infinitely variable waveform at an instant in time; then, we take another one a few instants later, and another. The process itself creates jumps or steps in the measurements—the brief periods between samples. If the samples are not taken frequently enough, the steps are large, the analog waveform is not represented accurately, and the quality suffers badly. It is exactly the same as the difference between a low-resolution image and a high-resolution image; low-res images are kind of blurry and not great, and hi-res images are crisp, sharp, and detailed.

Dealing with the transition between the steps in the digital measurement is known as quantization. We are limited to a range of whole numbers on the measurement scale (no fractions or decimal places are possible) because 1 byte of information can represent only values 0–255. The sample values of the voice scale are limited to values measuring a maximum peak of +127 and a minimum low of –127 to correspond with the positive and negative amplitude of the analog wave. When the codec encounters a measurement that is not a whole number on that scale, the measurement is artificially adjusted one way or the other so that it does fall exactly on the whole number. This introduces a small amount of inaccuracy into the digitization of analog audio; increasing the number of samples per second reduces the inaccuracy, but it can never be eliminated because the curve of the analog waveform is infinite. (This, incidentally, is why some people say that vinyl records sound better than digital tracks. They are right in theory; it's just that in reality not very many people care enough about your all-tube amp and your diamond-gimbaled turntable with the moon-rock needle to go to all that trouble and expense just for the ultimate analog audio experience. An iPod is much more convenient and easier to carry.)

The third step is encoding, or applying a binary value to the quantized measurement. Notice in Figure 1-12 that the 127 positive and negative values are not evenly spaced. This is by design. To achieve a more accurate numeric value (and thus, a more accurate reconstructed signal at the other end), the amplitude values more common in human speech are tightly packed near the middle, whereas the "fringe amplitudes" on the high and low end of the spectrum are more spaced apart.

The codec uses the 8 binary bits in each byte as two components: a positive/negative indicator and the numeric representation. As shown in Figure 1-13, the first bit indicates positive or negative, and the remaining seven bits represent the actual numeric value of 0–127.

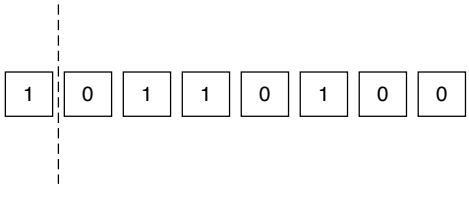


Figure 1-13 *Encoding Voice into Binary Values*

Because the first bit in Figure 1-13 is a 1, you read the number as positive. The remaining 7 bits represent the number 52. This is the digital value used for one quantized voice sample. Remember, the Nyquist theorem dictates that you need to take 8000 of those samples every single second. Do the math: We have 8000 samples per second times the 8 bits in each sample, for a product of 64,000 bits per second. It's no coincidence that uncompressed audio (including that from the G.711 audio codec) generates a 64-kbps payload of digitized voice. Once the sampling device assigns numeric values to all these analog signals and encapsulates them using Real-time Transport Protocol (RTP) and User Datagram Protocol (UDP), a router can place them into an IP packet and send them across a network.

Note There are two forms of the G.711 codec: μ-law (used primarily in the United States and Japan) and a-law (used everywhere else). The quantization method described in the preceding paragraph represents G.711 a-law. G.711 μ-law codes in exactly the opposite way. If you were to take all the 1 bits in Figure 1-13 and make them 0s and take all the 0 bits and make them 1s, you would have the G.711 μ-law equivalent. If two devices that must communicate together use different version of G.711, the μ-law side must do the conversion to a-law.

The last and optional step in the digitization process is to apply compression measures. High-compression codecs such as G.729 enable you to compress the number of samples sent and thus use less bandwidth. This is possible because sampling human voice 8000 times a second produces many samples that are similar or identical. For example, say the word *cow* out loud to yourself. That takes about a second to say, right? If not, say it slower until it does. Now, listen to the sounds you are making. There's the distinguished "k" sound that starts the word, then you have the "ahhhhhh" sound in the middle, followed by the "wa" sound at the end. If you were to break that into 8000 individual samples, chances are most of them would sound the same.

The process G.729 (and most other compressed codecs) uses to compress this audio is to send a sound sample once and simply tell the remote device to continue playing that sound for a certain time interval. This is often described as "building a codebook" of the human voice traveling between the two endpoints. Using this process, G.729 is able to reduce bandwidth down to 8 kbps for each call—a very significant reduction in bandwidth.

Unfortunately, significantly reducing the amount of bandwidth comes at a cost. Quality is negatively impacted by the compression process. Early on in the voice digitization years, the engineers working on the project created a measurement system known as the mean opinion score (MOS) to rate the quality of the various voice codecs. The test that rates the quality of voice is simple: A person listens to a caller say the sentence, "Nowadays, a chicken leg is a rare dish," and rates the clarity of this sentence on a scale of 1–5. Table 1-2 shows how each audio codec fared in MOS testing.

Key Topic

Table 1-2 Audio Codec Bandwidth and MOS Values

Codec	Bandwidth Consumed	MOS
G.711	64 kbps	4.1
G.722	64 kbps	4.2*

Codec	Bandwidth Consumed	MOS
Internet Low	15.2 kbps	4.1
Bitrate Codec (iLBC)		
G.729	8 kbps	3.92
G.726	32 kbps	3.85
G.729a	8 kbps	3.7
G.728	16 kbps	3.61

*Note: MOS scores for G.722 vary depending on testing methodology. G.722 is generally accepted as "better" than G.711 in terms of speech quality.

Table 1-2 leads into a relevant discussion about audio coder/decoders (codecs). You can use quite a few different audio codecs on your network, each geared for different purposes and environments. For example, some codecs are geared specifically for environments in which audio is sent through satellite link and bandwidth is limited. These codecs sacrifice audio quality to achieve very low-bandwidth transmissions. Other codecs are designed to meet a requirement for higher quality, and consequently use more bandwidth.

In the realm of Cisco Unified Communications, you will hear two codecs frequently referenced: G.711 and G.729. This is because every Cisco IP phone includes a codec that can encode/decode voice in either of these two formats (and depending on the phone model, several other codecs as well). G.711 is the "common ground" between all VoIP devices. For example, if a Cisco IP phone is attempting to communicate with an Avaya IP phone, they may support different compressed codecs but can at least agree on G.711 when communicating.

More recently, Cisco has begun to use G.722 as the default codec on new IP phone models and in firmware for existing models that can support it. G.722 is classified as a wideband codec, meaning it reproduces a wider range of frequencies and consequently has perceptibly better audio quality than G.711. At the same time, G.722 uses the same 64-kbps bandwidth as G.711 (or less in some implementations) and is only a slightly more complex codec to process. Nailing down a MOS score for G.722 is difficult because it can operate in several different modes, and different test methods and conditions produce very different scores. Speaking subjectively, a G.722 call on a Cisco IP phone sounds great—clearly better than a G.711 call.

Key Topic

Note G.729 comes in two different variants: G.729a (annex A) and G.729b (annex B). G.729a sacrifices some audio quality to achieve a much more processor-efficient coding process. G.729b introduces support for voice activity detection (VAD), which makes voice transmissions more efficient. You learn more about these variants in the following section.

The Role of Digital Signal Processors

Cisco designed its routers with one primary purpose in mind: routing. Moving packets between one location and another is not a processor-intensive task, and thus Cisco routers are not equipped with the kind of memory and processing resources typical PCs are

equipped with. For example, from a router's perspective, having 256 MB of RAM is quite a bit. From a PC's perspective, 256 MB barely helps you survive the Microsoft Windows boot process.

Moving into the realm of VoIP, the network now requires the router to convert loads of incoming voice calls into digitized, packetized transmissions (and, of course, the reverse of that process as well). This task would easily overwhelm the resources you have on the router. This is where DSPs come into play. DSPs offload the processing responsibility for voice-related tasks from the processor of the router. This is similar to the idea of purchasing an expensive video card for a PC to offload the video processing responsibility from the PC's processor.

Specifically, a DSP is a chip that performs all the sampling, encoding, and compression functions on audio (and, in current hardware, video, too) coming into your router. If you were to equip your router with voice interface cards (VICs), allowing it to connect to the PSTN or analog devices, but did not equip your router with DSPs, the interfaces would be worthless. The interfaces would be able to actively connect to the legacy voice networks, but would not have the power to convert any voice into packetized form.

DSPs typically come as chips to install in your Cisco router, as shown in Figure 1-14.

Figure 1-14 *DSP Chip*

Some Cisco routers can also have DSPs embedded on the motherboard or added in riser cards. Above all, it is important for you to add the necessary number of DSPs to your router to support the number of active voice and video calls, conferences, and transcoding (converting one codec to another) sessions you plan to support.

Tip Cisco provides a DSP calculator that provides the number of DSP chips you need to purchase based on the voice network you are supporting. You can find this tool at http://www.cisco.com/web/applicat/dsprecal/index.html (Cisco.com login required). Keep in mind that a growing network will always require more DSP resources. It is usually best to pack the router full with as many DSP resources as you can fit in it; you're going to need them!

You can add DSP chips either directly to a router's motherboard (if the router supports this) or to the network modules you add to the router to support voice cards. Cisco bundles these DSP chips into packet voice DSP modules (PVDM), which resemble memory SIMMs (refer to Figure 1-14). At the time of this writing, there are two types of PVDM chip available: PVDM2 and PVDM3. PVDM3s are more powerful, more efficient, have the additional capability of processing video as well as audio, and even include power-saving features when idle. Based on the DSP requirements given by the Cisco DSP calculator, you can then purchase one or more of the following PVDMs:

- **PVDM3-16:** 16-channel high-density voice and video DSP module
- **PVDM3-32:** 32-channel high-density voice and video DSP module
- **PVDM3-64:** 64-channel high-density voice and video DSP module
- **PVDM3-128:** 128-channel high-density voice and video DSP module
- **PVDM3-192:** 192-channel high-density voice and video DSP module
- **PVDM3-256:** 256-channel high-density voice and video DSP module

Not all codecs are created equal. Some codecs consume more DSP resources to pass through the audio conversion process than other codecs consume. Table 1-3 shows the codecs considered medium and high complexity.

Table 1-3 Medium- and High-Complexity Codecs

Medium Complexity	High Complexity
G.711 (a-law and µ-law)	G.728
G.726	G.723
G.729a, G.729ab	G.729, G.729b
—	iLBC

Generally speaking, the DSP resources are able to handle roughly double the number of medium-complexity calls per DSP as high-complexity calls.

Note Newer DSP chips (PVDM3) can handle calls more efficiently and can handle more high-complexity calls per chip than older DSP hardware. To find the exact number of calls per DSP, use the Cisco DSP calculator tool mentioned in the previous tip.

Understanding RTP and RTCP

When you walk into the VoIP world, you encounter a whole new set of protocol standards. Think of the Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP) as the protocols of voice. RTP operates at the transport layer of the OSI model on top of UDP. Having two transport layer protocols is odd, but that is exactly what is happening here. UDP provides the services it always does: port numbers (that is, session multiplexing) and header checksums (which ensure that the header information does not become corrupted). RTP adds time stamps and sequence numbers to the header information. This allows the remote device to put the packets back in order when it receives them at the remote end (function of the sequence number) and use a buffer to remove jitter (slight delays) between the packets to give a smooth audio playout (function of the time stamp). Figure 1-15 represents the RTP header information contained in a packet.

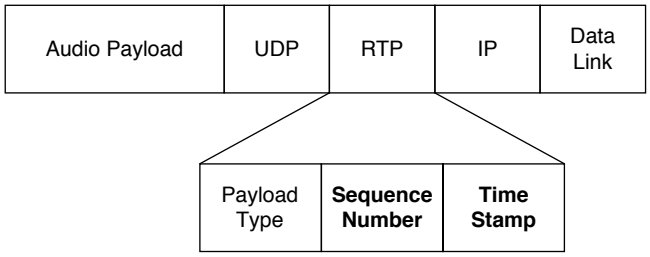


Figure 1-15 *RTP Header Information*

The Payload Type field in the RTP header is used to designate what type of RTP is in use. You can use RTP for audio or video purposes.

Key Topic

Once two devices attempt to establish an audio session, RTP engages and chooses a random, even UDP port number from 16,384 to 32,767 for each RTP stream. Keep in mind that RTP streams are one way. If you are having a two-way conversation, the devices establish dual point-to-point RTP streams, one in each direction. The audio stream stays on the initially chosen port for the duration of the audio session. (The devices do not dynamically change ports during a phone call.)

At the time the devices establish the call, RTCP also engages. Although this protocol sounds important, its primary job is statistics reporting. It delivers statistics between the two devices participating in the call, which include the following:

- Packet count
- Packet delay
- Packet loss
- Jitter (delay variations)

Although this information is useful, it is not nearly as critical as the actual RTP audio streams. Keep this in mind when you configure QoS settings.

As the devices establish the call, the RTP audio streams use an even UDP port from 16,384 to 32,767, as previously discussed. RTCP creates a separate session over UDP between the two devices by using an odd-numbered port from the same range. Throughout the call duration, the devices send RTCP packets at least once every 5 seconds. The Cisco Unified Communications Manager (CUCM) or CUCM Express (CME) router can log and report this information, which allows you to determine the issues that are causing call problems (such as poor audio, call disconnects, and so on) on the network.

Note RTCP uses the odd-numbered port following the RTP port. For example, if the RTP audio uses port 17,654, the RTCP port for the session will be 17,655.

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 1-5 lists and describes these key topics and identifies the page numbers on which each is found.

Key Topic

Table 1-5 Key Topics for Chapter 1

Key Topic Element	Description	Page Number
Figure 1-3	Illustrates the wired connections to an analog phone	7
List	Two methods used to deliver signaling with digital circuits	10
Figure 1-7	Illustrates TDM	10
Tip	Specific signaling time slot for T1 and E1 circuits using CCS	12
List	Components of the PSTN	12
Table 1-2	Common audio codecs, bandwidth consumption, and MOS rating	20
Note	PVDM ratings	21
Text	RTP concepts and port ranges	24

Complete the Tables from Memory

Table 1-6 is a study aid we call a "memory table." Print a copy of Appendix D, "Memory Tables" (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Table 1-6 Memory Table for Chapter 1

Topic	Purpose	Hardware Affiliation
Sampling	Measures analog waveform many times per second	Performed by codec in DSP internal to analog-to-digital device (for example, IP phone, gateway)
Quantizing	Adjusts sample measurement data to closest binary value	Performed by DSP
Encoding	Assigns a binary value to the sample	Performed by DSP
Compression	Optional, reduces the amount of binary data to represent the encoded sample	Performed by DSP

Topic	Purpose	Hardware Affiliation
Channel associated signaling	"Robs" some bits from the audio channel to deliver addressing and feature signaling	Associated with T1/E1 circuits
Common channel signaling	Uses a separate, dedicated channel for addressing and feature signaling	Associated with ISDN circuits (BRI, PRI)
RTP	Real-time Transport Protocol	Carries digitized voice payload

Definitions of Key Terms

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

analog signal, loop start signaling, ground start signaling, glare, time-division multiplexing (TDM), channel associated signaling (CAS), common channel signaling (CCS), robbed bit signaling (RBS), Q.931, local loop, private branch exchange (PBX), key system, Signaling System 7 (SS7), E.164, quantization, Nyquist theorem, mean opinion score (MOS), G.722, G.711, G.726, G.728, G.729, Real-time Transport Protocol (RTP), Real-time Transport Control Protocol (RTCP)

This page intentionally left blank

This chapter covers the following topics:

- **Unified Communications:** This section covers the core Cisco unified applications supporting voice and video collaboration over IP networks.
- **Understanding Cisco Unified Communications Manager Express:** This section discusses the target market segment for CME, key CME features, and communication between CME and Cisco IP phones.
- **Understanding Cisco Unified Communications Manager:** This section introduces key CUCM features, CUCM database architecture, and CUCM-to-Cisco IP phone interaction.
- **Understanding Cisco Unity Connection:** CUC provides traditional voicemail functionality as well as several other advanced messaging capabilities in an enterprise-class application. This section describes the CUC application and its capabilities.
- **Understanding CUCM Instant Messaging and Presence:** CUCM IM and Presence (IMP) aggregates and publishes telephony users' presence status and supports enterprise instant messaging and all-in-one applications such as Cisco Jabber. This section highlights the key features and interactions of CUCM IMP.
- **Understanding Video Communication Server and TelePresence Management Suite:** Supporting an increasing emphasis on video communication and collaboration requires additional products to provide and control these specialized functions. The Cisco Video Communication Server (VCS) and VCS Expressway provide video endpoint registration and call control, and firewall traversal for external video clients. Cisco TelePresence Management Suite (TMS) provides scheduling, management, and control of TelePresence resources to improve the manageability and user utility of a TelePresence investment.

CHAPTER 2

Understanding the Components of Cisco Unified Communications

Have you ever heard the saying, "You don't know what you don't know?" With the speed of technology development constantly increasing, the chances of this being true for you increase as well. Unfortunately, that can lead to missed opportunities to implement some really great features (at best) or increase your company's productivity and efficiency (at worst). This chapter resolves that issue (at least, as it relates to the core Cisco Unified products). What are all these servers and software? What do they do? How can they benefit my company? These are all questions we will unpack as you read this chapter.

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

Foundation Topics Section	Questions Covered in This Section
Understanding Cisco Unified Communications Manager Express	1–4
Understanding Cisco Unified Communications Manager	5–8
Understanding Cisco Unity Connection	9–10
Understanding CUCM IM and Presence	11

1. Which of the following products would support integrated FXS ports?

   a. Cisco Unified Communications Manager Express
   b. Cisco Unified Communications Manager
   c. Cisco Unified Presence
   d. Cisco Unity Connection

2. Which of the following signaling methods can CME use for endpoint control? (Choose two.)

   a. SCCP
   b. SIP
   c. H.323
   d. MGCP

3. Two users are talking on Cisco IP phones to each other in the same office. Midway through the call, an administrator reboots the CME router. What happens to the current call?

   a. The call is immediately disconnected.
   b. The call disconnects once the TCP keepalive between the Cisco IP phones and the CME router fails.
   c. The call remains active; however, no supplemental features (such as hold, transfer, and so on) are available for the remainder of the call.
   d. The call remains active, and the Cisco IP phones enable SIP Proxy mode for RTP.

4. Which of the following equipment allows the CME router to convert analog audio into VoIP packets?

   a. CPU/processor
   b. Digital signal processor
   c. SIP codec conversion
   d. Codec IOS enablement

5. Which of the following key features supported by CUCM does CME not support?

   a. SIP/SCCP endpoint control
   b. Redundancy
   c. PSTN gateway functionality
   d. VMware deployment on Unified Computing System platform

6. If a CUCM Publisher server fails, which of the following events occur?

   a. A CUCM Subscriber takes over Publisher functions until the original Publisher server preempts the role.
   b. A CUCM Subscriber takes over Publisher functions permanently; if the original Publisher server returns, it is demoted to a Subscriber role.
   c. Administrative access to the CUCM database becomes read-only; user-facing features are writable to the Subscriber.
   d. Outside calling is disabled until the CUCM Publisher returns to the network.

7. How many redundant CUCM servers does a Cisco IP phone support for failover purposes (not including SRST devices)?

   a. 2
   b. 3
   c. 4
   d. 6

8. How many call processing servers does Cisco support in a standard CUCM cluster (that is, not a "megacluster")?

   a. 2
   b. 3
   c. 6
   d. 8
   e. 9

9. When run on a single server, Cisco Unity Connection can support up to 20,000 mailboxes. When combining two Cisco Unity Connection servers in an active/active redundancy pair, how many mailboxes are supported?

   a. 20,000
   b. 35,000
   c. 40,000
   d. 45,000

10. Which of the following governs the number of concurrent calls supported by a Cisco Unity Connection server?

    a. Trunk ports
    b. Voicemail ports
    c. SIP proxy server
    d. CUCM SCCP hunt group

11. Cisco Unified Presence supplies which of the following capabilities? (Choose two.)

    a. Cisco Unified Personal Communicator
    b. Enterprise IM Solution
    c. Visible status indicators of IP Phone users
    d. Multipoint audio and HD video

Foundation Topics

Unified Collaboration

As you glance through the Cisco product suite for IP voice and video, it appears that Cisco is trying to say something. The resounding theme again and again is "unified" (with "collaboration" coming in at a close second). When you peel back the glossy marketing surface, you find that there is a lot more to "unified" than just VoIP. The technology crosses boundaries and brings together all communication into one, seamless framework. The interaction we experience today was only seen in the science-fiction movies of decades ago: rooms full of corporate strategists interacting with a partner company half-way around the world through huge flat-panel monitors surrounding the conference desk. Virtual workgroups comprised of telecommuting individuals sharing whiteboards, documentation, and project plans in real time; a "road warrior" sales manager leading the video-streamed team meeting from a mobile device in his car (while safely pulled over on the side of the road, of course). No longer fiction—although I am still waiting for my flying car.

The Cisco collaboration strategy encompasses all electronic communication types: voice, video, and data. For CICD, we are going to focus on four core Cisco Unified Communications Collaboration products:

- Cisco Unified Communications Manager Express
- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Unified Communications Manager IM and Presence

Keep in mind that these are the "core" solutions, and you can add many additional applications to expand the features and functionalities of the system. For example, the Cisco Unified Contact Center platforms allows you to add call-center capabilities to your network, such as skills-based call routing, call queuing, live monitoring of conversations, and so on. Cisco WebEx adds enhanced conference-call capabilities, document collaboration, and training platforms. Dedicated video collaboration systems such as TelePresence offer distributed HD video and multi-channel audio for a virtual collaboration experience that is startlingly true to life. The list goes on, but the CICD exam concentrates on these four core components of the system.

My goal in the rest of this book is to give you the information you need to become familiar with each of the core Unified Communications platforms. Keep in mind that "familiar" does not equate to "expert." Just as the Cisco CCNA certification was created to lay the foundation skills needed to manage day-to-day route/switch operations in a Cisco-based network (and hopefully lead you into the CCNP certification), the CCNA Collaboration (CICD exam) certification will lay this same foundation as it relates to VoIP (and perhaps lead you into CCNP Collaboration certification). As you go through this book, you might be astonished (and perhaps overwhelmed) at just how much technology you learn, and that experience will continue throughout your career as you see just how much further the technology goes.

We begin by discussing Cisco Unified Communication Manager Express (CME).

Note Originally, Cisco Unified Communications Manager (CUCM) and Cisco Unified Communications Manager Express (CME) used to be called Cisco CallManager (CCM) and Cisco CallManager Express (CME), respectively. Years later, the CallManager name lives on because it's just easier to say. So, if you hear someone call it CallManager, it means they've been at this for a while.

Understanding Cisco Unified Communications Manager Express

A Cisco router can perform an impressive array of tasks: routing tables, routing protocols, security with access lists, Network Address Translation (NAT), virtual private networking (VPN), intrusion detection, firewall, plus a few others. On top of all that, the Cisco router you have been using for years might also run your IP telephony network. That was the goal with the Cisco Unified Communications Manager Express (CME) platform. Your Cisco Integrated Services Router (ISR) platform not only performs all of those tasks, but can also terminate analog and digital voice circuits (such as FXO, FXS, and T1 ports); support VoIP endpoints (such as Cisco IP phones); and even handle the more advanced features, such as conference calling, video telephony, and automatic call distribution (ACD). Depending on the platform you use, CME can scale to support up to 450 IP phones, which makes it a good solution for small and even some midsize businesses.

Although current CME versions are intended to operate on the ISR Generation 2 (G2) platforms, you can also run it on the original ISR platforms (such as the 1800, 2800, or 3800 series), provided you have the proper IOS (RAM and flash memory upgrades are a good idea, too). Cisco integrates CME into the IOS software itself. Since the release of IOS 15, a product authorization key (PAK) is needed to activate the CME feature set. Table 2-2 shows the current ISR G2 platforms available and the maximum number of phones supported on each platform.

Table 2-2 Unified CME Supported ISR G2 Platforms

Platform	Maximum Phones
Cisco 881 and 887VA ISR G2	5
Cisco 2901 ISR G2	35
Cisco 2911 ISR G2	50
Cisco 2921 ISR G2	100
Cisco 2951 ISR G2	150
Cisco 3925 ISR G2	250
Cisco 3945 ISR G2	350
Cisco 3925E ISR G2	400
Cisco 3945E ISR G2	450

Platform	Maximum Phones
Cisco 4321 ISR G2	50
Cisco 4331 ISR G2	100
Cisco 4351 ISR G2	250
Cisco 4431 ISR G2	350
Cisco 4451-X ISR G2	450

Keep in mind that these figures are current at the time of this writing, but they may change as hardware platforms upgrade and become more powerful.

CME Key Features

Because CME runs on a Cisco router, it has the unique advantage of acting as an all-in-one device for controlling Cisco IP phones and trunking to the public switched telephone network (PSTN) through various connections. The following are the key features supported by CME:

- **Call processing and device control:** The CME router acts as the all-in-one call control device. It handles the signaling to the endpoints, call routing, call termination, and call features.
- **Command-line or GUI-based configuration:** Because Cisco integrated CME directly into the IOS, you have the full capability of command-line configuration. You can also use a GUI utility, such as Cisco Configuration Professional (CCP), to administer it with a friendlier interface.
- **Local directory service:** The CME router can store a local user database you can use for authentication in the IP telephony (IPT) network and for the IP phone directory listing.
- **Computer Telephony Integration (CTI) support:** CTI allows the IPT network to integrate with the applications running on the data network. For example, you could use the Cisco Unified CallConnector to make one-click calls directly from your Microsoft Outlook contact list.
- **Trunking to other VoIP systems:** Although CME can run as a standalone deployment interfacing directly with the PSTN, it can also integrate with other VoIP deployments. For example, you could use CME for a small, 40-user office and have it connect directly over your IP WAN network (which could itself be the Internet) to the corporate headquarters, which uses a Cisco Unified Communications Manager (CUCM) cluster.
- **Direct integration with Cisco Unity Express (CUE):** CUE, which runs through a module installed in a Cisco router, can provide voicemail services to the IP phones supported by CME.

Note The CICD course has removed CUE from its list of topics. We make mention of CUE from time to time for context and interest, but as of this writing, CUE is no longer listed on the CICD exam blueprint.

CME Interaction with Cisco IP Phones

Although there is much to be learned about how a Cisco IP phone contacts and registers with a CME router (which is discussed in Chapter 3, "Understanding Cisco IP Phones"), let's focus on the role of CME after a phone has completed registration. This gives you an idea of how the CME router interacts with the Cisco IP phones and routes calls across the data network. This discussion also lays the foundation for how the other call-management applications support the IPT network. First, let's follow the VoIP flow shown in Figure 2-1.

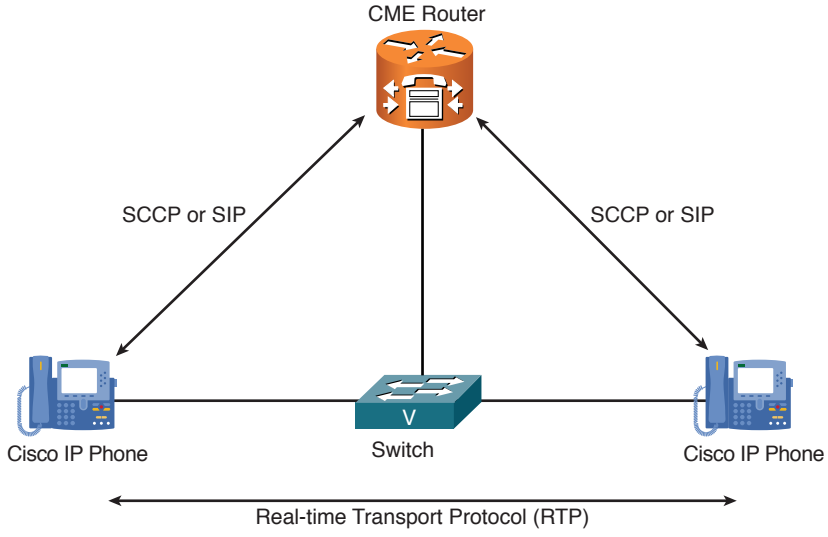


Figure 2-1 *CME Call Flow for On-Network Cisco IP Phones*

Key Topic

Essentially, the relationship between CME and the Cisco IP phones is similar to the relationship between a mainframe and dumb terminals. CME controls virtually every action performed at the Cisco IP phones. For example, if a user picks up the handset, an off-hook state is sent from the Cisco IP phone to the CME router using either Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP). We discuss these protocols in Chapter 3, but in a nutshell, SCCP and SIP are both signaling protocols that allow the call-management platform (CME, in this case) to communicate with and control an IP phone. As the user begins to dial digits, digits are sent to the CME router (again, via SCCP or SIP). After the user completely dials the phone number of the other Cisco IP phone shown in Figure 2-1, CME sends signaling messages causing the called-party phone to ring (and the calling-party phone to play ringout). When the user answers the ringing phone, CME instructs the IP phones to send the voice packets directly and steps out of the communication stream. The phones now communicate directly using the Real-time Transport Protocol (RTP), which handles the actual audio stream between the devices.

The fact that CME is not involved in the RTP stream and instructs the IP phones to communicate directly is important for two reasons: First, it (at least partially) eliminates the CME router as a point of failure. After CME establishes the RTP stream between the IP phones, it could crash, reboot, or catch fire and the conversation between the two endpoints would continue unhindered (provided the fire didn't get too bad, I suppose). The other benefit is that the

CME router does not become a bottleneck for the RTP stream. If the links to the CME router became saturated or the router ran out of resources, RTP packets could be dropped, causing the call quality to degrade. Keep in mind that we're only talking about the RTP stream, which contains only the audio of the call. All the phone features (such as hold, transfer, conference, and so on) are still managed using SCCP or SIP, so those would not be available until the CME router came back online. Likewise, after the users disconnect from the call, the phone would not be available to place or receive any calls until the CME router returned online.

Note This discussion assumes a CME deployment where there is no backup call-management device. This is common for smaller organizations.

Let's broaden the discussion by following a call from a Cisco IP phone to an analog phone attached to the PSTN shown in Figure 2-2.

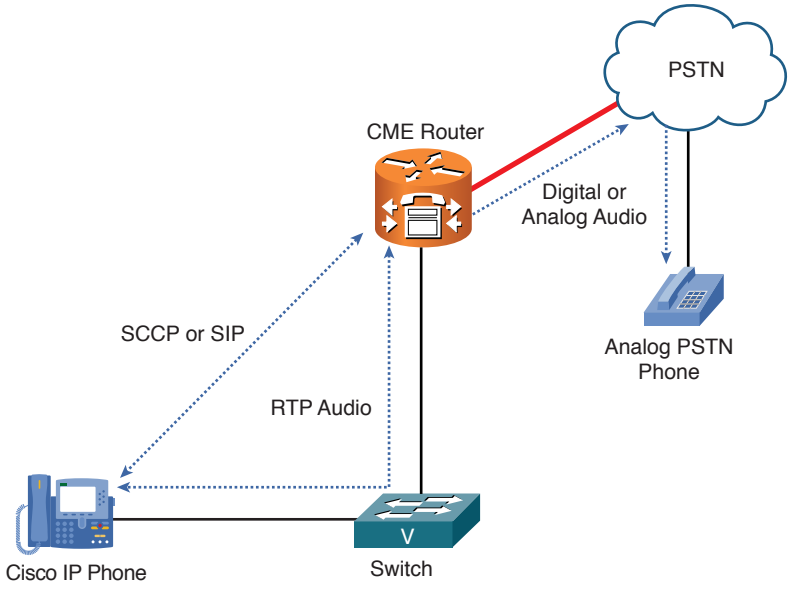


Figure 2-2 *CME Call Flow for Calls to the PSTN*

As the user of the Cisco IP phone picks up the phone to place the call, all the signaling is handled by SCCP or SIP. After the user finishes dialing the phone number of the PSTN phone, the CME router determines (due to its dial plan) that the call should be routed out a PSTN-connected interface. CME now assumes the role of voice gateway and signals to the PSTN to establish the call on behalf of the Cisco IP phone. Keep in mind that this is "traditional" telephony signaling as discussed in Chapter 1, "Traditional Voice Versus Unified Voice," because the CME router is attached to the PSTN using a digital (T1/E1) or analog (FXO) trunk. Once the audio for the call connects, the CME router assumes the role of converting between VoIP audio and PSTN audio. Because this conversion is processor intensive, the CME router is equipped with digital signal processors (DSPs), which are simply additional "mini processors" dedicated to voice functions.

Note Many VoIP deployments now connect to the PSTN using an Internet telephony service provider (ITSP) rather than a traditional TSP. In this case, the CME router relays the voice call over a SIP trunk rather than over an analog or digital circuit.

The CME router has now established two different "legs" of the call: one to the PSTN and the other to the Cisco IP phone. It stands in the middle, independently handling signaling from both sides in two different formats. Unlike the first example, the CME router is now a critical piece of the ongoing RTP audio flow. If it were to fail in the middle of the call, the audio for the call would also fail.

Understanding Cisco Unified Communications Manager

When Cisco first released CallManager 2.4, it ran as an application on Microsoft Windows NT 4.0, supported by the Internet Information Server (IIS) web server. Needless to say, Cisco has come a long way as CUCM moves through the 10.x versions and beyond. It now runs as a Linux-based VMware guest on certified hardware platforms and acts as the powerful call processing component of the Cisco Unified Communications collaboration solution. Think of CUCM as the "director" behind any large organization's Cisco IPT solution. It provides the core device control, call routing, permissions, features, and connectivity to outside applications. In a nutshell, the importance of CUCM to Cisco VoIP is critical. With that being said, don't let the size and complexity of CUCM overwhelm you. Cisco has done a commendable job of allowing you to manage nearly every CUCM option through a well-designed web-based graphical user interface (GUI).

CUCM Key Features

Although CUCM supports numerous capabilities, here are some of the most important:

Key Topic

- **Full support for audio and video telephony:** The core feature provided by CUCM; in the same way CME acts as the call control agent in a small organization, CUCM supports audio and video calls for midsize to global enterprise-class corporations.
- **Appliance-based operation:** Modern CUCM versions run as an appliance, which means the underlying operating system is hardened (secured) and inaccessible.
- **VMware installation:** CUCM is intended for deployment in a virtual machine, using VMware ESXi as the host OS on approved hardware. VMware provides ease of manageability, hardware utilization efficiency, performance, and strong host security for a highly reliable and scalable virtual machine infrastructure. The Cisco Unified Computing System (UCS) hardware is the primary supported and recommended hardware, and itself provides ease of hardware management, failover, migration, and top-tier performance and reliability.
- **Redundant server cluster:** CUCM supports redundant servers configured in a cluster relationship. The clustering capabilities replicate both database information (containing static data such as directory numbers and route plans) and real-time information (containing dynamic data, such as active calls and device registration information). A single standard CUCM cluster can scale to 40,000 IP secure or nonsecure phones running SCCP or

SIP. Cisco can also design a "megacluster" option for qualifying customers, taking the theoretical maximum number of IP phones to 80,000 in a single cluster. (Remember this is a special-case scenario; for your exam, think of the standard cluster sizing of 40,000 phones as the maximum.)

- **Intercluster and voice gateway control and communication:** Even though a standard CUCM cluster has a limit of 40,000 IP phones, you can create as many clusters as you like (with up to 40,000 IP phones each) and connect them together using intercluster trunk connections. In addition to using Intercluster trunk links to call outside of your own cluster, CUCM can also connect to voice gateways (such as a Cisco router), which can connect to various other voice networks (such as the PSTN or legacy PBX systems).
- **Built-in disaster recovery system (DRS):** As a built-in feature, the CUCM DRS service allows you to back up the CUCM database system to a (noncluster) Secure FTP (SFTP) server.
- **Directory service support or integration:** VoIP networks can use network user accounts for a variety of purposes (phone control, attendant console control, and so on). CUCM has the capability to be its own directory server to hold user accounts, or it can integrate into an existing corporate Lightweight Directory Access Protocol (LDAP) directory structure (such as Microsoft Active Directory) and pull user account information from there.

CUCM Database Replication and Interacting with Cisco IP Phones

Even though CUCM can scale to a massive size, it interacts with Cisco IP phones in a similar manner to CME. Remember that CUCM is typically deployed in a cluster; the CUCM cluster relationship includes two types of communication:

- **CUCM database replication:** The CUCM IBM Informix database includes all the "static" data of the cluster (directory numbers, route plan, calling permissions, and so on). The Publisher replicates this data as a read-only database to all the Subscriber servers in the cluster. (A more detailed description of the roles of Publisher and Subscriber follows.)
- **CUCM runtime data:** As the name implies, the runtime data encompasses anything that happens in "real time" in the CUCM cluster. For example, when a device registers with a CUCM server, it communicates to all the other servers that it now "owns" that IP phone and the extension (directory number or DN) associated with it. CUCM uses a method designed specifically by Cisco for this type of communication: intracluster communication signaling (ICCS).

Although the CUCM ICCS data is very important for functionality, there's not very much of it. All the servers in the CUCM cluster form TCP sessions to each other for ICCS communication (TCP ports 8002 to 8004). Then, whenever something of interest happens (such as a phone registering, a call initiation, a call disconnect, and so on), the servers inform each other of the event. Setting up all this ICCS communication takes almost no configuration on your part (other than adding the CUCM server to the cluster). The amount of network traffic generated by ICCS is variable; assuming 10,000 busy-hour call attempts, ICCS generates about 1.5 Mbps per server—in other words, not a lot, even in a busy system—but that traffic is critical to the system working properly.

Key Topic

In contrast, the CUCM database replication traffic volume is much heavier, but under normal operation it is not any more difficult to manage than ICCS; it just works behind the scenes. The CUCM Informix database uses a one-way push replication in which the Publisher holds the master copy of the database. Changes to the database (such as the addition or modification of users, phones, dial plan, and so on) are implemented on the Publisher, which replicates the database changes to the Subscribers as a read-only copy. Figure 2-3 illustrates this relationship.

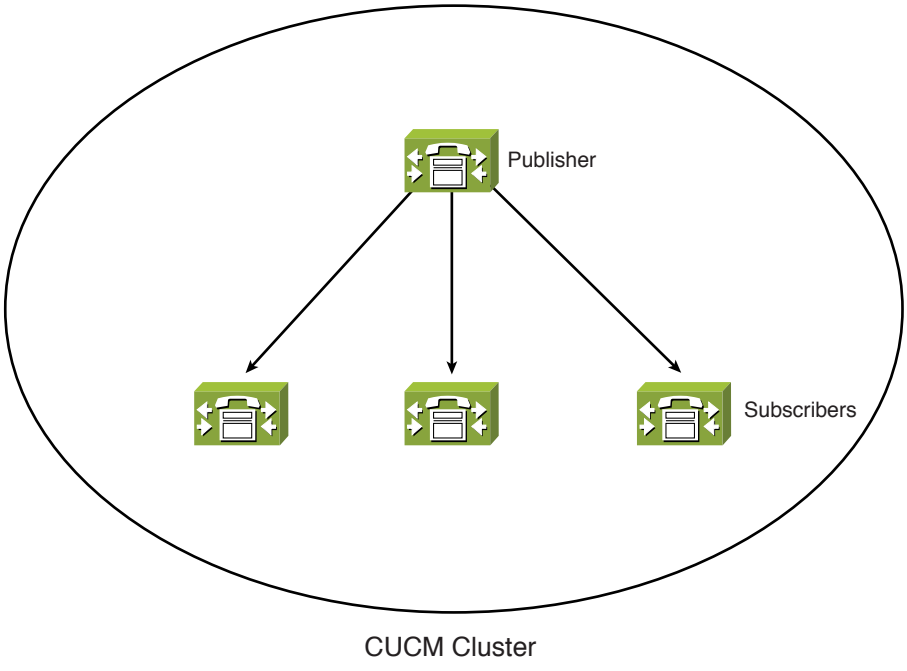


Figure 2-3 *CUCM Database Relationship*

A standard CUCM cluster supports a single Publisher and up to 19 Subscribers, of which 8 can be configured as call-processing nodes. Think of the call-processing Subscribers as the "workhorses" of the IPT network. These servers provide all call control signaling, call routing decisions, and call restrictions. The other 11 Subscribers do not perform call processing; in large clusters, they are assigned various dedicated roles such as TFTP server, conference bridges, music on hold, or annunciator servers. In small-to-medium deployments, the Publisher typically performs only two primary functions: It maintains the only writable copy of the database and serves TFTP requests. Because the Publisher serves such a critical role in maintaining the only writable copy of the CUCM database, it is usually kept from all the heavier work of call processing; in very large systems, Cisco recommends moving the TFTP role to one (or more likely two) dedicated Subscribers. The TFTP role is critical to the operation of Cisco IP phones and devices such as gateways, because then bulk of their configuration is downloaded from these TFTP servers. We cover this in more detail in Chapter 3.

Tip In smaller environments, it is okay to use the Publisher for both database management and call processing. However, when the server becomes heavily loaded (this is dependent on server performance and cluster activity but is generally accepted to be around 1000 phones/users), it is generally a best practice to pull the Publisher out of call processing and leave that work to the Subscribers. Likewise, once you exceed about 1250 users, Cisco recommends moving the TFTP server role to a dedicated server.

Note If the Publisher has the only writable copy of the database, what happens if it fails? In this case, the CUCM cluster simply carries on with the last replicated copy of the read-only database. The only limitation is that you can no longer make changes to the database (such as adding a new IP phone, changing the route plan, modifying a music on hold selection, and so on). The only exception to this is the set of user-facing features, which includes functions such as forwarding your phone, enabling the message waiting light, pressing the Do Not Disturb button, and several others. The CUCM Subscribers are able to write these changes to their local database and replicate them to the other Subscribers in the cluster (and eventually back to the Publisher when you have restored connectivity). Allowing the user-facing features to write to the Subscriber database means that the users will never know when a Publisher failure has occurred. This capability emerged in CUCM Version 6.2 and later. Before this version, a Publisher failure would have significantly impacted the user experience.

Once you understand the database replication piece of CUCM, the call flow is nearly identical to CME, as shown in Figure 2-4.

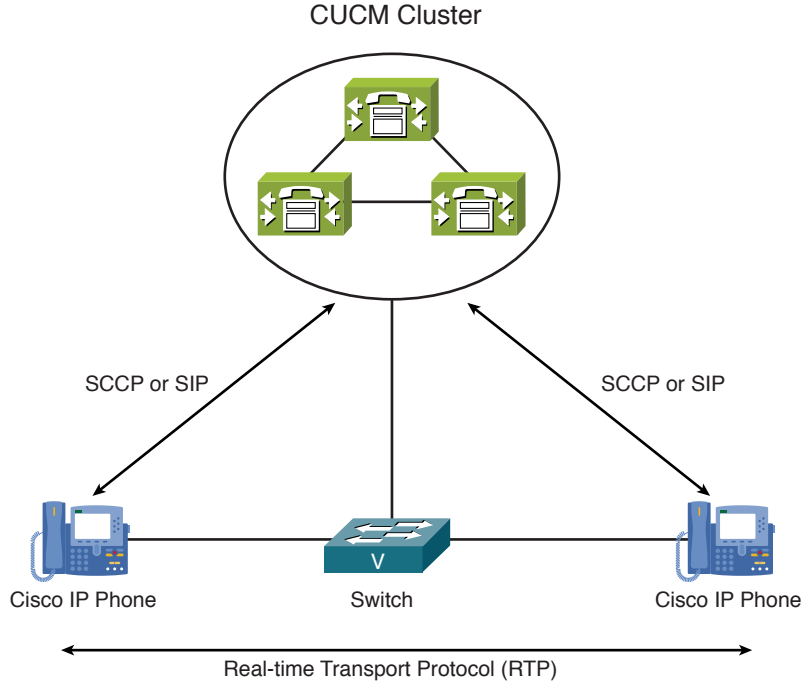


Figure 2-4 *CUCM Call Processing*

As with CME, the primary CUCM server used by the Cisco IP phone receives the SCCP or SIP off-hook message and responds appropriately in a stimulus/response fashion until the call is placed. One difference is that the IP phones can now use redundant servers (as opposed to the single CME router). Based on your configuration, a phone can use a list of up to three redundant CUCM servers for failover purposes. If the primary server is down, it uses the secondary. If the secondary is also down, it uses the tertiary. Because your CUCM cluster can support up to eight call processing servers, you can manually load balance the IP phones by assigning different primary, secondary, and tertiary CUCM servers to different groups of phones.

Key Topic

Note A common mistake when first learning CUCM functions is to confuse the primary server with the Publisher database role. Remember, the primary purpose of the Publisher is to maintain the writable copy of the database. It will most likely not be the primary call-processing server of an IP phone (except in very small environments). One of the eight designated call-processing Subscribers will be the IP phone's primary server.

Understanding Cisco Unity Connection

Long before the Cisco "unified" product campaign, there was the Cisco Unity product (not to be confused with Cisco Unity Connection, or even Cisco Unity Express). Although most people identify Cisco Unity as "the voicemail solution" for your VoIP network, Cisco designed it to be much more. The term *unity* related to messages: voice messages for sure, but also email messages, fax messages, and even instant messages. The goal of Unity was to make any message retrievable from any voice-enabled device or application. For example, a caller could leave a voicemail that you could retrieve from an e-mail client inbox. You could listen to your e-mails from a mobile device or have them faxed to an offsite fax machine. Essentially, regardless of how a message was left, you could retrieve it using a variety of clients.

Just like the original Cisco CallManager software, Cisco Unity ran on a Microsoft Windows Server OS and typically used a Microsoft Exchange e-mail server (or sometimes Lotus Domino) as the message store for voicemail. Cisco introduced Unity Connection as a smaller, feature-rich alternative using the same appliance-based model as CUCM years after the original Cisco Unity release. As time passed, Cisco gradually transitioned to positioning Unity Connection as the flagship enterprise messaging platform. Table 2-3 depicts the various voicemail solutions you can use for your IPT network and their scalability limits.

Table 2-3 Cisco Voice Messaging Systems Comparison

Platform	Maximum Mailboxes	Platform	Redundancy
Cisco Unity Express	300	Router	Not supported
Cisco BE 6000	1000	VMware on UCS	Active/active, capability hardware dependent
Cisco Unity	15,000 per server	Windows Server	Active/passive
Cisco Unity Connection	20,000 per server	VMware on UCS	Active/active

In addition to supporting more mailboxes, Cisco Unity Connection now supports features (such as personal call transfer rules and speech recognition) that are not available in the other Cisco voice-messaging products.

Note The Redundancy column shown in Table 2-3 shows the type of failover supported by the voicemail solutions. CUE does not support any failover. The original Cisco Unity supported active/passive, which meant a backup server would sit idle until the primary server failed. Cisco Unity Connection supports active/active, allowing the redundant servers to load balance the mailboxes.

Cisco Unity Connection Key Features

The following are some of the notable features of Cisco Unity Connection:

- **Proven appliance-based platform:** Cisco Unity Connection is built on top of the same stable, hardened, appliance-based operating system as CUCM. (These two software products even use the same installation media.)
- **Up to 20,000 mailboxes per server:** Cisco Unity Connection scales to a massive size per server. Even though Unity Connection supports a single-server configuration, most organizations will opt for a high availability pair of servers.
- **Access voicemails from anywhere:** Cisco Unity Connection allows voicemail retrieval from phone, e-mail, web browser, mobile devices, and instant messenger platforms.
- **LDAP directory server integration:** Similar to CUCM, Cisco Unity Connection can integrate with an existing corporate directory (such as Microsoft Active Directory) to avoid creating and maintaining a duplicate user database.
- **Microsoft Exchange support:** Cisco Unity Connection can integrate with an existing Microsoft Exchange deployment to enable features such as different call treatment based on your Exchange calendar, e-mail text-to-speech (hear your emails read to you from a phone), manage Exchange calendar (accept, decline, cancel, and so on) from a phone, and so on.
- **Voice Profile for Internet Mail (VPIM) support:** VPIM is a standard allowing the integration of voicemail servers from different vendors enabling you to exchange messages with a user on a totally separate messaging system as if they had a mailbox on your system.
- **Active/active high availability:** Cisco Unity Connection uses a Publisher/Subscriber cluster similar to CUCM between a pair of servers. Both servers can accept client requests (giving it the active/active redundancy). The largest Cisco Unity Connection VMware deployment can support up to 250 voicemail ports (essentially allowing 250 people to check their voicemail at a time). By creating a high-availability pair, you can now support 500 voicemail ports.

Key Topic

Note The active-active pair of servers can support up to 20,000 mailboxes in a redundant fashion. (The maximum number of mailboxes, whether on a single standalone CUC server or an active/active pair is 20,000.) If one of the servers in a Unity Connection high-availability pair fails, all 20,000 mailboxes are still available, but the number of voicemail ports is reduced to the maximum supported by the single server.

Cisco Unity Connection and CUCM Interaction

Outside of the BE6000, where CUCM and Unity Connection reside on a single server, Cisco Unity Connection operates independently from CUCM. As a matter of fact, you can run Cisco Unity Connection as a voicemail server for other non-Cisco VoIP deployments or even PBX systems; it is not tied exclusively to the CUCM product. Because of this, there is not a simple "click this button in CUCM to magically integrate with Cisco Unity Connection." Instead, you set up Cisco Unity Connection as an outside system that CUCM can communicate with using the SCCP or SIP signaling protocols, using a helpful wizard interface that simplifies the process. Figure 2-5 illustrates this integration.

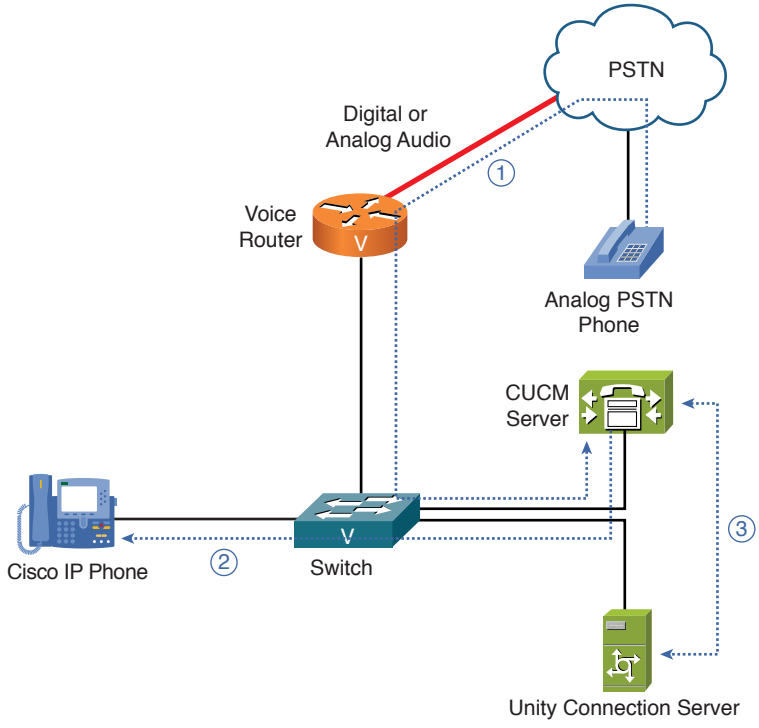


Figure 2-5 *CUCM and Cisco Unity Connection Integration*

Key Topic

Although you can dive into much detail regarding the communication between CUCM and Unity Connection, let's start by breaking down the high-level diagram shown in Figure 2-5:

1. An incoming call from the PSTN arrives at the voice gateway. The voice gateway routes the incoming call to the CUCM server.
2. CUCM receives the call and directs it to the appropriate IP phone (signaling using SCCP or SIP). If someone does not answer the IP phone or diverts the call to voicemail, CUCM forwards the call to the preconfigured voicemail pilot number that rings the Unity Connection server.
3. CUCM transfers the call (once again using SCCP or SIP) to the Unity Connection server. The extension of the originally called phone is contained in the signaling messages, which allows Unity Connection to send the call to the correct voicemail box.

After the caller leaves a message on the voicemail server, Cisco Unity Connection signals (via SCCP or SIP) CUCM to light the voicemail indicator on the Cisco IP phone, alerting the user that he has a voice message waiting. All this interaction between CUCM and Unity Connection is done using voicemail ports, which are licensed features. The more voicemail port licenses you purchase for the Unity Connection server, the more concurrent communication it supports. You should consider calls to the auto-attendant, checking voicemail, leaving voicemail, message notification, and message waiting indicator (MWI) communication in calculating the number of required voicemail ports.

Note Cisco Unity Connection can fully integrate and support CME deployments. Many organizations use a centralized Unity Connection voicemail cluster to support several CME-based remote offices.

Understanding Cisco Unified CM IM and Presence

Cisco Unified Communications Manager Instant Messaging and Presence (IMP) enhances the utility of integrated VoIP and data networks. Many people use IM clients to communicate in their personal lives; it's convenient, simple, effective, and fun. With applications such as Google Hangouts, Skype, Windows Live Messenger, and Facebook Messenger, you are able to see the status of a buddy (available, busy, offline, and so on) and decide whether now is a good time to chat with them. People love using these chat tools so much that they naturally want to use them for work, too. However, in business environments, the use of these apps is often restricted because of security concerns or regulatory compliance requirements.

It is usually a smart idea to give people the tools they want and need to do the job, instead of trying to lock things down harder and aggravate the users. The trick is to find a way to meet the needs of the users while still ensuring that the security and legal obligations of the company are protected. This is where IMP comes in: The server software, in conjunction with a variety of IM clients (the one we are most interested in is of course Cisco Jabber), gives people secure IM with full presence status indication allowing you to see the status of users (are they on the phone, off the phone, not available, in a meeting and so on) before you pick up the phone to dial or IM chat them. In addition to this core functionality, IMP adds the following capabilities to your voice network:

- **Enterprise instant messaging:** Unified Presence incorporates the Jabber Extensible Communication Platform (XCP), which is an industry-standard method of communicating between different IM clients.
- **Message compliance:** Many industries must follow strict compliance regulations for instant message communications. Cisco Presence supports logging functionality for all types of IM communication (even conversations encrypted with Transport Layer Security [TLS]).
- **Interdomain federation:** Using interdomain federation connections from Unified Presence, you can connect your organization to other domains, such as Google Talk or WebEx Connect, thus giving you worldwide reach, even to the extent of allowing customers to immediately and directly connect to their support contact internally.

- **Jabber XCP extensibility:** XCP allows you to extend Unified Presence into nearly any area of the data or voice network. XCP can allow features such as peer-to-peer file sharing, application sharing, video-conference systems, and so on. XCP integrates with nearly any infrastructure, such as directory services, databases, and web portals.
- **Secure messaging:** Applications integrating into Unified Presence can use IPsec or TLS standards to encrypt and secure all communication.

IMP can operate in Unified Communications mode, which is integrated with CUCM and supports up to 45,000 users, or in IM-Only mode, which sets up IMP as a standalone app without an integrated CUCM and supports up to 75,000 users. A third mode, Microsoft Lync Interoperability mode, provides integration with users of Microsoft Office Communicator and CUCM for up to 40,000 users. The user counts listed here are not "hard" limits; they are just the limit of user counts Cisco has validated and recommends.

Cisco Jabber

You will hardly find any documentation available about IMP without seeing a mention of Cisco Jabber. Once you understand the purpose of Jabber, you'll understand why. This single software application brings together several frequently used services in a single location: soft phone, presence, instant messaging, visual voicemail, employee directory, communication history, video, and web conferencing. When you initially see Jabber, it looks like another IM client (The Windows and OS X versions are shown in Figure 2-6); under the hood, it's much more.

Figure 2-6 *Cisco Jabber*

At its core, Jabber serves as an IM client, supporting peer-to-peer chat, multiuser chat, and persistent chat. Persistent chat uses the idea of "rooms," which allow users to join existing chat sessions and see the conversation history (rather than simply the new messages appearing after they have joined). Jabber uses LDAP for user searches and to add contacts. Because Jabber connects to the IMP server which in turn connects to the CUCM, you are able to see not only the status of a user as it relates to IM conversations, but you can also see the status of their phone (off hook, on hook, and so on).

From Jabber, you can start both voice and video calls with video resolutions up to high definition (HD) quality. Jabber can act as a full softphone, allowing audio and video calls from other audio (and video-capable) devices (IP phones, softphones, and so on) in the network, or it can control your desk phone remotely instead. Jabber also gives you visual voicemail (a feature that makes checking and retrieving voicemail very easy).

Perhaps the most exciting feature of Jabber is that it is available on every platform your users are likely to use: Windows, OS X, iOS, Android, and BlackBerry. Some of those platforms do not support the full feature set yet, but that does not detract from its astonishing capabilities and usefulness.

Understanding Video Communication Server and TelePresence Management Suite

Video calling is an increasingly important component of business communications. For the purposes of CICD, we can organize video calls into three categories:

- **Internal desktop calls:** These are calls placed between video-capable endpoints such as 9971 phones with attached video cameras or Jabber clients with integrated webcam video. The key distinction here is that the endpoints involved with the video call are registered to the CM cluster.
- **TelePresence calls:** Calls placed using specialized TelePresence endpoints (whether full-scale TelePresence suites or desktop TelePresence terminals). TelePresence deserves its own category, not only because of the specialized equipment involved, but also because it can be quite independent of the CM cluster in managing its own call control.
- **External video calls:** These are calls connecting external video endpoints that do not register to the CM cluster (such as business-to-business partners or customers) to internal video endpoints that are registered to the CM cluster. These calls must traverse the corporate firewall in order to connect to internal endpoints on the corporate LAN.

Cisco VCS Control and VCS Expressway

One of the goals implicit in Cisco's video strategy is to facilitate "video everywhere." The first category of video calls noted above is easy: The CM cluster is perfectly capable of handling the call control for its own registered video-capable endpoints. TelePresence calls, in much the same way, are typically managed by the Video Communication Server (VCS) and TelePresence Management Suite, which we discuss later in this section. But if we are to include all the categories of video calling listed earlier, we need to address the more complicated scenario: How we can incorporate video endpoints that we do not own and do not control—the ones that belong to our partners and customers? How do we allow a customer or a business partner to use their video endpoint to call one of ours—and how do we do that on demand and still make it simple and secure?

The Cisco Video Communications Server (VCS) is the solution to this rather tricky problem. The VCS can be deployed in two ways:

- VCS Control is a self-contained video endpoint call control system. This deployment is intended for customers who do not have a CM cluster but who have video endpoints and want to easily make calls to other video endpoints, including those that are registered to another organization's CM cluster. The call signaling is sent via a SIP trunk to the CM clusters they need to connect to.
- For on-demand scenarios where the caller endpoint does not have a VCS Control server (and may not even have a video endpoint), you can deploy VCS Expressway. This is a solution that allows the caller to signal our CM cluster that they want to set up a video call to one of our CM-registered internal endpoints. Firewall traversal is handled by two VCS Expressway servers, one called Expressway Core and the other Expressway Edge. The Edge server lives in the demilitarized zone (DMZ) outside the firewall and has a trusted relationship with the VCS Core server inside the firewall. This setup allows outside-to-inside on demand call setup while preserving firewall integrity and security.

  One of the really cool things that VCS Expressway Core/Edge setup allows is the deployment of Jabber Guest. This application (which has multiple caller platform capabilities) allows callers to click a website link and establish a video call on demand, even if they do not have a video endpoint or soft client installed. This scenario is ideal for customer support environments.

TelePresence Management Suite

Cisco TelePresence is a powerful, complex, and valuable system—and if we are being honest, it can be pretty expensive. But the benefits of using virtual meetings with HD video resolution and multichannel audio are very real, and customers quickly realize not only the "coolness factor" benefit but also actual and significant dollar-cost and time savings.

If you have a TelePresence capability, one of the challenges you must quickly deal with is the fact that pretty soon everybody wants to use it for meetings and collaboration. That's what you want, of course—to make the most of your investment. But it has to be managed, and that is what Cisco TelePresence Management Suite (TMS) does.

For administrators, TMS provides the following:

- Provisioning tools to simplify the rapid deployment thousands of TelePresence users and endpoints across multiple locations within an organization
- Centralized administration of all TelePresence infrastructure resources
- Real-time management of all conferences
- Comprehensive phone book synchronization with a variety of concurrent sources
- Built-in ready-to-use reports, in addition to support for customized reporting on TelePresence resource utilization

For users, TMS provides the following:

- Ease of scheduling, including integration with Exchange/Outlook scheduling and single-button or single-click to initiate a TelePresence call
- Ease of use for contacts and phone books from multiple sources

Exam Preparation Tasks

Review All the Key Topics

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

Table 2-4 Key Topics for Chapter 2

Key Topic Element	Description	Page Number
Text	CME interaction with IP phones; functions of SCCP and SIP	35
List	Key features of CUCM	37
Text	Understanding the CUCM Publisher and Subscriber roles and relationships	39
Note	Understanding the difference between a primary CUCM server and the Publisher server	41
Note	CUC Maximum mailbox count whether standalone or Active-Active server par	42
List	Method used to route incoming calls to Cisco Unity Connection server from CUCM	43

Complete the Tables from Memory

Table 2-5 is a study aid we call a "memory table." Print a copy of Appendix D, "Memory Tables" (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Table 2-5 Memory Table for Chapter 2

Product	Capacity (Phones, Users, Mailboxes, and So On)	Platform
CME	Max 450 phones	Runs on ISR router
CUCM	Max 40,000 phones per cluster	Runs on UCS/VMware appliance platform
IMP	Max 45,000 users with CUCM cluster integration	Runs on UCS/VMware appliance
CUC	Max 20,000 mailboxes	Runs on UCS/VMware appliance

Definitions of Key Terms

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

Cisco Unified Communications Manager (CUCM), Cisco Unified Communications Manager Express (CME), Cisco Unity Connection, Cisco Unified Presence, automatic call distribution (ACD), Skinny Client Control Protocol (SCCP), Session Initiation Protocol (SIP), Real-time Transport Protocol (RTP), Internet telephony service provider (ITSP), digital signal processors (DSP), Cisco Unity Express (CUE), interactive voice response (IVR), CUCM Publisher, CUCM Subscriber, intracluster communication signaling (ICCS), Voice Profile for Internet Mail (VPIM), Cisco Unified Personal Communicator

This chapter covers the following topics:

- **Connecting and Powering Cisco IP Phones:** To provide a centralized power system, Cisco IP phones may receive their power from a centralized source using PoE. This section discusses the different options for PoE and the selection criteria for each.
- **VLAN Concepts and Configuration:** VLANs allow you to segment the switched network into multiple logical pieces to provide management and security boundaries between the voice and data network. This section discusses the concepts and configuration behind VLANs.
- **Understanding Cisco IP Phone Boot Process:** This section discusses the foundations of the Cisco IP phone boot process. Understanding this process is important to troubleshooting issues with the IP telephony system.
- **Configuring a Router-Based DHCP Server:** This section discusses configuring a Cisco router as a DHCP server for your network.
- **Setting the Clock of a Cisco Device with NTP:** Because a VoIP network heavily depends on accurate time, the sole focus of this section is keeping the clocks accurate on Cisco devices by using NTP.
- **IP Phone Registration:** Once the Cisco IP phone receives all its network configuration settings, it is ready to communicate with a call processing agent. This section describes the processes and protocols that make it happen.
- **Quality of Service:** VoIP traffic must be prioritized and protected; if voice packets are lost or excessively delayed in transit through the network, the audio quality of the calls degrades quickly and seriously. This section describes how QoS configurations on network routers and switches provide the guarantees of bandwidth and delay that voice traffic needs to sound good.

CHAPTER 3

Understanding Cisco IP Phones

You walk into a brand new corporate headquarters building. On each desk sits a Cisco 9971 IP phone with a full-color display, two line instances, and a built-in camera. The employees are busy taking phone calls; Jaime is checking her visual voicemail while Jaden is booking a TelePresence room and Jaine is on a video call with Tom.

How did we get here? How do you take a newly constructed building and transform it into a functional unified communications system? That is what this chapter is all about: We walk through the key concepts and technologies used to build a Cisco Voice over IP (VoIP) network. By the time you are done with this chapter, you will have all the conceptual knowledge you need to have in place before you can move into the installation and configuration of the Cisco VoIP system.

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

Foundation Topics Section	Questions Covered in This Section
Connecting and Powering Cisco IP Phones	1–2
VLAN Concepts and Configuration	3–8
Understanding Cisco IP Phone Boot Process	9
Configuring a Router-Based DHCP Server	10
Setting the Clock of a Cisco Device with NTP	11
IP Phone Registration	12
Quality of Service	13

1. Which of the following is an industry standard used for powering devices using an Ethernet cable?

   a. Cisco inline power

   b. 802.1Q

   c. 802.3af

   d. Local power brick

2. Which of the following are valid methods for powering a Cisco IP phone? (Select all that apply.)
   a. Power brick
   b. Crossover coupler
   c. PoE
   d. Using pins 1, 2, 3, and 4
3. Which of the following terms are associated with a VLAN? (Choose two.)
   a. IP subnet
   b. Port security
   c. Broadcast domain
   d. Collision domain
4. Which of the following trunking protocols would be used to connect a Cisco switch to a non-Cisco switch device?
   a. VTP
   b. 802.3af
   c. 802.1Q
   d. ISL
5. How should you configure a Cisco Catalyst switch port supporting voice and data VLANs that is connected to a Cisco IP phone?
   a. Multi-VLAN access
   b. Trunk
   c. Dynamic
   d. Dynamic desired
6. How does a device attached to a Cisco IP phone send data to the switch?
   a. As tagged (using the voice VLAN)
   b. As untagged
   c. As tagged (using the data VLAN)
   d. As tagged (using the CoS value)
7. Which of the following commands should you use to configure a port for a voice VLAN 12?
   a. **switchport mode voice vlan 12**
   b. **switchport trunk voice vlan 12**
   c. **switchport voice vlan 12**
   d. **switchport vlan 12 voice**

8. Which of the following commands would you use to forward DHCP requests from an interface connected to the 172.16.1.0/24 subnet to a DHCP server with the IP address 172.16.100.100?

   a. **forward-protocol 172.16.1.0 255.255.255.0 172.16.100.100**
   b. **forward-protocol dhcp 172.16.1.0 255.255.255.0 172.16.100.100**
   c. **ip helper-address 172.16.1.0 172.16.100.100**
   d. **ip helper-address 172.16.100.100**

9. How does the Cisco switch communicate voice VLAN information after a Cisco IP phone has received PoE and started the boot process?

   a. Through CDP
   b. Using 802.1Q
   c. Using the proprietary ISL protocol
   d. Voice VLAN information must be statically entered on the Cisco IP phone.

10. Which DHCP option provides the IP address of a TFTP server to a Cisco IP phone?

    a. Option 10
    b. Option 15
    c. Option 150
    d. Option 290

11. Which of the following NTP stratum numbers would be considered the best?

    a. Stratum 0
    b. Stratum 1
    c. Stratum 2
    d. Stratum 3

12. Which of the following protocols could be used for Cisco IP phone registration? (Choose two.)

    a. SCCP
    b. SIP
    c. DHCP
    d. H.323

13. Which of the following is not an area you can use QoS to manage?

    a. Packet jitter
    b. Variable delay
    c. Fixed delay
    d. Router queuing

Foundation Topics

Connecting and Powering Cisco IP Phones

Before we can get to the point of plugging in phones and having users placing and receiving calls, we must first lay the foundational infrastructure of the network. This includes technologies such as Power over Ethernet (PoE), voice VLANs, and Dynamic Host Configuration Protocol (DHCP). The network diagram shown in Figure 3-1 represents the placement of these technologies. As you read this chapter, each section will act as a building block to reach this goal. The first item that we examine is power for the Cisco IP phones.

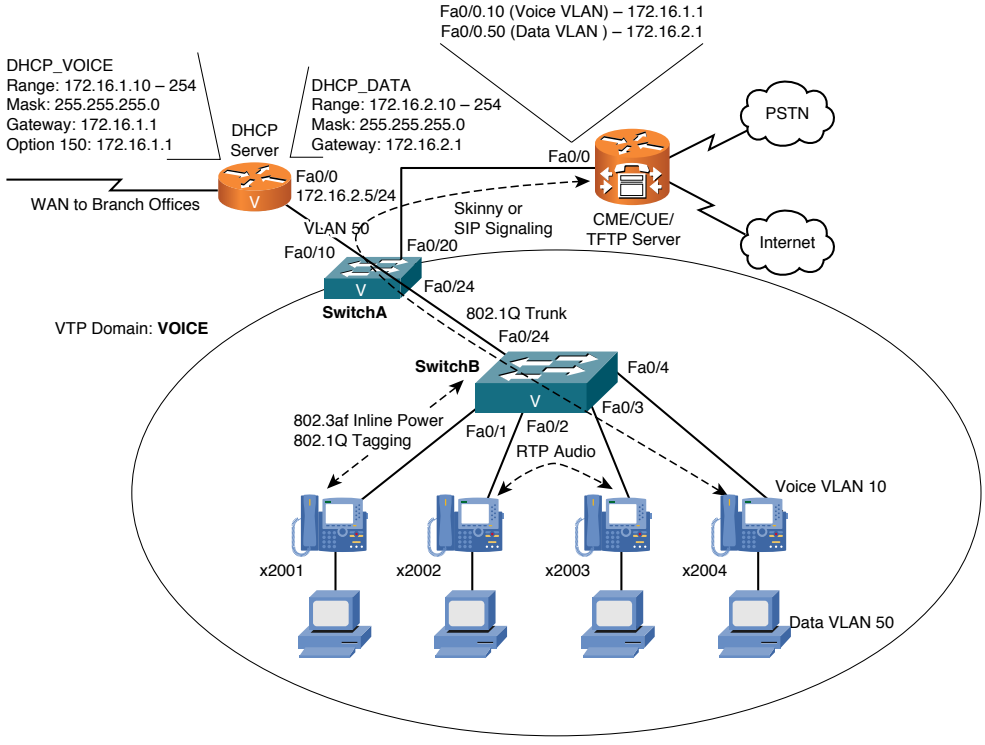


Figure 3-1 *VoIP Network*

Cisco IP phones connect to switches just like any other network device (such as PCs, IP-based printers, and so on). Depending on the model of IP phone you are using, it may also have an extra port which is used to connect the PC to the network through the phone. Figure 3-2 illustrates the connections on the back of a Cisco 7960 IP phone; newer phones are similar.

The ports shown in Figure 3-2 are as follows:

- **RS232 (or AUX):** Connects to a expansion module (such as a 7915, 7916, or Color Key Expansion Module)
- **10/100 SW:** Used to connect the IP phone to the network
- **10/100 PC:** Used to connect a co-located PC (or other network device) to the IP phone

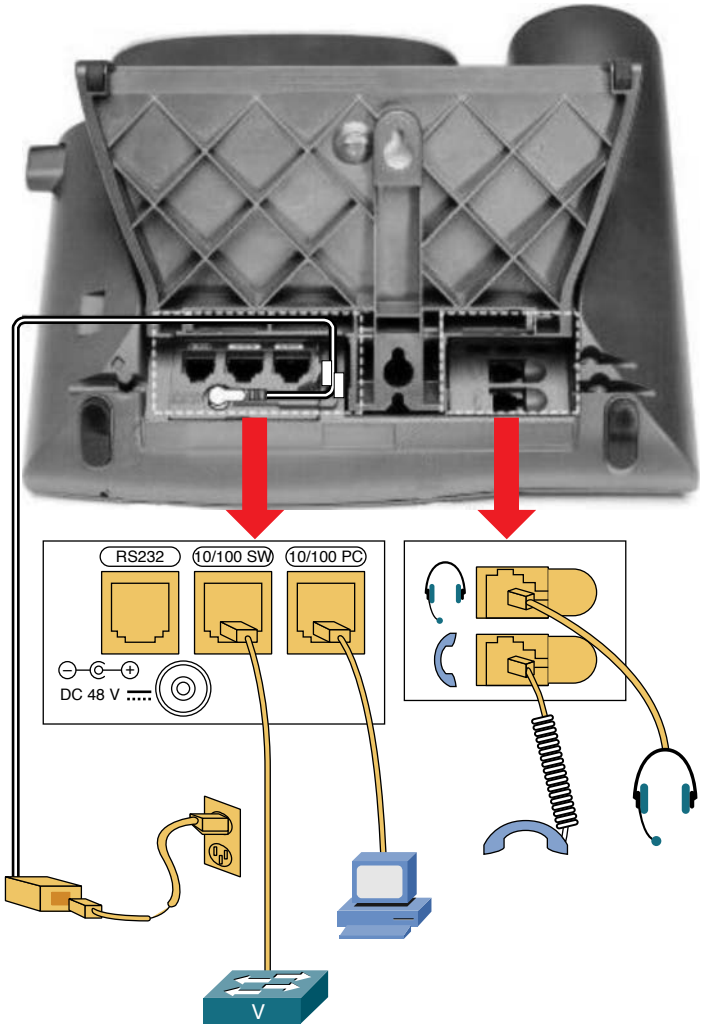


Figure 3-2 *Cisco IP Phone Ethernet Connections*

After you physically connect the IP phone to the network, it needs to receive power in some way. There are four potential sources of power in a Cisco VoIP network:

- Cisco Catalyst switch PoE (or third-party PoE switch)
- Power patch panel PoE
- Mid-span power injector
- Cisco IP phone power brick (wall power)

Let's dig deeper into each one of these power sources.

Cisco Catalyst Switch PoE

The terms *inline power* and *PoE* refer to the capability to send electricity over an Ethernet cable to power a connected device. There is a wide variety of devices that can attach to a PoE connection and receive all the power they need to operate. In addition to Cisco IP phones, other common PoE devices include wireless access points, paging speakers, and video surveillance equipment.

Powering devices through an Ethernet cable offers many advantages over using a local power supply. First, you have a centralized point of power distribution. Many users expect the phone system to continue to work even if the power is out in the company offices. By using PoE, you can connect the switch powering the IP phones to an uninterruptible power supply (UPS) instead of placing a UPS at the location of each IP phone. PoE also enables you to power devices that are not conveniently located next to a power outlet. For example, it is a common practice to mount wireless access points in the ceiling, where power is not easily accessible. Finally, PoE eliminates much of the "cord clutter" at employees' desks.

Third-party switches from vendors other than Cisco will deliver PoE and power Cisco IP phones, but they may not support Cisco proprietary configurations and capabilities that make management, quality of service (QoS), and traffic control easier and more powerful.

PoE became an official standard (802.3af) in 2003. However, the IP telephony industry was rapidly evolving before this. To power the IP phones without an official PoE standard, some proprietary methods were created, one such method being Cisco inline power.

Note The IEEE standards body has created the 802.3at PoE standard (also called PoE Plus), the goal of which is to increase the current maximum PoE wattage from 15.4W to 25.5W. In addition, some proprietary implementations of PoE have reached 51W of power by using all four pairs of wire in the Ethernet cable.

Powering the IP Phone Using a Power Patch Panel or Coupler

Many companies already have a significant investment in their switched network. To upgrade all switches to support PoE would be a significant expense. These organizations may choose to install intermediary devices, such as a patch panel, that are able to inject PoE on the line. The physical layout for this design is demonstrated in Figure 3-3.

By using the powered patch panel, you still gain the advantage of centralized power and backup without requiring switch upgrades.

Note Keep in mind that Cisco switches must also provide QoS and voice VLAN support capabilities, which may require switch hardware upgrades. Be sure that your switch supports these features before you consider a power patch panel solution.

Inline PoE injectors provide a low-cost PoE solution for single devices (one device per injector). These are typically used to support wireless access points or other "single spot" PoE solutions. Using only inline PoE injectors for a large IP phone network would make a mess

of your wiring infrastructure and exhaust your supply of electrical outlets (because each inline PoE coupler requires a dedicated plug).

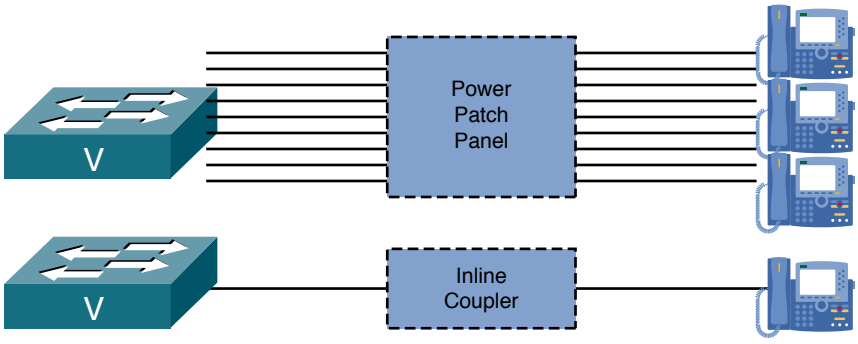


Figure 3-3 *Design for Power Patch Panels or Inline Couplers*

Powering the IP Phone with a Power Brick

Using a power brick to power a device is so simple that it warrants only brief mention. Thus, the reason for this section is primarily to mention that most Cisco IP phones do not ship with power supplies. Cisco assumes most VoIP network deployments use PoE. If you have to choose between purchasing power bricks and upgrading your switch infrastructure, it is wise to check the prices of the power bricks. The average Cisco IP phone power brick price is between $30 and $40. When pricing out a 48-switchport deployment, purchasing power bricks for all the IP phones may very well be in the same price range as upgrading the switch infrastructure.

Note Some devices exceed the power capabilities of the 802.3af or 802.3at PoE standards. For example, when you add a sidecar module to a Cisco IP phone (typically to support more line buttons), PoE connections can no longer support the device. These devices will need a power brick adapter.

VLAN Concepts and Configuration

After the IP phone has received power and booted, it must determine its VLAN assignment. Because of security risks and congestion associated with having data and voice devices on the same network (not to mention making QoS implementation easier), Cisco recommends isolating IP phones in VLANs dedicated to voice devices. To understand how to implement this recommendation, let's first review a few key VLAN concepts.

VLAN Review

Nowadays, it is rare to find any reasonably sized network that is not using VLANs in some way. VLANs allow you to break up switched environments into multiple broadcast domains; a VLAN is therefore defined as a Layer 3 segmentation performed at Layer 2 (by the switch, in other words). Here is the basic summary of a VLAN:

A VLAN = A broadcast domain = An IP subnet

There are many benefits to using VLANs in an organization, some of which include the following:

- **Increased performance:** By reducing the size of the broadcast domain, network devices run more efficiently.
- **Improved manageability:** The division of the network into logical groups of users, applications, or servers allows you to understand and manage the network better.
- **Physical topology independence:** VLANs allow you to group users regardless of their physical location in the campus network. If departments grow or relocate to a new area of the network, you can simply change the VLAN on their new ports without making any physical network changes.
- **Increased security:** A VLAN correlates to a subnet; the VLAN and subnet create and define exactly the same broadcast domain. You should not attempt to have a single subnet in use in multiple VLANs, nor must multiple subnets in a single VLAN; VLANs and subnets must always be deployed one to one. To reach other subnets (VLANs), you must pass through a router (Layer 3) device. Any time you send traffic through a router, you have the opportunity to add filtering options (such as access lists) and other security measures.

VLAN Trunking/Tagging

VLANs are able to transit between multiple individual switches, as shown in Figure 3-4.

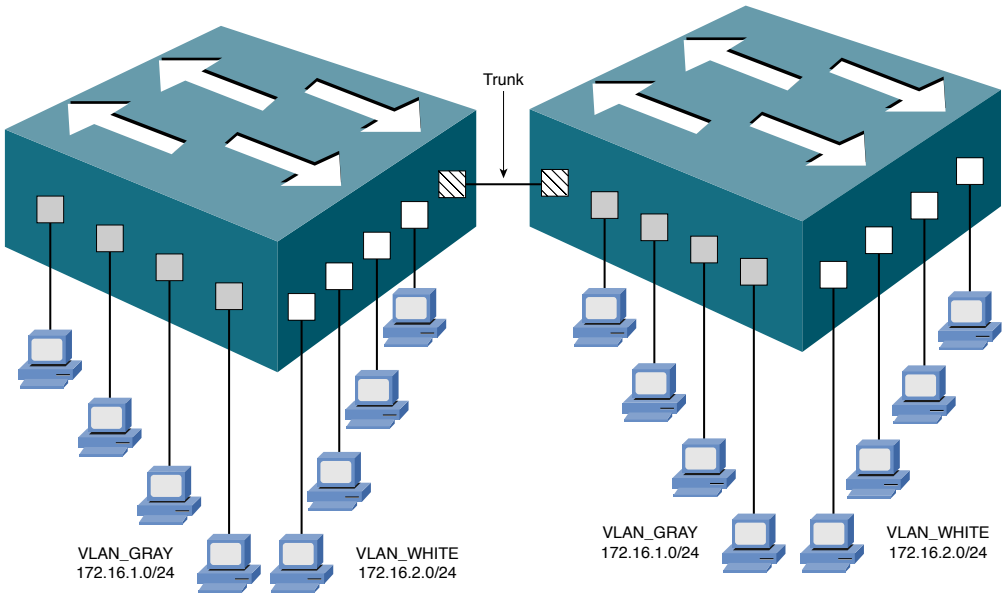


Figure 3-4 *VLANs Move Between Switches*

If a member of VLAN_GRAY sends a broadcast message, it goes to all VLAN_GRAY ports on both switches. The same holds true for VLAN_WHITE. To accommodate this, the connection between the switches must carry traffic for multiple VLANs. This type of port is known as a trunk port.

Trunk ports are often called tagged ports because the switches send frames between each other with a VLAN "tag" in place. Figure 3-5 illustrates the following process:

1. HostA (in VLAN_GRAY) wants to send data to HostD (also in VLAN_GRAY). HostA transmits the data frame to SwitchA.
2. SwitchA receives the frame, updates the MAC table with HostA's MAC and tags the frame with the VLAN number of the GRAY VLAN. Switch A then looks up the destination MAC of the frame and determines that HostD is available through Fast Ethernet 0/24 port (HostD's MAC address has previously been learned on this port). Because Fast Ethernet 0/24 is configured as a trunk port, SwitchA transmits the frame to SwitchB with the VLAN_GRAY tag intact.
3. SwitchB processes the VLAN_GRAY-tagged frame because its Fast Ethernet 0/24 port is also configured as a trunk. As the frame is sent out of the correct port to HostD, the VLAN_GRAY tag is removed from the header.
4. The untagged frame is sent to HostD.

Key Topic

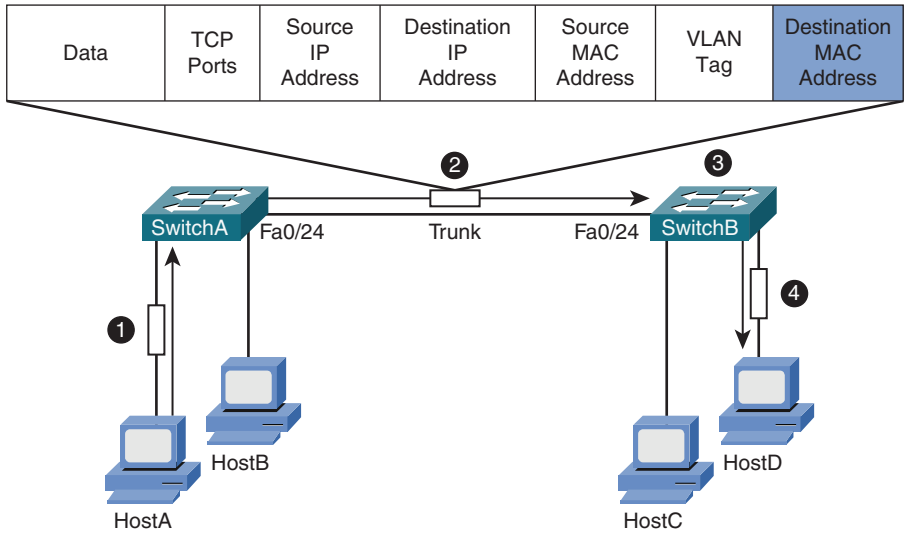


Figure 3-5 *VLAN Tags*

Using this process, the PC never knows what VLAN it belongs to. The VLAN tag is applied by the switch as the frame is processed by the incoming port, and preserved as the frame crosses a trunk link between switches. The VLAN tag is removed when exiting the port to the destination PC. Always keep in mind that VLANs are a switching concept; the PCs never participate in the VLAN tagging process.

Note Some server-class network cards support trunking, which allows you to extend the VLAN tagging into the server so that it can perform different operations based on the source VLAN of the frame. DHCP is one example: multiple source VLANs need IP address assignments in different subnets, so using a trunk connection on a single network interface is one way to simplify DHCP server implementation.

VLANs are not a Cisco-only technology. Just about all managed switch vendors support VLANs. For VLANs to operate in a mixed-vendor environment, a common trunking or "tagging" protocol must exist between them. The protocol in common usage is the IEEE standard 802.1Q. All vendors design their switches to recognize and understand the 802.1Q tag, which is what allows us to trunk between switches in any environment.

Understanding Voice VLANs

Key Topic

It is a common and recommended practice to separate voice and data traffic by using VLANs. There are already easy-to-use applications available, such as Wireshark and Voice Over Misconfigured Internet Telephones (VOMIT), that could allow intruders to capture voice conversations on the network and convert them into WAV data files. Separating voice and data traffic using VLANs provides an additional security layer by preventing data applications from reaching the voice traffic. It also gives you a simpler method to deploy QoS, prioritizing the voice traffic over the data using the VLAN as an identifier.

Note Implementing encrypted audio using Secure Real-Time Protocol (SRTP) will mitigate the security concerns over captured audio. However, there are still plenty of very good reasons to keep the voice traffic in its own designated VLAN.

One initial difficulty you can encounter when separating voice and data traffic is the fact that PCs are often connected to the network using the Ethernet port on the back of a Cisco IP phone. Because you can assign a switchport to only a single VLAN, it initially seems impossible to separate voice and data traffic. That is, until you see that Cisco IP phones support 802.1Q tagging.

The switch built in to Cisco IP phones has much of the same hardware that exists inside of a full Cisco switch. The incoming switchport is able to receive and send 802.1Q tagged packets. This gives you the capability to establish a special type of connection called a *multi-VLAN access port* between the Cisco switch and IP phone, as shown in Figure 3-6.

You might think of the connection between the switch and IP phone a "mini-trunk" because a typical trunk can transmit a large number of VLANs (in fact, by default it's all VLANs). In this case, the IP phone tags its own packets with the correct voice VLAN (VLAN 25, in the case of Figure 3-6). Because the switch receives this traffic on a port supporting tagged packets (our multi-VLAN access port), the switch can read the tag and keep the voice traffic in the correct VLAN. The PC's data packets pass through the IP phone and to the switch untagged. The switch assigns these untagged packets to whatever VLAN you have configured on the switchport for data traffic, at ingress.

Key Topic

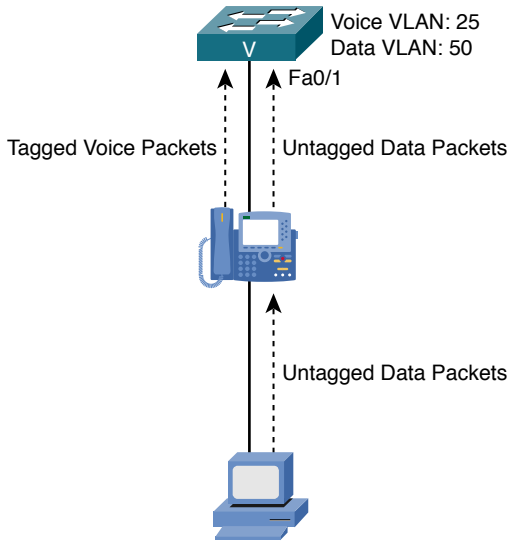


Figure 3-6 *Separating Voice and Data Traffic Using VLANs*

Key Topic

Note Traditionally, a switch port on a Cisco switch that receives tagged packets is referred to as a trunk port. However, when you configure a switch port to connect to a Cisco IP phone, you configure it as an access port (for the untagged data from the PC) while supporting tagged traffic from the IP phone. These ports are called multi-VLAN access ports.

VLAN Configuration

Configuring a Cisco switch to support voice VLANs is a fairly simple process. First, add the VLANs to the switch, as shown in Example 3-1.

Key Topic

Example 3-1 *Adding and Verifying Data and Voice VLANs*

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name VOICE
Switch(config-vlan)# vlan 50
Switch(config-vlan)# name DATA
Switch(config-vlan)# end
Switch# show vlan brief
VLAN     Name                Status      Ports
1        default             active      Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                         Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                         Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                         Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                         /18, Fa0/19, Fa0/20, Fa0/21
                                         /22, Fa0/23, Fa0/24, Gi0/1
                                         /2
```

```
10       VOICE                active
50       DATA                 active
1002     fddi-default         act/unsup
1003     token-ring-default   act/unsup
1004     fddinet-default      act/unsup
1005     trnet-default        act/unsup
```

VLANs 10 (VOICE) and 50 (DATA) now appear as valid VLANs on the switch. Now that the VLANs exist, you can assign the ports connecting to Cisco IP phones (with PCs connected to the IP phone) to the VLANs, as shown in Example 3-2.

Key Topic

Example 3-2 *Assigning Voice and Data VLANs*

```
Switch# configure terminal
Switch(config)# interface range fa0/2 - 24
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# spanning-tree portfast
Switch(config-if-range)# switchport access vlan 50
Switch(config-if-range)# switchport voice vlan 10
Switch(config-if-range)# end
Switch# show vlan brief
VLAN     Name                 Status    Ports
1     default                 active     Gi0/1, Gi0/2
10     VOICE                  active     Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                         Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                         Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                         Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                         Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                         /22, Fa0/23, Fa0/24
50     DATA                   active     Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                         Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                         /10, Fa0/11, Fa0/12, Fa0/13
                                         /14, Fa0/15, Fa0/16, Fa0/17
                                         /18, Fa0/19, Fa0/20, Fa0/21
                                         Fa0/22, Fa0/23, Fa0/24
1002     fddi-default           act/unsup
1003     token-ring-default     act/unsup
1004     fddinet-default        act/unsup
1005     trnet-default          act/unsup
```

Note When connecting Cisco IP phones to a switch, you should also enable PortFast (using spanning-tree portfast, as shown in Example 3-2) because the IP phones boot quickly and request a DHCP-assigned address before a typical port with spanning-tree enabled would go active. Also, keep in mind that port Fa0/1 does not appear in the Example 3-2 output because it is configured as a trunk port. (Ports 2–24 are not considered trunks by Cisco IOS.)

The ports are now configured to support a voice VLAN of 10 and a data VLAN of 50. This syntax is a newer form of configuration for IP phone connections. In the "old days," you would configure the interface as a trunk port because the switch was establishing a trunking relationship between it and the IP phone. This was less secure because hackers could remove the IP phone from the switch port and attach their own device (another managed switch or PC) and perform a VLAN-hopping attack. The more modern syntax configures the port as a "multi-VLAN access port" because an attached PC will be able to access only VLAN 50. Only an attached Cisco IP phone can access the voice VLAN 10.

Note Keep in mind that Cisco IP phones receive the voice VLAN configuration from the switch via Cisco Discovery Protocol (CDP). After it receives the voice VLAN number, the IP phone begins tagging its own packets. Non-Cisco IP phones cannot understand CDP packets. This typically requires you to manually configure each of the non-Cisco IP phones with its voice VLAN number from a local phone configuration window (on the IP phone).

Understanding the Cisco IP Phone Boot Process

Now that you know about the VLAN architecture used with Cisco IP phones, we can turn our attention to the IP phones themselves. By understanding the IP phone boot process, you can more fully understand how the Cisco IP phone operates (which aids significantly in troubleshooting Cisco IP phone issues). Here is the Cisco IP phone boot process, start to finish:

1. The Cisco IP phone connects to an Ethernet switch port. If the IP phone and switch support PoE, the IP phone receives power via PoE.
2. As the Cisco IP phone powers on, the Cisco switch delivers voice VLAN information to the IP phone using CDP. The Cisco IP phone now knows what VLAN it should use for its voice traffic.
3. The Cisco IP phone broadcasts a DHCP request (which is constrained within the voice VLAN) asking for an IP address on its voice VLAN.
4. The DHCP server responds with an IP address offer. When the Cisco IP phone accepts the offer, it receives all the DHCP options that go along with the DHCP request. DHCP options include items such as default gateway, DNS server information, domain name information, and so on. In the case of Cisco IP phones, a specific DHCP option is required, known as Option 150. This option directs the IP phone to a TFTP server. (You learn more about this in the upcoming section, "Configuring a Router-Based DHCP Server.")
5. After the Cisco IP phone has the IP address of the TFTP server, it contacts the TFTP server and downloads its configuration file. Included in the configuration file is a list of valid call processing agents (such as Cisco Unified Communications Manager or Cisco Unified Communications Manager Express).
6. The Cisco IP phone attempts to contact the first call processing server (the primary server) listed in its configuration file to register. If this fails, the IP phone moves to the next server in the configuration file. This process continues until the IP phone registers successfully or the list of call processing agents is exhausted.

Configuring a Router-Based DHCP Server

We have so far made it to Step 4 in the preceding IP phone boot process. The phones in our network now need to receive IP address and TFTP server information. In the network design scenario used in this chapter, we use the WAN branch router as the DHCP server. Using a router as a DHCP server is a common practice in smaller networks. Once you move into larger organizations, DHCP services are typically centralized onto server platforms. Either DHCP option is capable of sending TFTP server (Option150) information to the IP phones.

Example 3-3 shows the syntax used to configure a WAN branch router as a DHCP server.

Example 3-3 *Configuring Router-Based DHCP Services*

```
WAN_RTR# configure terminal
WAN_RTR(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.9
WAN_RTR(config)# ip dhcp excluded-address 172.16.2.1 172.16.2.9
WAN_RTR(config)# ip dhcp pool DATA_SCOPE
WAN_RTR(dhcp-config)# network 172.16.2.0 255.255.255.0
WAN_RTR(dhcp-config)# default-router 172.16.2.1
WAN_RTR(dhcp-config)# dns-server 4.2.2.2
WAN_RTR(dhcp-config)# exit
WAN_RTR(config)# ip dhcp pool VOICE_SCOPE
WAN_RTR(dhcp-config)# network 172.16.1.0 255.255.255.0
WAN_RTR(dhcp-config)# default-router 172.16.1.1
WAN_RTR(dhcp-config)# option 150 ip 172.16.1.1
WAN_RTR(dhcp-config)# dns-server 4.2.2.2
```

Note This example uses a Cisco router as a DHCP server. Using a router as a DHCP server is simple and stable and makes sense if there is already a router in place that could perform DHCP in addition to its routine jobs. That said, most larger organizations use a Windows server or some other centralized device for DHCP services. Even Cisco Unified Communications Manager includes DHCP server capabilities. In these cases, you typically need to configure an **ip helper-address** <*central DHCP server IP address*> on the router to forward DHCP requests to the central DHCP server for the voice VLAN devices.

The way in which Cisco routers approach DHCP configurations differs slightly from most other DHCP servers. Most DHCP servers allow you to specify a range of IP addresses that you would like to hand out to clients. Cisco routers take the opposite approach: You first specify a range of addresses that you do not want to hand out to clients (using the **ip dhcp excluded-address** syntax from global configuration mode). Configuring the excluded addresses before you configure the DHCP pools ensures that the Cisco router does not accidentally hand out IP addresses before you have a chance to exclude them from the range. The DHCP service on the router will begin handing out IP addresses from the first nonexcluded IP address in the network range. In Example 3-3, this is 172.16.1.10 for the voice scope and 172.16.2.10 for the data scope.

Key Topic

The VOICE_SCOPE DHCP pool includes the option 150 syntax. This creates the custom TFTP server option to be handed out to the Cisco IP phones along with their IP address information. In this case, the TFTP server of the IP phones is the same as the default gateway because in this example the CME router is the call processing agent. As mentioned in the section "Understanding the Cisco IP phone Boot Process," the TFTP server holds the configuration files for the phones. When you configure a Cisco IP phone in Cisco Unified Communications Manager (CUCM) or CME, an XML configuration file is generated and stored on a TFTP server. These XML configuration files have a filename format of SEP<IP Phone MAC Address>.cnf.xml and contain a base configuration for the IP phone (specifying language settings, URLs, and so on). Most importantly, these XML files contain a list of up to three CUCM server or CME IP addresses the Cisco IP phone uses for registration. After the IP phone receives the XML file, it attempts to register with the first CUCM or CME server listed in the file. If it is unable to reach that server, it moves down to the next until the list is exhausted (at which point the IP phone reboots and tries it all over again).

Note If the Cisco IP phone has not yet been configured in CUCM or CME (no SEP<MAC>.cnf.xml file exists on the TFTP server), the IP phone requests a file named XMLDefault.cnf.xml. This is a base configuration file typically used for a feature called Auto-Registration (allowing phones to register without being configured).

Tip Many people often wonder the meaning of SEP at the beginning of the configuration filename. SEP stands for Selsius Ethernet Phone. Selsius was the name of the company Cisco acquired when they first began manufacturing VoIP technology.

Setting the Clock of a Cisco Device with NTP

The next task to prepare the network infrastructure to support a Cisco VoIP network is to set the time. Having an accurate time on Cisco devices is critical for several reasons. Here is a quick list of just some of the reasons why you want an accurate clock on your network devices:

- It allows Cisco IP phones to display the correct date and time to your users.
- It assigns the correct date and time to voicemail tags.
- It gives accurate times on call detail records (CDRs), which are used to track calls on the network.
- It plays an integral part in multiple security features on all Cisco devices.
- It tags logged messages on routers and switches with accurate time information.

When Cisco routers and switches boot, many of them default their date and time to noon on March 1, 1993. You have two options in setting the clock: manually, using the clock set command from the privileged EXEC mode, or automatically, using the Network Time Protocol (NTP).

Devices setting the clock using NTP always have a more accurate time clock than a manually set clock. Likewise, all the NTP-enabled devices on your network will have the exact same time. These advantages make NTP the preferred clock-setting method. The accuracy of the clock on your device depends on the stratum number of the NTP server. A stratum 1 time server is one that has a GPS clock or atomic clock directly attached. The device that receives its time from this server via NTP is considered a stratum 2 device. The device that receives its time from this stratum 2 device via NTP is considered a stratum 3 device, and so on. There are many publicly accessible stratum 2 and 3 (and even some stratum 1) devices on the Internet.

Note You can obtain a list of publicly accessible NTP servers at http://www.ntp.org.

After you obtain one or more NTP servers to use, you can configure NTP support on your Cisco devices by using the syntax in Example 3-4.

Example 3-4 *Configuring a Cisco Router to Receive Time via NTP*

```
WAN_RTR# configure terminal
WAN_RTR(config)# ntp server 64.209.210.20
WAN_RTR(config)# clock timezone ARIZONA -7
```

The first command, **ntp server** <*ip address*>, configures your Cisco device to use the specified NTP server; 64.209.210.20 is one of many publicly accessible NTP servers. If this is the only command you enter, your clock on your device will set itself to the universal time coordinated (UTC) time zone. To accurately adjust the time zone for your device, use the **clock timezone** <*name*> <*hours*> command. The previous syntax example set the time zone for Arizona to –7 hours from UTC.

Now that we configured the router to synchronize with an NTP server, we can verify the NTP associations and the current time and date using the commands shown in Example 3-5.

Example 3-5 *Verifying NTP Configurations*

```
WAN_RTR# show ntp associations
address            ref clock         st  when   poll  reach  delay    offset    disp
*~64.209.210.20    138.23.180.126    3    14    64    377    65.5     2.84      7.6
  * master (synced), # master (unsynced), + selected, - candidate, ~ configured
WAN_RTR# show clock
11:25:48.542 CA1_DST Mon Dec 13 2010
```

The key information from the **show ntp associations** command is just to the left of the configured NTP server address. The asterisk indicates that your Cisco device has synchronized with this server. You can configure multiple NTP sources for redundancy, but the Cisco device will only choose one master NTP server to use at a time.

After you configure the Cisco router to synchronize with an NTP server, you can configure it to provide date and time information to a CUCM server, which can then provide that date and time information to the Cisco IP phones in your network. To allow other devices (such

as a CUCM server) to pull date and time information from a Cisco router using NTP, use the **ntp master** <*stratum number*> command from global configuration mode. For example, entering **ntp master 4** instructs the Cisco router to deliver date and time information to requesting clients, marking it with a stratum number of 4.

Note Example 3-4 illustrates configuring a Cisco router to support NTP. This is necessary if you are supporting a Cisco IP Telephony network using Communication Manager Express (CME). If you were using a full CUCM solution, you'd also configure NTP on the CUCM server, typically pointing the CUCM to the router for NTP.

IP Phone Registration

Now that the Cisco IP phone has gone through the complete process, it is ready to register with the call-management system (CME or CUCM). Before we discuss this final step, keep in mind what the phone has gone through up to this point:

1. The phone has received Power over Ethernet (PoE) from the switch.
2. The phone has received VLAN information from switch via CDP.
3. The phone has received IP information from the DHCP server (including Option 150).
4. The phone has downloaded its configuration file from the TFTP server.

The Cisco IP phone is now looking at a list of up to three call processing servers (depending on how many you have configured) that it found in the configuration file it retrieved from the TFTP server. The phone tries to register with the first call processing server. If that fails, it continues down the list it received from the TFTP server until the phone makes it through all the listed call processing servers (at which point it reboots if it finds no servers online).

If the IP phone finds an active server in the list, it goes through the registration process using either the Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP). The protocol the phone uses depends on the firmware it is using. A Cisco IP phone might use either protocol depending on the model; some use only SCCP, some can use either, and some only SIP. As the SIP protocol matures, widespread support for it continues to grow. Because SIP is an industry standard, using it across your network provides benefits such as vendor neutrality and inter-vendor operation.

Note The SIP standard is moving so quickly, by the time you read this, SCCP may not be the most popular protocol for Cisco IP Telephony networks. SCCP will most likely be phased out over several years.

Regardless of the protocol used, the registration process is simple: The Cisco IP phone contacts the call processing server and identifies itself by its MAC address. The call processing server looks at its database and sends the operating configuration to the phone. The operating configuration is different than the settings found in the configuration XML file located on the TFTP server. The TFTP server configuration is "base level settings," including items such as device language, firmware version, call processing server IP addresses, port numbers, and so on. The operating configuration contains items such as directory/line numbers, ring tones and

softkey layout (on-screen buttons). Although the TFTP server configuration is sent using the TFTP protocol, the operating configuration is sent using SCCP. A SIP phone gets everything from the TFTP config file download.

The signaling protocol (SIP or SCCP) is then used for the majority of the phone functionality following registration. For example, as soon as a user picks up the handset of the phone, it sends a SCCP or SIP message to the call processing server indicating an off-hook condition. The server quickly replies with a SCCP or SIP message to play dial tone and collect digits. As the user dials, digits are transmitted to the call processing server using SCCP or SIP; call progress tones, such as ringback or busy, are delivered from the call processing server to the phone using SCCP or SIP. Hopefully, you get the idea: The Cisco IP phone and call processing server have a dumb terminal and mainframe style of relationship, and the signaling communication between them is either SCCP or SIP.

Quality of Service

Quality of service (QoS) is a topic that is referenced in nearly every chapter of this book. For a VoIP network to operate successfully, the voice traffic must have priority over the data traffic as it traverses its way from one end of the network to the other. The Cisco definition of QoS is as follows:

> Quality of service is the ability of the network to provide better or special service to a set of users and applications at the expense of other users and applications.

That sounds exactly like what the voice traffic needs as it crosses the network: better or "special" service than the typical data traffic, such as web browsing, FTP transfers, e-mail traffic, and so on. The voice traffic needs this not so much because of bandwidth requirements (VoIP uses very little bandwidth compared to most data applications), but rather delay requirements. Unlike data, the time it takes a voice packet to get from one end of the network to the other is critical. If a data packet crossing the network experiences delay, a file transfer might take a couple more seconds to complete or a web page might take a half second longer to load. From a user's perspective, this is not a big deal. However, if voice traffic crossing the network experiences delay, conversations begin to overlap (a person begins speaking at the same time as another person); the conversation breaks up; and, in some extreme cases, the voice call drops. The key here is that we hear the network problems in real-time as it messes up our phone conversation; people notice, and it is unacceptable because we are used to speech sounding like speech.

To combat these issues, you need to ensure not only that there is bandwidth available for VoIP traffic, but that the VoIP traffic gets the first bandwidth available. This means if a bottleneck occurs in the network and a router has to queue traffic before it is sent, the router will move the waiting voice traffic ahead of the data traffic and give transmit priority to the voice packets. Accomplishing this is the job of QoS. QoS is not a tool in itself, but rather, a category of many tools aimed at giving you complete control over the traffic crossing your network. There might be times when you just use a single QoS tool aimed at decreasing the delay of traffic. Other times, you might employ multiple QoS tools to control delay, reserve bandwidth, and compress data that is heading over the WAN. How and when you use each of the QoS tools depends on the network requirements of your traffic and the characteristics (such as bandwidth, delay, and so on) of the network supporting the traffic.

Understanding the Enemy

Before you can deploy QoS successfully, you need to know what you are fighting against. The following are the enemies of your VoIP traffic:

Key Topic

- **Lack of bandwidth:** Multiple streams of voice and data traffic competing for a limited amount of bandwidth.
- **Delay:** The time it takes a packet to move from the original starting point to the final destination. Delay comes in three forms:
  - **Fixed delay**: Delay values that you cannot change. For example, it takes a certain amount of time for a packet to travel specific geographical distances. This value is considered fixed. QoS cannot impact fixed delay issues.
  - **Variable delay**: Delay values that you can change. For example, queuing delay (how long a packet waits in a router's interface queue) is variable because it depends on how many packets are currently in the queue. You can impact queuing delay by selectively moving voice packets ahead of data packets.
  - **Jitter (delay variations)**: Describes packets that have different amounts of delay between them. For example, the first voice packet of a conversation might take 100 ms to reach a destination, whereas the second voice packet might take 110 ms. There is 10 ms of delay variation (jitter) between these packets.
- **Packet loss:** Packets lost because of a congested or unreliable network connection.

These enemies plague every network environment; however, the stakes are much higher when you add VoIP traffic to an existing data network. Users are accustomed to a PBX-style environment that has a separate network and dedicated bandwidth assigned just for voice traffic. The tolerance for crackling, echoing, or dropped calls from a voice network is very low.

QoS is designed to keep voice traffic running smoothly during temporary moments of congestion on the network. You should be very clear on this point: While QoS marking and classification (when configured) are continuously in operation, QoS output queuing policies only kick in and do their job when the interface is congested. If there is no problem, QoS traffic prioritization is not triggered. QoS is not a "magic bullet" that can solve any network scenario. For example, if there is a network environment in which the WAN link is constantly lacking bandwidth, adding voice to the link and expecting QoS to take care of the situation is like rearranging the deck chairs on the sinking Titanic. QoS can only do so much; either your data applications will perform so slowly they are no longer functional or your voice traffic will experience quality issues. This also goes the other way; if you have a network environment where fiber-optic cable is the norm and gigabit speeds abound, you might never experience network congestion. These environments will get little to no gain by using QoS because most QoS tools only engage during times of network congestion.

Your goal with QoS is to provide consistent, guaranteed bandwidth to voice traffic in such a way that there is low, consistent delay from one end of the network to the other. To accomplish this, you need to have QoS in some form at each point of the network where congestion might exist. This means doing an end-to-end audit of your network to determine the traffic types that exist and the service levels required for those traffic types.

Requirements for Voice, Video, and Data Traffic

The different traffic types that cross your network every day each have their own QoS requirements. Some of these requirements might be very loose; the network would essentially need to fail for the application to stop working. Other requirements might be very tight, requiring high-speed connectivity with low delay for the application to work successfully. This section describes general goals for voice, video, and data.

Tip Several QoS software utilities are available that will analyze your network traffic and report the bandwidth and delay each traffic type receives from the network.

Network Requirements for Voice and Video

Unlike data traffic, voice traffic is predictable. Whereas data traffic can jump considerably if a large web download or file transfer is started, voice traffic remains a consistent value for each call entering and leaving the network. The actual amount of bandwidth required for voice is heavily dependent on the codec you are using.

In addition to bandwidth requirements, voice traffic has the following additional one-way requirements:

Key Topic

- **End-to-end delay:** 150 ms or less
- **Jitter:** 30 ms or less
- **Packet loss:** 1% or less

Video traffic has identical delay requirements as voice but consumes a lot more bandwidth. In addition, the bandwidth can vary depending on how much movement is in the video (lots of movement increases the bandwidth required for video considerably).

Network Requirements for Data

It is impossible to give one sweeping guideline for all data applications, because every data application that exists has its own QoS requirement. When designing QoS for the data applications on your network, divide your applications into no more than four or five broad categories. For example:

- **Mission-critical applications:** These applications are critical to your organization and require dedicated bandwidth amounts.
- **Transactional applications:** These applications are typically interactive with users and require rapid response times. For example, a technical support employee might use a database application to retrieve caller information based on previous case ID values.
- **Best-effort applications:** These applications are noncritical or uncategorized. For example, web browsing, e-mail, and FTP file transfers fall into this category.
- **Scavenger applications:** These nonproductive applications typically have no business need, but consume excessive amounts of bandwidth. For example, peer-to-peer file-sharing applications fall into this category.

You can assign each of these data application categories a specific level of QoS. You can then map the actual applications to these categories using a variety of methods (such as incoming interface, exit interface, access lists, and so on).

QoS Mechanisms

Key Topic

With the applications requiring different levels of QoS, multiple models and mechanisms emerged to address the needs. Today, the following models are available for you to deploy QoS:

- **Best effort:** Best effort makes the list simply because this is the model every network uses by default. On the positive side, the best-effort model requires absolutely no effort at all on your end to implement. No QoS mechanisms are used, and all traffic is treated on a first-come, first-served basis. Of course, this does not address the QoS requirements of most network environments today.
- **Integrated services (IntServ):** The IntServ model works through a method of reservations. For example, if a user wants to make an 80-kbps VoIP call over the data network, the network designed purely to the IntServ model would reserve 80 kbps on every network device between the two VoIP endpoints using the Resource Reservation Protocol (RSVP). For the duration of the call, 80 kbps of bandwidth would not be available for any other use other than the VoIP call. Although the IntServ model is the only model that provides *guaranteed* bandwidth, it also has scalability issues because each router must track every single traffic flow. If enough reservations are made, the network simply runs out of bandwidth.
- **Differentiated services (DiffServ):** The DiffServ model is the most popular and flexible model to use for implementing QoS. In this model, you can configure every device to respond with a variety of QoS methods based on different traffic classes. You can specify what network traffic goes into each class and how each class is treated. Unlike the IntServ model, the traffic is not absolutely guaranteed (because the network devices do not completely reserve the bandwidth). However, DiffServ gets so close to guaranteed bandwidth (some Cisco documentation refers to it as "almost guaranteed" bandwidth), while at the same time addressing the scalability concerns of IntServ, that it has become the standard QoS model used by most organizations around the world.

Key Topic

The QoS model you use is primarily a strategy or mindset of how you design and implement QoS throughout your network. The QoS mechanisms themselves are a series of tools that combine together to deliver the levels of service your network traffic needs to survive. Each of these tools fits into one of the following categories:

- **Classification and marking:** These tools allow you to identify and mark a packet so network devices can easily identify it as it crosses the network. Typically, the first device that receives the packet identifies it using tools such as access-lists, incoming interfaces, or deep packet inspection (which looks at the application data itself). These tools can be processor intensive and delay the packet, so after the packet is initially identified, it is then marked. The marking can be in the Layer 2 (data link) header (allowing switches to read it) and/or the Layer 3 (network) header so routers can read it. Then, as the packet crosses the rest of the network, the network devices simply look at the marking to classify it rather than digging deep in the packet.

- **Congestion management:** All of the QoS queuing strategies fall under this umbrella, which are typically the primary tools you will use to implement QoS network-wide. The queuing strategies define the rules the router should apply when congestion occurs. For example, if a T1 WAN interface is completely saturated with traffic, the router begins holding packets in memory (queuing) to send them when bandwidth is available. All the queuing strategies aim to answer one question: When there is bandwidth available, what packet goes first?
- **Congestion avoidance:** Most QoS mechanisms engage only when congestion occurs on the network. The aim of congestion avoidance tools are to drop enough packets of non-essential (or not-as-essential) traffic to the network to avoid heavy congestion occurring in the first place.
- **Policing and shaping:** You can think of policing as one of the few "anti-QoS" mechanisms available. Rather than guaranteeing a certain amount of bandwidth, policing limits the amount of bandwidth certain network traffic can use. This is useful for many of the typical "bandwidth hogs" on the network: peer-to-peer applications, web surfing, FTP, and so on. You can also use shaping to limit the amount of bandwidth certain network traffic can use. It is designed for networks where the actual speed allowed is slower than the physical speed of the interface. The difference between the two mechanisms is that shaping queues (delays) excess traffic (and tries to send it later), whereas policing typically drops (discards) excess traffic.
- **Link efficiency:** As the name implies, this final group of tools focus on delivering the traffic in the most efficient way. For example, some low-speed links might work better if you take the time to compress your network traffic before it is sent. (Compression is one of the link efficiency tools.)

Understanding QoS completely is a fairly massive undertaking. At the CCNA Collabortion level, Cisco has chosen to highlight two of the key QoS Categories: link efficiency mechanisms and queuing algorithms.

Link Efficiency Mechanisms

As network technology progresses and spreads around the world, links slower than T1 speed (1.544 Mbps) are becoming increasingly rare. However, there are still many of these slower links in existence. There are typically two challenges facing these connections:

- Lack of bandwidth makes it difficult to send the amount of data required in a timely fashion.
- Slower link speeds can have a significant impact on end-to-end delay due to the serialization process (the amount of time it takes the router to put the packet from its memory buffers onto the wire). On these slow links, the larger the packet, the longer the serialization delay. For example, sending a 1500-byte packet on a 56-kbps link adds 214 ms just in serialization delay.

To address these challenges, the following link efficiency mechanisms have been introduced:

- **Payload compression:** Compresses application data being sent over the network so the router sends less data across the slow WAN link.

- **Header compression:** Some traffic (such as VoIP) may have a small amount of application data (RTP audio) in each packet but send many packets overall. In this case, the amount of header information becomes a significant factor and often consumes more bandwidth than the data itself. Header compression addresses this issue directly by eliminating many of the redundant fields in the header of the packet. RTP header compression (also called Compressed Real-time Transport Protocol [cRTP]) reduces a 40-byte header down to just 2 bytes (or 4 bytes with error correction). That is a big savings in bandwidth, but it comes at the prices of additional delay as the CPU does the work of compressing.
- **Link fragmentation and interleaving (LFI):** LFI addresses the issue of serialization delay by chopping large packets into smaller pieces before they are sent. This allows the router to move critical VoIP traffic in between the now-fragmented pieces of the data traffic (which is called "interleaving" the voice). You can use LFI on PPP connections (by using multilink PPP) or on Frame Relay connections (using FRF.12 or FRF.11 Annex C).

Tip One major thing to understand: Link efficiency mechanisms are not a magic way to get more bandwidth. Each of them has their own drawback: Compression adds delay, and processor load and link fragmentation increase the amount of actual data being sent on the line (because all the fragmented packets now need their own header information). Cisco does not recommend using these methods on links faster than T1 speed.

Queuing Algorithms

Queuing define the rules the router should apply when congestion occurs. The majority of network interfaces use basic first-in, first-out (FIFO) queuing by default. In this method, whatever packet arrives first is sent first. Although this seems fair, not all network traffic is created equal. The primary goal of queuing is to ensure that the network traffic servicing your critical or time-sensitive business applications gets sent before nonessential network traffic. Beyond FIFO queuing, there are three primary queuing algorithms in use today:

Key Topic

- **Weighted fair queuing (WFQ):** WFQ tries to balance available bandwidth among all senders evenly (thus the "fair" queuing). By using this method, a high-bandwidth sender gets less priority than a low-bandwidth sender. On Cisco routers, WFQ is often the default method applied to serial interfaces.
- **Class-based weighted fair queuing (CBWFQ):** This queuing method allows you to specify guaranteed amounts of bandwidth for your various classes of traffic. For example, you could specify that web traffic gets 20 percent of the bandwidth, whereas Citrix traffic gets 50 percent of the bandwidth (you can specify values as a percent or a specific bandwidth amount). WFQ is then used for all the unspecified traffic (the remaining 30 percent, in the previous example).
- **Low-latency queuing (LLQ):** LLQ is often referred to as PQ-CBWFQ because it is exactly the same thing as CBWFQ but adds a priority queuing (PQ) component. When you specify that certain network traffic should go into the priority queue, the router then not only guarantees that traffic bandwidth, but also guarantees it the first bandwidth. For example, using pure CBWFQ, Citrix traffic might be guaranteed 50 percent of the bandwidth, but it may only get that bandwidth after the router has fulfilled some other traffic guarantees.

When using LLQ, the priority traffic always gets sent before any other guarantees are fulfilled. As you might guess, this works very well for VoIP, making LLQ the preferred queuing algorithm for voice.

Although there are many other queuing algorithms available, these three encompass the methods used by most modern networks.

Applying QoS

By nature, you can apply most of the QoS mechanisms discussed as the network traffic leaves a router (because you cannot control the order the router receives traffic; it simply arrives). Table 3-2 summarizes the QoS methods discussed and the direction you can apply them on your router.

Key Topic

Table 3-2 Applying QoS to Input and Output Interfaces of a Router

QoS Methods Applied as Traffic Enters the Router (Input)	QoS Methods Applied as Traffic Leaves the Router (Output)
Classification	Congestion management
Marking	Marking
Policing	Congestion avoidance
	Shaping
	Policing
	Compression
	Fragmentation and interleaving

As you can see, you can apply some QoS methods (such as policing) in either direction.

Using Cisco AutoQoS

Deploying QoS can be complex. To help simplify the implementation of QoS, Cisco created a mechanism called AutoQoS, which allows you to enable a variety of QoS mechanisms with little QoS knowledge. AutoQoS works so well out of the box that many network administrators who have full knowledge of the QoS capabilities and configuration on Cisco devices use it anyway. AutoQoS deploys a template QoS configuration in line with Cisco QoS best practices, based on the bandwidth and encapsulation you configured under each of your router or switch interfaces. This template-based QoS deployment offers multiple advantages to manual QoS configuration:

- **Reduces the time of deployment:** Entering a single command on a device is much less time-consuming than the potentially complex QoS configurations.
- **Provides configuration consistency:** Using a single-command QoS template on each device ensures that all the devices use a similar QoS configuration that is not as prone to forgotten commands or mistypes.
- **Reduces deployment cost:** It takes some time and training to get fully up to speed on everything QoS has to offer.

- **Allows manual tuning:** You can manually adjust and tune the template-based configuration deployed by AutoQoS to fit your specific network QoS requirements.

Before you can deploy AutoQoS on your network, you must first establish the trust boundary for your voice traffic. To understand the concept of a trust boundary, you must first have a basic understanding of QoS markings. As a device sends traffic, that traffic might or might not have QoS markings attached to it. These markings might or might not be trustworthy. For example, a Cisco IP phone marks all of its traffic with an extremely high priority. In this case, the markings are trustworthy because the audio traffic from the phone does indeed need high-priority service. However, a technology-savvy user might configure a computer to mark traffic from it with the same high-priority marking as the voice traffic. In this case, the marking is not trustworthy.

Now, we can jump back to the concept of a trust boundary. The trust boundary is the point of the network where you begin trusting that the network traffic is accurately identified with the correct QoS marking. Depending on the capabilities of the devices on your network, you can begin applying QoS markings close to the user devices, as shown in Figure 3-7.

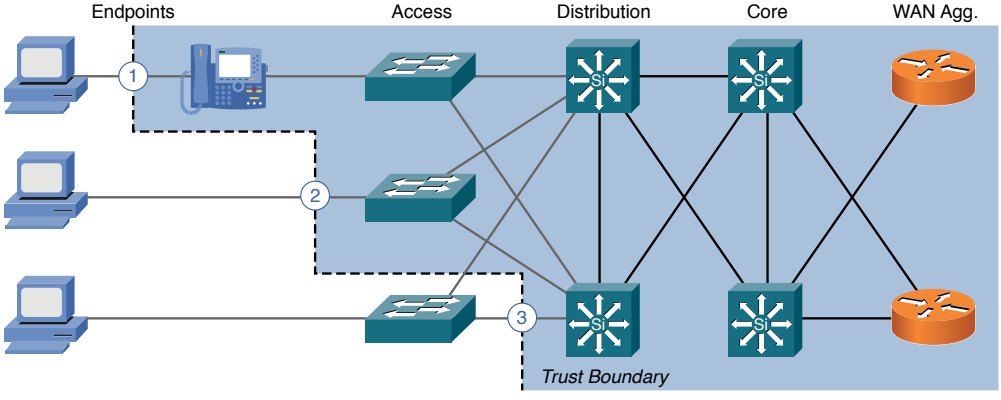


Figure 3-7 *Possible QoS Trust Boundaries*

Cisco IP phones have the ability to mark their own traffic as high priority and strip any high-priority markings from traffic sent by the attached PC. If you are using the Cisco IP phone to mark traffic, you have extended the trust boundary to point 1 shown in Figure 3-7. This is the ideal trust point because it distributes the QoS marking process to many Cisco IP phones rather than forcing the switches to apply QoS markings to a higher volume of traffic.

If you have PCs attached to the network and you have access layer switches with QoS capabilities, you can begin marking at these devices (point 2 in Figure 3-7). If your access layer switches do not have QoS capabilities, then the first possible place you can apply QoS markings is at the distribution layer switches (point 3 in Figure 3-7). This will work just fine; however, it adds an extra load to the distribution layer switches. Likewise, you will have network traffic passing through access layer switches without any QoS treatment. Although this is usually a safe bet—because access layer switches typically have higher-speed connections, on which congestion is rare—it is always best to apply QoS in as many places as possible where there is a potential bottleneck.

Note AutoQoS uses Cisco Discovery Protocol (CDP) to detect Cisco IP phones on Cisco switches and properly configure the QoS settings. This ensures that a user cannot disconnect their IP phone and attach another device to receive high-priority network treatment. Be sure you do not disable CDP on switch ports supporting Cisco IP phones.

Now, we have come to the point of configuring AutoQoS. Enabling AutoQoS is accomplished through a single command applied under interface configuration mode. To enable AutoQoS in your network, you must first identify the interfaces to which applying AutoQoS makes sense. AutoQoS does not need to be applied under every switch and router interface in your network (although it probably would not hurt anything if you were to do this). It primarily should be applied to interfaces on which the devices or applications need special or preferred treatment over others. Figure 3-8 shows a typical network. The interfaces labeled A represent areas of the network where you would use AutoQoS.

As you can see from Figure 3-8, you type this one command many times. Before you enter the AutoQoS command, always ensure that you have entered the correct bandwidth statement under the serial interfaces of your routers, because a router cannot auto-detect the actual speed of a WAN connection. A router can detect all other interfaces without requiring the bandwidth command.

Note AutoQoS uses a sophisticated queuing method known as low-latency queuing (LLQ). This queuing method provisions a specific amount of bandwidth for the various types of network traffic, including voice. Using AutoQoS features with incorrectly configured bandwidth commands can cause substandard network service.

The AutoQoS command syntax might be slightly different depending on where you enter it. The syntax in Example 3-6 enables AutoQoS for the interfaces shown in Figure 3-8 that are connected to the Cisco IP phones.

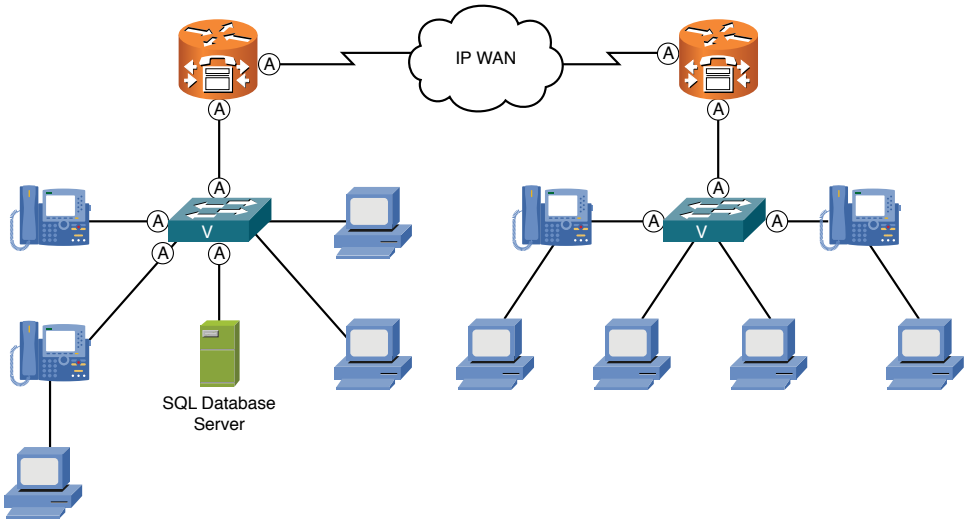


Figure 3-8 *AutoQoS Configuration Points*

Example 3-6 *Enabling AutoQoS on the Access Layer Switch Ports*

```
Voice_Switch# show run interface FastEthernet 0/3
Building configuration...
Current configuration : 169 bytes
!
interface FastEthernet0/3
    description CONNECTION TO IP PHONE
    switchport access vlan 10
    switchport mode access
    switchport voice vlan 5
    spanning-tree portfast
end
Voice_Switch# config term
Enter configuration commands, one per line.        End with CNTL/Z.
Voice_Switch(config)# interface fa0/3
Voice_Switch(config-if)# auto qos ?
        voip  Configure AutoQoS for VoIP
Voice_Switch(config-if)# auto qos voip ?
        cisco-phone                          Trust the QoS marking of Cisco IP Phone
        cisco-softphone                    Trust the QoS marking of Cisco IP SoftPhone
        trust                                              Trust the DSCP/CoS marking
Voice_Switch(config-if)# auto qos voip cisco-phone
Voice_Switch(config-if)# ^Z
Voice_Switch# show run interface FastEthernet 0/3
Building configuration...
Current configuration : 510 bytes
!
interface FastEthernet0/3
        description CONNECTION TO IP PHONE
        switchport access vlan 10
        switchport mode access
        switchport voice vlan 5
        mls qos trust device cisco-phone
        mls qos trust cos
        auto qos voip cisco-phone
        wrr-queue bandwidth 10 20 70 1
        wrr-queue min-reserve 1 5
        wrr-queue min-reserve 2 6
        wrr-queue min-reserve 3 7
        wrr-queue min-reserve 4 8
        wrr-queue cos-map 1 0 1
        wrr-queue cos-map 2 2 4
        wrr-queue cos-map 3 3 6 7
        wrr-queue cos-map 4 5
        priority-queue out
        spanning-tree portfast
end
```

Notice the options given by the context-sensitive help when the auto qos voip ? command was entered. Entering the command **auto qos voip cisco-phone** or **auto qos voip cisco-softphone** only enables the trust boundary if CDP detects a Cisco IP phone or Cisco IP Communicator (or equivalent Cisco IP softphone device) attached to the port. If a user removes this device, the trust boundary is broken and is not restored until the device is reattached. If you enter the command auto qos voip trust, the switch trusts the markings from the attached device regardless of what it is. You need to use this command if you purchase non-Cisco IP phones. Keep in mind that if you use this command, the network susceptible to users removing the non-Cisco IP phone and attaching rogue devices.

Note Before the **auto qos voip** command is entered under the Fast Ethernet 0/3 interface in Example 3-6, a **show run** command was performed so that you could see the current syntax entered under the interface. Notice how many commands are generated after entering the **auto qos voip** command. It is beneficial that the Cisco switch (and router) shows you all the individual commands so that you can optionally tune the settings to exactly fit your environment.

If the configuration generated by the **auto qos voip** command is not desired, you can remove this configuration simply by entering **no auto qos voip**.

Example 3-7 shows the AutoQoS syntax to use on the switch for the interface connecting to the router.

Example 3-7 *Enabling AutoQoS on the Switch-Router Uplink*

```
Voice_Switch# show run interface FastEthernet 0/1
Building configuration...
Current configuration : 169 bytes
!
interface FastEthernet0/1
        description CONNECTION TO ROUTER
        switchport access vlan 10
        switchport mode access
        spanning-tree portfast
end
Voice_Switch# config term
Enter configuration commands, one per line.  End with CNTL/Z.
Voice_Switch(config)# interface fa0/1
Voice_Switch(config-if)# auto qos voip trust
Voice_Switch(config-if)# ^Z
Voice_Switch# show run int fa0/1
Building configuration...
Current configuration : 369 bytes
!
interface FastEthernet0/1
        description CONNECTION TO ROUTER
```

```
        switchport access vlan 10
        switchport mode access
        mls qos trust cos
        auto qos voip trust
        wrr-queue bandwidth 10 20 70 1
        wrr-queue min-reserve 1 5
        wrr-queue min-reserve 2 6
        wrr-queue min-reserve 3 7
        wrr-queue min-reserve 4 8
        wrr-queue cos-map 1 0 1
        wrr-queue cos-map 2 2 4
        wrr-queue cos-map 3 3 6 7
        wrr-queue cos-map 4 5
        priority-queue out
end
```


You can configure the interface between the switch and router with the **auto qos voip trust** command, because you would consider the QoS markings from the router as trusted.

Finally, you can enable AutoQoS on the router's Fast Ethernet and Serial interfaces with the syntax shown in Example 3-8.

Example 3-8 *Enabling AutoQoS on Router Interfaces*

```
CME_Voice# show run int fa0/0
Building configuration...
!
interface FastEthernet0/0
        ip address 172.30.4.3 255.255.255.0
        ip nat inside
        ip virtual-reassembly
        duplex auto
        speed auto
end
CME_Voice# show run int s0/1/0
Building configuration...
!
interface Serial0/1/0
        bandwidth 512
        ip address 10.1.1.1 255.255.255.0
        encapsulation ppp
        no fair-queue
        clock rate 2000000
end
CME_Voice# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CME_Voice(config)# interface FastEthernet 0/0
```

```
CME_Voice(config-if)# auto ?
        Discovery        Configure Auto Discovery
        Qos                                Configure AutoQoS
CME_Voice(config-if)# auto qos voip trust
CME_Voice(config-if)# exit
CME_Voice(config)# interface Serial 0/1/0
CME_Voice(config-if)# auto qos voip trust
CME_Voice(config-if)# ^Z
CME_Voice# show run int fa0/0
Building configuration...
!
interface FastEthernet0/0
        ip address 172.30.4.3 255.255.255.0
        ip nat inside
        ip virtual-reassembly
        duplex auto
        speed auto
        auto qos voip trust
        service-policy output AutoQoS-Policy-Trust
end
CME_Voice# show run int s0/1/0
Building configuration...
!
interface Serial0/1/0
        bandwidth 512
        no ip address
        encapsulation ppp
        auto qos voip trust
        no fair-queue
        clock rate 2000000
        ppp multilink
        ppp multilink group 2001100116
end
```

The changes to the router interfaces look relatively tame compared to the amount of syntax entered under the switch interfaces; however, what you do not see are the many other commands that were entered in other configuration modes of the router to create class maps, policy maps, multilink interfaces, and so on.

Note In Example 3-8, after entering the **auto ?** command under the Fast Ethernet interface, notice that one of the options you are given is **auto discovery**. This enables a cool version of AutoQoS that allows the router to monitor your network for an extended time to discover known types of data, voice, and video traffic that are considered higher priority based on common high-priority application types. After the router captures enough traffic, it generates QoS policy recommendations that you can choose to apply or ignore.

Table 3-3 summarizes the different variations of AutoQoS commands you can enter on Cisco switch and router platforms.

Key Topic

Table 3-3 AutoQoS Syntax Variations

Command	Platform	Description
auto qos voip	Router or Layer 3 switch	Enables AutoQoS without trusting any existing markings on packets. The router re-marks all traffic types using access lists or Network-Based Application Recognition (NBAR) to identify traffic (higher processor-utilization tasks).
auto qos voip trust	Router or switch	This configuration explicitly trusts QoS markings set by the attached device and does not rely on CDP to verify a Cisco IP phone is attached.
auto qos voip cisco-phone	Switch	Enables AutoQoS, trusting any existing QoS markings that enter the interface only if the switch detects a Cisco IP phone attached through CDP.
auto qos voip cisco-softphone	Switch	Enables AutoQoS, trusting any existing QoS markings that enter the interface only if the switch detects a Cisco IP SoftPhone (such as Cisco IP Communicator) attached through CDP.

Note QoS engineers identify what have been called QoS markings in the previous section as class of service (CoS) and type of service (ToS) markings. CoS is a marking that exists in the Layer 2 header of a frame, which a switch can identify. ToS is a marking that exists in the Layer 3 header of a packet, which a router can identify.

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 3-4 lists and describes these key topics and identifies the page number on which each is found.

Key Topic

Table 3-4 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
Figure 3-5	Trunking tag concepts	59
Figure 3-6	Separating voice and data traffic using VLANs	61
Examples 3-1 and 3-2	Configuring voice and data VLANs	61
Note	CDP delivers voice VLAN information	61
Text	Cisco phones receive DHCP Option 150 to download an .xml configuration file via TFTP	65
Text	Two primary signaling protocols to Cisco IP phones are SIP and SCCP	67
List	Three areas of concern when deploying QoS	69
List	Key delay requirements for voice and video traffic	70
List	Three common QoS models	71
List	Categories of QoS mechanisms	71
List	Specific link efficiency mechanisms	72
List	Specific queuing algorithms	73
Table 3-2	Directions you can apply various QoS mechanisms	74
Table 3-3	AutoQoS syntax variations	81

Complete the Tables from Memory

Table 3-5 is a study aid we call a "memory table." Print a copy of Appendix D, "Memory Tables" (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Table 3-5 Memory Table for Chapter 3

Feature/Concern	Definition	Purpose
DHCP Option 150	TFTP server IP address	Required for IP phone downloads
NTP	Centralized clock synchronization	Critical for log timestamps, certificates, CDRs, time display
QoS	Prioritizes voice traffic at the expense of other traffic	Critical to maintain acceptable delay and jitter for good voice quality
Delay	End-to-end travel time of a packet	Maximum 150 ms for voice packets
Jitter	Delay variation between packets	Maximum 30 ms
Loss	Packet loss in transit	Less than 1%
AutoQoS	Automates QoS consistent best-practices deployment	Simpler than manual config; manually tunable

Definitions of Key Terms

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

802.3af , 802.3at, Power over Ethernet (PoE), Cisco inline power, Cisco Discovery Protocol (CDP), virtual LAN (VLAN), trunking, 802.1Q, Dynamic Trunking Protocol (DTP), Skinny Client Control Protocol (SCCP), Session Initiation Protocol (SIP), Network Time Protocol (NTP), QoS, link efficiency, classification, marking, policing, queuing, LLQ, priority queuing, WFQ, CBWFQ, fragmentation, interleaving, DSCP, AutoQoS.

This chapter covers the following topics:

- **Preparing the CME Router for Cisco Configuration Professional:** This section details the required steps to get the router ready for Cisco Configuration Professional (CCP) to connect to and configure the router.
- **Managing CME Using CCP:** CCP has evolved to become the most fully functional all-in-one graphic interface for managing your CME router. This section discusses the CCP interface and its initial configuration tasks.

CHAPTER 4

Getting Familiar with CME Administration

This chapter covers one of the interesting decisions in the evolution of the CCNA Voice / CICD course. After a great deal of discussion, Cisco decided to remove much of the Communication Manager Express (CLI) content from the CME learning objectives. This decision was not taken lightly; people have strong opinions about this, myself included. The CLI is the most powerful and arguably the fastest method of configuring CME; in the real world, many admins working with CME are using the command line exclusively. But the fact is that there is already a lot of stuff to learn for the exam, and parts of the CLI were deferred to more advanced study.

As the author of the Official Certification guide, my primary goal is to give you the information you need to pass the exam. My secondary goal is to help you understand the systems discussed in the book at a level of proficiency that makes you able to set them up and administer them at a basic level. Given that, here is what I have done for this new edition: I have removed large parts of the CLI from the body of the book and moved it to an appendix at the end. I did this mostly because removing it lines up with the exam blueprint and the CICD course, but keeping it available makes it a great reference to have handy. And, of course, it is always possible that the people who create the exam might change their minds again and put the CLI back into the exam after we print this book, and if they do you will still have the CLI material to study.

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

Foundation Topics Section	Questions Covered in This Section
Preparing the CME Router for CCP	1–3
Managing CME Using CCP	4–7

1. Which of the following is not necessary to configure the CME router to support CCP?
   a. Enabling write operations to the router's flash
   b. Creating a privilege level 15 user account
   c. Enabling HTTP services on the router
   d. Configuring Telnet or SSH for local logins
2. Which two methods will allow CCP to connect to the CME router?
   a. Connect the PC's network card to the Console port of the router and set it to obtain an IP address automatically.
   b. Copy the default configuration file to NVRAM, set your PC to obtain an IP address automatically, and reload your 2921 model router.
   c. Erase the startup-config file in NVRAM, set your PC to obtain an IP address automatically, and reload the router.
   d. Copy the default configuration file to NVRAM, give your PC a static IP address of 10.1.1.2/24, and reload the router.
   e. Copy the default configuration file to NVRAM, set your PC to obtain an IP address automatically, and reload your 1921 model router.
3. Which of the following commands are required to enable CCP to configure the CME router? (Choose three.)
   a. **ip http secure-server**
   b. **ip http server**
   c. **username** *username* **privilege 15 password** *password*
   d. **aaa authentication login default group radius**
   e. **line vty 0 15**
   f. **login local**
4. What type of archive can you download from Cisco to reinstall all support files for the integrated GUI back into the router flash?
   a. .TAR file
   b. .ZIP file
   c. .GZ file
   d. .RAR file
5. Which version of CCP installs into the flash of a Cisco router?
   a. There is only one CCP version, which cannot install into the router flash.
   b. CCP integrates with the SDM utility in the router's flash.
   c. CCP Lite.
   d. CCP Express.

6. Which of the following best describes a community in CCP?
   a. A group of users managed by a single administrator
   b. A group of up to 10 devices enabled for CCP configuration
   c. A group of up to 5 devices enabled for CCP configuration
   d. A group of similar devices that share a common configuration
7. How does the communication change by selecting the Connect Securely check box when adding a device to a CCP community?
   a. You are prompted for the router's enable secret password rather than the VTY line password.
   b. Only level 15 user accounts are permitted to access the device.
   c. CCP uses HTTPS/SSH to connect to the device.
   d. CCP permits only communication over an IPSec managed connection.

Foundation Topics

Preparing the CME Router for Cisco Configuration Professional

Before CCP can connect to and configure a router (or switch), basic IP connectivity must be established so that the PC running CCP can access the device. Then, the web service (and/or secure web service) on the device must be activated. Next, an account with privileged exec access must be created, and finally, the router configured to use the local username database for authentication of CCP connections. The following four configurations summarize the key elements for getting CCP to work must be entered on the device:

Key Topic

- **Reachable IP address:** CCP must be able to reach the CME router on the IP address you specify.
- **Level username and password:** Define an administrative account that CCP will use to connect to and configure the CME router.
- **Integrated HTTP services:** Enable the device's HTTP server to allow the CCP utility to discover the CME router.
- **Local authentication for Telnet/SSH:** CCP logs in to the CME router using the privileged account defined above to apply configurations based on the GUI interaction.

Example 4-1 shows the configuration of a CME router to support CCP-based configuration.

Key Topic

Example 4-1 *Configuring the CME Router to Support CCP*

```
CME_Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CME_Router(config)# interface GigabitEthernet 0/0
CME_Router(config-if)# ip address 172.30.100.77 255.255.255.0
CME_Router(config-if)# no shutdown
CME_Router(config-if)# exit
CME_Router(config)# username Neo privilege 15 secret ci$co
CME_Router(config)# ip http server
CME_Router(config)# ip http secure-server
! Note that the previous line is optional.
! Secure-server enables HTTPS communication.
! HTTPS is desirable but not mandatory.
CME_Router(config)# line vty 0 15
CME_Router(config-line)# login local
CME_Router(config-line)# transport input telnet ssh
CME_Router(config-line)# end
CME_Router#
```

Managing CME Using CCP

Managing CME using CCP offers a number of advantages, some of them obvious and others not as evident. First, many small offices employ an all-in-one administrator whose knowledge and time is spread across many different technologies. Requiring this level of administrator to learn a complete command-line operating system to interact with CME is unrealistic. Similarly, some offices use consultants or contract network administrators to manage their network. Providing an easy-to-use graphical user interface (GUI) allows one of the more technically inclined users at the office to take care of the day-to-day administration (changing directory numbers, adding phones, and so on) without the involvement of dedicated IT staff. Finally, the point-and-click of a graphic interface can be more efficient at times than typing configuration commands.

Although Cisco has released multiple GUI management tools to configure CME over the years, two primary tools are used today: the integrated CME GUI and Cisco Configuration Professional (CCP).

CME Integrated GUI

The integrated CME GUI is powered by HTML and JAR (Java) files loaded into the flash of the CME router. Typically, the CME router ships with these files preloaded by Cisco into the flash; however, you can also download a .TAR package of files from Cisco.com (assuming you have a valid support contract) and extract the files into the flash of the router. With minimal command-line configuration (assigning an IP address and enabling the HTTP server), you can have the integrated CME GUI up and running quickly, as shown in Figure 4-1.

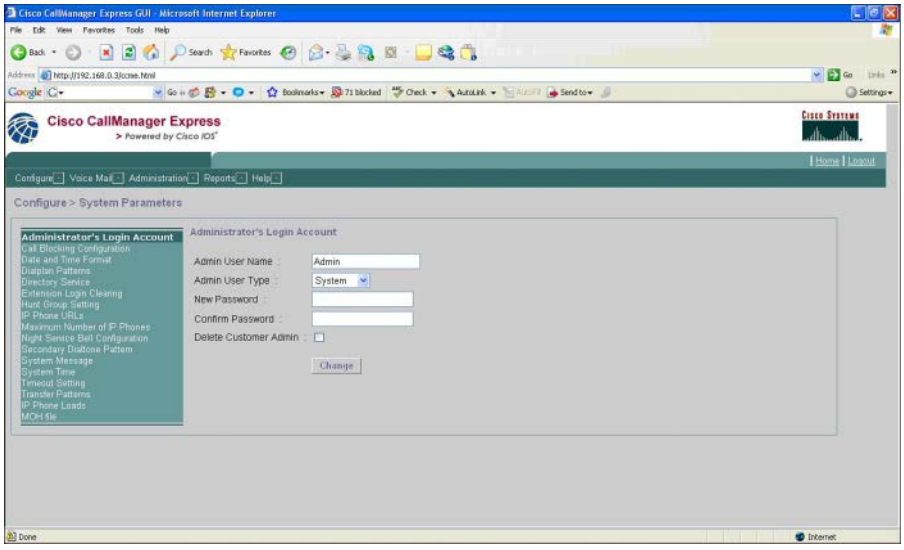


Figure 4-1 *Integrated CME GUI*

Although the integrated CME GUI is not "pretty" by today's standards, it is functional, which enables you to handle most core functions of CME: adding/changing phone configurations, modifying the dial plan, configuring hunt groups, and so on.

Cisco Configuration Professional

While Cisco focused the integrated CME GUI on configuring only the telephony aspects of the CME router, it created CCP to configure *all* major aspects of the CME router. It enables simple (and often wizard-based) configuration of the router, firewall, intrusion prevention system (IPS), virtual private network (VPN), Unified Communications, and common WAN and LAN features and configurations. You can download the latest version of the CCP software from the Cisco website free of charge. CCP is roughly a 200-MB installation on a local PC. After you install it, you can manage any supported Cisco platform using the utility. You do not need to install anything on the managed devices, but they do require the configurations described in the previous section. Most brand new devices have a default startup-config file loaded that implements the necessary configs when you boot them, and all you have to do is get the correct IP address on your PC (and some models have a DHCP service running by default, so you do not even need to set the IP manually). You can also download the appropriate startup-config file for your device from Cisco if you want, instead of configuring it yourself.

Note Cisco has also created Cisco Configuration Professional Express (CCP Express), which is similar to the CCP utility but is loaded into the flash of the router instead of running on a PC as an application. CCP Express only focuses on configuring basic LAN/WAN connections, firewall, and Network Address Translation (NAT). It is not able to configure Unified Communications features.

When you initially open CCP, it prompts you to configure a community, as shown in Figure 4-2.

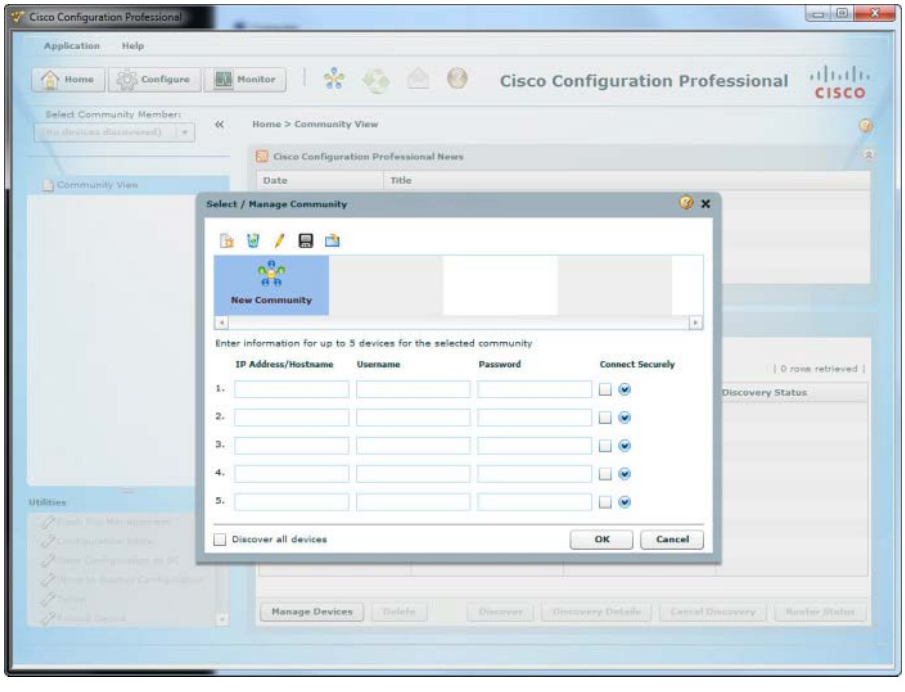


Figure 4-2 *Creating a CCP Community of Managed Devices*

A *community* is a group of devices you want to manage using CCP. Before you can add a device, you must configure it with the four elements discussed in the previous section, "Preparing the CME Router for Cisco Configuration Professional."

By default, CCP attempts to connect to the router using Telnet and HTTP, which are both unencrypted protocols and therefore not desirable. Secure connections are always better. By simply checking the **Connect Securely** check box in CCP (as shown in Figure 4-3), it now uses SSH and HTTPS to connect to and configure the CME route. This also requires that you have enabled the HTTPS service and allowed SSH transport on the vty lines of the device you want to manage.

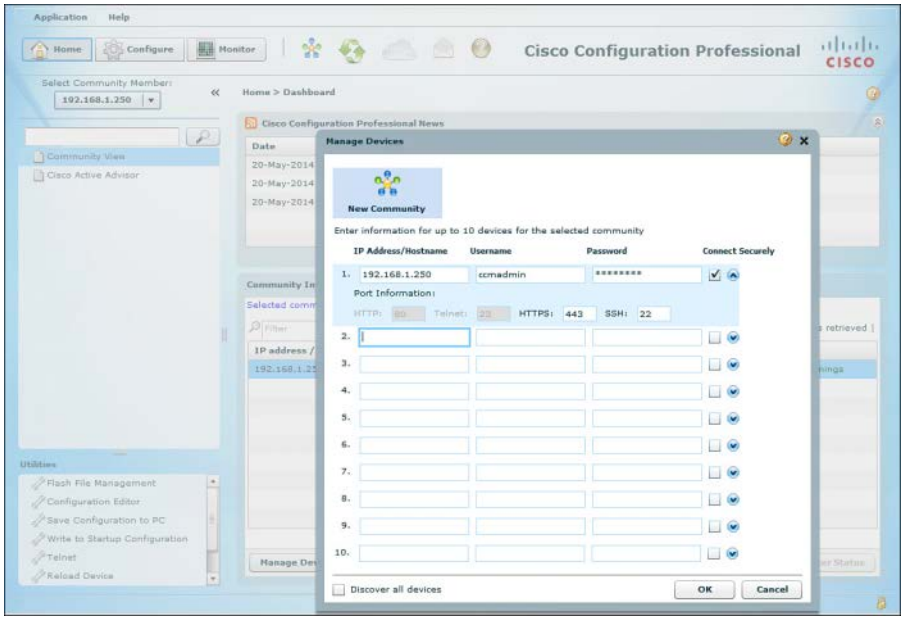


Figure 4-3 *Connecting to the CME Router Securely*

After you connect to the CME router, CCP runs a discovery process, which identifies the router hardware, software, interfaces, and modules. After this process completes, you can configure the device. Although CCP has many configuration options available relating to routing and security, we primarily focus on the Unified Communications features, as shown in Figure 4-4.

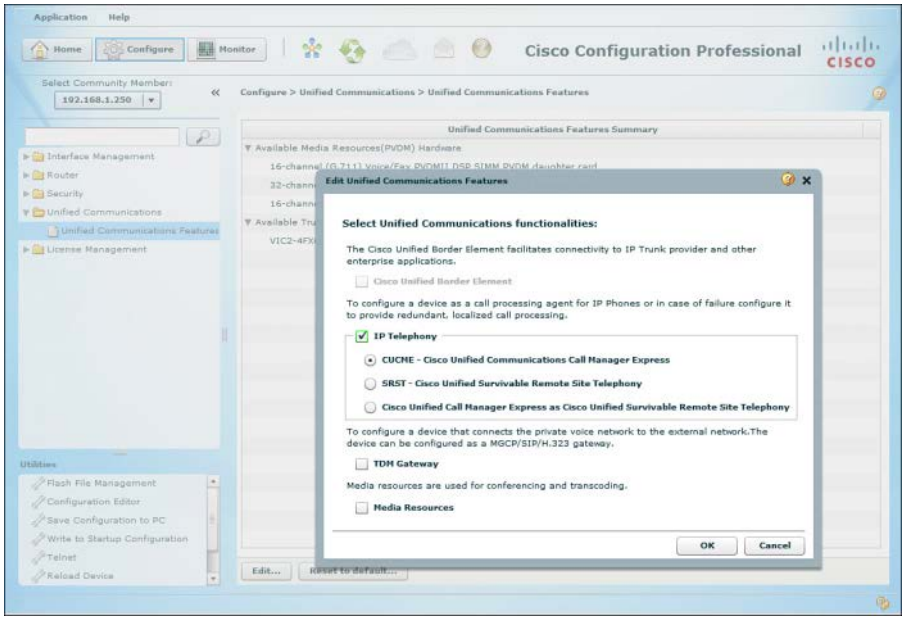


Figure 4-4 *Unified Communications Initial Configuration*

When you initially expand the Unified Communications folder under the Configuration section of CCP, you see only one available option: Unified Communications Features. Only one option appears because you have not yet configured the CME router to support CME features. As you can see from Figure 4-4, CCP enables you to configure the router in one of four ways:

Key Topic

- **Cisco Unified Border Element:** Known as CUBE, this option sets up the router as an IP telephony gateway for IP-to-IP services, such as IP Telephony Service Provision (IP-TSP). CUBE provides typical edge services such as NAT/PAT, and adds VoIP-specific functionality for billing, security, call admission control, quality of service, and SIP negotiation.
- **IP Telephony - CUCME:** CCP configures the router as a standalone CME system. This is the option you will be learning about in some detail.
- **IP Telephony - SRST:** Enables the IP phones to use the CME router as a failover device should they lose connectivity with the CUCM cluster.
- **IP Telephony - Cisco Unified Call Manager Express as Cisco Unified Survivable Remote Site Telephony:** Providing a similar capability to SRST, but with the full feature set of CME. The tradeoff for gaining all those features is that the router cannot support as many phones in SRST mode as the same router in SRST-only mode could.

The remaining two check boxes configure gateway functionality (which may be configured either instead of, or in addition to, CME functionality) and media resources, which allows you to configure onboard DSP chips for use as audio conferencing or transcoder resources.

Note If you choose the Gateway option shown in Figure 4-4, you have the ability to select three suboptions. None configures the router as a voice gateway only (does not support IP phones). Cisco Unified SRST and Cisco Unified CME as SRST enable the IP phones to use the CME router as a failover device should they lose connectivity with the primary call-management system. These topics are discussed in the CIPT1 and CIPT2 CCNP Collaboration titles.

After CCP applies the initial CME configuration to the router, the Unified Communications menu refreshes to display additional configuration options, which will vary depending on the selections made on the Features screen. The upcoming chapters discuss several of these configuration screens as we move on and continue to focus on using CCP to set up CME.

Tip I think that I need to add a few words about installing CCP in the real world. Application development and operating system development get out of sync and can cause compatibility issues, typically when trying to run CCP on Windows 7 and 8 machines. Java has also had some compatibility issues, and we sometimes find ourselves in the situation where an application such as CCP requires an older version of Java, which is not secure and maybe even not available any more. There are ways to make it all work, and there are several good threads in the Cisco support forums and elsewhere on the Internet that go into detail on exactly how to do that. It does work well once you get all the pieces in place; you just need to do your research and pay attention to detail. It is not related to the exam, so I do not go into that detail here.

One of the best pieces of advice I can give you is this: Build a virtual machine to run CCP (or any other apps that are "picky" with their requirements). Doing so means that you can make a customized Windows install that has exactly the settings and software needed to make it work with each application, and which can be locked down so that it can't be updated and wreck those settings. The virtual machine can also be prevented from accessing anything other than its intended devices to improve security. You should be learning about building virtual machines anyway, and this tactic will become a very useful one as you move forward.

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 4-2 lists and describes these key topics and identifies the page numbers on which each is found.

Table 4-2 Key Topics for Chapter 4

Key Topic Element	Description	Page Number
List	Requirements for supporting connection from CCP	88
Example 4-1	Accessing the telephony-service configuration of a CME router	88
List	The modes of VoIP configuration supported by CCP	92

Complete the Tables from Memory

Table 4-3 is a study aid we call a "memory table." Print a copy of Appendix D, "Memory Tables" (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Table 4-3 Memory Table for Chapter 4

Chapter Concept	Activity	Where or What?
Configure CME router to support CCP	Four configurations required to support CCP	IP address, level 15 username and password, HTTP/S server enabled, local authentication for Telnet/SSH
Integrated web-based GUI	Basic CME configuration	http://<CME_IP>/ccme.html
CCP Community	Group of up to 5 devices under CCP management	Initial CCP setup dialog

This page intentionally left blank

This chapter covers the following topics:

- **Describe End Users in CME:** This section reviews the theory of end user configuration in CME.
- **Create or Modify End Users and Endpoints in CME Using the CCP GUI:** This section reviews and describes the capabilities and features of CCP, demonstrates the creation and management of end users in CME using the CCP application, and explains the creation and configuration of endpoints in CME using CCP.

CHAPTER 5

Managing Endpoints and End Users in CME

Continuing in our process of understanding and implementing CME, this chapter covers how the various components of end users and endpoints in CME are configured and how they interact to create a functional system.

As previously noted, the CICD course has deemphasized the command-line interface (CLI), and the sections on endpoint and end-user implementation in this chapter focus primarily on the CCP graphical user interface (GUI) and to a lesser extent on the built-in CME GUI. As before, the CLI appendix will provide you with a reference to the commands that CCP generates to write the CLI configuration.

"Do I Know This Already?" Quiz

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

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

Foundation Topics Section	Questions
Describe End Users in CME	1–7
Create or Modify End Users and Endpoints in CME Using the CCP GUI	8–10

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

1. CME provides three user access levels. What are they? (Choose three.)
   a. Remote user
   b. System administrator
   c. Privileged user
   d. End user
   e. Customer administrator
2. Which command activates the router's web server?
   a. **http server enable**
   b. **forward-protocol http**
   c. **www webedit**
   d. **ip http server**
3. Which command authenticates GUI users against entries in the running configuration?
   a. **ip http authentication local**
   b. **ip authentication aaa**
   c. **web-service local-auth**
   d. **aaa new-model http**
4. What does the command **web admin system name** *username* **password** *password* do?
   a. Identifies a web GUI configuration profile tag
   b. Defines the system administrator user for CME
   c. Defines the customer administrator user for CME
   d. Enables the router web server for the specified user
5. Which of the following are capabilities of the CCP GUI? (Choose all that apply.)
   a. Dynamic routing configuration
   b. VPN configuration
   c. Unified Communications configuration
   d. Access list configuration
6. Harry is building a 9971 phone in CME. He is explaining some of the differences between the SIP configuration he is creating and the SCCP configuration built for a 7970. Which of the following would be an accurate statement by Harry?
   a. An ephone-dn is assigned to a SIP ephone.
   b. A voice register dn is assigned to a SIP ephone.
   c. A voice register dn is assigned to a SIP voice register global.
   d. A voice register dn is assigned to a SIP voice register pool.

7. Which of the following are required steps to create a phone with a functioning line in CME? (Choose all that apply.)

   a. Create a phone (ephone).
   b. Create an extension (ephone-dn).
   c. Associate the extension with the phone.
   d. Autoregister the phone.

8. Bob has decided not to use an external TFTP server for all his new SIP phone firmware loads, even though that is possible and would work fine. Instead he has chosen to let the CME router provide TTP services for phone firmware from the flash directory. Bob knows that setting up the TFTP services and commands is possible at the command line, but he would rather use CCP if possible. Which of the following is true for Bob?

   a. Bob can only use CCP to set up phone firmware and TFTP if he first copies the firmware files to flash using the CLI.
   b. Bob can either use existing firmware files or upload new ones to the router flash using CCP under the Unified Communications menu.
   c. Bob cannot use CCP to set up and configure phone firmware files; this must be done manually at the CLI.
   d. Although CCP can set up and configure firmware and TFTP services, it is not necessary because CME v10.x has the necessary configurations in place as a factory default.

9. In CME, how would you create a directory entry and an internal caller ID name that is visible on the IP phones registered to the system?

   a. Create an extension using CCP
   b. Create a phone using CCP
   c. Create a directory entry list using CCP
   d. Create an address list service using the CLI

10. Which of the following is true of the relationship between users, phones, and extensions in CME?

    a. A user must be associated with a phone.
    b. Once a user is associated with a phone, his presence status is automatically monitored for on-hook/off-hook condition.
    c. Associating a user with a phone allows that user to make changes to their phone, including speed dials and ringer choices.
    d. There is no telephony functionality at all if the user is not associated with the phone.

Foundation Topics

Describe End Users in CME

CME is an application that by its very nature is directly involved with its users. People use phones to reach other people. Some of those people are responsible for managing the CME system, and in turn some of those people may have more or less authority and administrative privilege than others.

This section covers the different levels of user privilege in CME and how they are set up and applied.

User Access Levels in CME

In any organization, when we look at the information technology environment, there are a few common characteristics. One almost universal truth is this: There are people who use the applications and systems as part of their daily job responsibilities, and there are other users whose daily job responsibility *is* the applications and systems. The first group we will call end users, and the second group we will call administrators. Some administrators have more power and authority over the systems and applications than others, according to their capability, knowledge, and assigned responsibility.

When it comes to the CME application, this pattern still holds true. In CME, we can define three levels of user:

- **System administrators** have the authority to configure all aspects of the CME system and phone features, including (but not limited to) adding phones and users, creating the dial plan, managing calling privileges, and implementing features.
- **Customer administrators** can perform adds, moves, and changes to phones and users but do not have access to system-level configurations.
- **Phone users** can customize certain aspects of their own phones such as speed dials, log in using their user ID and password to services such as Extension Mobility, and can search the user directory to place a call.

The intent, of course, is to provide certain users with the ability to perform routine administrative tasks while protecting the system from inadvertent misconfigurations due to their lack of knowledge.

Creating Users in CME

As always, the command line is ultimately the only method used to create users; the GUI just makes life a little easier by putting a friendly face between you and the CLI. We created a system administrator account using the CLI back in Chapter 4, "Getting Familiar with CME Administration," when we set up a privileged user account for CCP. We could make many other system administrator accounts if we needed to, using either the CLI or the built-in GUI. There are, of course, other CLI commands to create customer administrator accounts and ordinary users; you can see them in Appendix C, "Managing CME Using the Command Line." For this section, let's look at the GUI options for user creation.

Creating Users with the CME GUI

CME comes with a built-in GUI (which predates and is totally separate from CCP) to provide both system administrator- and customer administrator-level access. The GUI files are closely tied to the version of CME running on the router; as always, to achieve success you must keep the version of IOS software, CME and GUI files tightly coordinated per the documentation or face the dreaded "it just doesn't work" situation.

Enabling the CME Built-In GUI

Carefully select and download the correct GUI tar archive for your version of CME, and use TFTP to copy the .tar file to the router flash. Then use the **archive tar /xtract** command to extract all the GUI files to flash.

Tip Different implementations of CME use different storage locations for the GUI files. Some place the files in the root of the flash directory; others specify a flash:/GUI directory. In my experience, placing the files in the root of flash works well.

After you download and extract the GUI files to flash on the router, you have a little bit of command line work to do to get it running. The list that follows summarizes the steps to get the built-in GUI running:

Step 1. Download the GUI files, being certain of version compatibility with the CME and IOS version in use.

Step 2. Extract the GUI files to flash.

Step 3. If you have not already done so (as part of the CCP setup), enable the HTTP server on the router.

Step 4. Configure the router with the path to the GUI files.

Step 5. Set the method of HTTP authentication. (We will use the local usernames and passwords list, although other centralized methods such as AAA and TACACS+ are possible.)

Step 6. Create the CME system administrator account. (This may be the same account as the one you used for CCP, or it may be different. In either case, a special command is required to assign CME web GUI authority to the user account.)

Step 7. Enable editing of ephone-dn and system time from the CME GUI.

Example 5-1 summarizes the commands to perform those actions.

Example 5-1 *Commands to Enable the CME GUI*

```
Router> enable
Router# configure terminal
Router(config)# ip http server
! enables the http server
Router(config)# ip http path flash:
! sets the http path to the root of the flash directory
Router(config)# ip http authentication local
! configures the router to use the local list of usernames and passwords for web GUI
authentication
Router(config)# telephony-service
Router(config-telephony)# web admin system name username password password
! configures the specified user as a CME System Administrator
Router(config-telephony)# dn-webedit
! (Optional) Enables the ability to add directory numbers through the web interface.
Router(config-telephony)# time-webedit
! Enables the ability to set the phone time for the CME system through the web inter-
face.
```

At this point, assuming that you have basic IP connectivity in place, you should be able to launch a supported browser and connect to the CME built-in GUI at the URL of http://<cme_ip_address>/ccme.html. Figure 5-1 shows the CME built-in GUI home page.

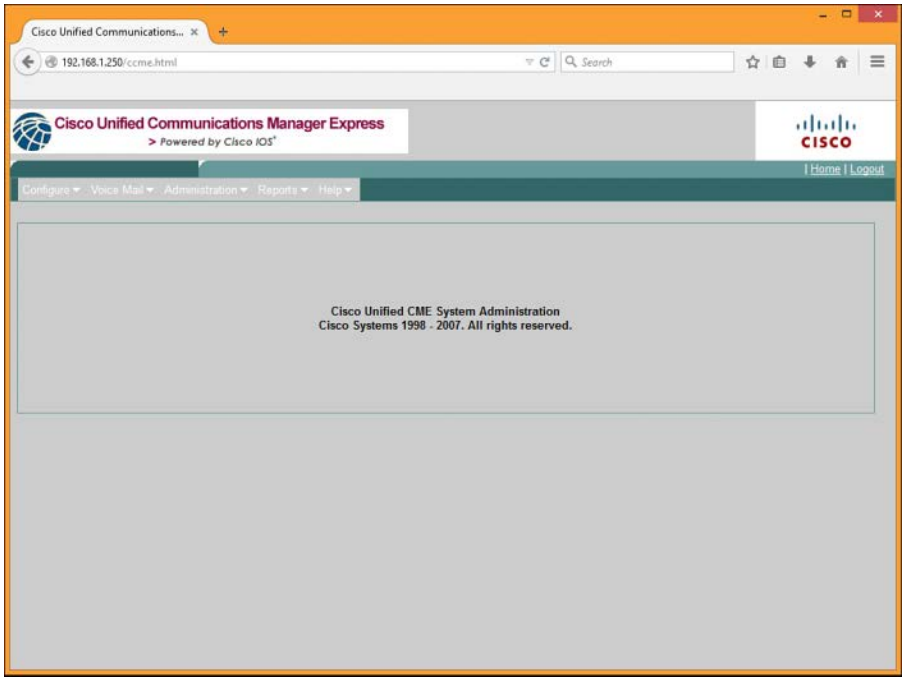


Figure 5-1 *CME Built-In GUI Home Page*

Tip You may find that saving your running-config and reloading the router will get the GUI to work properly if it did not the first time. And remember, the GUI files version must be correct for the CME version in use, which must in turn be supported by the right IOS version on the correct hardware!

Using the CME Built-In GUI to Create the Customer Admin

In the CME GUI, from the Configure menu, select **System Parameters**, then **Administrator's Login Account**. In the work pane to the right, change the selection for Admin User Type to **Customer**. Type the new password and confirm it; then click **Change**, as shown in Figure 5-2.

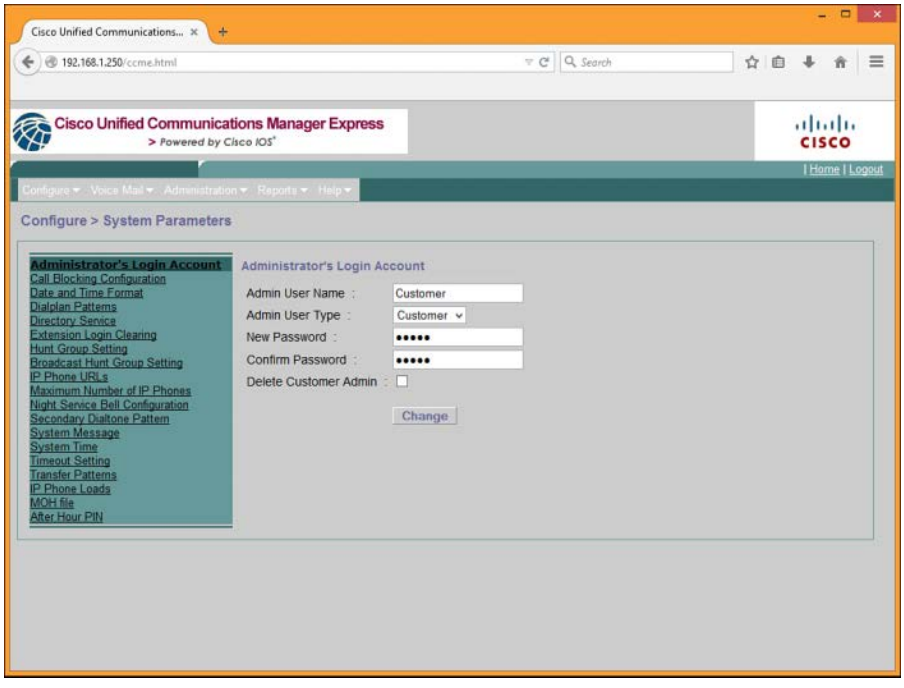


Figure 5-2 *Setting Up the Customer Admin Account Using the CME GUI*

Key Topic

Now that we have created a system admin and a customer admin, we can examine the creation of ordinary users. Users are created and defined by a simple entry in the router's running configuration; again, the CLI is at work in the background even though we will work with CCP to create our ordinary users. In CME, the relationship between the user and the ephone-dn on one hand and the user and the ephone on the other is significant. Knowing how the components of users, ephone-dn, and ephone fit together is key to your understanding this section about CME users. Let's break it down in plain English first, and then attach the concepts to the config.

Most people are confused by the concepts and terms *ephone* and *ephone-dn*. First of all, ephone means "Ethernet phone" and refers to the physical phone hardware as represented

by the CLI lines that configure it for operation in CME. Ephones are identified by the device type (7970, for example) and MAC address. Other configurations can be applied to the ephone to control button capabilities assignments such as speed dials and intercom, softkey templates, and many other system and feature configurations—including the associated username. The associated username is important because it allows that named user to modify the phone configuration—adding a speed dial or setting the ringer, for example—from the CME GUI.

The relationship between the ephone-dn and the user differs slightly. An ordinary user is not allowed to modify the ephone-dn configuration. Associating the user to an ephone-dn serves multiple purposes:

- Provides caller ID for internal calls
- Builds the system directory
- Allows for presence status monitoring of the ephone-dn (on-hook, off-hook, or unknown/unregistered)
- Applies the ephone-dn configuration to the ephone when the associated user logs in on the phone with Extension Mobility

So, what we end up with is a user who is associated with an ephone, which has one of the buttons configured with an ephone-dn, which is associated with the same user. The result is that the user can see and modify the way the phone is configured (to an extent, at least), and the user (and perhaps the user's presence status) is displayed in the directory along with the associated ephone-dn, allowing us to search for the user and call them right from the directory listing.

We should also make a point of knowing the parallels to ephones and ephone-dn in a Session Initiation Protocol (SIP) configuration; CME fully supports SIP endpoints, and many new phone models are exclusively SIP. The configurations are completely different, executed under a different configuration prompt (voice register global instead of telephony-service at the CLI), but there are very clear parallels:

- An SCCP phone is defined by creating an ephone.
- A SIP phone is defined using a voice register pool.
- An SCCP phone is associated with an ephone-dn.
- A SIP phone is associated with a voice register dn.

Table 5-2 provides a quick reference for you to keep those terms straight.

Table 5-2 SCCP Versus SIP Configuration Components

Component	SCCP	SIP
IP phone	**ephone**	**voice register pool**
Directory number	**ephone-dn**	**voice register dn**
Telephony configuration	**telephony-service**	**voice register global**

The built-in GUI can add new ephone-dn numbers and associate them to user names, but to make it possible to create new ephones in the CME GUI, you need to have auto-registration enabled; otherwise, it complains that there is "No new phone to add!" Let's turn our attention to the CCP interface now, to examine its capabilities including adding phones, users, and extensions (ephone-dn) manually.

Create or Modify End Users and Endpoints in CME Using the CCP GUI

For this section, the use of CCP for the configuration and management of CME is our primary interest. We will examine the CCP interface and its general capabilities, and although the focus remains on Unified Communications configurations, you will gain some insight into the other capabilities for GUI-based configuration that CCP offers as well.

General Capabilities of CCP

CCP provides a single interface to configure the majority of capabilities and features of supported hardware platforms and IOS versions. From the Configure menu shown in Figure 5.3, an administrator can access the following menus and options. (This is not a complete list, just some of the highlights.)

- **Interface Management:** Configure interface connections, IP addressing, telephony trunk setup, and so on
- **Router:** Time, router access, DHCP, DNS, routing, ACLs, NAT, QoS, and so on
- **Security:** Firewall, VPN, network access control, intrusion prevention, and so on
- **Unified Communications:** Unified Communications features, telephony settings, user, phones and extensions, VoIP settings, trunks, dial plans, telephony features, media resources, and so on
- **License Management:** License dashboard
- **Utilities:** Flash file management, configuration editor, save config to PC, write to startup config, Telnet, reload device, ping and traceroute, view running config, view IOS **show** commands, and so on

For this book, we focus on the Unified Communications menu.

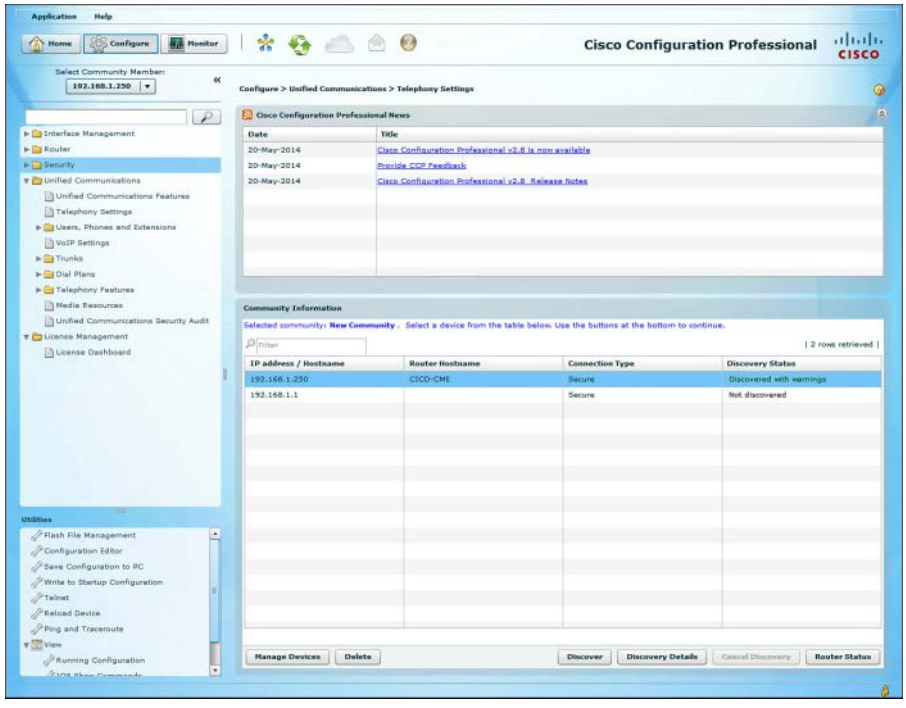


Figure 5-3 *The CCP Configure Menu*

CCP Unified Communications Configuration

We have already set up the Unified Communications features in Chapter 4, so the next entry for us to work on is telephony settings. On this screen, we identify what kinds of IP phones we will be using (SCCP, SIP, or both), in addition to how many of them and how many extensions as well. These settings are related to your licensing limits but have additional important implications because the router will reserve RAM memory for the number of phones you specify, so you will want to be accurate with your selections. In Figure 5-4, you can see that we have also selected the date and time format, the source IP address/interface for telephony signaling packets, and the secondary dial tone digit (which you may recognize as "Dial 9 for an outside line").

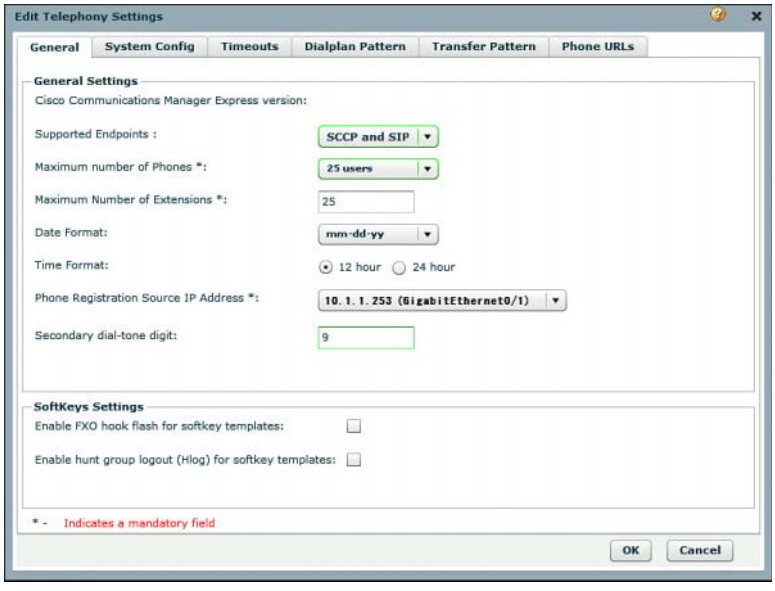


Figure 5-4 *The CCP Telephony Settings Screen*

Implementing End Users and Endpoints in CME

Key Topic

For the CME router to properly register and operate phones, we must identify the phone firmware files that each type of phone should load and which the TFTP service should therefore serve. We perform this action on the User, Phones and Extensions > Templates and Firmware > Phone Firmware screens. The Launch Wizard button starts a dialog which guides you through one of three choices:

1. Selecting and configuring firmware files already located in the router flash
2. Uploading firmware files from your local PC to flash and configuring them
3. Uploading firmware files from your local PC to flash without configuring them

CCP generates the necessary commands to specify the firmware load for each model of phone you specify and the TFTP and alias commands to allow the phones to download them when they attempt to register. Figure 5-5 shows the second option in use.

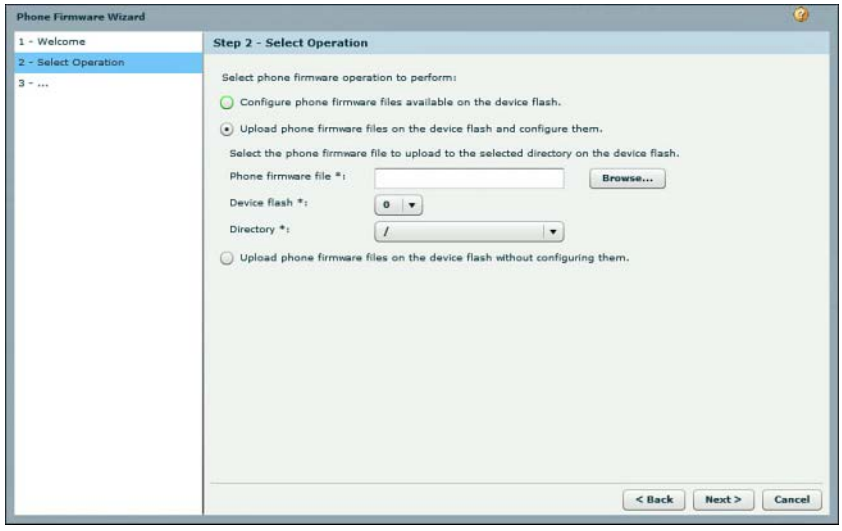


Figure 5-5 *The Phone Firmware Wizard*

Our next step is to create extensions. Remember that an extension (ephone-dn) is not just a number you can call; it also provides one of the associations for an end user as well as several other configuration options. Figure 5-6 shows the creation of extension 2002. Note that we have identified the username of Gord Downie for the extension, but the user association is not complete until we create a phone for Gord and associate the extension to it.

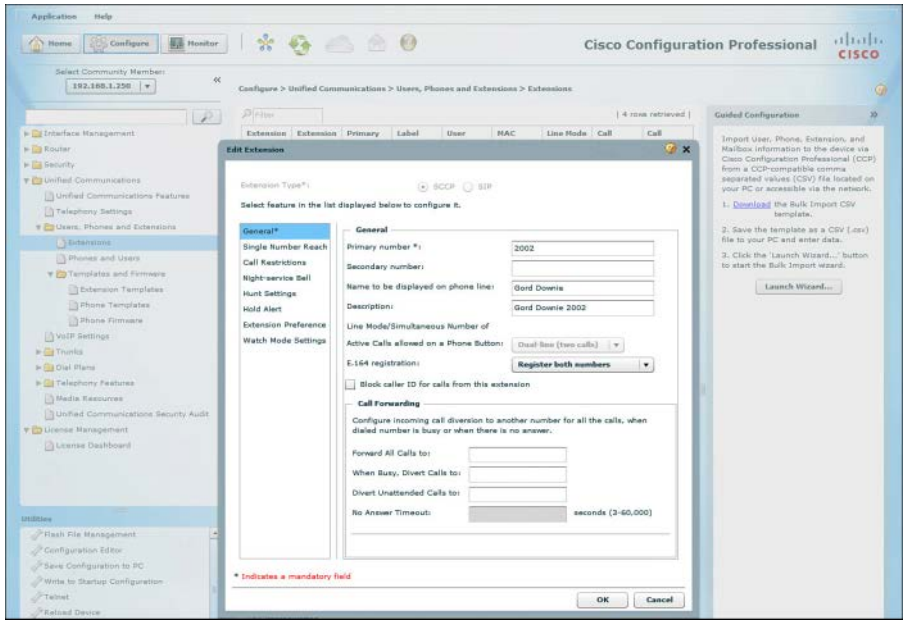


Figure 5-6 *Creating an Extension*

Now that we have extension 2002 defined for Gord Downie, we should make a phone for him and associate it to the extension. From the Phones and Users screen, select **Create** and enter the protocol, model, and MAC address for the new phone. From the list of extensions at the lower left, select the appropriate entry (2002 in this case) and move it to the Associated Extensions column by clicking the right arrow. Figure 5-7 shows this step completed.

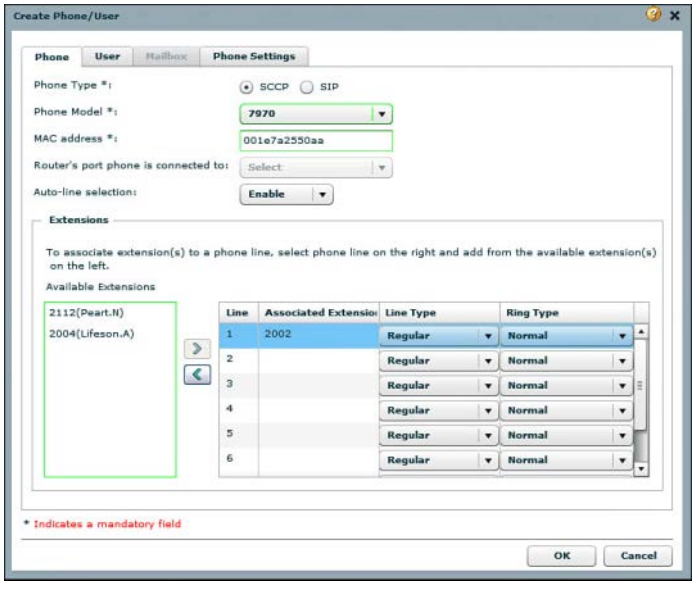


Figure 5-7 *Creating a Phone*

Next, we switch to the User tab. This is where we create the end user; note that in doing so on the Phone configuration screens, we automatically associate the user with the phone. Figure 5-8 shows us creating the end user, leaving the PIN and password blank. (The other drop-down option is Use Custom Password [PIN] Below.) Complete the phone and user creation operation by clicking **OK**.

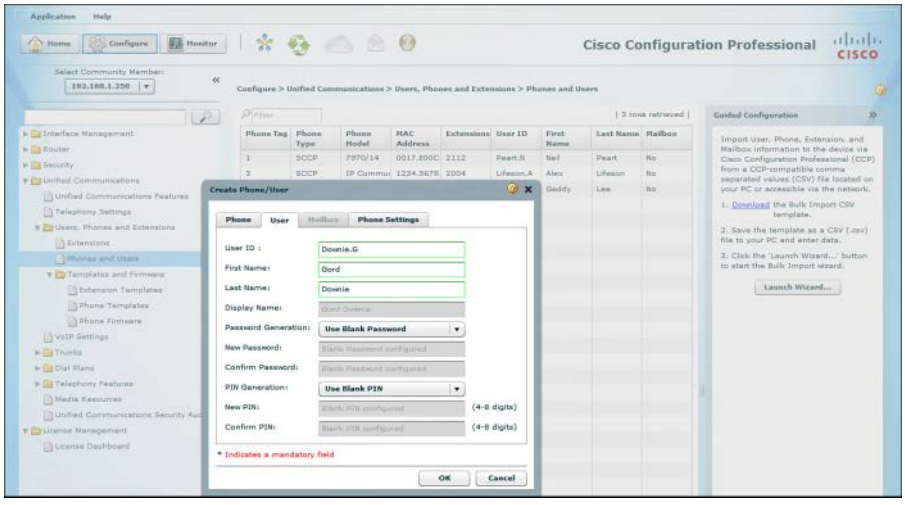


Figure 5-8 *Creating an End User Associated with the Phone*

That covers the learning objectives for provisioning end users and endpoints in CME.

We have implemented the required configuration to allow us to use the built-in GUI and CCP to create extensions, phones, and users and to associate users to phones and extensions. We have also set up the CME router to support phones with the correct firmware and TFTP commands. At this point, you should be able to ring phones, look at the directory, and see the internal calling name for IP phone-to-IP phone calls.

Note For those of you using this book as a step-by-step guide to setting up your voice lab to study for the exam, remember that CME is and always will be a CLI environment at heart. It is not unusual. Let's go one further and say it is *typical*—to need the CLI to get CME up and running. Whether this is due to your operating system settings, browser brand or version, or Java or other software or configuration is a separate issue, the objective for the exam is to learn what CCP can do and how. If you have to jump-start your CCP install using the CLI to get it running, do it.

Exam Preparation Tasks

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

Review All Key Topics

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

Key Topic

Table 5-3 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
Section	User access levels in CME	100
Section	Relationship between users, phones, and extensions	103
Section	Implementing end users and endpoints in CME	107

5

Complete the Tables from Memory

Table 5-4 is a study aid we call a "memory table." Print a copy of Appendix D, "Memory Tables" (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Table 5-4 Memory Table: CME User and Endpoint Concepts

Component	CME Element
IP phone model and MAC using SCCP	ephone
Extension assigned to a SCCP IP phone	ephone-dn
Extension assigned to IP phone using SIP	voice register dn
IP phone model and MAC using SIP	voice register pool
Three of the steps required to access the CME built-in GUI	Download and extract GUI files to flash; set IP HTTP path; define web admin account; enable dn-webedit and time-webedit
Three user access levels in CME	System admin, customer admin, ordinary/end user

Define Key Terms

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

ephone, ephone-dn, voice register global, voice register pool, voice register dn, system admin, customer admin, telephony service

This chapter covers the following topics:

- **Configuring Physical Voice Port Characteristics:** According to the OSI model, the physical layer is where it all begins. Similarly, some basic voice-port configuration items can prove essential to setting up your connections to the legacy voice environment. This section breaks down the key commands used in analog and digital voice connections.
- **Understanding and Configuring Dial Peers:** If there were one most important topic for all things related to voice in CME, this would be it. Dial peers define the "routing table" for your voice calls. This section discusses the configuration of both POTS and VoIP dial peers through many practical examples.
- **Understanding Router Call Processing and Digit Manipulation:** Even the simplest of all VoIP environments need to modify dialed digits or caller ID information for incoming and outgoing calls. This section breaks down the core digit-manipulation commands and explores the flow of a typical CME-handled call.
- **Understanding and Implementing CME Class of Restriction:** Just like you can use access lists to secure the data plane of your router, COR lists secure access to dialed numbers in your VoIP environment. This section discusses the concepts and configuration of COR lists.

CHAPTER 6

Understanding the CME Dial Plan

Connecting a voice gateway to another voice network is similar to connecting a router to a data network: Plugging in the cable is the easiest part of the configuration. After the physical connections are in place, the router configuration begins. Instead of routing tables, voice gateways build the logical dial plan through a system of dial peers. This chapter explores the configuration and testing of dial peers in a voice environment.

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

Foundation Topics Section	Questions Covered in This Section
Configuring Physical Voice Port Characteristics	1–2
Understanding and Configuring Dial Peers	3–6
Understanding Router Call Processing and Digit Manipulation	7–9
Understanding and Implementing CME Class of Restriction	10

1. Which of the following interface types would you use to connect an analog fax machine to the VoIP network?
   a. FXS
   b. FXO
   c. E&M
   d. BRI
2. Which of the following commands would you use to configure a T1 line to use channels 1 through 6 to connect to the PSTN using FXO loop start signaling?
   a. **pri-group 1-6 type fxo-loop-start**
   b. **pri-group 1 timeslots 1-6 type fxo-loop-start**
   c. **ds0-group 1-6 type fxo-loop-start**
   d. **ds0-group 1 timeslots 1-6 type fxo-loop-start**

3. You want to configure a dial peer to connect to a PBX system using a digital T1 CAS configuration. What type of dial peer would you create?
   a. Analog
   b. Digital
   c. POTS
   d. VoIP

4. You have the following configuration entered on your voice router:

   dial-peer voice 99 pots

   destination-pattern 115.

   port 1/0/0

   A user dials the number 1159. What digits does the router send out the port 1/0/0?
   a. 1159
   b. 115
   c. 11
   d. 59
   e. 9

5. What is the default codec used by a VoIP dial peer?
   a. G.711 μ-law
   b. G.711 a-law
   c. G.723
   d. G.729

6. Which of the following destination patterns could you use to match any dialed number up to 32 digits in length? (Choose two.)
   a. .+
   b. [0-32]
   c. T
   d. &

7. After you create a translation rule, how is it applied?
   a. To an interface
   b. To a translation profile
   c. Globally
   d. To a dial peer

8. Which of the following digit manipulation commands will work under a VoIP dial peer?
   a. **prefix**
   b. **forward-digits**
   c. **translation-profile**
   d. **digit-strip**
9. What is the final method used by a router to match an inbound dial peer for incoming calls?
   a. Using the **answer-address** command
   b. Using **dial peer 0**
   c. Using the **port** command
   d. Using the **destination-pattern** command
10. If an ephone-dn lacks an incoming COR list and attempts to dial a dial peer assigned an outgoing COR list, what behavior occurs?
    a. CME denies the call.
    b. CME permits the call.
    c. The call is rerouted to the next dial peer without an outgoing COR list.
    d. CME disables the ephone-dn lacking an incoming COR list.
11. You are considering using CCP to create COR configurations. Which of the following is true?
    a. CCP cannot configure COR; you must use the CLI.
    b. CCP creates partitions and search spaces at the command line, based on the entries made in the CCP GUI.
    c. CCP uses a single interface to create both incoming and outgoing COR lists.
    d. CCP implements forced authorization codes (FACs) for each call when you implement COR configurations; consequently, every call to the PSTN requires a FAC.

Foundation Topics

Configuring Physical Voice Port Characteristics

Before you can dive fully into the configuration of dial plans using dial peers, you must first think about the physical characteristics of the voice ports on the router. Obviously, the voice ports plug into cables, which eventually connect to far-end devices. Beyond that, you can tune a few additional settings on the router to allow the voice ports to operate exactly to your specification. This section divides the discussion of these configurations into analog and digital forms.

I've made a slight departure from the usual plan for this chapter; instead of moving all the command-line interface (CLI) info to the appendix, I have left most of the config here in the chapter. This is partly because it is important and deserves a full explanation, partly because having the explanation right in context with the CLI makes it easier to understand, and partly because it just made the chapter work better. Even if some of these concepts are not explicitly identified in the exam blueprint, they are fundamentally important to how CME works—and as always, the exam content could change at any time.

Configuring Analog Voice Ports

In a way similar to Ethernet, when you connect a cable to an analog voice port on a router, it just works (provided a signal is coming from the other end). The router receives the electrical signals from the line and processes them normally. In addition to normal call processing, each interface type has a few settings you can tune to change the way it operates with the other end of the connection. This section describes configuration options for foreign exchange station (FXS) ports and foreign exchange office (FXO) ports.

FXS Ports

FXS ports connect to end stations—that is, typical analog devices such as telephones, fax machines, and modems (shown in Figure 6-1).

Key Topic

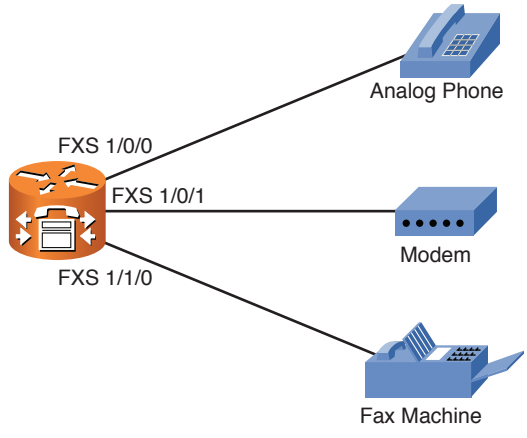


Figure 6-1 *FXS Port Connections*

When you are ready to configure your FXS voice ports, the best place to start is to find out what voice ports your router is equipped with. You can do this quickly by using the **show voice port summary** command, as shown in Example 6-1.

Example 6-1 *Identifying Voice Ports Using* **show voice port summary**

```
CICD-CME# show voice port summary
                                                          IN                OUT
PORT              CH      SIG-TYPE ADMIN   OPER    STATUS   STATUS    EC
==========        ==      ======== =====   ====    ======== ========        ==
0/0/0             --      fxs-ls   up      dorm    on-hook  idle            y
0/0/1             --      fxs-ls   up      dorm    on-hook  idle            y
0/2/0             --      fxo-ls   up      dorm    idle             on-hook y
0/2/1             --      fxo-ls   up      dorm    idle             on-hook y
0/2/2             --      fxo-ls   up      dorm    idle             on-hook y
0/2/3             --      fxo-ls   up      dorm    idle             on-hook y
```

Note If you are using your router for Cisco Unified Communication Manager Express (CME), each ephone-dn you configure shows up under the **show voice port summary** output as an EXFS port.

Based on the output from Example 6-1, you can see that this router is equipped with two FXS ports and four FXO ports.

FXS ports have three common areas of configuration:

- Signaling
- Call progress tones
- Caller ID information

You can use two types of signaling for analog FXS interfaces: ground start and loop start. The signal type dictates the method used by the attached device to signal that a phone is going off-hook. Table 6-2 briefly describes the differences between ground start and loop start signaling.

Table 6-2 Comparing Ground Start and Loop Start

Ground Start	Loop Start
Signals a new connection by grounding two of the wires in the cable temporarily	Signals by completing a circuit (by lifting the handset off-hook) and dropping the total DC voltage down on the line
Must be configured	Is the default
Typically used when connecting to PBX equipment	Typically used when connecting to analog devices, such as telephones, fax machines, and modems

If you have traveled to other countries, you probably noticed that phones sound different in different parts of the world. Based on your geographical location, dial tones might be higher or lower and busy signals might be fast or slow. These are all considered call progress tones: audio signals that inform the caller how the call is progressing. By default, the FXS port of your router uses the call progress tones from the United States. If your router is serving another part of the world, use the command shown in Example 6-2 to adjust the call progress tones.

Example 6-2 *Adjusting Call Progress Tones*

```
CICD-CME(config)# voice-port 0/2/0
CICD-CME(config-voiceport)# cptone ?
  locale   2 letter ISO-3166 country code

AR Argentina            IN India                PA Panama
AU Australia            ID Indonesia            PE Peru
AT Austria              IE Ireland              PH Philippines
BE Belgium              IL Israel               PL Poland
BR Brazil               IT Italy                PT Portugal
CA Canada               JP Japan                RU Russian Federation
CL Chile                JO Jordan               SA Saudi Arabia
CN China                KE Kenya                SG Singapore
CO Colombia             KR Korea Republic       SK Slovakia
C1 Custom1              KW Kuwait               SI Slovenia
C2 Custom2              LB Lebanon              ZA South Africa
CY Cyprus               LU Luxembourg           ES Spain
CZ Czech Republic       MY Malaysia             SE Sweden
DK Denmark              MT Malta                CH Switzerland
EG Egypt                MX Mexico               TW Taiwan
FI Finland              NP Nepal                TH Thailand
FR France               NL Netherlands          TR Turkey
DE Germany              NZ New Zealand          AE United Arab Emirates
GH Ghana                NG Nigeria              GB United Kingdom
GR Greece               NO Norway               US United States
HK Hong Kong            OM Oman                 VE Venezuela
HU Hungary              PK Pakistan             ZW Zimbabwe
IS Iceland
```

Simply enter the two-digit country code to change the sound of all the progress tones on the device attached to the FXS port.

Finally, you can use the syntax shown in Example 6-3 to configure caller ID information for the device attached to the FXS port.

Example 6-3 *Configuring FXS Port Caller ID Information*

```
CME_Voice(config)# voice port 0/0/0
CME_Voice(config voiceport)# station-id name 3rd Floor Fax
CME_Voice(config voiceport)# station-id number 5551000
```

This configuration allows other devices in your system to receive caller ID name and number information any time the device attached to the FXS port places a call to them.

FXO Ports

FXO ports act as a trunk to the public switched telephone network (PSTN) central office (CO) or private branch exchange (PBX) systems, as shown in Figure 6-2.

Key Topic

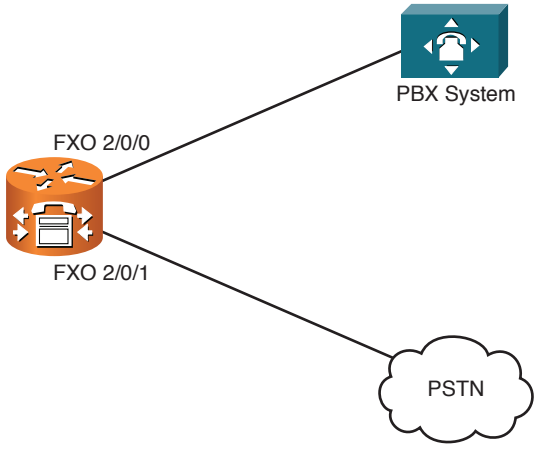


Figure 6-2 *FXO Port Connections*

FXO ports use many of the same commands as FXS ports, such as **signal** to set loop start or ground start signaling and **station-id** to set caller ID information. Two additional commands are of note:

- **dial-type**
- **ring number**

The **dial-type** *dtmf/pulse* command allows you to choose to use dual-tone multifrequency (DTMF) or pulse dialing. (Yes, some areas of the world still require the use of pulse dialing and rotary-dial phones. If you are installing a voice network into one of these areas, this command is for you.

The **ring number** *number* command allows you to specify the number of rings that should pass before the router answers an incoming call to the FXO port. By default, this is set to one ring, which causes the router to answer an incoming call immediately. There might be instances where the FXO port of the router is attached to a loop of other devices (such as in a home office environment) and the user wants the other devices to have a chance to answer the call before the router picks up the line and processes it. In this case, you can set the ring number to a higher value.

Configuring Digital Voice Ports

Cisco provides digital T1 and E1 ports in the form of voice and WAN interface cards (VWICs) for routers. These cards offer you the flexibility to configure them for a data connection or a voice connection. Unlike analog interfaces, you must configure digital interfaces before they will operate correctly because the router does not know the type of network you will be using. As discussed in Chapter 1, "Traditional Voice Versus Unified Voice," two types of voice network configurations exist: T1/E1 channel associated signaling (CAS) or common channel signaling (CCS), commonly referred to as ISDN Primary Rate Interface (PRI). The type of network to which you are connecting dictates the command you use to configure your VWIC card: **ds0-group** for T1/E1 CAS connections or **pri-group** for T1/E1 CCS connections.

Example 6-4 demonstrates how to configure all 24 channels of a T1 CAS interface to connect to a PSTN carrier.

Example 6-4 *Configuring a T1 CAS PSTN Interface*

```
CME_Voice# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CME_Voice(config)# controller t1 1/0
CME_Voice(config-controller)# framing ?
Esf   Extended Superframe
Sf    Superframe

CME_Voice(config-controller)# framing esf
CME_Voice(config-controller)# linecode ?
ami     AMI encoding
8zs     B8ZS encoding
CME_Voice(config-controller)# linecode b8zs
CME_Voice(config-controller)# clock source ?
free-running     Free Running Clock
internal         Internal Clock
line             Recovered Clock

CME_Voice(config-controller)# clock source line
CME_Voice(config-controller)# ds0-group ?
<0-23>   Group Number
CME_Voice(config-controller)# ds0-group 1 ?
timeslots   List of timeslots in the ds0-group
CME_Voice(config-controller)# ds0-group 1 timeslots ?
<1-24>   List of T1 timeslots
CME_Voice(config-controller)# ds0-group 1 timeslots 1-24 ?
type   Specify the type of signaling
<cr>
CME_Voice(config-controller)# ds0-group 1 timeslots 1-24 type ?
e&m-delay-dial        E & M Delay Dial
e&m-fgd               E & M Type II FGD
```

```
e&m-immediate-start   E & M Immediate Start
e&m-lmr               E & M land mobil radio
e&m-wink-start        E & M Wink Start
ext-sig               External Signaling
fgd-eana              FGD-EANA BOC side
fxo-ground-start      FXO Ground Start
fxo-loop-start        FXO Loop Start
fxs-ground-start      FXS Ground Start
fxs-loop-start        FXS Loop Start
none                  Null Signalling for External Call Control
<cr>

CME_Voice# show voice port summary
                                              IN       OUT
PORT    CH   SIG-TYPE    ADM OPER  STATUS   STATUS   EC
======  ==   ========    ========  ======   ======    ==
1/0:1   01   fxo-ls      up  down  idle     on-hook   y
1/0:1   02   fxo-ls      up  down  idle     on-hook   y
1/0:1   03   fxo-ls      up  down  idle     on-hook   y
1/0:1   04   fxo-ls      up  down  idle     on-hook   y
1/0:1   05   fxo-ls      up  down  idle     on-hook   y
1/0:1   06   fxo-ls      up  down  idle     on-hook   y
1/0:1   07   fxo-ls      up  down  idle     on-hook   y
1/0:1   08   fxo-ls      up  down  idle     on-hook   y
1/0:1   09   fxo-ls      up  down  idle     on-hook   y
1/0:1   10   fxo-ls      up  down  idle     on-hook   y
1/0:1   11   fxo-ls      up  down  idle     on-hook   y
1/0:1   12   fxo-ls      up  down  idle     on-hook   y
1/0:1   13   fxo-ls      up  down  idle     on-hook   y
1/0:1   14   fxo-ls      up  down  idle     on-hook   y
1/0:1   15   fxo-ls      up  down  idle     on-hook   y
1/0:1   16   fxo-ls      up  down  idle     on-hook   y
1/0:1   17   fxo-ls      up  down  idle     on-hook   y
1/0:1   18   fxo-ls      up  down  idle     on-hook   y
1/0:1   19   fxo-ls      up  down  idle     on-hook   y
1/0:1   20   fxo-ls      up  down  idle     on-hook   y
1/0:1   21   fxo-ls      up  down  idle     on-hook   y
1/0:1   22   fxo-ls      up  down  idle     on-hook   y
1/0:1   23   fxo-ls      up  down  idle     on-hook   y
1/0:1   24   fxo-ls      up  down  idle     on-hook   y
```

There are many commands to discuss in Example 6-4; you can verify your own router's T1 card setup with the **show controllers t1** command. This command enables you to identify the T1 interfaces on your router. These interfaces do not appear in the **show ip interface brief** output because the router does not know whether you will configure the interface as a voice or data connection (that is, whether it will end up with an IP address). After you

interface, you can then configure the necessary **framing** and **linecode** commands. These commands let you change how the T1 or E1 interface formats the frames it sends to the service provider. Set these values based on information received from the service provider to which you are connecting.

Note If you are in the United States, most service providers use extended super frame (ESF) framing and B8ZS linecoding.

After you set the framing and linecoding, you can set clocking. The command **clock source line** instructs the router to receive its interface clocking from the service provider. If you are connecting to a PSTN carrier, this is the norm. If your router is connecting to a PBX system inside your company, you can enter the command **clock source internal**, which allows the router to provide clocking information to the PBX system.

Finally, the **ds0-group** command configures the line as a T1 CAS connection and allows you to enter the specific number of time slots you want to provision. In Example 6-5, all 24 time slots are provisioned under DS0 group 1. You can choose any value from 0 to 23 for the group number. This value acts as an identifier for the time slots you place into it. You can provision a single T1 line for many different purposes. For example, you could create DS0 group 5 with time slots 1–5 that connect to an onsite PBX system. You could then create DS0 group 6 using time slots 6–24 that connect to the PSTN (provided the PBX system and PSTN carrier are provisioned for these same time slot settings). Figure 6-3 illustrates the physical design of this network type.

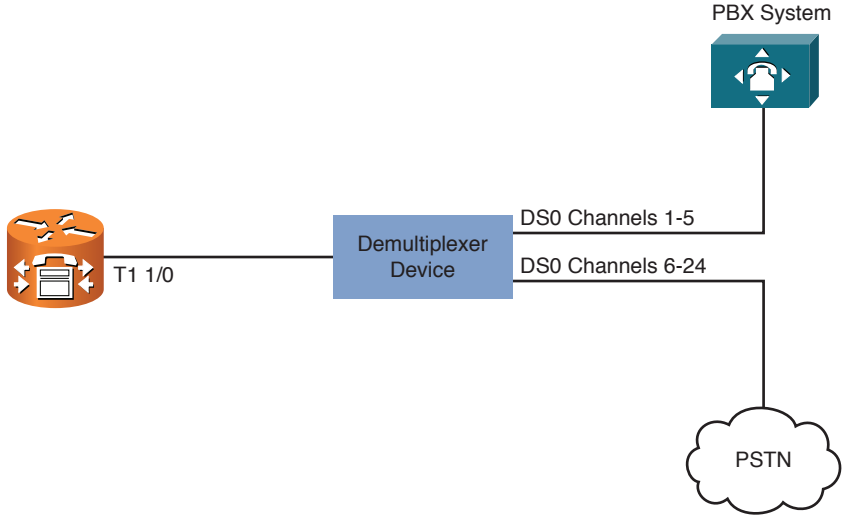


Figure 6-3 *Provisioning Multiple Connections with a Single T1 Interface*

Note The demultiplexing device shown in Figure 6-3 allows you to break the single T1 interface into multiple interfaces with specific channel assignments.

Notice that the **ds0-group** command also allows you to set the signaling type. This gives you the ability to connect to many different network types. A PSTN carrier typically uses FXO loop start signaling over the T1 CAS connection. (This might differ depending on your location and service provider.) PBX systems often support one of the various Ear and Mouth (E&M) signaling types.

After you enter the **ds0-group** command, the router automatically creates a voice port for each time slot you provision, as you can see from the **show voice port summary** output in Example 6-4. The port is listed as 1/0:1 because 1/0 represents the physical interface and the additional 1 represents the DS0 group number. Make a note of this port identifier because you need it to configure the dial peers. Each port listed represents a different channel on the T1 interface.

The digital T1/E1 interface for a CCS (ISDN PRI) PSTN connection is configured using similar syntax to the CAS. Example 6-5 demonstrates a configuration that provisions all 24 time slots of a VWIC interface as a PRI PSTN connection.

Example 6-5 *Configuring a T1 CCS PSTN Interface*

```
CME_Voice(config)# isdn switch-type ?
primary-4ess    Lucent 4ESS switch type for the U.S.
primary-5ess    Lucent 5ESS switch type for the U.S.
primary-dms100  Northern Telecom DMS-100 switch type for the U.S.
primary-dpnss   DPNSS switch type for Europe
primary-net     5NET5 switch type for UK, Europe, Asia and Australia
primary-ni      National ISDN Switch type for the U.S.
primary-ntt     NTT switch type for Japan
primary-qsig    QSIG switch type
primary-ts014   TS014 switch type for Australia (obsolete)
CME_Voice(config)# isdn switch-type primary-5ess
CME_Voice(config)# controller t1 1/0
CME_Voice(config-controller)# pri-group ?
nfas_d   Specify the operation of the D-channel timeslot.
service   Specify the service type
timeslots List of timeslots in the pri-group
<cr>
CME_Voice(config-controller)# pri-group timeslots ?
<1-24>  List of timeslots which comprise the pri-group
CME_Voice(config-controller)# pri-group timeslots 1-24 ?
nfas_d   Specify the operation of the D-channel timeslot.
service  Specify the service type Specify the service type
CME_Voice(config-controller)# pri-group timeslots 1-24
CME_Voice(config-controller)#^Z

CME_Voice# show voice port summary
                                     IN      OUT
PORT    CH   SIG-TYPE    ADM   OPER  STATUS  STATUS  EC
======  ==   ========    ===  =====  ======  ======   ==
```

```
1/0:23  01   isdn-voice  up   dorm   none    none    y
1/0:23  02   isdn-voice  up   dorm   none    none    y
1/0:23  03   isdn-voice  up   dorm   none    none    y
1/0:23  04   isdn-voice  up   dorm   none    none    y
1/0:23  05   isdn-voice  up   dorm   none    none    y
1/0:23  06   isdn-voice  up   dorm   none    none    y
1/0:23  07   isdn-voice  up   dorm   none    none    y
1/0:23  08   isdn-voice  up   dorm   none    none    y
1/0:23  09   isdn-voice  up   dorm   none    none    y
1/0:23  10   isdn-voice  up   dorm   none    none    y
1/0:23  11   isdn-voice  up   dorm   none    none    y
1/0:23  12   isdn-voice  up   dorm   none    none    y
1/0:23  13   isdn-voice  up   dorm   none    none    y
1/0:23  14   isdn-voice  up   dorm   none    none    y
1/0:23  15   isdn-voice  up   dorm   none    none    y
1/0:23  16   isdn-voice  up   dorm   none    none    y
1/0:23  17   isdn-voice  up   dorm   none    none    y
1/0:23  18   isdn-voice  up   dorm   none    none    y
1/0:23  19   isdn-voice  up   dorm   none    none    y
1/0:23  20   isdn-voice  up   dorm   none    none    y
1/0:23  21   isdn-voice  up   dorm   none    none    y
1/0:23  22   isdn-voice  up   dorm   none    none    y
1/0:23  23   isdn-voice  up   dorm   none    none    y
```

When configuring a CCS connection, the first step is to set the ISDN switch type to match the type of switch your local service provider is using. Example 6-5 sets this to **primary-5ess**. After you configure the switch type, the router allows you to enter the **pri-group** command. This works identically to the **ds0-group** command in that it allows you to provision a specific number of time slots for use with the PSTN carrier. This command does not allow you to select a signaling type because the router assumes ISDN PRI signaling.

Note This example assumes you have enough digital signal processor (DSP) resources to support a full PRI connection. If your router does not have enough DSPs, it displays an error message when you try to use the **pri-group** command. The error message says exactly how many channels the router can support.

After you enter the **pri-group** command, the router creates 24 ISDN voice ports that it will use for incoming and outgoing voice calls. This is verified with the **show voice port summary** command. Notice that the voice port is labeled with the identifier 1/0:23. This represents channel 23 (time slot 24) of the T1 ISDN PRI connection (channels are listed from 0–23, whereas time slots are listed 1–24), which is the dedicated signaling channel used to bring up the other 23 voice bearer channels.

Key Topic

Note When using T1 interfaces, channel 23 (time slot 24) is always the signaling channel. When using E1 interfaces, channel 16 (time slot 17) is always the signaling channel.

As before, make a note of this port identifier for the ISDN circuit. The router requires you to identify this interface when configuring your dial peers.

Understanding and Configuring Dial Peers

When you studied CCNA Routing and Switching, you learned about the concept of static routing. This method of routing allows you to manually enter destination networks that the router is able to reach on the data network. Dial peers use a concept similar to this; think of dial peers as static routes for your voice network. By default, the CME router only knows how to reach the ephone-dns you configure for the Cisco IP phones. You can connect the CME router to any number of FXS, FXO, or digital T1/E1 connections, but until you create dial peers for these connections, the router will not know how to use them.

Dial peers define voice reachability information. Simply put, these are the phone numbers you can dial. For example, you might connect an analog phone to the FXS port of the router. As soon as you make the connection, the analog phone receives a dial tone and is able to place calls. However, no one will be able to call the analog phone because it does not yet have a phone number—more accurately, because the router does not have a number to match to the FXS port to which the phone is connected. Using a dial peer, you can assign one or more phone numbers to this analog device. Furthermore, dial peers allow you to use wildcards to define ranges of phone numbers. This is useful when you want to define large groups of numbers available from a destination such as a PBX system or PSTN connection.

You can create two primary types of dial peers:

Key Topic

- **Plain old telephone service (POTS) dial peer:** Defines voice reachability information for any traditional voice connection (that is, any device connected to an FXS, FXO, E&M, or digital voice port)
- **Voice over IP (VoIP) dial peer:** Defines voice reachability information for any VoIP connection (that is, any device that is reachable through an IP address)

Figure 6-4 illustrates the placement of POTS and VoIP dial peers in a network.

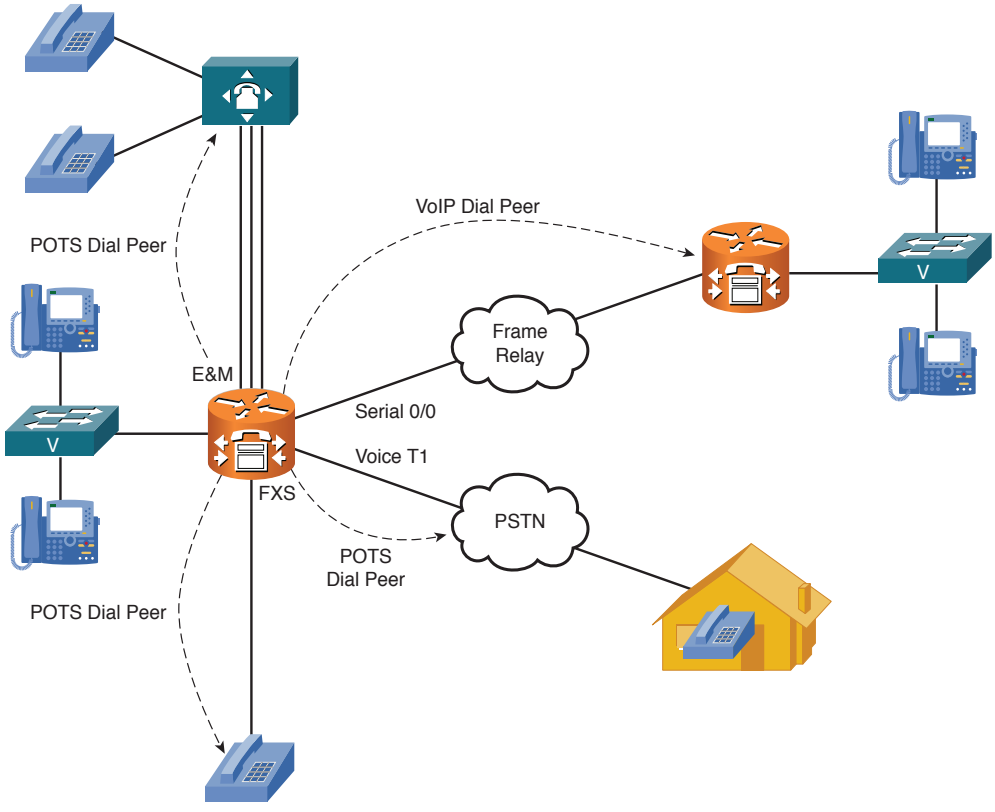


Figure 6-4 *POTS and VoIP Dial Peers*

Voice Call Legs

To accurately configure dial peers, you must first understand the concept of call legs. A call leg represents a connection to or from a voice gateway from a POTS or VoIP source. Figure 6-5 illustrates an example voice connection scenario.

Key Topic

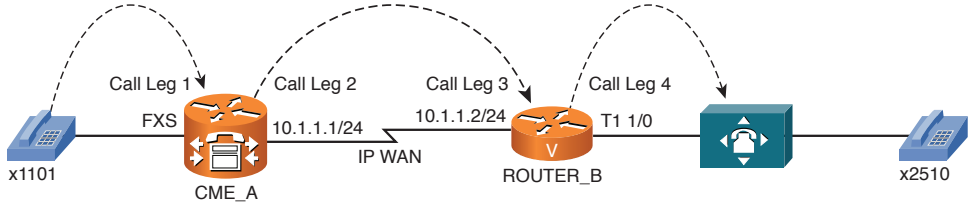


Figure 6-5 *Voice Connection Call Legs*

As illustrated in Figure 6-5, the phone on the left (extension 1101) makes a call to the phone on the right (extension 2510). For this call to pass through successfully, four call legs must exist:

- **Call leg 1:** The incoming POTS call leg from x1101 on CME_A
- **Call leg 2:** The outgoing VoIP call leg from CME_A to ROUTER_B
- **Call leg 3:** The incoming VoIP call leg on ROUTER_B from CME_A
- **Call leg 4:** The outgoing POTS call leg to x2510 from ROUTER_B

If the call were placed in the opposite direction (from x2510 to x1101), the same number of call legs would be needed, but in reverse. So, to provide a two-way calling environment that enables x1101 to call x2510 and vice versa, you need to configure a total of eight call legs.

It is critical to understand the concept of call legs to properly configure the dial peers on your router. Each call leg identified in Figure 6-5 represents a dial peer that must exist on your router. These dial peers define not only the reachability information (phone numbers) for the devices, but also the path the audio must travel. From CME_A's perspective, it receives audio from x1101 on an FXS port (call leg 1). CME_A must then pass that voice information over the IP network to 10.1.1.2 (call leg 2). From ROUTER_B's perspective, it receives a call from x1101 on the IP WAN network (call leg 3). It must then take that call and pass it to the PBX system out the digital T1 1/0 interface (call leg 4).

As you can see from Figure 6-5, call legs are matched on both the inbound and outbound directions. In the same way, you must configure dial peers to match voice traffic in both the inbound and outbound directions. In some cases, you can use a single dial peer for bidirectional traffic. For example, creating a single POTS dial peer for x1101 will match incoming and outgoing calls to x1101. At other times, you must create more than one dial peer for inbound and outbound traffic. For example, CME_A requires an outbound VoIP dial peer to send the call to ROUTER_B (10.1.1.2). ROUTER_B needs an inbound VoIP dial peer to receive the call from CME_A. As you see the multiple examples of dial peers in the upcoming sections, these concepts become clearer.

Note Keep in mind, the engine behind all this is the DSP resources in the CME router. These workhorses convert the analog audio to digital (VoIP packets), and vice versa. If the CME routers did not have any DSP resources, this conversion would not be possible.

Configuring POTS Dial Peers

As previously mentioned, you can use POTS dial peers to define reachability information for anything connected to your VoIP network from the traditional telephony world. This includes devices connected to FXO, FXS, E&M, and digital BRI/T1/E1 interfaces.

Tip If you are connecting to something that does not have an IP address (such as an analog phone, fax machine, PBX, or the PSTN), it is a POTS dial peer.

The network in Figure 6-6 demonstrates the configuration of POTS dial peers.

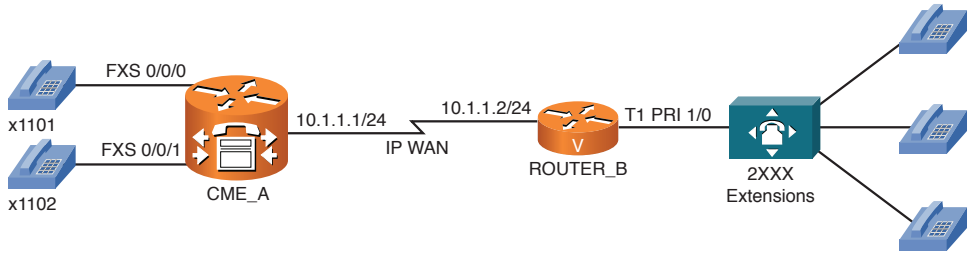


Figure 6-6 *Dial Peer Configuration Scenario*

The configuration begins with the CME_A router. To create POTS dial peers, you can use the syntax **dial-peer voice** *tag* **pots** from global configuration mode. The *tag* value can be any number you want (from 1 to 2,147,483,647), as long as it is unique on the router. Although this tag does not have any impact on the reachability information you assign to the devices, many administrators have a common practice of relating a dial peer tag value to the phone number of the device. Example 6-6 assigns the extensions shown in Figure 6-6 to the analog phones attached to the CME_A router's FXS ports.

Key Topic

Example 6-7 *Configuring POTS Dial Peers for FXS Ports*

```
CME_A(config)# dial-peer voice ?
  <1-2147483647>  Voice dial-peer tag
CME_A(config)# dial-peer voice 1101 ?
    mmoip    Multi Media Over IP
    pots                Telephony
    vofr                Voice over Frame Relay
    voip                Voice over IP
CME_A(config)# dial-peer voice 1101 pots
CME_A(config-dial-peer)# destination-pattern ?
    WORD    A sequence of digits - representing the prefix or full telephone number
CME_A(config-dial-peer)# destination-pattern 1101
CME_A(config-dial-peer)# port 0/0/0
CME_A(config-dial-peer)# exit
CME_A(config)# dial-peer voice 1102 pots
CME_A(config-dial-peer)# destination-pattern 1102
CME_A(config-dial-peer)# port 0/0/1
```

After you create the dial peer, you can then assign the phone number to the attached devices by using the **destination-pattern** and **port** commands. After you enter this configuration, you can place calls between the phones attached to the CME_A router. Before you place any calls, it is always best to verify the dial peer configuration.

Tip After a dial peer is created, you no longer need to specify the type of dial peer when entering the configuration mode. For example, to create a VoIP dial peer with tag 50, you enter **dial-peer voice 50 voip**. If you want to return to the configuration mode later, you need only enter **dial-peer voice 50**. If you want to change the type of dial peer (VoIP or POTS), you must delete the dial peer (**no dial-peer voice 50**) and create it again.

The **show dial-peer voice** command (without the **summary** keyword) shows you all the dial peers on your router, but uses about a page of output for each dial peer. Although this information can be useful at times, the summary view, which is shown in Example 6-7, is usually much easier to digest. Notice at the bottom of the output are the dial peer tags 1101 and 1102, displayed as POTS dial peers with the proper destination pattern and port assignments. The other dial peers listed (with tags 20005–20014) are dial peers created by the CME router for ephone-dns configured previously.

Example 6-7 *Verifying Dial Peers*

```
CME_A# show dial-peer voice summary
dial-peer hunt 0
                AD-          PRE-  DEST-      PRE   PASS   SESS-   OUT-
TAG    TYPE  MIN OPER  FIX   PATTERN    FER   THRU   TARGET  STAT  PORT
=====  ====  === ====  ====  =======    ====  =====  ======  ====  ======
20005  pots  up  up          1500$      0                    5     0/0/20
20006  pots  up  up          1501$      0                    5     0/0/21
20007  pots  up  up          1502$      0                    5     0/0/22
20008  pots  up  up          1503$      0                    5     0/0/23
20009  pots  up  up          1504$      0                    5     0/0/24
20010  pots  up  up          1505$      0                    5     0/0/25
20011  pots  up  up          1506$      0                    5     0/0/26
20012  pots  up  up          1507$      0                    5     0/0/27
20013  pots  up  up          1508$      0                    5     0/0/28
20014  pots  up  up          1509$      0                    5     0/0/29
1101   pots  up  up          1101       0                    up    0/0/0
1102   pots  up  up          1102       0                    up    0/0/1
```

You can test the configuration by placing a call between the devices. Example 6-8 shows a useful **debug** command that you can use to see the router process the dialed digits from the phone attached to the FXS port.

Example 6-8 *Using* **debug voip dialpeer** *to Analyze Digit Processing*

```
CME_A# debug voip dialpeer
voip dialpeer default debugging is on
.Jul  2 17:16:44.698: //-1/77671F238035/DPM/dpMatchPeersCore:
Calling Number=, Called Number=1, Peer Info Type=DIALPEER_INFO_SPEECH
.Jul  2 17:16:44.698: //-1/77671F238035/DPM/dpMatchPeersCore:
Match Rule=DP_MATCH_DEST; Called Number=1
.Jul  2 17:16:44.698: //-1/77671F238035/DPM/dpMatchPeersCore:
Result=Partial Matches(1) after DP_MATCH_DEST
.Jul  2 17:16:44.702: //-1/77671F238035/DPM/dpMatchPeersMoreArg:
Result=MORE_DIGITS_NEEDED(1)
.Jul  2 17:16:45.114: //-1/77671F238035/DPM/dpMatchPeersCore:
Calling Number=, Called Number=11, Peer Info Type=DIALPEER_INFO_SPEECH
.Jul  2 17:16:45.114: //-1/77671F238035/DPM/dpMatchPeersCore:
Match Rule=DP_MATCH_DEST; Called Number=11
```

```
.Jul  2 17:16:45.114: //-1/77671F238035/DPM/dpMatchPeersCore:
Result=Partial Matches(1) after DP_MATCH_DEST
.Jul  2 17:16:45.114: //-1/77671F238035/DPM/dpMatchPeersMoreArg:
Result=MORE_DIGITS_NEEDED(1)
.Jul  2 17:16:45.914: //-1/77671F238035/DPM/dpMatchPeersCore:
Calling Number=, Called Number=110, Peer Info Type=DIALPEER_INFO_SPEECH
.Jul  2 17:16:45.914: //-1/77671F238035/DPM/dpMatchPeersCore:
Match Rule=DP_MATCH_DEST; Called Number=110
.Jul  2 17:16:45.914: //-1/77671F238035/DPM/dpMatchPeersCore:
Result=Partial Matches(1) after DP_MATCH_DEST
.Jul  2 17:16:45.914: //-1/77671F238035/DPM/dpMatchPeersMoreArg:
Result=MORE_DIGITS_NEEDED(1)
.Jul  2 17:16:46.426: //-1/77671F238035/DPM/dpMatchPeersCore:
Calling Number=, Called Number=1101, Peer Info Type=DIALPEER_INFO_SPEECH
.Jul  2 17:16:46.426: //-1/77671F238035/DPM/dpMatchPeersCore:
Match Rule=DP_MATCH_DEST; Called Number=1101
.Jul  2 17:16:46.426: //-1/77671F238035/DPM/dpMatchPeersCore:
Result=Success(0) after DP_MATCH_DEST
.Jul  2 17:16:46.426: //-1/77671F238035/DPM/dpMatchPeersMoreArg:
Result=SUCCESS(0)
List of Matched Outgoing Dial-peer(s):
1: Dial-peer Tag=1101
```

Notice the highlighted output from the **debug** command in Example 6-8. This shows the router performing digit-by-digit call processing. As the attached phone dials each digit, the router processes that digit and attempts to find a match from among its dial peer configuration. For the first three dialed digits, the result is clear: more digits needed. After the caller dials the fourth digit, the router matches dial peer tag 1101 and processes the call.

Now, we can turn our attention to the POTS dial peer configuration on ROUTER_B, which has a T1 PRI connection to a PBX system hosting 2XXX extensions (four-digit extensions beginning with the number 2). In the earlier section "Configuring Digital Voice Ports," the physical characteristics of the T1 VWIC interface were configured to support T1 PRI connectivity (by using the **pri-group** command). When that command was entered, the router automatically created the voice port 1/0:23, which represented the signaling channel of the T1 PRI connection. Example 6-9 now configures the router to use this T1 PRI port anytime it receives a call for a 2XXX extension.

Example 6-9 *Configuring a POTS Dial Peer for a T1 Interface*

```
ROUTER_B(config)# dial-peer voice 2000 pots
ROUTER_B(config-dial-peer)# destination-pattern 2...
ROUTER_B(config-dial-peer)# no digit-strip
ROUTER_B(config-dial-peer)# port 1/0:23
```

It's that simple. Notice that you can use the . wildcard to represent any dialed digit. This instructs the router to send all 2XXX extensions out port 1/0:23 (the T1 PRI interface). One

additional command in this example brings up a big point of discussion: **no digit-strip**. This command prevents the router from automatically stripping dialed digits from this dial peer. Now, why would the router do that? Because of the POTS dial peer rule Cisco programmed into Cisco IOS. Here's the rule.

Key Topic

Digit-Stripping Rule of POTS Dial Peers

The router automatically strips any explicitly defined digit from a POTS dial peer before forwarding the call.

An explicitly defined digit is any non-wildcard digit. In the case of Example 6-9, 2 is an explicitly defined digit. This rule is in place primarily to assist with stripping outside dialing codes before sending calls to the PSTN. For example, organizations commonly require users to dial 9 to access an outside line (often receiving a second dial tone after they have dialed 9). However, if you keep this access digit prepended to the dialed phone number, the PSTN carrier rejects the call. Therefore, if you create a POTS dial peer with the **destination-pattern 9.....** command (for seven-digit dialing), the router automatically strips the explicitly defined 9 digit before sending the call to the PSTN.

In the case of Example 6-9, stripping the 2 digit before sending the call to the PBX system is not a desired behavior. Thus, the **no digit-strip** command prevents this automatic digit-stripping process.

Note The automatic digit-stripping function is specific to POTS dial peers. VoIP dial peers (discussed in the following section) do not automatically strip digits.

Configuring VoIP Dial Peers

In the scenario shown in Figure 6-7, the POTS dial peers now provide connectivity to the legacy voice equipment. However, CME_A and ROUTER_B are divided by an IP WAN connection that the legacy voice equipment must cross to achieve end-to-end communication.

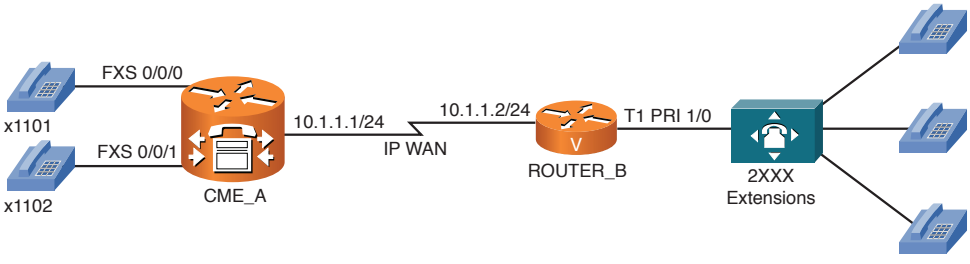


Figure 6-7 *Dial Peer Configuration Scenario*

To accomplish this connectivity, you must use VoIP dial peers because the call is crossing an IP-based network. Example 6-10 configures the necessary VoIP dial peers on the CME_A and ROUTER_B devices.

Key Topic

Example 6-10 *Configuring VoIP Dial Peers*

```
CME_A(config)# dial-peer voice 2000 voip
CME_A(config-dial-peer)# destination-pattern 2...
CME_A(config-dial-peer)# session target ?
  WORD  A string specifying the session target
CME_A(config-dial-peer)# session target ipv4:10.1.1.2
CME_A(config-dial-peer)# codec ?
        clear-channel  Clear Channel 64000 bps (No voice capabilities: data transport
only)
  g711alaw                    G.711 A Law 64000 bps
  g711ulaw                    G.711 u Law 64000 bps
  g722-48                     G722-48K 64000 bps - Only supported for H.320<->H.323
calls
  g722-56                     G722-56K 64000 bps - Only supported for H.320<->H.323
calls
  g722-64                     G722-64K 64000 bps - Only supported for H.320<->H.323
calls
  g723ar53                    G.723.1 ANNEX-A 5300 bps (contains built-in vad that
cannot be disabled)
  g723ar63                            G.723.1 ANNEX-A 6300 bps (contains built-in vad
that cannot be  disabled)
  g723r53                             G.723.1 5300 bps
  g723r63                             G.723.1 6300 bps
  g726r16                     G.726 16000 bps
  g726r24                     G.726 24000 bps
  g726r32                     G.726 32000 bps
  g728                        G.728 16000 bps
  g729br8                     G.729 ANNEX-B 8000 bps (contains built-in vad that can-
not be disabled)
  g729r8                            G.729 8000 bps
  ilbc                                    iLBC 13330 or 15200 bps
CME_A(config-dial-peer)# codec g711ulaw
ROUTER_B(config)# dial-peer voice 1100 voip
ROUTER_B(config-dial-peer)# destination-pattern 110.
ROUTER_B(config-dial-peer)# session target ipv4:10.1.1.1
ROUTER_B(config-dial-peer)# codec g711ulaw
```

The primary difference between the POTS and VoIP dial peer configuration is the use of the **session target** command rather than the **port** command. When you use the context-sensitive help after the **session target** command, the router simply replies with WORD. This means that whatever you enter after the command is somewhat freeform. Most of the time, you will use the syntax **ipv4:***ip_address* to enter a remote IP address, as shown in Example 6-10. This command also allows you to direct calls to DNS names (by using **dns:***name* syntax) or to a variety of call-management servers, such as H.323 gatekeepers or Session Initiation Protocol (SIP) proxy servers.

After you set the session target destination, you can optionally use the **codec** command to select the codec the router should use when placing a call to this destination.

Note If the codec values do not match between the two routers, the call fails and returns a reorder tone (fast busy signal). This is commonly called a codec mismatch. The default codec value for VoIP dial peers is G.729.

Finally, notice that the dial peer 1100 on ROUTER_B uses the command **destination-pattern 110.** to direct all calls starting with the digits 110 to the CME_A router. Without this wildcard, you would need to create two VoIP dial peers on ROUTER_B: one for x1101 and one for x1102.

Note Notice that dial-peer tag 2000 is used on the CME_A router for a VoIP dial peer and used on the ROUTER_B router for a POTS dial peer. This combination works just fine. The only restriction to keep in mind is that you cannot use the same dial peer tag value for different functions on the same router.

Using Dial Peer Wildcards

As you saw in the previous few sections, configuring dial peers (and destination patterns) without using wildcards would be extremely time consuming. By far, the most commonly used wildcard is the dot (.), which represents any dialed digit. You will find a few other wildcards useful in your configurations. Table 6-3 describes these wildcards.

Key Topic

Table 6-3 Wildcards You Can Use with the **destination-pattern** Command

Wildcard	Description
Period (.)	Matches any dialed digit from 0–9 or the * key on the telephone keypad. For example, 20.. matches any number from 2000 through 2099.
Plus (+)	Matches one or more instances of the preceding digit. For example, 5+23 matches 5523, 55523, 555523, and so on. This trend continues up to 32 digits, which is the maximum length of a dialable number.
Brackets ([])	Matches a range of digits. For example, [1-3]22 matches 122, 222, and 322. You can include a caret (^) before the entered numbers to designate a "does not match" range. For example, [^1-3]22 matches 022, 422, 522, 622, 722, 822, 922, and *22.
T	Matches any number of dialed digits (from 0–32 digits).
Comma (,)	Inserts a 1-second pause between dialed digits.

Note The pound symbol (#) on a telephone keypad is not a wildcard symbol. In CME, this key immediately processes a dialed number (i.e., stops the T.302 interdigit timer) when it is entered without waiting for additional digits. This is not the case for CM, where it is treated as a dialed digit.

Tip If you plan to create a dial peer using only the T wildcard as the destination pattern, Cisco recommends that you create the destination as .T. This requires a user to dial at least one digit to match the destination pattern. Otherwise, a phone left off-hook for too long without a dialed digit will match the destination pattern.

Typically, the brackets wildcard is the most difficult to understand, primarily because it is the most flexible. Table 6-4 shows a few examples of how it can be used.

Key Topic

Table 6-4 destination-pattern Brackets Wildcard Examples

Pattern	Description
555[1-3]...	Matches dialed numbers beginning with 555; having 1, 2, or 3 as the fourth digit; and ending in any three digits.
[14-6]555	Matches dialed numbers where the first digit is 1, 4, 5, or 6 and the last three digits are 555.
55[59]12	Matches dialed numbers where the first two digits are 55, the third digit is 5 or 9, and the last two digits are 1 and 2.
[^1-7]..[135]	Matches dialed numbers where the first digit is not 1–7, the second and third digits are any number, and the last digit is 1, 3, or 5.

These wildcards are most often used when creating dial plans for PSTN access. Initially, the most logical destination pattern choice for the PSTN may seem to be 9T (9 for an outside line followed by any number of digits). The problem with this is that Cisco designed the T wildcard to match variable-length strings from 0–32 digits. When a user dials an outside number, such as 14805551212, the router configured with the T wildcard will sit silently and wait for the user to dial more digits. By default, the router will wait for additional dialed digits for 10 seconds, which is the interdigit timeout (also called the T302 timer). Although you can force the router to process the call immediately after dialing the number by pressing the pound key (#), this is not something you would want to train all of your users to do.

Creating a PSTN dialing plan using wildcards other than T is not extremely difficult, as long as you think through the reachable PSTN numbers. Table 6-5 provides a sample PSTN dial plan that you could use in the United States.

Key Topic

Table 6-5 Sample PSTN Destination Patterns for North America

Pattern	Description
[2-9].....	Used for 7-digit dialing areas
[2-9]..[2-9].....	Used for 10-digit dialing areas
1[2-9]..[2-9].....	Used for 11-digit long-distance dialing
[469]11	Used for service numbers, such as 411, 611, and 911
011T	Used for international dialing

Note Although you can manually create an international dial plan without using the T symbol, doing so can become tedious.

Example 6-11 illustrates the configuration of a North American PSTN dial plan on a router. In this example, the T1 CAS voice port 1/0:1 is connected to the PSTN, and internal users must dial 9 for outside PSTN access.

Example 6-11 *Configuring a North American PSTN Dial Plan*

```
VOICE_RTR(config)# dial-peer voice 90 pots
VOICE_RTR(config-dial-peer)# description Service Dialing
VOICE_RTR(config-dial-peer)# destination-pattern 9[469]11
VOICE_RTR(config-dial-peer)# forward-digits 3
VOICE_RTR(config-dial-peer)# port 1/0:1
VOICE_RTR(config-dial-peer)# exit
VOICE_RTR(config)# dial-peer voice 91 pots
VOICE_RTR(config-dial-peer)# description 10-Digit Dialing
VOICE_RTR(config-dial-peer)# destination-pattern 9[2-9]..[2-9].....
VOICE_RTR(config-dial-peer)# port 1/0:1
VOICE_RTR(config-dial-peer)# exit
VOICE_RTR(config)# dial-peer voice 92 pots
VOICE_RTR(config-dial-peer)# description 11-Digit Dialing
VOICE_RTR(config-dial-peer)# destination-pattern 91[2-9]..[2-9].....
VOICE_RTR(config-dial-peer)# forward-digits 11
VOICE_RTR(config-dial-peer)# port 1/0:1
VOICE_RTR(config-dial-peer)# exit
VOICE_RTR(config)# dial-peer voice 93 pots
VOICE_RTR(config-dial-peer)# description International Dialing
VOICE_RTR(config-dial-peer)# destination-pattern 9011T
VOICE_RTR(config-dial-peer)# prefix 011
VOICE_RTR(config-dial-peer)# port 1/0:1
VOICE_RTR(config-dial-peer)# exit
```

Two commands in this syntax deal with the automatic digit-stripping feature of POTS dial peers: **forward-digits** *number* and **prefix** *number*. The **forward-digits** *number* command allows you to specify the number of right-justified digits you want to forward. Notice the first dial peer 90 in Example 6-11. With a destination pattern of 9[469]11, the router would automatically strip the 9 and the two 1s from the pattern before sending the call; this is because of the default behavior of POTS dial peers, which is to strip (remove) all the digits that match the destination pattern before forwarding them on to the target of the dial peer. By entering the command **forward-digits 3**, the router forwards the last three right-justified digits (411, 611, or 911) and only strips the 9.

The **prefix** *number* command adds any specified digits to the front of the dialed number before routing the call. This is useful for dial peer 93 in Example 6-11. Because international

numbers can be a variable length, it is impossible to tell what value to enter for the **forward-digits** command. By using the **prefix 011** command in conjunction with the automatic digit-stripping feature of POTS dial peers, the explicitly-defined digits 9011 are stripped from the dialed string, and the **prefix** command then adds the 011 back in its place as the dialed digits are sent to the PSTN, making a valid international dialed string of any length.

Private Line Automatic Ringdown

Although not directly related to dial peer configuration, private line automatic ringdown (PLAR) configurations rely heavily on existing dial peers to complete a call. Ports configured with PLAR capabilities automatically dial a number as soon as the port detects an off-hook signal. The most obvious use for PLAR configurations is emergency phones in locations such as company elevators or parking garages. Example 6-12 designates x1101 (shown in Figure 6-8) as a PLAR extension that immediately dials x1102 as soon as a user lifts the receiver.

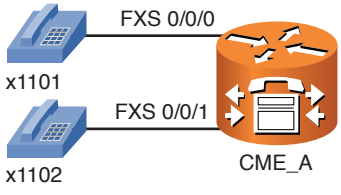


Figure 6-8 *PLAR Configuration*

Key Topic

Example 6-12 *FXS PLAR Configuration*

```
CME_A(config)# voice-port 0/0/0
CME_A(config-voiceport)# connection ?
  plar      Private Line Auto Ringdown
  tie-line  A tie line
  trunk     A Straight Tie Line
CME_A(config-voiceport)# connection plar ?
  WORD      A string of digits including wild cards
  Tied      dedicated tie to this number
CME_A(config-voiceport)# connection plar 1102
```

The FXS voice port 0/0/0 is now hard-coded to dial the number 1102 as soon as a user lifts the handset.

PLAR can also be useful in a variety of other circumstances. One common scenario is using FXO connections to the PSTN, as shown in Figure 6-9.

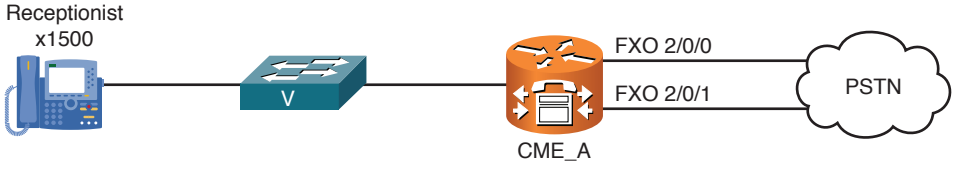


Figure 6-9 *FXO PSTN Connections*

Although the **destination-pattern** command from dial peer configuration mode is useful for dictating what can go out the PSTN FXO ports, it is not too useful for handling what comes in the FXO ports. When the CME_A router shown in Figure 6-9 receives an incoming call from the PSTN, the call information sent from the PSTN carrier does not include dialed number information. (This is known as Dialed Number Identification Service [DNIS].) It includes caller ID information (known as Automatic Number Identification [ANI]), but this does not help the router to know where to send the call when it is received.

As a result, calls into the CME_A router hear a second dial tone played after they dial into the CME_A router from the PSTN. This is essentially the router saying, "Yes, I received your call; please tell me what to do now." If the caller on the phone were to dial 1500, the CME_A router would forward them to the receptionist. However, the likelihood of a PSTN caller doing this is slim. This is where PLAR comes to the rescue. Example 6-13 configures two analog FXO ports as PLAR connections for incoming calls.

Example 6-13 *FXO PLAR Configuration*

```
CME_A(config)# voice-port 2/0/0
CME_A(config-voiceport)# connection plar 1500
CME_A(config-voiceport)# exit
CME_A(config)# voice-port 2/0/1
CME_A(config-voiceport)# connection plar 1500
CME_A(config-voiceport)# exit
```


If you enter the connection **plar 1500** command under both FXO ports, the router receives incoming calls from the PSTN and immediately forwards them to the receptionist phone rather than playing a second dial tone.

Note Configuring PLAR connections for incoming calls is something you only need to do for analog FXO trunks. Digital PSTN connections (such as T1 or E1) receive DNIS information for incoming calls, which the router can use for Direct Inward Dial (DID) services.

Understanding Router Call Processing and Digit Manipulation

Understanding how the router processes dialed digits is critical to accurately implementing dial peers. There are two primary rules to guide you in your dial peer strategy:

Key Topic

- The most specific destination pattern always wins.
- When a match is found, the router immediately processes the call.

This section presents examples of these rules in action. Example 6-14 shows the dial peers for a router.

Example 6-14 *Sample Dial Peer Configuration 1*

```
dial-peer voice 1 voip
  destination-pattern 555[1-3]...
  session target ipv4:10.1.1.1
dial-peer voice 2 voip
  destination-pattern 5551...
  session target ipv4:10.1.1.2
```

If a user dials the number 5551234, both dial peers match, but the router chooses to use dial peer 2 because it is a more specific match (5551... matches 1000 numbers while 555[1-3]... matches 3000 numbers). Now, Example 6-15 shows what happens if you add a third dial peer to this configuration.

Example 6-15 *Sample Dial Peer Configuration 2*

```
dial-peer voice 1 voip
  destination-pattern 555[1-3]...
  session target ipv4:10.1.1.1
dial-peer voice 2 voip
  destination-pattern 5551...
  session target ipv4:10.1.1.2
dial-peer voice 3 voip
  destination-pattern 5551
  session target ipv4:10.1.1.3
```

If the user again dials 5551234, the router uses dial peer 3 to route the call. Likewise, the router processes only the 5551 digits and drops the 234 digits. This can be useful for emergency patterns such as 911 or 9911 (in North America) because the call is immediately routed when a user dials this specific pattern.

Tip If you ever have a question of which dial peer will match a specific string, Cisco routers include a handy testing feature. From privileged mode, enter the command **show dialplan number** *number*, where *number* is the number you want to test. The router displays all the matching dial peers in the order in which the router will use them. The router lists more specific matches first.

Tip Because the router immediately routes the call after it makes a specific match, it is best to avoid overlapping dial plans if possible.

Avoiding overlapping dial plans may be impossible at times. In these cases, you need to get creative with your dial peers to accomplish your objectives. For example, if you are required to have a dial peer matching the destination pattern 5551 while a second dial peer has the destination pattern 5551..., you could use a configuration like Example 6-16 as a solution.

Example 6-16 *Sample Dial Peer Configuration 3*

```
dial-peer voice 2 voip
 destination-pattern 5551...
 session target ipv4:10.1.1.2
dial-peer voice 3 voip
 destination-pattern 5551T
 session target ipv4:10.1.1.3
```

Notice the T wildcard after 5551, which matches 0–32 digits. Users dialing extension 5551 now have to press the pound key (#) after they finish dialing or wait the 10-second inter-digit timeout period. You could also accomplish this objective by using some fancy digit-manipulation techniques, which you learn about in an upcoming section.

Matching Inbound and Outbound Dial Peers

When a router receives a voice call, it must always match a dial peer in some way for the router to process the call. Although this might seem like a simplistic statement, there is actually a lot of strategy that must be in place to accomplish this in both the inbound and outbound direction. Take the scenario presented in Figure 6-10, which expands on the call leg scenario that opened this section on dial peers.

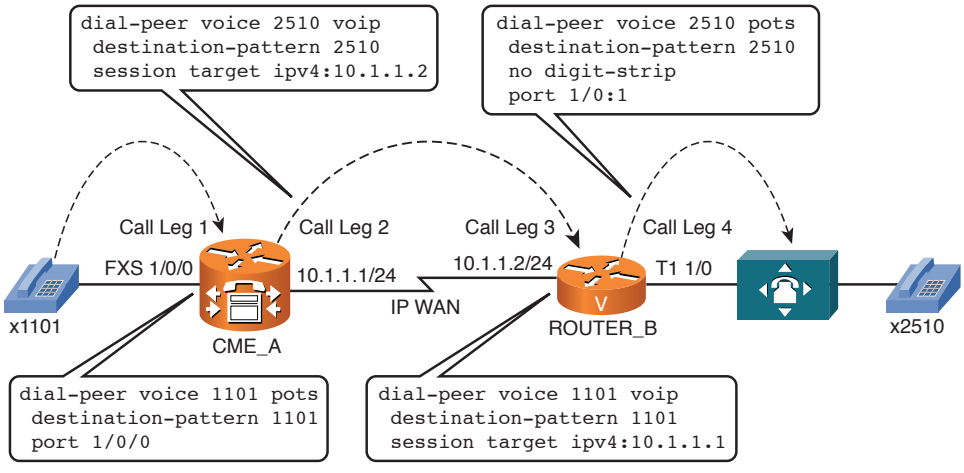


Figure 6-10 *Inbound and Outbound Dial Peers*

In addition to the call legs, Figure 6-10 displays the dial-peer configurations necessary to complete end-to-end calls from x1101 to x2510 and vice versa. Now, matching the outbound dial peers is easy: Take the dialed digits and compare them to the destination patterns under the dial peers you configured on the router to find the most specific match. For example, if x1101 dials x2510, the CME_A router looks at its dial peers and realizes there is a VoIP dial peer match directing the call to the IP address 10.1.1.2. When ROUTER_B receives the call, it realizes the dialed digits are an exact match to the POTS dial peer 2510, which causes the router to send the call out the T1 interface to the attached PBX system.

This process explains how the router matches the outbound dial peers (shown in Figure 6-10 as call leg 2 and call leg 4), but how does the route match the inbound dial peers? A router matches inbound dial peers through the following five methods:

Key Topic

1. Match the dialed number (DNIS) using the **incoming called-number** dial peer configuration command.
2. Match the caller ID information (ANI) using the **answer-address** dial peer configuration command.
3. Match the caller ID information (ANI) using the **destination-pattern** dial peer configuration command.
4. Match an incoming POTS dial peer by using the **port dial-peer configuration** command.
5. If no match has been found using the previous four methods, use dial peer 0.

Look at Figure 6-10. Call legs 2 and 4 are accounted for as outbound dial peers matched by using the dialed number (DNIS) information against the **destination-pattern** command under the dial peers. Here's how the router uses the previous list of five rules to match the inbound dial peers.

For call leg 1:

1. (NO MATCH) 2510 (the dialed number) does not match an **incoming called-number** dial peer configuration command on the CME_A router because this command does not exist in the configuration.
2. (NO MATCH) x1101 caller ID information (ANI) does not match an **answer-address** dial peer configuration command on the CME_A router because this command does not exist in the configuration.
3. (NO MATCH) x1101 caller ID information (ANI) does not match the **destination-pattern** dial peer configuration command on the CME_A router because x1101 does not have any caller ID information. That is, the phone itself does not provide caller ID information to the router because an analog phone does not know its own phone number.
4. (MATCH) x1101 comes in FXS port 1/0/0, which matches an incoming POTS dial peer on the CME_A router by using the **port** dial peer configuration command (port 1/0/0).

Using the five-step matching process, the CME_A router is able to match an inbound dial peer using the incoming port value of the attached analog phone. The CME_A router then processes the outbound dial peer (call leg 2), and the call arrives at ROUTER_B. Once again, ROUTER_B works through the five-step process to match an inbound dial peer.

For call leg 3:

1. (NO MATCH) 2510 (the dialed number) does not match an **incoming called-number** dial peer configuration command on ROUTER_B because this command does not exist in the configuration.
2. (NO MATCH) x1101 caller ID information (ANI) does not match an **answer-address** dial peer configuration command on ROUTER_B because this command does not exist in the configuration.

3. (MATCH) x1101 caller ID information (ANI) does match the **destination-pattern** dial peer configuration command for the VoIP dial peer 1101 on ROUTER_B.

In this case, the VoIP dial peer 1101 on ROUTER_B doubles as both the outgoing dial peer for calls placed to x1101, and as an incoming dial peer for calls coming from x1101.

Now, to see the inbound matching process in its entirety, imagine that there is no VoIP dial peer 1101 on ROUTER_B, as shown in Figure 6-11.

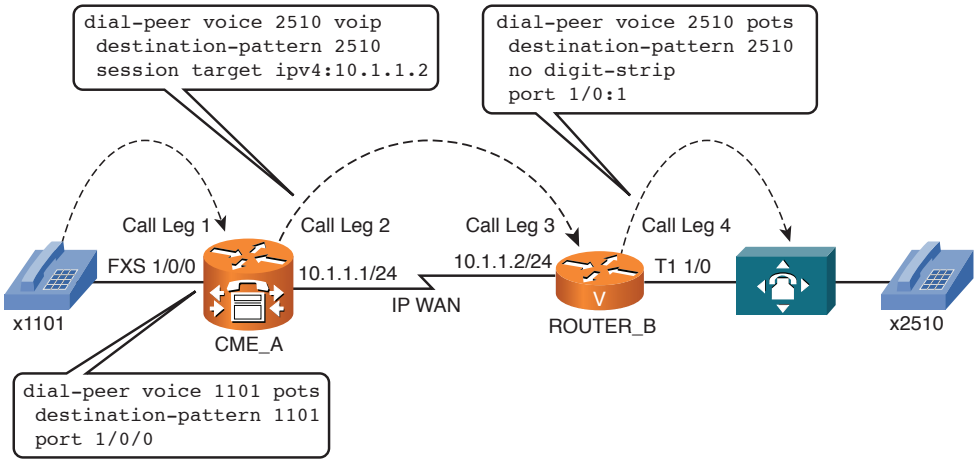


Figure 6-11 *Matching Inbound Dial Peers Using Dial Peer 0*

The first result is that you could not place calls to x1101 from ROUTER_B (or the PBX system attached to ROUTER_B). However, what if x1101 called x2510? The CME_A and ROUTER_B routers have enough information to match the outbound call legs. ROUTER_B is just missing the information for the inbound dial peer (call leg 3). Here's how the decision process would flow:

1. (NO MATCH) 2510 (the dialed number) does not match an **incoming called-number** dial peer configuration command on ROUTER_B because this command does not exist in the configuration.
2. (NO MATCH) x1101 caller ID information (ANI) does not match an **answer-address** dial peer configuration command on ROUTER_B because this command does not exist in the configuration.
3. (NO MATCH) x1101 caller ID information (ANI) does not match **the destination-pattern** dial peer configuration command because the VoIP dial peer 1101 was removed on ROUTER_B.
4. (NO MATCH) x1101 did not come in a POTS interface (FXS, FXO, E&M, Voice BRI/T1/E1 digital interface) that could be matched using the **port** command; rather, x1101 came across a VoIP connection.
5. (MATCH) Because ROUTER_B could not find a match using the previous four methods, it uses dial peer 0.

So, this now raises the question, "What is dial peer 0?" Dial peer 0 is like a default gateway dial peer that appears when there is no dial peer match (this applies only for inbound dial peers, not for outbound dial peers). Although this allows the call to complete, you have no control over dial peer 0. You cannot configure it nor change any of its default settings. Dial peer 0 uses the following, unchangeable settings:

Key Topic

- **Any voice codec:** Dial peer 0 handles any incoming voice codec; it is not hard-coded to any specific codec.
- **No DTMF relay:** DTMF relay sends dialed digits outside of the audio stream. This is useful because compressed codecs often distort dialed tones on the call.
- **IP Precedence 0:** This is probably the most painful default of dial peer 0. Setting the traffic to IP Precedence (IPP) to 0 strips all QoS markings. The router now treats the voice traffic the same as the data traffic.
- **Voice Activity Detection (VAD) enabled:** VAD allows you to save bandwidth by eliminating voice traffic during periods of silence on the call.
- **No Resource Reservation Protocol (RSVP) support:** The lack of RSVP goes right along with the lack of any QoS for the voice calls. The router does not reserve any bandwidth specifically for dial peer 0 calls.
- **Fax-rate voice:** The router limits the bandwidth available to fax signals to the maximum allowed by the VoIP codec. This could devastate fax calls if you are using a low-bandwidth compressed codec.
- **No application support:** Dial peer 0 cannot refer calls to outside applications, such as an interactive voice response (IVR) system.
- **No DID support:** Dial peer 0 cannot use the DID feature to automatically forward calls from an outside PSTN carrier to internal devices.

In light of this list of dial peer 0 features, it is best to always match an inbound dial peer where you can control the configuration.

Using Digit Manipulation

Digit manipulation is the process of adding or removing digits from a dialed number to help a call reach an intended destination. You have already seen a few of the digit manipulation commands during the discussion of the automatic digit-stripping feature of POTS dial peers (such as the **no digit-strip** and **forward-digit** commands). Before we look at some practical examples, Table 6-6 shows a list of common digit-manipulation commands you can use on a Cisco router.

Key Topic

Table 6-6 Common Digit-Manipulation Methods on Cisco Routers

Command	Mode	Description
prefix digits	POTS dial peer	Allows you to specify digits for the router to add before the dialed digits. Example: **prefix** 011 adds the numbers 011 to the front of the originally dialed number.
forward-digits number	POTS dial peer	Allows you to specify the number of right-justified digits to forward. Example: **forward-digits 4** forwards only the rightmost 4 digits from the dialed number.

Command	Mode	Description
[no] **digit-strip**	POTS dial peer	Enables or disables the default digit-stripping behavior of POTS dial peers. Example: **no digit-strip** turns off the automatic digit-stripping behavior under a POTS dial peer.
num-exp match	Global	Transforms any dialed number matching the match string into the digits specified in the set string. Example: **num-exp 4... 5...** matches any 4-digit dialed number beginning with 4 into a 4-digit number beginning with 5 (4123 becomes 5123). Example: **num-exp 0 5000** matches the dialed digit 0 and changes it to 5000.
digits set digits		
voice translation-profile	Global and POTS or VoIP dial peer	Allows you to configure a translation profile consisting of up to 15 rules to transform numbers however you want. The translation profile is created globally and then applied to any number of dial peers (similar to an access list).

Following are four practical scenarios in which these digit-manipulation commands can prove to be useful.

Practical Scenario 1: PSTN Failover Using the prefix Command

One of the benefits of using VoIP communication over traditional telephony is the ability to have more than one path to a destination. Figure 6-12 shows a commonly encountered scenario.

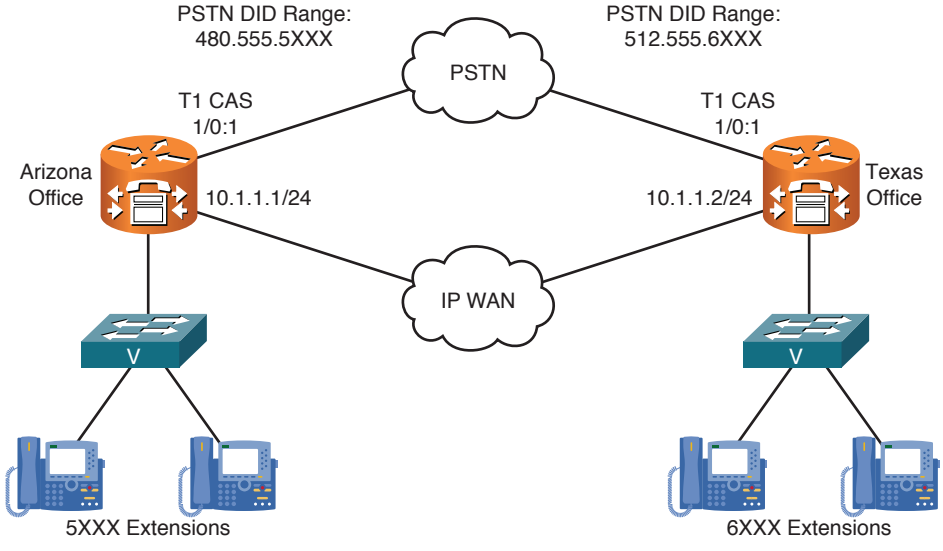


Figure 6-12 *Multiple Voice Paths*

The organization shown in Figure 6-12 prefers to use the IP WAN as its primary communication path between Arizona and Texas. However, if the IP WAN should fail, calls between the offices should use the PSTN as their communication path.

One of the benefits of using VoIP is the merging of voice networks into one, seamless communication path. Because calls are traveling over the IP WAN, users in the Arizona office can dial the users in the Texas office using their four-digit (6XXX) extension. Likewise, users in the Texas office can dial the users in the Arizona office using their four-digit (5XXX) extension. It would be inconvenient to require all the users in the Arizona office to dial the Texas office using the PSTN DID range rather than the four-digit extension (and vice versa).

Using a combination of the preference and prefix commands, you can allow this failover transformation to occur dynamically, as shown in Example 6-17.

Example 6-17 *Dynamic WAN to PSTN Failover Implementation*

Key Topic

```
Arizona(config)# dial-peer voice 10 voip
Arizona(config-dial-peer)# destination-pattern 6...
Arizona(config-dial-peer)# session target ipv4:10.1.1.2
Arizona(config-dial-peer)# preference 0
Arizona(config-dial-peer)# exit
Arizona(config)# dial-peer voice 11 pots
Arizona(config-dial-peer)# destination-pattern 6...
Arizona(config-dial-peer)# port 1/0:1
Arizona(config-dial-peer)# preference 1
Arizona(config-dial-peer)# no digit-strip
Arizona(config-dial-peer)# prefix 1512555
Texas(config)# dial-peer voice 10 voip
Texas(config-dial-peer)# destination-pattern 5...
Texas(config-dial-peer)# session target ipv4:10.1.1.1
Texas(config-dial-peer)# preference 0
Texas(config-dial-peer)# exit
Texas(config)# dial-peer voice 11 pots
Texas(config-dial-peer)# destination-pattern 5...
Texas(config-dial-peer)# port 1/0:1
Texas(config-dial-peer)# preference 1
Texas(config-dial-peer)# no digit-strip
Texas(config-dial-peer)# prefix 1480555
```

The **preference** command allows the router to determine which dial peer it should use in the case where the destination patterns are identical. It might seem counterintuitive, but the router considers lower preferences to be better than higher preferences (the preference value can be any number from 0–10). The default preference for a dial peer is 0. Thus, the **preference 0** command in Example 6-17 under dial peer 10 on both routers is redundant.

Key Topic

Tip If you create multiple dial peers with exactly equal destination patterns and preferences, the router will randomly choose a dial peer to use.

Looking at the Arizona router in Example 6-17, you can see that dial peer 10 is the more preferred path to the Texas router. Because the connection uses VoIP dial peers, no

automatic digit stripping occurs and no digit-manipulation commands are required. (Keep in mind that the no digit-strip, forward-digits, and prefix commands are only valid under POTS dial peers anyhow.)

If the IP connection between Arizona and Texas fails, the Arizona router begins using the next most preferred dial peer, which is dial peer 11. To overcome the automatic digit-stripping feature of POTS dial peers, the **no digit-strip** command is used. (Otherwise, the router would strip the 6 digit from the dialed number.) Because a four-digit number is invalid on the PSTN, the prefix 1512555 command adds the necessary prefix information to get the call across the PSTN.

Note If the IP WAN fails, all the active calls established during the WAN failure will disconnect and be required to redial. There is no "dynamic failover" mechanism for calls already established.

Practical Scenario 2: Directing Operator Calls to the Receptionist

This practical scenario is fairly simple. The organization shown in Figure 6-13 wants to direct all calls to the operator number 0 to the receptionist at extension 5000.

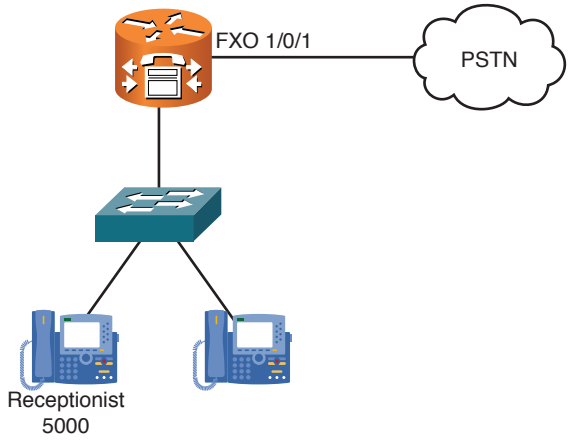


Figure 6-13 *Redirecting Operator Calls*

Because this is a "universal" transformation (you always want to change the dialed number 0 to 5000), you can accomplish this objective using the **num-exp** global configuration command, which is shown in Example 6-18.

Example 6-18 *Transforming Dialed Numbers Using* **num-exp**

```
Voice_RTR(config)# voice-port 1/0/1
Voice_RTR(config-voiceport)# connection plar 0
Voice_RTR(config-voiceport)# exit
Voice_RTR(config)# num-exp 0 5000
```

Now, anytime the number 0 is dialed from anywhere in the organization (could be an IP phone, FXS port, and so on), the voice router automatically transforms it to 5000 and then searches for a dial peer allowing it to reach the number 5000.

Note The router applies the **num-exp** command the instant it receives a dialed number, even before it attempts to match an inbound dial peer.

Practical Scenario 3: Specific POTS Lines for Emergency Calls

As organizations move more to VoIP connections, they are finding cost-saving benefits by eliminating traditional telephony connections at remote offices in favor of centralizing all PSTN calls (and toll charges) at a central site. Figure 6-14 illustrates this type of network design.

This type of call routing allows an organization to get higher call volume from a single location, which typically allows the organization to negotiate cheaper long-distance rates with its PSTN carrier.

Note Some countries restrict businesses from forwarding PSTN calls over the IP WAN. You should always check with the local government regulations before you do this. Thankfully, the United States is not one of those countries.

Although the centralization of PSTN calls offers significant cost savings, the remote sites need to keep at least one local PSTN connection for emergency calling. This is because PSTN carriers provide location information to emergency service providers based on the POTS connection. If emergency calls from the remote offices were to traverse the IP WAN and leave the PSTN connection at the central site, the emergency service provider would receive location information for the central site.

Depending on the size of the remote office, you can typically dedicate one or two analog FXO ports for emergency calls. The configuration in Example 6-19 configures the necessary dial peers for dual FXO ports connected to the PSTN. This example assumes the FXO ports are 1/0/0 and 1/0/1.

Example 6-19 *Dynamic WAN-to-PSTN Failover Implementation*

```
REMOTE_RTR(config)# dial-peer voice 10 pots
REMOTE_RTR(config-dial-peer)# destination-pattern 911
REMOTE_RTR(config-dial-peer)# port 1/0/0
REMOTE_RTR(config-dial-peer)# no digit-strip
REMOTE_RTR(config-dial-peer)# exit
REMOTE_RTR(config)# dial-peer voice 11 pots
REMOTE_RTR(config-dial-peer)# destination-pattern 9911
REMOTE_RTR(config-dial-peer)# port 1/0/0
REMOTE_RTR(config-dial-peer)# forward-digits 3
REMOTE_RTR(config-dial-peer)# exit
REMOTE_RTR(config)# dial-peer voice 12 pots
```

```
REMOTE_RTR(config-dial-peer)# destination-pattern 911
REMOTE_RTR(config-dial-peer)# port 1/0/1
REMOTE_RTR(config-dial-peer)# no digit-strip
REMOTE_RTR(config-dial-peer)# exit
REMOTE_RTR(config)# dial-peer voice 13 pots
REMOTE_RTR(config-dial-peer)# destination-pattern 9911
REMOTE_RTR(config-dial-peer)# port 1/0/1
REMOTE_RTR(config-dial-peer)# forward-digits 3
```

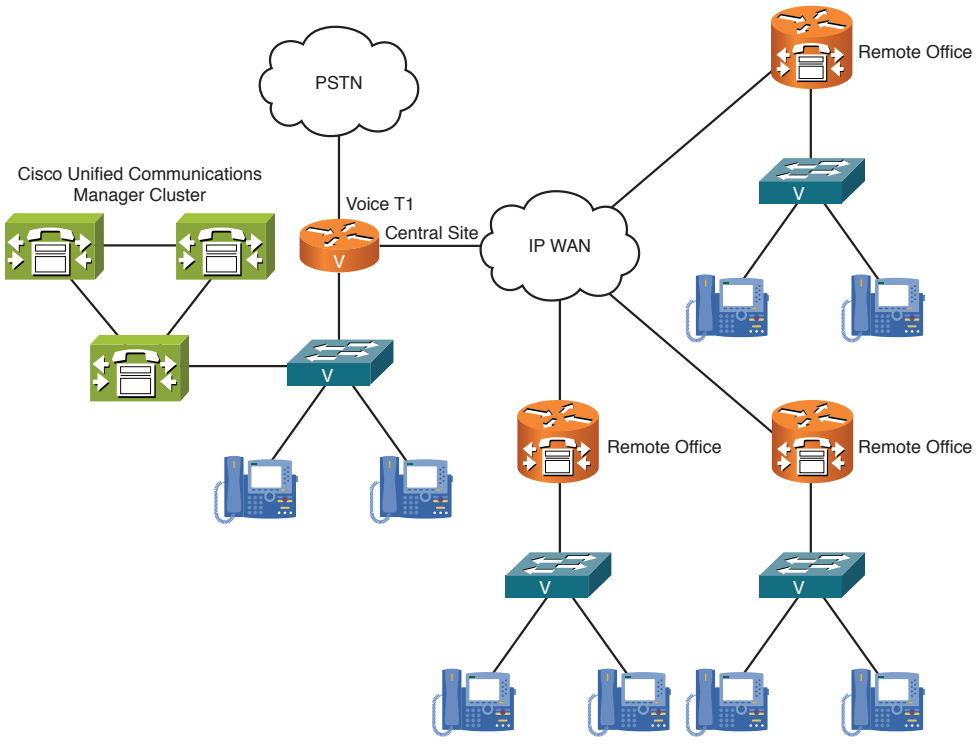


Figure 6-14 *Centralizing PSTN Access*

This configuration creates two identical destination patterns for the two FXO ports. Because the **preference** command is not used to indicate a more preferred dial peer, the router will randomly choose one of the FXO ports as an exit point anytime a user dials 911 or 9911. (The additional 9 may be entered if users are accustomed to dialing 9 for an outside line.) The dial peers created for the 911 destination pattern (dial peers 10 and 12) are also assigned the **no digit-strip** command. Otherwise, the automatic digit-stripping rule of POTS dial peers would strip any explicitly defined digits (which are all of them in this case; the router would not send any digits to the PSTN). The dial peers created for the 9911 destination pattern (dial peers 11 and 13) are assigned the **forward-digits 3** command to send the right-justified three digits (911, in this case) to the PSTN and allow the automatic digit-stripping rule to remove the initial 9 access code.

Practical Scenario 4: Using Translation Profiles

The digit manipulation commands discussed thus far allow you to perform "minor translations" to a number. For example, you can add some digits using the **prefix** command or ensure digits do or do not get stripped with the **forward-digits** command. The **num-exp** command allows you to make the biggest changes of all, but these changes are applied globally to the router, which might not give you the flexibility all situations require. Translation profiles are useful to address these needs. If you find yourself saying, "I want to change this dialed number to that dialed number, but only when it goes out this port," you need a translation profile.

Working with translation profiles is definitely not as easy as working with the "simple" digit manipulation methods discussed earlier. Implementation of translation profiles requires a three-step process:

Step 1. Define the rules that dictate how the router will transform the number.

Step 2. Associate the rules into a translation profile.

Step 3. Assign the translation profile to a dial peer.

In a way, this is similar to access-list configuration on a router.

To demonstrate the configuration of translation profiles, consider the scenario illustrated in Figure 6-15.

The headquarters of this organization uses the DID range from a PSTN provider of 602.555.6XXX. This allows PSTN callers to dial directly into the organization without being redirected by a receptionist. Typically, when you lease a block of DID numbers, the PSTN carrier will strip the numbers down to a four-digit extension. In this case, the DID block assigned to the organization (6XXX) does not match its internal extension range (5XXX). The administrator of this network would like to translate all 6XXX dialed numbers to 5XXX, but only if these dialed numbers come in from the T1 PSTN interface, so as to not interfere with the numbering scheme of the remote office. To accomplish this, he cannot use the **num-exp 6... 5...** global configuration command because it will interfere with dialing the 6XXX extensions at the remote office. This situation is ideal for translation profiles.

The first step to configure translation profiles is to create the translation rules. These use the general syntax shown in Example 6-20.

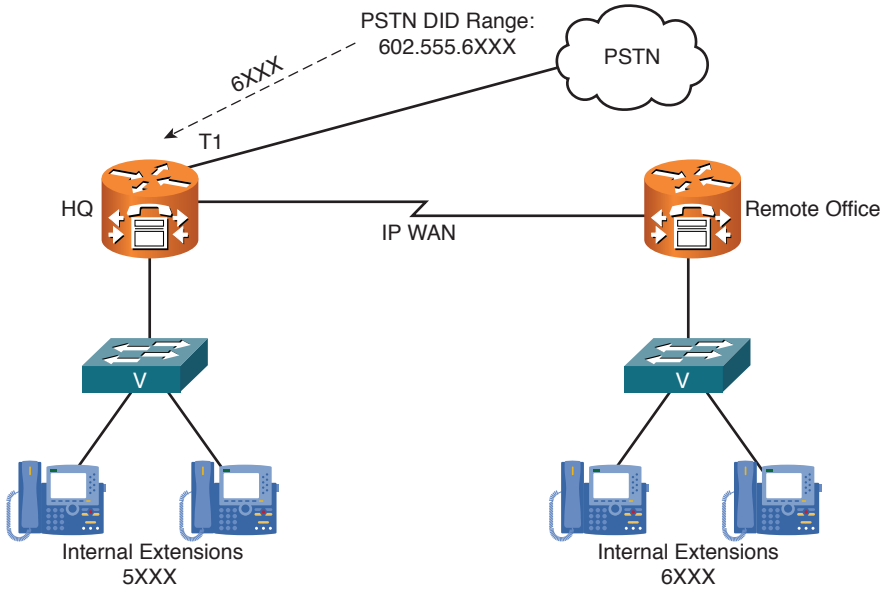


Figure 6-15 *Translating DID Ranges to Internal Extensions*

Example 6-20 *Translation Rule General Syntax*

```
Router(config)# voice translation-rule rule number
Router(cfg-translation-rule)# rule 1 /match/ /set/
Router(cfg-translation-rule)# rule 2 /match/ /set/
Router(cfg-translation-rule)# rule 3 /match/ /set/ ...and so on
```

Example 6-21 configures the necessary translation rule for the scenario in Figure 6-15.

Example 6-21 *Configuring Translation Rules*

```
HQ_RTR(config)# voice translation-rule 1
HQ_RTR(cfg-translation-rule)# rule 1 ?
/WORD/   Matching pattern
reject   Call block rule
HQ_RTR(cfg-translation-rule)# rule 1 /6/ ?
/WORD/  Replacement pattern
HQ_RTR(cfg-translation-rule)# rule 1 /6/ /5/
```

The syntax in the rule 1 command may look a little cryptic. The first entry between the set of forward slashes (/) is the **match** statement. This tells the router "Look for the number 6." The entry between the second set of forward slashes is the **set** statement. This tells the router "Replace the 6 you found from the match statement with a 5." In this case, the router changes the first 6 that is found to a 5.

Thankfully, Cisco does not leave you "hoping" that the translation rule will work properly after it is applied to the interface. You can use the **test voice translation-rule** command from privileged mode to test the rules you create before you apply them, as shown in Example 6-22.

Example 6-22 *Testing Translation Rules*

```
HQ_RTR# test voice translation-rule 1 6546
Matched with rule 1
Original number: 6546   Translated number: 5546
Original number type: none   Translated number type: none
Original number plan: none   Translated number plan: none
HQ_RTR# test voice translation-rule 1 6677
Matched with rule 1
Original number: 6677   Translated number: 5677
Original number type: none   Translated number type: none
Original number plan: none   Translated number plan: none
```

Example 6-22's output indicates the translation rule tests successfully. 6546 is translated to 5546 and 6677 is translated to 5677.

Next, you need to take the voice translation rule and assign it to a translation profile. The translation profile designates whether the translation rule will change the calling (caller ID or ANI) or called (dialed number or DNIS) information. Example 6-23 assigns translation rule 1 to a translation profile called CHANGE_DID.

Example 6-23 *Assigning Translation Rules to a Translation Profile*

```
HQ_RTR(config)# voice translation-profile ?
WORDTranslation profile name
HQ_RTR(config)# voice translation-profile CHANGE_DID
HQ_RTR(cfg-translation-profile)# translate ?
called           Translation rule for the called-number
calling          Translation rule for the calling-number
redirect-called  Translation rule for the redirect-number
redirect-target  Translation rule for the redirect-target
HQ_RTR(cfg-translation-profile)# translate called ?
<1-2147483647>   Translation rule tag
HQ_RTR(cfg-translation-profile)# translate called 1
```

Example 6-23 assigns translation rule 1 as a called (dialed number) translation. Because the scenario requires you to change the DID information, this is the proper assignment. Assigning the translation rule as a calling translation would change the caller ID of a person calling into the organization.

The last step is to assign the translation profile. The configuration assumes that the router is using POTS dial peer 100 as the inbound dial peer for calls coming from the PSTN:

```
HQ_RTR(config)# dial-peer voice 100 pots
HQ_RTR(config-dial-peer)# translation-profile incoming CHANGE_DID
```

Notice that the example applies the translation profile in the incoming direction. This causes it to affect calls coming in from the PSTN rather than outgoing calls. The translation profile is now in effect, accomplishing the objective of the scenario.

Note You can do far more with translation profiles (and far more complex patterns that you can match with translation rules). This is covered more in the CCNP Voice certification track.

With all these various methods of digit manipulation, two questions quickly arise: Which method gets applied first? Will the router remove added prefix digits because of the automatic digit-stripping rule? Figure 6-16 answers these questions by displaying the order of operations for outgoing POTS dial peers. The order remains the same for VoIP dial peers; however, most digit-manipulation commands apply only to POTS dial peers.

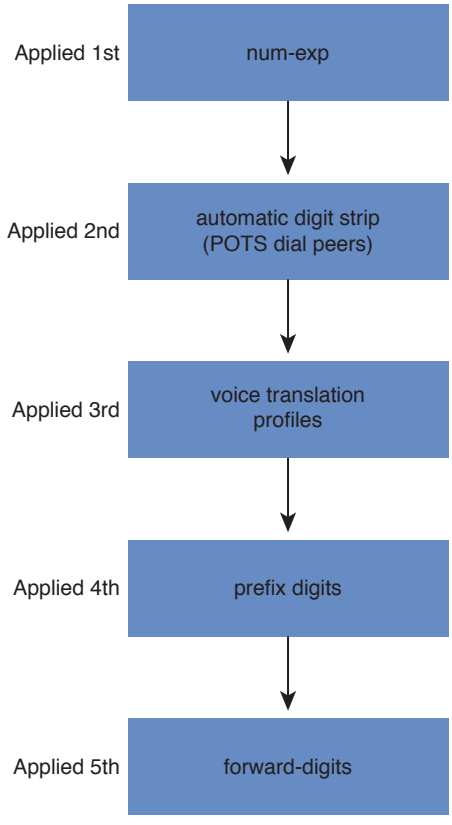


Figure 6-16 *Digit Manipulation Order of Operation for POTS Dial Peers*

Using CCP to Configure a CME Dial Plan

If you prefer, you can also use the Cisco Configuration Professional (CCP) to modify the CME dial plan. Cisco neatly organized all dial plan configurations in a Dial Plans folder, shown in Figure 6-17.

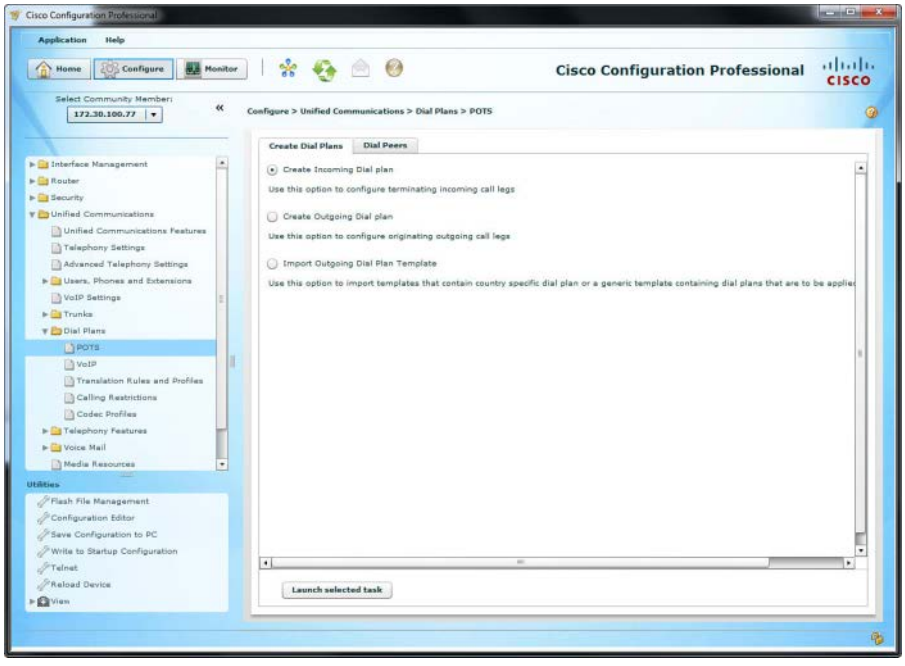


Figure 6-17 *Configuring a Dial Plan Using CCP*

Notice that the first two items under the Dial Plans folder of CCP is POTS and VoIP. These correlate to the two categories of dial peers you most frequently configure in CME. Selecting the POTS configuration item brings up the Create Dial Plan menu. In an attempt to ease the configuration, Cisco provides three wizard-like configuration items:

- **Create Incoming Dial Plan:** Allows you to configure inbound dial-peers using PSTN trunks.
- **Create Outbound Dial Plan:** Allows you to configure outbound dial-peers using PSTN trunks. The wizard also provides you the ability to specify access digits (such as dialing 9 for an outside line) and caller ID information.
- **Import Outgoing Dial Plan Template:** Allows you to import a dial plan from a CSV file template.

After you get more comfortable with the CME configuration, you will likely access the Dial Peers tab (next to the Create Dial Plans tab shown in Figure 6-17). In this configuration pane, you can create manually configured dial peers through a GUI configuration. Figure 6-18 shows the creation of a ten-digit dialing PSTN dial peer.

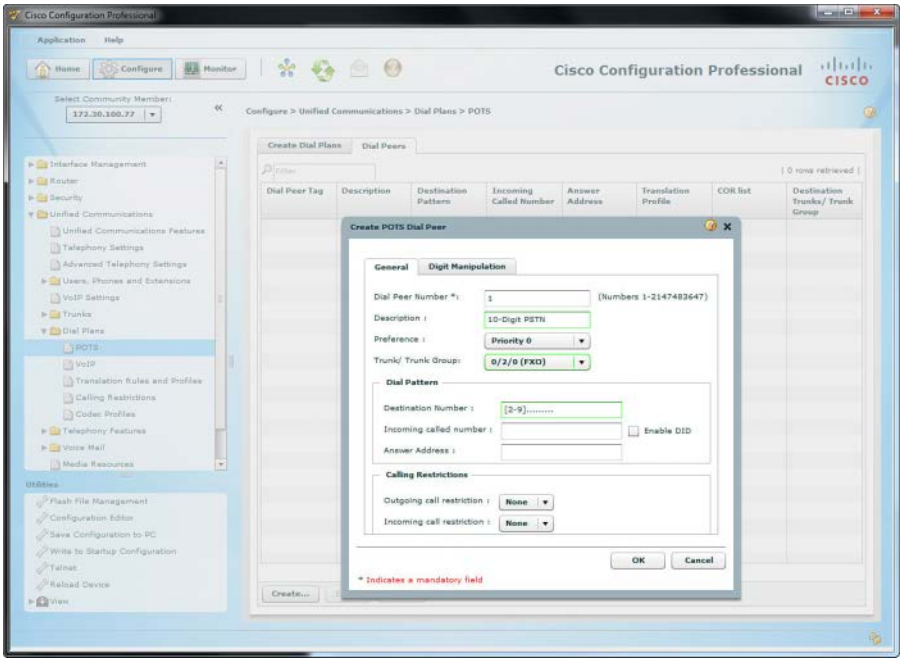


Figure 6-18 *Configuring Dial Peers Using CCP*

Unlike the POTS dial peer configuration window in CCP, the VoIP dial peer configuration does not have the wizard-based configuration items; it allows only manual dial peer creation.

Understanding and Implementing CME Class of Restriction

If you implement what you've seen so far, you can create a powerful VoIP system that supports both internal (ephone) and external (dial peer) dialing. However, there might be times when you want to prevent some users from calling certain numbers, such as the following examples:

- Prevent standard employees from making international calls, but allow management to place international calls without restriction
- Block certain high-cost numbers (such as 1-900 numbers in the United States)
- Prevent certain internal phones from reaching executive office directory numbers

This list goes on and on, but you get the idea: Sometimes, it is necessary to place calling restrictions on users of the VoIP network. If you were implementing this feature in the full Cisco Unified Communications Manager (CUCM) platform, you would use a feature called Partitions and Calling Search Spaces (CSS). In the CME environment, the equivalent feature is called incoming and outgoing class of restriction (COR) lists.

Without a doubt, COR lists take some practice before the concept sinks in fully. At a high-level view, here's how the process works:

1. A user picks up his IP phone and is immediately associated with an incoming COR list (which lists the "tags" he can access).
2. The user dials, causing CME to match an outgoing dial peer.
3. If the outgoing dial-peer requires a COR tag, CME checks to see whether that tag is listed in the user's incoming COR list.
4. If the tag is listed in the user's incoming COR list, CME permits the call.
5. If the tag is not listed in the user's incoming COR list, CME denies the call.

Note I know the word *tag* is vague, but when you see the configuration of COR lists, you will understand why I chose this word.

Here's a play on the famous quote in *The Matrix*: "Unfortunately, no one can be told what COR lists are. You have to see them for yourself." Let's walk through a practical configuration example (see Figure 6-19).

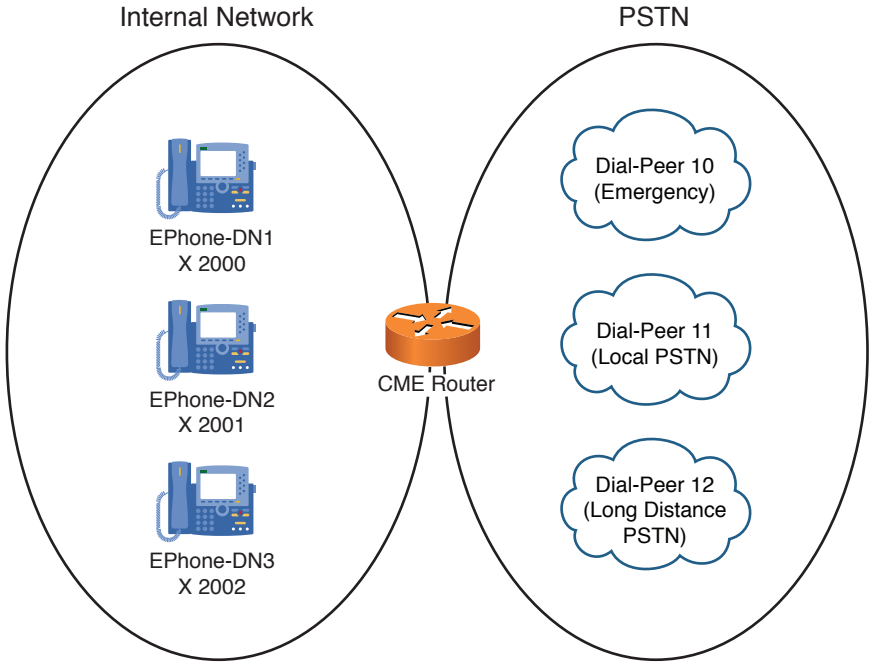


Figure 6-19 *Practical COR List Example*

As shown in Figure 6-19, three phones are on the internal network:

- Ephone-dn 1 (x2000)
- Ephone-dn 2 (x2001)
- Ephone-dn 3 (x2002)

In addition, there are three POTS dial peers connecting to the PSTN:

- Dial peer 10 (emergency calls, destination-pattern 911)
- Dial-peer 11 (local PSTN calls, destination-pattern [2-9].....)
- Dial-peer 12 (long-distance PSTN calls, destination-pattern 1.....)

A corporation wants to implement the following restrictions in CME:

- Ephone-dn 1 (x2000) represents a lobby phone that should only be able to dial internal extensions and place emergency calls.
- Ephone-dn 2 (x2001) represents an employee phone that should be able to dial internal extensions and place emergency and local PSTN calls.
- Ephone-dn 3 (x2002) represents a manager phone that should have no calling restrictions.

Based on these requirements, we can begin the COR list implementation on the CME router. It breaks down into the following steps:

Step 1. Define the COR tags we will use for the restrictions.

Step 2. Create the outbound COR lists.

Step 3. Create the inbound COR lists.

Step 4. Assign the outbound COR lists.

Step 5. Assign the inbound COR lists.

This seems like an extensive process, but it goes rather quickly when you get to enter the syntax.

To tackle the first step, we must define the tags we will use for the restrictions. I've been calling them *tags* because they are simply names that you create. Some documentation calls them COR list members, whereas other documentation calls them keys. Here, we call them tags. The tag names you create are typically based on the restrictions you want to apply. Example 6-24 shows the process of defining these tags.

Example 6-24 *Defining COR List Tags*

```
Router# configure terminal
Router(config)# dial-peer cor custom
Router(config-dp-cor)# name 911
Router(config-dp-cor)# name LOCAL
Router(config-dp-cor)# name LD
```

At this point, we defined the tags 911, LOCAL, and LD, which represent the various outgoing restrictions we can place. At this point, these tags are doing absolutely nothing, but because we defined the names, the CME router allows us to use them to create COR lists. We first create the outgoing COR lists that we will apply to the PSTN dial peers, as shown in Example 6-25.

Example 6-25 *Creating Outgoing COR Lists*

```
Router(config)# dial-peer cor list 911-CALL
Router(config-dp-corlist)# member 911
Router(config-dp-corlist)# exit
Router(config)# dial-peer cor list LOCAL-CALL
Router(config-dp-corlist)# member LOCAL
Router(config-dp-corlist)# exit
Router(config)# dial-peer cor list LD-CALL
Router(config-dp-corlist)# member LD
Router(config-dp-corlist)# exit
```

We will eventually apply the COR lists shown in Example 6-25 as outgoing COR lists (to the PSTN dial peers). If you were to read these COR lists in plain English, the 911-CALL COR list would say, "For this COR list to allow the call, the caller must be assigned the 911 tag." The LOCAL-CALL COR list would say, "For this COR list to allow the call, the caller must be assigned the LOCAL tag." Hopefully, you get the idea, but keep in mind that the COR lists are not doing anything because we have not yet applied them to the dial peers. Next, we create the incoming COR lists, as shown in Example 6-26.

Example 6-26 *Creating Incoming COR Lists*

```
Router(config)# dial-peer cor list 911-ONLY
Router(config-dp-corlist)# member 911
Router(config-dp-corlist)# exit
Router(config)# dial-peer cor list 911-LOCAL
Router(config-dp-corlist)# member 911
Router(config-dp-corlist)# member LOCAL
Router(config-dp-corlist)# exit
Router(config)# dial-peer cor list 911-LOCAL-LD
Router(config-dp-corlist)# member 911
Router(config-dp-corlist)# member LOCAL
Router(config-dp-corlist)# member LD
Router(config-dp-corlist)# exit
```

We will eventually apply the COR lists shown in Example 6-26 to the ephone-dns to grant calling privileges. If you were to read these COR lists in plain English, the 911-ONLY COR list would say, "Anyone assigned to this COR list can call dial peers requiring the 911 tag." The 911-LOCAL COR list would say, "Anyone assigned to this COR list can call dial peers requiring the 911 or LOCAL tags."

Note You might wonder, "How do these COR lists say different things when they're created the same way?" Fair question, and likely the heart of what makes COR lists so confusing. Both the inbound and outbound COR lists are created the same way, but the effect they have is based on how you apply them. If you apply a COR list in the outbound direction, it says, "I will require a caller to have the defined tags to complete a call." If you apply a COR list in the inbound direction, it says, "I will assign these tags to a caller, which grant the ability to place a call."

Now, we can move to the final two steps: assigning the inbound and outbound COR lists. Example 6-27 shows how this is done.

Example 6-27 *Assigning Outbound and Inbound COR Lists*

```
Router(config)# dial-peer voice 10 pots
Router(config-dial-peer)# corlist outgoing 911-CALL
Router(config-dial-peer)# exit
Router(config)# dial-peer voice 11 pots
Router(config-dial-peer)# corlist outgoing LOCAL-CALL
Router(config-dial-peer)# exit
Router(config)# dial-peer voice 12 pots
Router(config-dial-peer)# corlist outgoing LD-CALL
Router(config-dial-peer)# exit
Router(config)# ephone-dn 1
Router(config-ephone-dn)# corlist incoming 911-ONLY
Router(config-ephone-dn)# exit
Router(config)# ephone-dn 2
Router(config-ephone-dn)# corlist incoming 911-LOCAL
Router(config-ephone-dn)# exit
Router(config)# ephone-dn 3
Router(config-ephone-dn)# corlist incoming 911-LOCAL-LD
Router(config-ephone-dn)# exit
```


Note Example 6-27 assumes dial peers 10, 11, and 12 have been previously configured with the necessary destination-pattern and port values to correctly route the call to the PSTN.

Example 6-27 puts it all together. You might need to flip back through the last couple pages to see the building examples to fill the pieces in your own mind. To see this in action, we follow a call originated from the lobby phone (ephone-dn 1):

1. Someone picks up the lobby phone and calls 4805551212.
2. CME immediately assigns the lobby phone the 911-ONLY COR list, which assigns the tag 911.
3. CME matches the outbound dial peer 11, which is assigned the outgoing COR list LOCAL-CALL.
4. The outgoing LOCAL-CALL COR list requires the LOCAL tag.
5. Because the lobby phone was only assigned the 911 tag (and not LOCAL), the call fails with a reorder tone.

Okay, you have now seen how COR lists deny a call. Let's now follow a call that succeeds from the employee phone (ephone-dn 2):

1. An employee picks up her phone and calls 4805551212.
2. CME immediately assigns the employee phone the 911-LOCAL COR list, which assigns the tags 911 and LOCAL.

3. CME matches the outbound dial peer 11, which is assigned the outgoing COR list LOCAL-CALL.
4. The outgoing LOCAL-CALL COR list requires the LOCAL tag.
5. Because the employee phone is assigned the 911 and LOCAL tags, the call completes successfully.

Note In the previous COR list scenarios, the incoming COR list are applied to ephone-DNs and the outgoing COR list are applied to dial peers. Although this is the most common configuration, you can apply incoming and outgoing COR lists to any combination of calling or called entities. For example, you might apply an incoming COR list to a PSTN dial peer to restrict which internal extensions a PSTN caller can reach.

That's the foundation of COR lists! Now, with that understanding, there are a couple important rules of COR lists that you should know:

Key Topic

Rule 1: If there is no outgoing COR list applied, the call is always routed.

Rule 2: If there is no incoming COR list applied, the call is always routed.

Typically, Rule 1 usually makes perfect sense. For example, if you created a PSTN dial-peer that you'd like all phones to access, simply do not apply an outgoing COR list. After that is done, the PSTN dial peer does not require any COR list tags to pass the call through. Now, regardless of the incoming COR list applied to an ephone-dn (or a complete lack of COR list applied to the ephone-dn), the call to the PSTN dial peer completes successfully.

However, Rule 2 seems to make no sense at all. If a calling entity (like an ephone-dn) does not have an incoming COR list, it is able to call any other entity regardless of the outgoing COR list assigned. Nonetheless, this is the way the rule works. Think of it this way: If a calling entity does not have an incoming COR list, no calling restrictions are applied to the device. By using this approach, Cisco has lessened the potential of causing outages when applying COR to your CME router. COR always requires an inbound COR list meeting an outbound COR list. If either of those entities is missing, CME permits the call.

With these two rules in mind, we could make our previous configuration example more efficient. You might remember that the scenario required the manager phone (ephone-dn 3) to be able to call any of the listed dial-peers. To accomplish this, we created a COR list called 911-LOCAL-LD that listed all three COR tags. However, in light of Rule 2, we could have simply not assigned ephone-dn 3 an incoming COR list, and we would have accomplished the same objective.

We could have applied a similar efficiency for emergency calling. Every ephone-dn in our scenario had the ability to make emergency calls. This was granted to them because every ephone-dn had the 911 tag assigned to their incoming COR list. However, in light of Rule 1, we could have not assigned an outgoing COR list to dial-peer 10 (which was used for emergency calls). At that point, any of the ephone-dns would be able to use the dial-peer regardless of their incoming COR list.

Tip Even though the previous two rules can make your configuration more efficient, it might help other administrators who not as familiar with CME to add the extra configuration shown in Examples 6-24 through 6-27. Assigning all calling/called entities a COR list makes it less likely that one would "slip through the cracks."

Key Topic

Using CCP to Implement COR

Now that you have a good foundation for the theory and implementation of CME COR, it is time to look at the CCP interface and see how it is done there.

From the Unified Communications > Dial Plans > Calling Restrictions screen, make sure that you are looking at the Outgoing Call Types tab and click **Create**. Then, simply enter the name of your custom COR list tags one at a time (the ones from Example 6-24, in our case). Figure 6-20 shows how you would build the outgoing COR lists from Example 6-25. In the Create Permission window, enter the name of the COR list and select member tags from the Available Call Types list (which we just made in the previous screen).

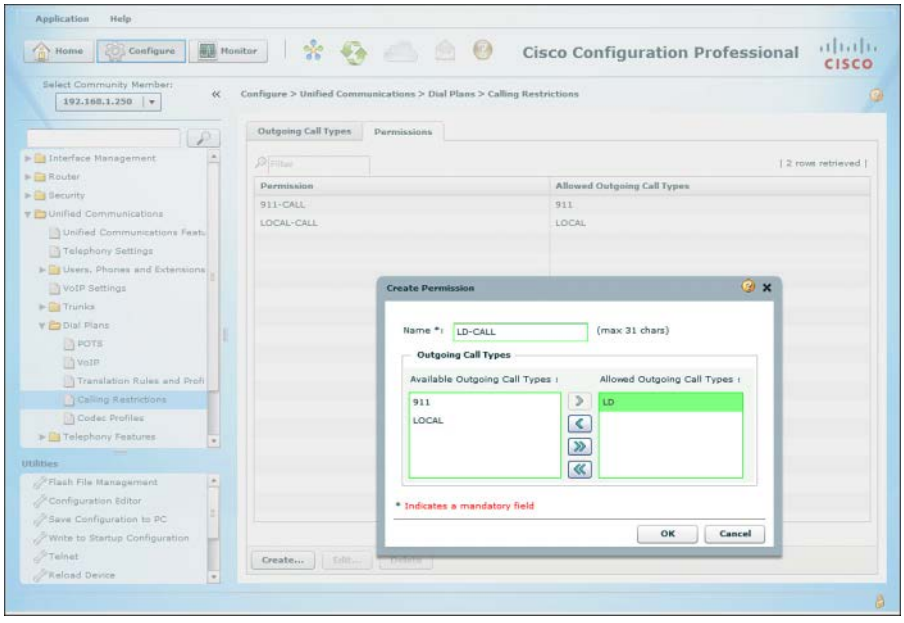


Figure 6-20 *Creating Outgoing COR Lists Using CCP*

Next, using the very same interface, we create the incoming COR lists from Example 6-26, as shown in Figure 6-21.

6

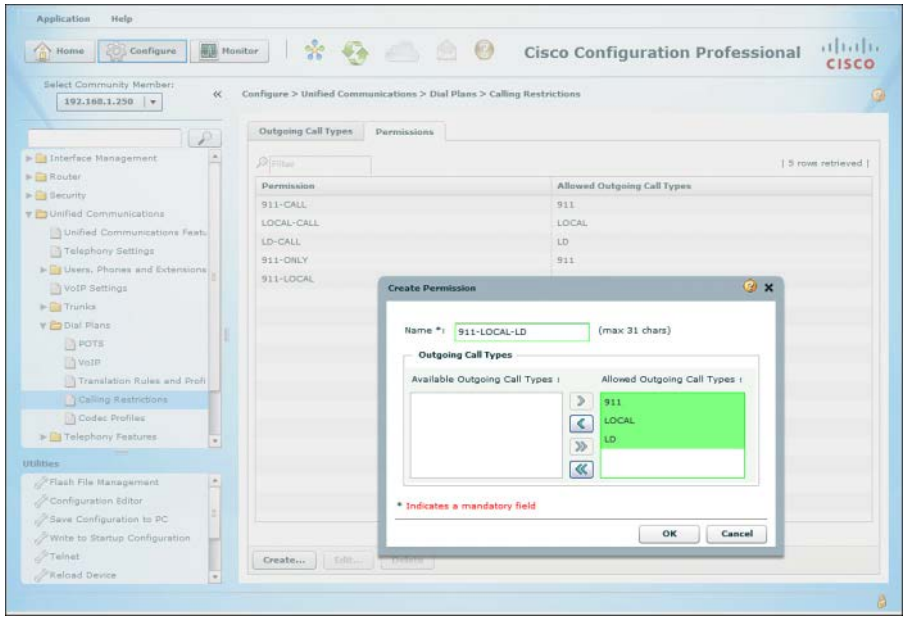


Figure 6-21 *Creating Incoming COR Lists Using CCP*

Next, from the Unified Communications > Dial Plans > POTS > Dial Peers tab, select your dial peers one at a time, and on the configuration page in the Calling Restrictions section, choose the appropriate COR from the Outgoing Call Restriction drop-down. Figure 6-22 shows us setting the 11-digit dial peer with the LD-CALL COR.

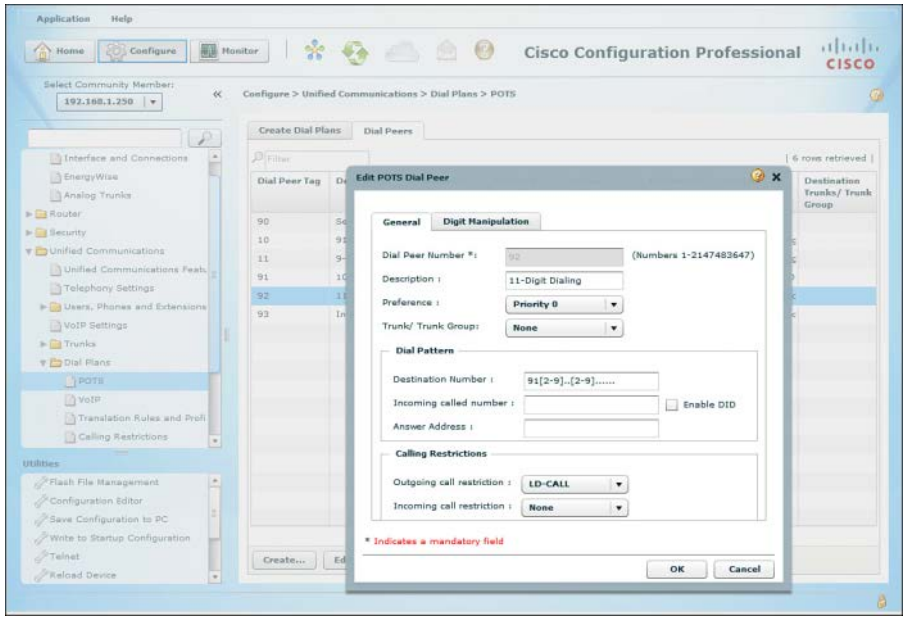


Figure 6-22 *Setting Dial Peer Class of Restriction*

The last piece is to apply the correct COR membership settings to the extensions. In CCP, navigate to **Unified Communications > User, Phones and Extensions > Extensions**, and select your extensions one at a time. Click **Edit**, and in the configuration window, select **Call Restrictions** in the left pane. Note that there are settings for both incoming permissions and outgoing permissions. Figure 6-23 shows the Outgoing Permissions drop-down, with our available COR lists. Choose the appropriate COR membership, and then click **OK** to save your changes. Make the appropriate changes for the other extensions one at a time. Remember, if you choose not to apply a COR list to an extension, that extension will be able to dial any destination number.

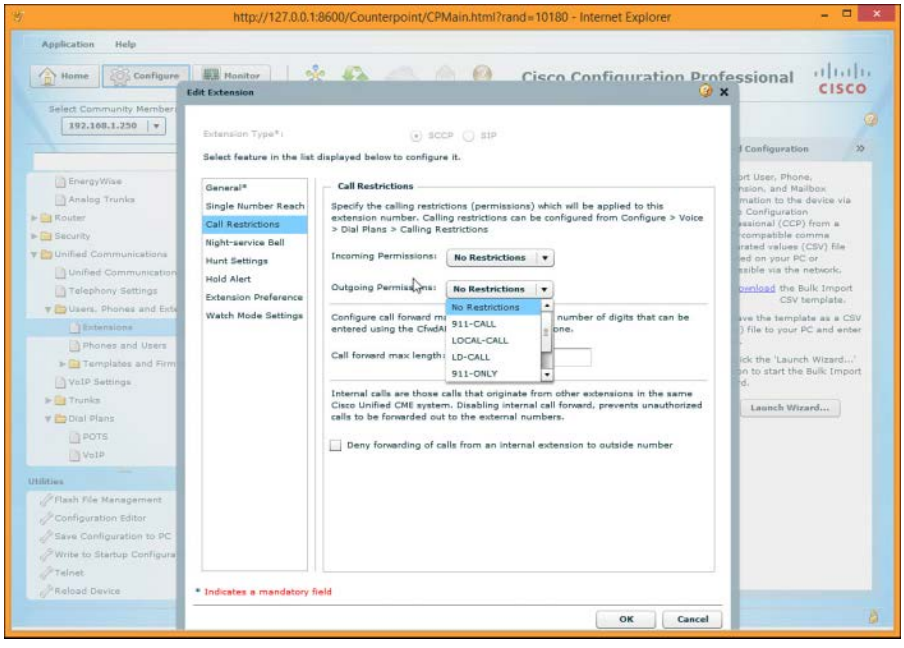


Figure 6-23 *Using CCP to Set COR Membership on an Extension*

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 6-7 describes these key topics and identifies the page number on which each is found.

Key Topic

Table 6-7 Key Topics for Chapter 6

Key Topic Element	Description	Page Number
Figure 6-1	Illustrates the use of analog FXS ports	116
Figure 6-2	Illustrates the use of analog FXO ports	119
Note	Signaling channel information for T1 and E1 interfaces	125
List	Description of POTS and VoIP dial peers	125
Figure 6-5	Illustrates the use of call legs to design dial peer configurations	126
Example 6-7	Basic POTS dial peer configuration	128
Text	Highlights the automatic digit-stripping rule of POTS dial peers	131
Example 6-10	Basic VoIP dial peer configuration	132
Table 6-3	Summarizes dial peer wildcards	133
Table 6-4	Provides examples of using the dial peer bracket wildcard	134
Table 6-5	Provides a sample PSTN dialing plan for North America	134
Example 6-12	Basic PLAR configuration using FXS interfaces	136
List	Highlights the rules Cisco routers use to handle overlapping dial peers	137
List	The method a router uses to match inbound dial peers	140
List	Characteristics of dial peer 0	142
Table 6-6	Summarizes digit-manipulation commands	142
Example 6-17	Implementing WAN to PSTN failover using preference and prefix commands	144
Tip	Tip on how the router handles identical dial peers	144
List	Two key rules of COR lists	158

Definitions of Key Terms

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

Dialed Number Identification Service (DNIS), Automatic Number Identification (ANI), dial peer, foreign exchange station (FXS) ports, foreign exchange office (FXO) ports, private line automatic ringdown (PLAR), Direct Inward Dial (DID), class of restriction (COR)

This chapter covers the following topics:

- **Configuring a Voice Network Directory:** This section walks through the creation of a local directory of CME devices, which gives your users an easier method to find and dial local DNs.
- **Configuring Call Forwarding:** This section discusses the concepts and configuration of the call-forwarding features in the CME environment.
- **Configuring Call Transfer:** This section discusses the concepts and configuration of the call-transfer features in the CME environment.
- **Configuring Call Park:** This section discusses the concepts and configuration of the call park features in the CME environment.
- **Configuring Call Pickup:** This section discusses the concepts and configuration of the call pickup features in the CME environment.
- **Configuring Intercom:** This section discusses the concepts and configuration of the intercom features in the CME environment.
- **Configuring Paging:** This section discusses the concepts and configuration of the paging features in the CME environment.
- **Configuring After-Hours Call Blocking:** This section discusses the methods you can use to allow or deny specific dialing patterns in the after-hours time frame for all or specific IP phones.
- **Configuring CDRs and Call Accounting:** This section discusses the configuration of CDRs and call-accounting features.
- **Configuring Music on Hold:** This section discusses the configuration of Music on Hold (MoH) with CME.
- **Configuring Single Number Reach:** This section discusses the configuration of Single Number Reach using CME.
- **Configuring Ephone Hunt:** This section describes and discusses the configuration of ephone hunt in CME, using CCP.
- **Configuring Night Service:** This section describes and discusses the configuration of the Night Service feature in CME, using CCP.
- **Configuring Shared Ephone-dn:** This section covers the simple feature of shared ephone-dn (shared line).
- **Describe Extension Mobility:** This section discusses the Extension Mobility feature in CME.

CHAPTER 7

Enabling Telephony Features with CME

After implementing the ephone, ephone-dn, and dial-peer concepts, you now have an IP telephony network that can make and place internal and external calls. Beyond basic telephony, organizations expect modern telephony systems to support a whole host of features, such as call transfer, Music on Hold (MoH), conference calling, and so on. This chapter is dedicated to adding these types of features to the CME voice network.

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

Foundation Topics Section	Questions Covered in This Section
Configuring a Voice Network Directory	1
Configuring Call Forwarding	2–3
Configuring Call Transfer	4–5
Configuring Night Service	6
Configuring Call Pickup	7
Configuring Intercom	8
Configuring Paging	9
Configuring Single Number Reach	10

1. What process must you follow to build the local phone directory for the CME environment?
   a. Assign directory entries under each ephone-dn using the **directory** command.
   b. Allow CME to automatically build the directory when you associate the user to the extension using CCP.
   c. Assign directory entries under each ephone using the **directory** command.
   d. Enter the directory configuration mode and begin associating ephone-dn values with directory entry values.

2. What three conditions can be configured for call forwarding settings in CCP?
   a. Forward all calls
   b. Forward when busy
   c. Forward all to voicemail
   d. Forward unattended calls
3. What happens if the user selects Do Not Disturb on his phone but there is no Call Forward setting configured for that line?
   a. The call is automatically forwarded to voicemail.
   b. The call is automatically forwarded to the operator.
   c. The call is dropped.
   d. The call information is displayed on the phone screen, but it does not ring and the visual indicator lamp does not blink.
4. Which of the following transfer modes does a Cisco router support by default?
   a. Blind
   b. Consult
   c. Full-blind
   d. Full-consult
5. What is required to provide call transfer capability to CME users?
   a. Add the Transfer softkey to the softkey template configuration for the phone.
   b. No action is required because the default template includes the Transfer softkey.
   c. Enable H.420 full-consult transfer at the CLI.
   d. Add the Call Park softkey to the phone template because transfer operations are performed using the Call Park feature in CME.
6. Which of the following is true of the CME Night Service feature? (Choose all that apply.)
   a. Night Service is a legacy feature that has been deprecated in current versions of CME.
   b. Night Service automatically activates the auto-attendant during closed hours.
   c. Up to three IP phones can be designated for Night Service.
   d. Night Service rings a designated ephone-dn during a specified schedule, or when manually activated using a code.
7. By default, what does pressing the PickUp softkey allow you to do in a Cisco Unified CME environment?
   a. Pick up a ringing phone in your group
   b. Pick up a ringing phone in another group
   c. Answer your own ringing phone
   d. Pick up a specific ringing extension (which you must specify)

8. You are watching an administrator configure an intercom line using CCP. You notice that the intercom directory number was autocreated as A200208. What is the significance of this number? (Choose two.)
   a. The *A* in A200208 indicates that this is the first intercom button on the phone.
   b. The *A* in A200208 prevents the number from being dialed from an IP phone.
   c. A200208 is autogenerated to indicate that an intercom button is configured on button 8 to ring the target phone that has extension 2002.
   d. A200208 is autogenerated to indicate that an intercom button is configured on the phone with extension 2002, on button 8.

9. What is the maximum number of paging groups to which a Cisco IP phone can belong?
   a. 1
   b. 5
   c. 25
   d. No practical limit

10. A user is on an active call at the office using his desk phone. Midway through the call, he presses the Mobility softkey on the screen of his IP phone. What process occurs?
   a. The call transfers to his preconfigured single number reach number.
   b. CME places the call on hold and allows retrieval from a remote phone.
   c. CME places the call on hold and allows retrieval from a predefined call park number.
   d. The user logs out of the phone and then logs in to a new phone where he retrieves the call.

Foundation Topics

Configuring a Voice Network Directory

As you have already seen, Cisco IP phones support a local directory that you can update from the Cisco Unified Communication Manager Express (CME) router as you are configuring devices.

You can enter names under ephone-dn configuration mode either as you are configuring new lines for the organization or separately, after you configure the lines. These names are used both for building the internal corporate phone directory (often called the local directory) and for caller ID information.

Most of the current Cisco IP phone models allow you to browse the corporate directory by pressing the Directory button on the phone itself. Some low-end IP phones may not have a dedicated Directory button, but instead have a menu-driven process to get there. After you press the Directory button, you are able to browse categories, including Missed Calls, Received Calls, and so on. Move down to the option showing the Local Directory, as shown in Figure 7-1.

Figure 7-1 *Browsing Phone Directories*

After you select the local directory, the IP phone gives you the option to search by first or last name by typing in a user's name as a string on the IP phone. You can enter as many characters as you like to filter down the number of results, or simply press the **Select** softkey to see the entire corporate directory, as shown in Figure 7-2.

Figure 7-2 *Local CME Directory*

By default, Cisco Unified CME organizes the local directory alphabetically by first name. You can change this setting by using the **directory** command from telephony service configuration mode. In addition, you can also add manual entries to the directory by using the **directory entry** command. This is useful for devices in the company that do not have an explicit ephone-dn configuration. Example 7-1 demonstrates these two commands in action.

Example 7-1 *Configuring Manual Local Directory Entries*

```
CME_Voice(config-telephony)# directory ?
  entry             Define new directory entry
  first-name-first  first name is first in ephone-dn name field
  last-name-first   last name is first in ephone-dn name field
CME_Voice(config-telephony)# directory last-name-first
CME_Voice(config-telephony)# directory entry ?
  <1-100>  Directory entry tag
  clear    clear all directory entries
CME_Voice(config-telephony)# directory entry 1 ?
  WORD  A sequence of digits representing dir. number
CME_Voice(config-telephony)# directory entry 1 1599 ?
  name  Define directory name
CME_Voice(config-telephony)# directory entry 1 1599 name ?
  LINE  A string - representing directory name (max length: 24 chars)
CME_Voice(config-telephony)# directory entry 1 1599 name Corporate Fax
```

Note As you can see from the context-sensitive help, you can add up to 100 manual entries to the local CME directory. Also, keep in mind that sorting alphabetically by last name flips all the information in the directory to list last name first. CME will list the Corporate Fax directory entry just added as Fax Corporate.

If you are using the Cisco Configuration Professional (CCP) to manage caller ID and local directory configurations, the graphical user interface (GUI) performs the caller ID assignment for you when you associate a user with a phone/extension. You might remember that the CCP utility does not associate extensions (ephone-dns) directly to phones (ephones). Instead, after you create the necessary extensions and phones, they are linked together through the user account. Once you add a first name and last name to the user account, the name is applied to the extension associated to that user account. As shown in Figure 7-3, the user account Peter Rock is associated with extension 1501 (using the Phones/Extensions tab, not pictured in Figure 7-3).

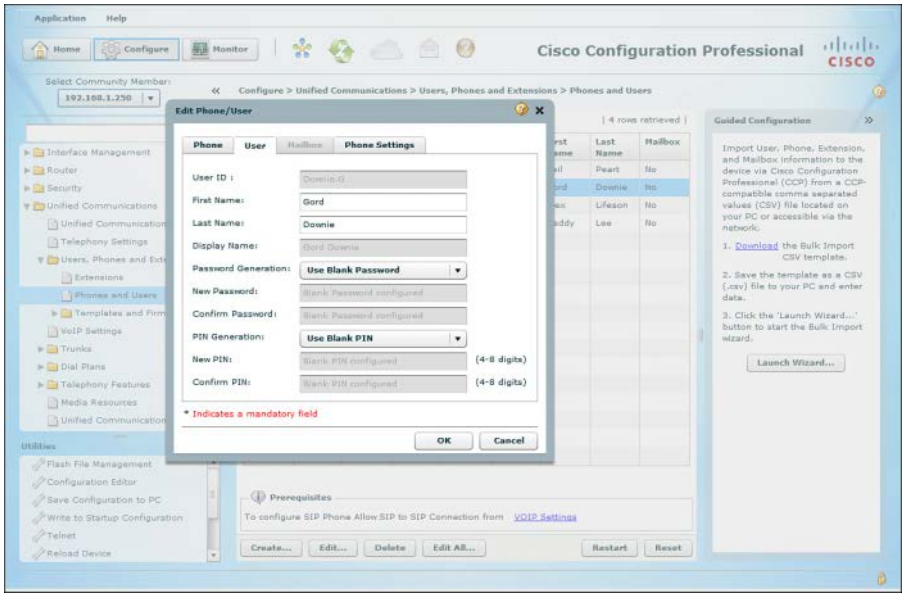


Figure 7-3 *Assigning Directory Information Using CCP*

Likewise, you can find the directory sorting option under **Unified Communications > Advanced Telephony Settings > System Config** (shown in Figure 7-4).

Finally, you can create manual directory entries by navigating to **Unified Communications > Telephony Features > Directory Services** (shown in Figure 7-5).

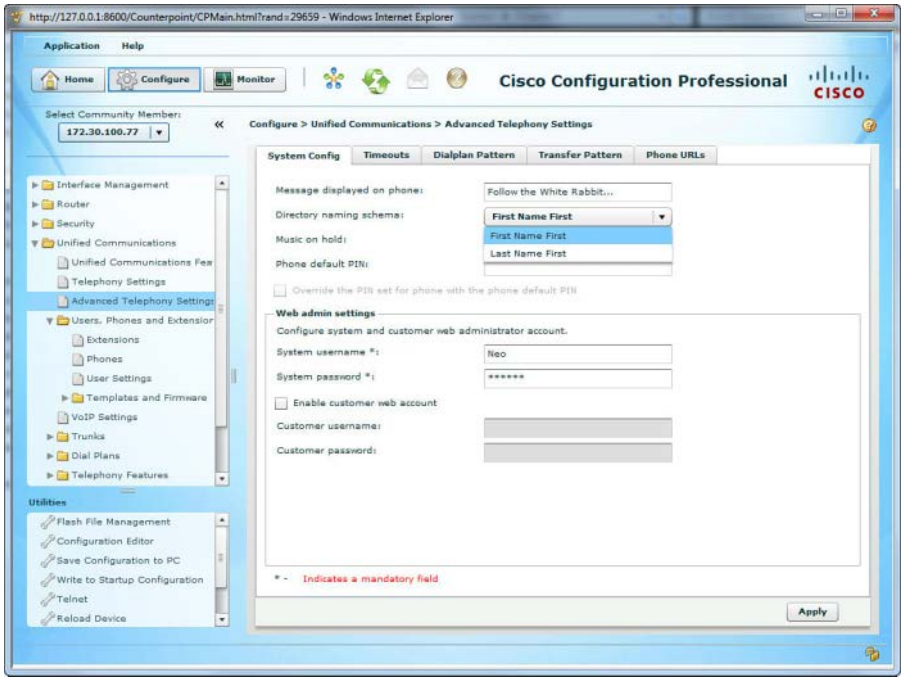


Figure 7-4 *CCP Directory Sorting Options*

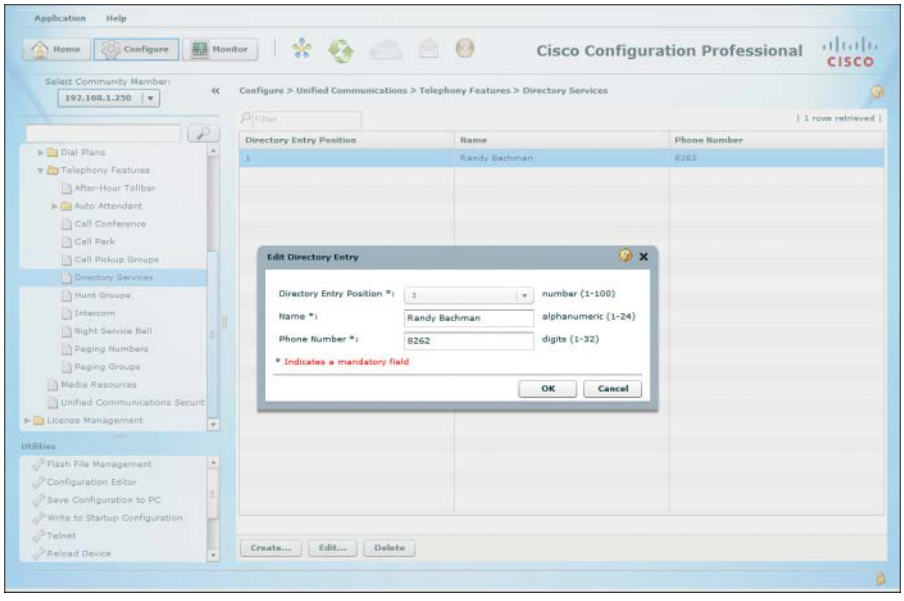


Figure 7-5 *Adding Manual Directory Entries with CCP*

Configuring Call Forwarding

There are two methods used to forward calls to a different destination: from the IP phone (the user's method) and from the Cisco IOS CLI (the administrator's method). This section describes both methods and also provides an overview of the **call-forward pattern** command.

Forwarding Calls from the IP Phone

To forward calls from the IP phone, just press the **CFwdAll** softkey button, as shown in Figure 7-6. The IP phone beeps twice and allows you to enter a number. Enter the number to which all calls on the IP phone will forward, and then press the pound key (#) on the phone so that it knows you are done entering the number. To cancel call forwarding, press the **CFwdAll** button a second time.

Tip If you want to forward all calls directly to voicemail, press the **CFwdAll** button followed by the **Messages** button on the IP phone.

Figure 7-6 *Forwarding Calls from the Cisco IP Phone*

Forwarding Calls from the CLI

Forwarding calls from the command line gives you more options than does forwarding calls from the IP phone, as shown in Example 7-2. As usual, although the majority of CLI command knowledge has been de-emphasized for the CICD exam, it is still a useful thing to know, so it is presented here for your benefit and enjoyment.

Key Topic

Example 7-2 *Forwarding Calls from the Cisco IOS CLI*

```
CME_Voice(config)# ephone-dn 21
CME_Voice(config-ephone-dn)# call-forward ?
  all             forward all calls
  busy            forward call on busy
  max-length      max number of digits allowed for CFwdAll from IP phone
  night-service   forward call on activated night-service
  noan            forward call on no-answer
```

```
CME_Voice(config-ephone-dn)# call-forward busy 1599
CME_Voice(config-ephone-dn)# call-forward noan 1599 ?
  timeout  Ringing no answer timeout duration
CME_Voice(config-ephone-dn)# call-forward noan 1599 timeout ?
  <3-60000>  Ringing no answer timeout duration in seconds
CME_Voice(config-ephone-dn)# call-forward noan 1599 timeout 25
```

These options allow you to forward calls that are busy or not answering (noan) to a different extension. Although this is typically a voicemail number (which 1599 represents in Example 7-3), this could also be another IP phone if this DN was a member of a hunt group.

Tip In Canada and the United States, the phone rings for 2 seconds followed by 4 seconds of silence. Knowing this can be useful in calculating a good no answer (noan) timeout value.

Also notice that you can specify a max-length value after the **call-forward** command. Using this, you can restrict the IP phone from forwarding to external destinations. If you enter the command **call-forward max-length 0**, CME makes the IP phone call forwarding feature unavailable to the Cisco IP phone. The CFwdAll button will dim on the IP phone and become inaccessible.

Tip At this point, you should have a good idea that plenty of configurations under each ephone-dn are similar to all the others. Make an ephone-dn (and ephone) template in Notepad (or some other text editor) in which you list all the common configuration commands you will be applying in your environment. That way, if you ever need to add new ephone-dns, you will already have a template listing the common commands you need to enter.

Using the call-forward pattern Command to Support H.450.3

There is one additional command to discuss here, which is available from telephony service configuration mode: **call-forward pattern**. This command enables you to enter a pattern for numbers that will support the H.450.3 call forwarding standard.

To understand the benefits of H.450.3, you must first understand what happens with typical VoIP forwarding. When a call enters the network and hits a forwarded device, that device takes responsibility for the call and becomes a tandem hop in the call flow. That means that the voice traffic now forwards through the IP phone that forwarded the call. This can cause quality problems if the device that forwarded the call is a large geographical distance away from the phone receiving the forwarding call. The H.450.3 standard represents a method that allows the CME router to redirect the call directly to the final destination instead of acting as a tandem hop. Figure 7-7 illustrates this concept.

Key Topic

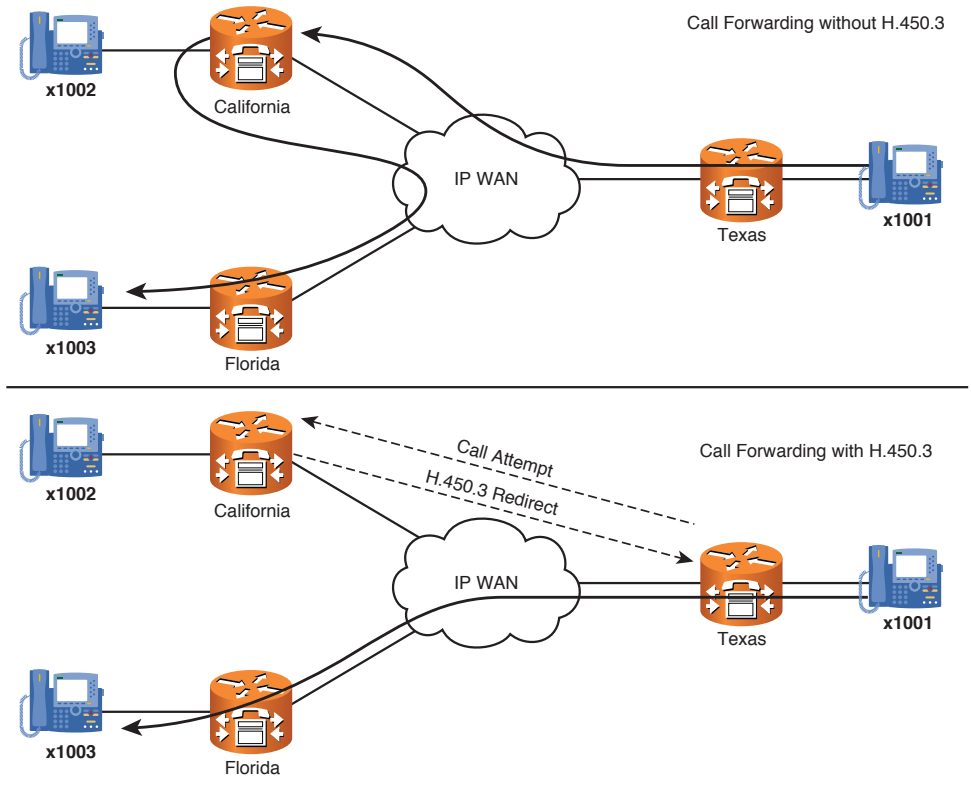


Figure 7-7 *Forwarding Calls with and Without H.450.3 Standards*

In Figure 7-7, the IP phone with x1002 is forwarded to the IP phone with x1003. The top part shows the VoIP call flow without H.450.3 when x1001 places a call to x1002. Notice that the VoIP traffic must pass through the California CME router to reach Florida. This can cause intense quality of service (QoS) problems with the call, such as audio clipping, distortion, and even call drops. This symptom is commonly called *hairpinning* the call.

The bottom part shows the call with H.450.3 support enabled. When the call reaches California, CME sends an H.450.3-based redirect message, instead of accepting the call and forwarding it on to Florida. The VoIP traffic then travels directly from x1001 in Texas to Florida rather than passing through California to get there.

Entering **call-forward pattern** *pattern* from telephony service configuration mode tells CME which numbers should support the H.450.3 standard. Entering the pattern 15.. tells CME, "I want all four-digit numbers that begin with 15 to support H.450.3." Thus, all calls to 15XX extensions would support H.450.3 call forwarding.

Note There is much more to be said about the H.450.3 standard. There is also more configuration that should be in place to fully support H.450.3. This is intended to be a "sneak peek" of the standard, which the CCNP Voice certification track fully explores.

If you prefer to use CCP to make forwarding modifications, you can find the settings under the Advanced tab of the Extensions configuration window (**Unified Communication > Users, Phones, and Extensions > Extensions**), as shown in Figure 7-8.

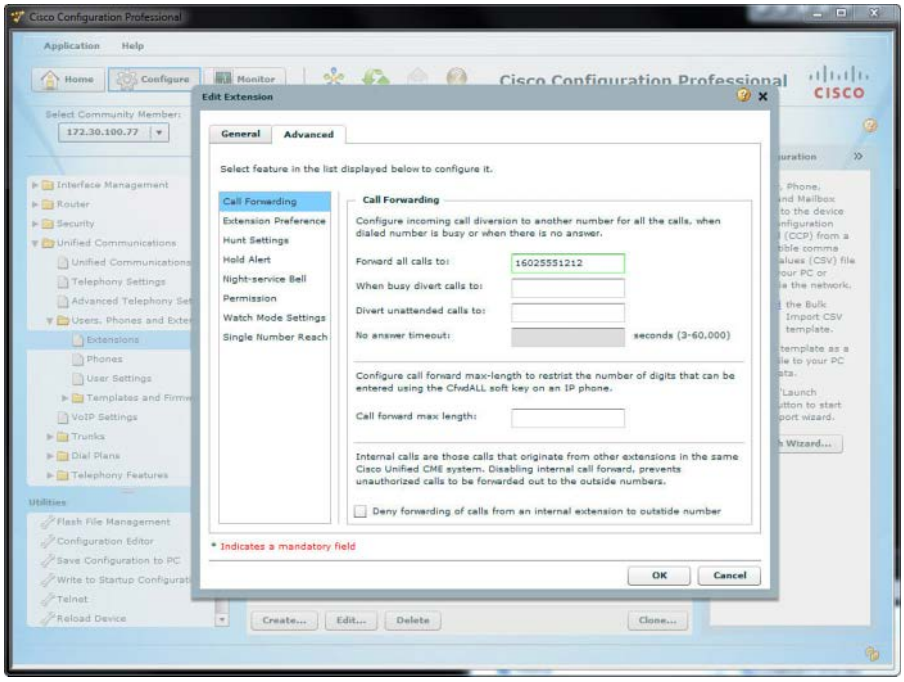


Figure 7-8 *Configuring Call Forwarding Using CCP*

Configuring Call Transfer

Transferring calls is another basic requirement of a business phone system. To transfer a call, press the **Trnsfer** softkey while on an active call. (Note that this is not a typo: Trnsfer without the *a* is correct.) When you do, you hear another dial tone, at which point you can dial the phone number to which you want to transfer your active call. What happens from there depends on the transfer method configured on the CME router. Two transfer methods are available:

Key Topic

- **Consult:** Consult transfer allows you to speak with the other party before transferring the call. After you dial the number to which you want to transfer the call, you can wait for the other party to answer and speak with them before transferring the call. Pressing the Trnsfer softkey a second time transfers the call, dropping you out of the conversation. Consult transfers require a second line (or dual-line configuration). This is the default transfer mode in CME. However, the specific method of transfer used by default in CME is full-consult.
- **Blind:** Blind transfer immediately transfers the call after you dial the number. (You do not hit the Trnsfer softkey a second time.) Blind transfers can work in a single-line configuration.

To configure the transfer method used, see Example 7-3.

Example 7-3 *Configuring CME Transfer Methods System-Wide*

```
CME_Voice(config)# telephony-service
CME_Voice(config-telephony)# transfer-system ?
  full-blind     Perform call transfers without consultation using H.450.2 or SIP
    REFER standard methods
  full-consult   Perform H.450.2/SIP call transfers with consultation using second
    phone line if available, fallback to full-blind if second line unavailable.
    This is the recommended mode for most systems. See also 'supplementary-service'
    commands under 'voice service voip' and dial-peer.
  local-consult  Perform call transfers with local consultation using second phone
    line if available, fallback to blind for non-local consultation/transfer
    target. Uses Cisco  proprietary method.
CME_Voice(config-telephony)# transfer-system full-consult
```

As you can see from the context-sensitive help, three transfer methods are available: full-blind, full-consult, and local-consult. The full-blind, full-consult, and local-consult describe the transfer methods introduced at the beginning of this section. The full-blind and full-consult methods use the industry-standard H.450.2 method of transferring. Just like call forwarding, you do not want to hairpin the call and cause potential QoS issues each time you transfer. If you use the H.450.2 standard when transferring a call, the CME router completely drops the call from the transferring phone and starts a new call at the phone to which the call was transferred.

The local-consult method uses a Cisco proprietary transfer method that performs a consult transfer if multiple lines or dual-line configurations are available but will revert to blind transfers if only a single line is available. Cisco proprietary transfers work similar to the H.450 standard. The only problem is this transfer method results in hairpinned calls if you have non-Cisco IP telephony systems on your network.

Note You can also configure transfer modes individually for each ephone-dn by using the **transfer-mode blind/consult** syntax from ephone-dn configuration mode. Configuring the transfer mode this way uses H.450 standards and overrules the system-wide setting.

By default, the Cisco router restricts transfers to devices that are not locally managed. This is usually a good policy because transferring outside of the company can result in toll fraud. For example, a user could transfer an outside caller to an international number, causing the toll charges to be billed to the organization rather than the outside caller. If you would like to allow transfers outside of the locally managed devices, you can use the **transfer-pattern** *pattern* command from telephony service mode, where *pattern* represents numbers to which you would like to allow transfers. Example 7-4 configures the Cisco Unified CME router to allow transfers to 5XXX extensions and local 10-digit public switched telephone network (PSTN) numbers.

Key Topic

Example 7-4 *Configuring CME Transfer Patterns to Allow Outside Transfers*

```
CME_Voice(config)# telephony-service
CME_Voice(config-telephony)# transfer-pattern ?
  WORD  digit string pattern for permitted non-local call transfers
CME_Voice(config-telephony)# transfer-pattern 5...
CME_Voice(config-telephony)# transfer-pattern 9.........
```

Cisco CCP also allows the configuration of transfer patterns. These are found under **Unified Communications > Advanced Telephony Settings**. The simple configuration window shown in Figure 7-9 allows you to simply click the **Add** button and add manually configured transfer patterns directly into the CCP interface.

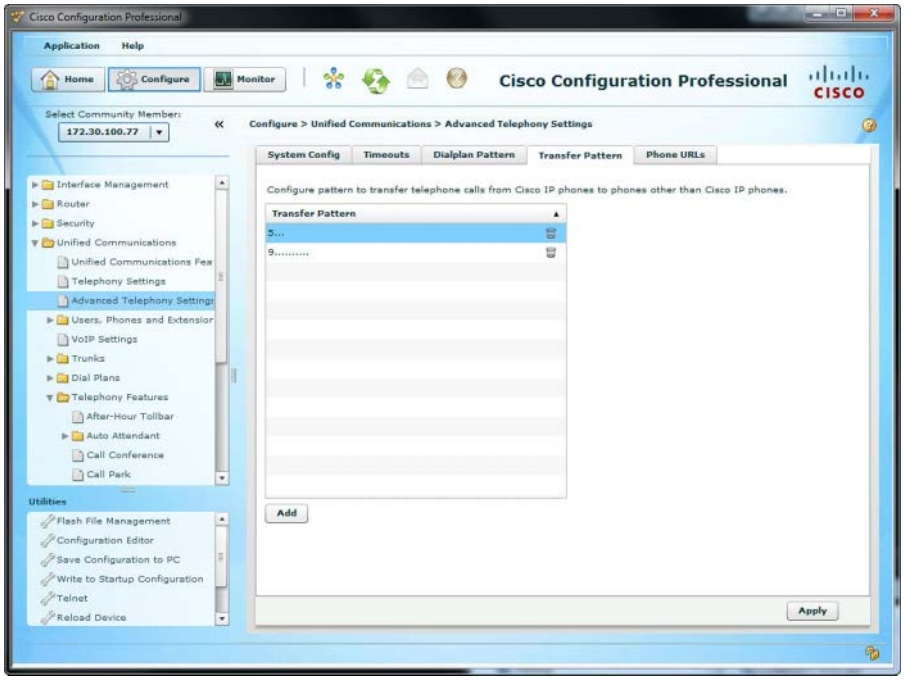


Figure 7-9 *Using CCP to Configure Transfer Patterns*

Configuring Call Park

Typically, when you place a call on hold, you can retrieve the call only from the original phone where you placed the call on hold. Shared-line systems bend the rules by allowing you to retrieve the call from any phone with the same shared line assignment. The call park feature takes this one step further by allowing you to retrieve the call from any phone in the organization. Call park "parks" the caller on hold at an extension rather than on a specific line. Any IP phone that can dial the park extension number can retrieve the call.

The call park system works by finding free ephone-dns in the Cisco Unified CME configuration that you have not assigned to an IP phone and have specifically designated as a call park slot. You can either allow CME to park calls randomly at the first available ephone-dn

or allow users to choose the extension where the call is parked. Each of these scenarios fits different environments. Calls being parked at random extensions might work well for a warehouse environment with a voice-paging system. When an employee has a call, the receptionist could announce, "Larry, you have a call on 5913," over the loudspeaker, at which point Larry could go to a phone and dial the extension to pick up the call on hold.

Choosing extensions would work well for an electronics superstore in which each department responded to a known extension number. For example, software could be extension 301, cameras could be extension 302, and so on. The receptionist can then park multiple calls on a single call park number. (This requires multiple ephone-dns assigned the same extension.) As the specific department retrieves the calls, CME distributes them in the order in which they were parked. The call parked longest is answered first.

You can configure call park simply by adding an ephone-dn designated for call park purposes. Example 7-5 creates two ephone-dns designated for call park.

Example 7-5 *Configuring Call Park Ephone-DNs*

```
CME_Voice(config)# ephone-dn 50
CME_Voice(config-ephone-dn)# number 3001
CME_Voice(config-ephone-dn)# name Maintenance
CME_Voice(config-ephone-dn)# park-slot
CME_Voice(config-ephone-dn)# exit
CME_Voice(config)# ephone-dn 51
CME_Voice(config-ephone-dn)# number 3002
CME_Voice(config-ephone-dn)# name Sales
CME_Voice(config-ephone-dn)# park-slot ?
  reserved-for  Reserve this park slot for the exclusive use of the phone with the
  extension  indicated by the transfer target extension number
  timeout       Set call park timeout
  <cr>
CME_Voice(config-ephone-dn)# park-slot timeout ?
  <0-65535>  Specify the park timeout (seconds) before the call is returned to the
    number it was  parked from
CME_Voice(config-ephone-dn)# park-slot timeout 60 ?
  limit  Set call park timeout count limit
CME_Voice(config-ephone-dn)# park-slot timeout 60 limit ?
  <1-65535>  Specify the number of park timeout cycles before the call is disconnected
CME_Voice(config-ephone-dn)# park-slot timeout 60 limit 10 ?
  notify    Define additional extension number to notify for park timeout
  recall    recall transfer back to originator phone after timeout
  transfer  Transfer to originator or specified destination after timeout limit
    exceeded
  <cr>
CME_Voice(config-ephone-dn)# park-slot timeout 60 limit 10 recall ?
  alternate  Transfer to alternate target if original target is busy
  retry      Set recall/transfer retry interval if target is in use
  <cr>
CME_Voice(config-ephone-dn)# park-slot timeout 60 limit 10 recall
```

Look at the configuration of ephone-dn 50 in Example 7-5. Designating a call park extension is as simple as entering the **park-slot** command under ephone-dn configuration mode.

Note When planning to configure call park, keep in mind that each parked call consumes an ephone-dn slot (regardless of single- or dual-line configurations). You may need to increase the number of ephone-dns (max-dn) that your CME deployment supports.

Example 7-5 also shows that you have many options when you designate call park–specific ephone-dns. Table 7-2 explains where you can use these options.

Table 7-2 Options for Use with the **park slot** Command

Command	Function
reserved-for *dn*	Allows you to reserve the call park slot for the directory number (DN) you enter. Other phones are not able to use the call park slot.
timeout *seconds*	Specifies the number of seconds CME should wait before notifying the phone that parked the call that the call is still parked. To notify, CME rings that phone for one second and displays a message on the LCD display.
limit *count*	Limits the number of timeout intervals a parked call can reach. After this limit is reached, the parked call is disconnected. As a side note, setting this value high is recommended. Customers tend to get bothered when they are on hold for an extended period and then are disconnected.
notify *dn*	Notifies a different DN, in addition to the phone that parked the call, when the parked call reaches timeout period.
only	Used with the prior notify syntax; instructs CME to only ring the DN specified with the notify command rather than ring the original phone.
recall	Causes the call to return (transfer back) to the original phone that parked the call after the parked call reaches the timeout period.
transfer *dn*	Causes the call to transfer to a specified DN after the parked call reaches the timeout period.
alternate *dn*	Allows you to specify an alternate transfer destination should the destination DN specified in the transfer command be on the phone.
retry *seconds*	Sets the amount of time before CME attempts to transfer a parked call again.

There's plenty of flexibility in configuring your call park options. After you have at least one ephone-dn designated for call park (by using the **park-slot** command), the Park softkey appears on the IP phones on an active call.

Note You must restart or reset the IP phones after you configure the initial ephone-dn designated call park before the Park softkey will appear on active calls. You can accomplish this by using the **restart** or **reset** command from telephony service configuration mode.

To park a call, simply press the **Park** softkey while on an active call. CME finds a parking slot for the call and send a message back to the phone that parked the call, as shown in Figure 7-10.

When the user parks the call, CME allocates the first available park slot. Sometimes, you might want to designate which parking slot the call gets, in cases such as those in which each department of the company is assigned a unique call park number. In this case, you can transfer the call (using the Trnsfer softkey) directly into the parking slot you want.

Figure 7-10 *IP Phone After Parking a Call*

Note If you want to use a call park system in which each department has its own call park slot, it may be beneficial to configure multiple ephone-dns assigned to each department designated for call park. Otherwise, you will be able to park only one call for each department.

You can answer parked calls in one of three ways:

- Dial directly into the call park slot. For example, lifting a phone handset and dialing 3001 answers whatever call is parked at 3001.
- Press the **PickUp** softkey and dial the call park number that you want to answer.
- From the phone at which the call was parked, press the **PickUp** softkey followed by an asterisk (*) to recall the most recently parked call back to the phone.

Using CCP to configure call park features automates the process quite a bit. First, navigate to the call park configuration window (**Unified Communications > Telephony Features > Call Park**). Once you arrive there, you can click the **Create** button to bring up the Create Call Park Entry configuration window. Entering a name creates a description label in the IOS for the call park entry. CCP then gives you the option to select the number of slots (call park numbers) as well as the starting number for slots. For example, applying the configuration shown in Figure 7-11 creates 10 park slots, numbered from 1300 through 1309.

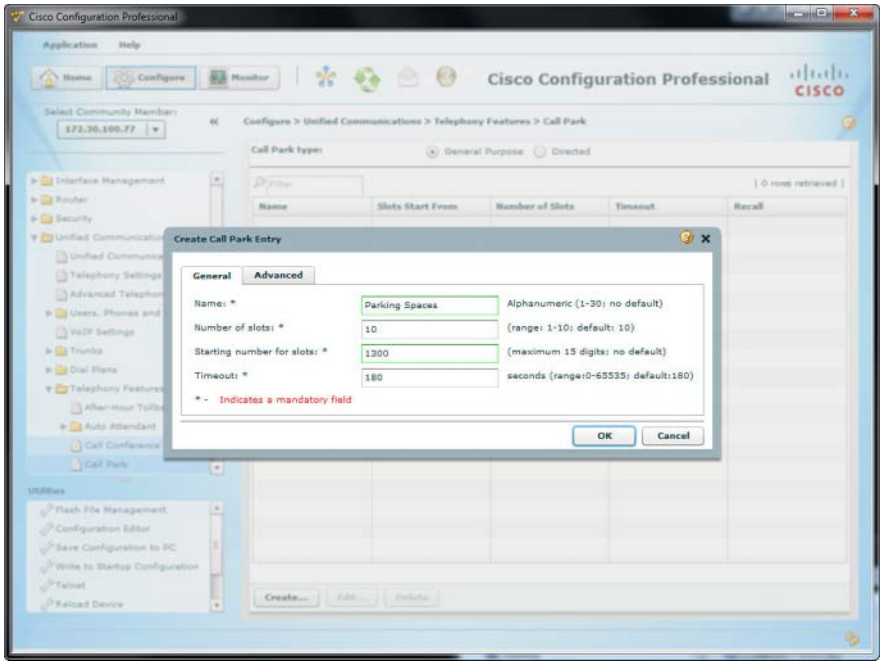


Figure 7-11 *Configuring Call Park Using CCP*

In addition, the Advanced tab of the Call Park Entry configuration window (shown in Figure 7-12) gives you numerous options (discussed in Table 7-2) to modify call park features.

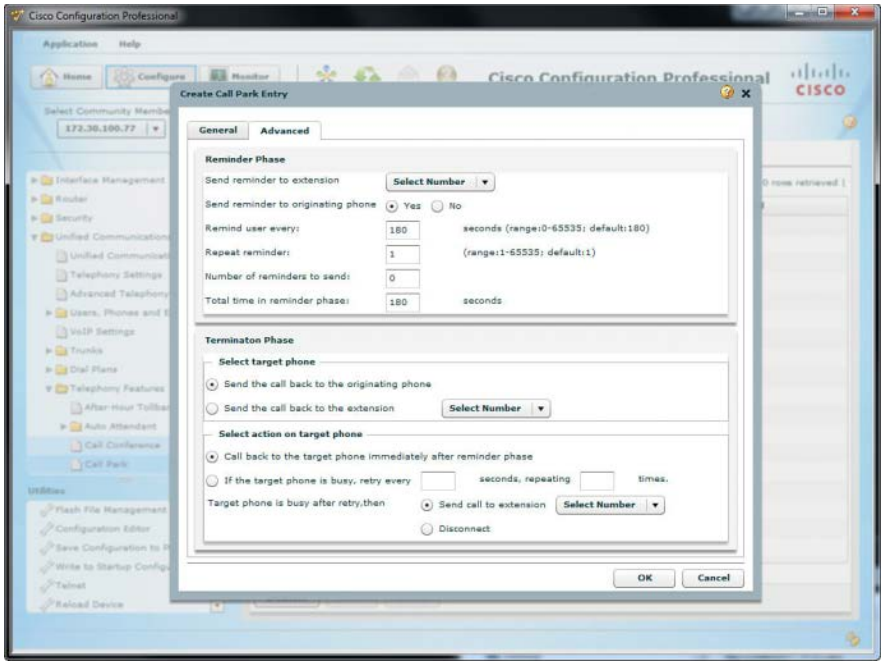


Figure 7-12 *Advanced Call Park Features Available from CCP*

Configuring Call Pickup

Michael works in the sales department at Widget Things, Inc. Being the newest member to the group, he works the late shift, covering calls from 10:30 a.m. to 7:30 p.m. Around 6:00 p.m., the last coworker leaves, and Michael handles all the incoming calls alone. Unfortunately, many of Widget Things' customers have the direct contact information for other sales employees, so a typical evening for Michael consists of running around answering phone calls coming in on the IP phones of the five other sales reps. This is where call pickup features can help.

Call pickup allows you to answer another ringing phone in the organization from your local phone. This is accomplished by pushing the PickUp softkey on the IP phone while another phone is ringing. The call automatically transfers to the local phone, where you can answer it. Of course, the organization is large, and there could be many ringing phones at the same time, so call pickup also gives you the ability to divide the phones into groups. You assign each of these groups a number in the CME configuration, as shown in Figure 7-13.

Based on the softkey used, the users can answer other ringing phones in their own group or enter other group numbers to answer the ringing phones in that group.

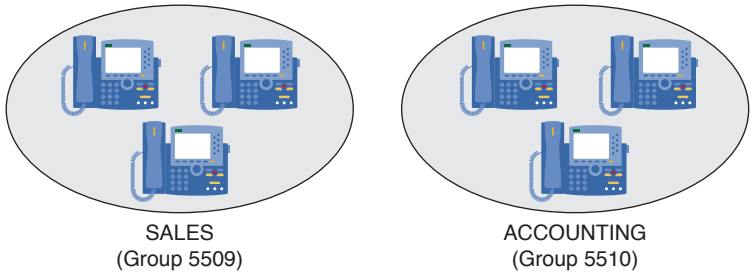


Figure 7-13 *Designing Call Pickup Groups*

The configuration of call pickup is incredibly simple: Just design your groups of phones and assign the ephone-dns to the groups. Example 7-6 assigns ephone-dns 1, 2, and 3 to the SALES group and ephone-dns 4, 5, and 6 to the ACCOUNTING group, as shown in Figure 7-13.

Key Topic

Example 7-6 *Configuring Call Pickup*

```
CME_Voice(config)# ephone-dn 1
CME_Voice(config-ephone-dn)# pickup-group 5509
CME_Voice(config-ephone-dn)# ephone-dn 2
CME_Voice(config-ephone-dn)# pickup-group 5509
CME_Voice(config-ephone-dn)# ephone-dn 3
CME_Voice(config-ephone-dn)# pickup-group 5509
CME_Voice(config-ephone-dn)# ephone-dn 4
CME_Voice(config-ephone-dn)# pickup-group 5510
CME_Voice(config-ephone-dn)# ephone-dn 5
CME_Voice(config-ephone-dn)# pickup-group 5510
CME_Voice(config-ephone-dn)# ephone-dn 6
CME_Voice(config-ephone-dn)# pickup-group 5510
```

Note When you assign the first ephone-dn to a call pickup group number, CME creates the call pickup group. No additional command is needed for the call pickup group creation.

After you assign the ephone-dns to the respective call pickup groups, users can begin answering other ringing phones. CME permits three methods to answer other ringing phones:

Key Topic

- **Directed pickup:** You can pick up another ringing phone directly by pressing the **PickUp** softkey and dialing the DN of the ringing phone. CME then transfers the call and immediately answers it at your local phone.
- **Local group pickup:** You can pick up another ringing phone in the same call pickup group as your phone by pressing the **GPickUp** button and entering an asterisk (*) when you hear the second dial tone.
- **Other group pickup:** You can pick up a ringing phone in another group by pressing the **GPickUp** button and entering the other group number when you hear the second dial tone.

If multiple phones are ringing in the user's call pickup group, CME answers the oldest ringing phone when the user invokes call pickup.

Note The GPickUp softkey functions differently depending on the call pickup configuration in CME. If there is only one group configured in CME, pressing the GPickUp button automatically answers the call from your own group number. You will not hear a second dial tone, and you do not need to dial an asterisk to signify your own group, because only one group is defined. After you configure multiple groups in CME, you hear a second dial tone after pressing the GPickUp softkey; at this point, you can dial either an asterisk for the local group or another group number.

Tip By default, users can pick up other ringing phones managed by CME by using the directed pickup method, described previously, regardless of the destination device being assigned to a Call Pickup group. To disable this feature, enter the command **no service directed-pickup** from telephony service configuration mode. After you enter this command, the PickUp softkey on the IP phones operates as a local group pickup button. Pressing the softkey then immediately answers ringing calls in your own local pickup group.

To create pickup groups in CCP, navigate to the Call Pickup Groups configuration window (**Unified Communications > Telephony Features > Call Pickup Groups**) and click the **Create** button. The user-friendly configuration window allows you to define the pickup group number and allocate which extensions you want to include in the pickup group, as shown in Figure 7-14.

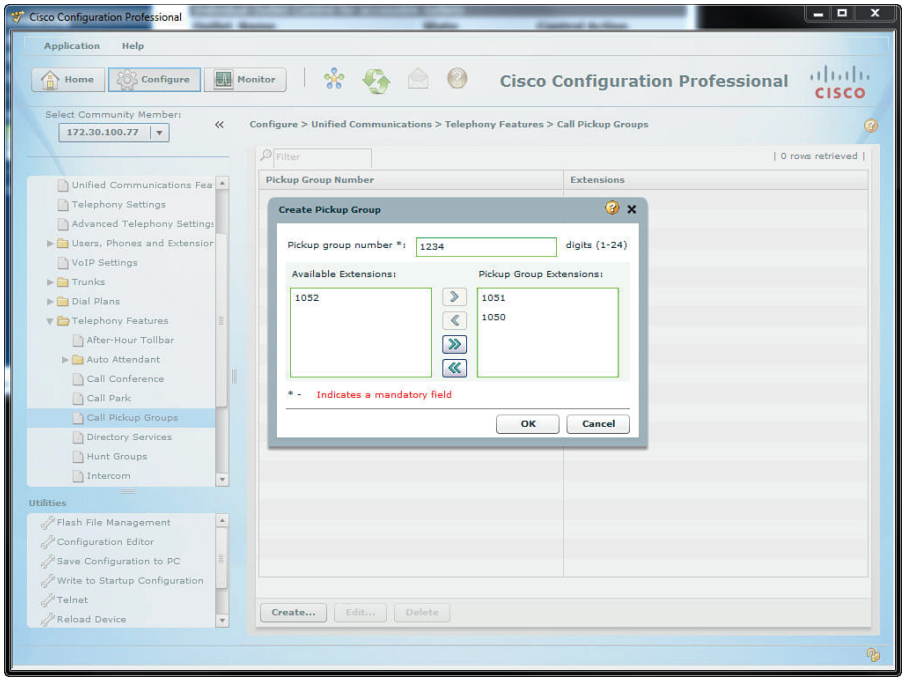


Figure 7-14 *Configuring Call Pickup Groups in CCP*

If you were to click the Deliver button with the CCP configuration shown in Figure 7-14, the CCP delivers the following commands to the Cisco router:

```
ephone-dn 2 dual-line
    pickup-group 1234
    exit
ephone-dn 1 dual-line
    pickup-group 1234
    exit
```

Configuring Intercom

Intercom configurations are common in traditional phone systems. This feature allows an administrative assistant and executive to work closely together by having a speakerphone "tether" between them.

Technically, the way intercom deployments work is through a speed-dial and auto-answer speed-dial configuration. If the administrative assistant presses the button configured as an intercom, it speed dials the executive's phone, which auto-answers the call on muted speakerphone. To establish two-way communication, the executive deactivates mute (by pressing the **Mute** button). Understanding this helps make the intercom configuration much clearer.

To configure intercom functionality, you must configure two new ephone-dns, one for each side of the intercom connection. These intercom lines should be assigned a number, just like any other ephone-dn. However, to prevent others from accidentally (or purposely) dialing the intercom and ending up on muted speakerphone for a random IP phone, the number should be something users cannot dial from other IP phones. The configuration in Example 7-7 accomplishes this objective.

Key Topic

Example 7-7 *Configuring Intercom*

```
CME_Voice(config)# ephone-dn 60
CME_Voice(config-ephone-dn)# number A100
CME_Voice(config-ephone-dn)# intercom A101 label "Manager"
CME_Voice(config-ephone-dn)# exit
CME_Voice(config)# ephone-dn 61
CME_Voice(config-ephone-dn)# number A101
CME_Voice(config-ephone-dn)# intercom A100 label "Assistant"
CME_Voice(config-ephone-dn)# exit
CME_Voice(config)# ephone 1
CME_Voice(config-ephone)# button 2:60
CME_Voice(config-ephone)# restart
restarting 0014.1C48.E71A
CME_Voice(config-ephone)# exit
CME_Voice(config)# ephone 2
CME_Voice(config-ephone)# button 2:61
CME_Voice(config-ephone)# restart
restarting 0019.D122.DCF3
```


Notice the number assigned to ephone-dn 60 is A100. You cannot dial this number from a Cisco IP phone keypad, but you can assign it to a speed-dial button. The **intercom** command acts like a speed-dial button on the ephone-dn. In the case of ephone-dn 60, the command **intercom A101** dials the number A101, which is assigned to ephone-dn 61. Because ephone-dn 61 is also configured with the **intercom** command, it auto-answers the incoming call on muted speakerphone. The label syntax allows you to assign a logical name to the speed-dial; otherwise, the A101 or A100 label will show up next to the line button on the phone. There are three other arguments you can use with the **intercom** command to tune the functionality:

- **barge-in:** Automatically places an existing call on hold and causes the intercom to immediately answer.
- **no-auto-answer:** Causes the phone to ring rather than auto-answer on speakerphone.
- **no-mute:** Causes the intercom to answer with unmuted speakerphone rather than muted. Although this is beneficial to allow immediate two-way conversation, you run the risk of one side barging into existing conversations or background noise.

CCP can also configure Intercom functionality. To do this, navigate to **Unified Communications > Telephony Features > Intercom** and click the **Create** button. The configuration window shown in Figure 7-15 allows you to select the user and speed-dial button you want to assign intercom functionality.

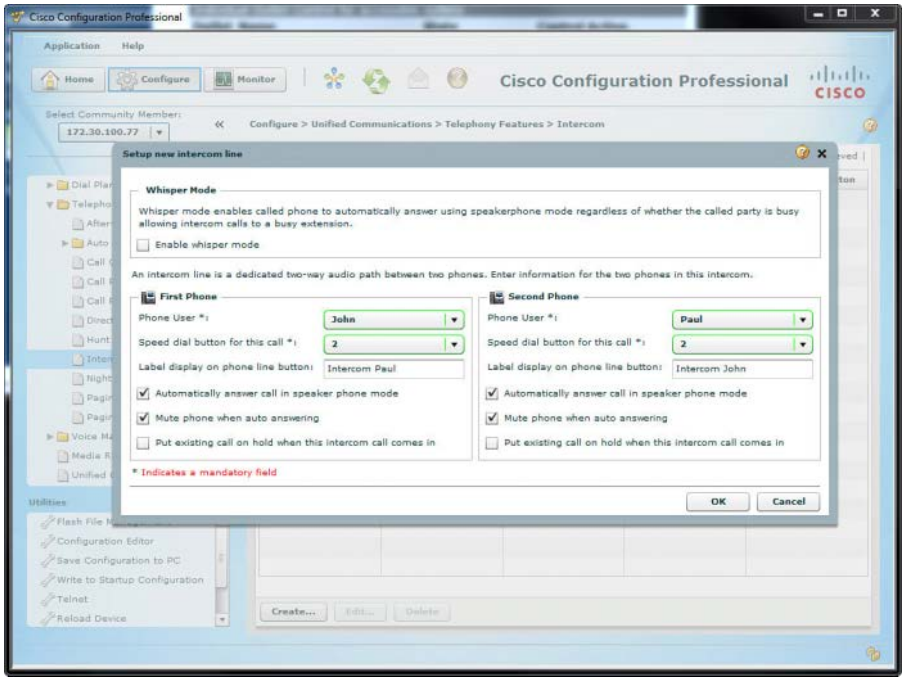


Figure 7-15 *Configuring Intercom in CCP*

After you click the **Deliver** button, CCP applies the following syntax to the router. Notice that CCP also uses alphanumeric speed dials to prevent other users from accessing the intercom functionality inadvertently. The number is automatically generated in this way: A *primary-extension-of-source-phone Button-number*. So, if you create an intercom on button 2 of the phone with extension 1050, to the phone with extension 1051, the autogenerated intercom number is A105002:

```
ephone-dn 5
 number A105002
 description Intercom
 intercom A105102 label "Intercom Paul"
 exit
ephone-dn 4
 number A105102
 description Intercom
 intercom A105002 label "Intercom John"
 exit
ephone-dn 5
 name ""
 exit
```

```
ephone 2
 button  2:5
 restart
 exit
ephone-dn 4
 name ""
 exit
ephone 3
 button  2:4
 restart
 exit
```

Configuring Paging

Paging is similar to the intercom concept; however, it provides only a one-way automatic path for communication. This is useful to allow broadcast messages, such as emergency notifications or to notify employees of holding calls.

The CME paging system works by designating an ephone-dn as a paging number. Calls to the DN of this ephone-dn broadcast to the IP phones that you assigned to this paging group. Figure 7-16 illustrates this concept.

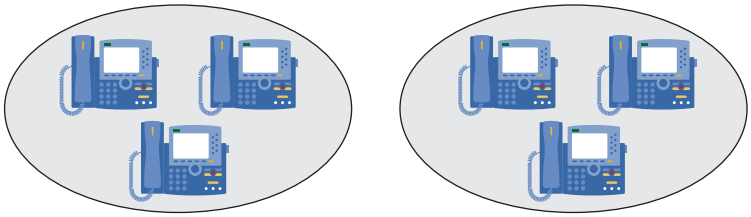


Figure 7-16 *Call Paging Functionality*

As shown in Figure 7-16, calls to DN 5555 page the three phones assigned to that paging group. Calls to 5556 do the same for the paging group 81.

Key Topic

Note You can assign an IP phone to only one paging group. However, CME allows you to create paging numbers that page multiple paging groups, thus providing directed and company-wide paging functionality.

CME supports paging in unicast and multicast configurations. Paging in unicast configuration causes the CME router to send individual messages to each one of the IP phones in the group. So, if six IP phones were assigned to paging group 80, a page to the group would cause the CME router to stream six individual audio signals to the devices. Because of the overhead this causes, CME limits unicast paging groups to a maximum of ten IP phones.

Multicast configuration allows the CME router to send one audio stream, which only the IP phones assigned to the paging group will receive. This allows a virtually limitless number of IP phones in each paging group. Sounds like the winning option, right? The catch is this: To support multicast paging, you must configure the foundation network environment to support multicast traffic. Some of these configurations can get complex and are covered in the CCNP certification track.

The three paging configurations are unicast paging, multicast paging, and multiple-group paging. Example 7-8 shows unicast, single-group paging.

Key Topic

Example 7-8 *Configuring Unicast, Single-Group Paging*

```
CME_Voice(config)# ephone-dn 80
CME_Voice(config-ephone-dn)# number 5555
CME_Voice(config-ephone-dn)# paging
CME_Voice(config-ephone-dn)# exit
CME_Voice(config)# ephone 1
CME_Voice(config-ephone)# paging-dn 80
CME_Voice(config-ephone)# exit
CME_Voice(config)# ephone 2
CME_Voice(config-ephone)# paging-dn 80
```

Calls to the paging number 5555 now page both ephones 1 and 2 using unicast paging. To convert the configuration in Example 7-8 to multicast paging, you could modify the **paging** command with the following syntax:

```
CME_Voice(config)# ephone-dn 80
CME_Voice(config-ephone-dn)# paging in 239.1.1.100 port 2000
```

The IP address that follows the **paging** command is a multicast address. Think of this as a "radio frequency" that the IP phones tune to each time a page occurs. Just like a car radio tuning to a specific FM frequency to hear a radio station, the IP phones tune into the IP address 239.1.1.100 and hear the audio stream for the paging system. As previously mentioned, you must configure your network to properly support multicast traffic. Otherwise, your switches treat this multicast traffic just like it treats broadcasts, flooding your network on all ports each time a page occurs.

The paging configuration in Example 7-9 demonstrates the configuration of a multiple-group paging system. Ephones 1 and 2 continue to use ephone-dn 80 as their dedicated paging group. Ephones 3 and 4 use ephone-dn 81. This time, a third paging group enables you to page both paging groups at once. This gives an organization the flexibility to page specific departments or the company as a whole.

Example 7-9 *Configuring Multiple-Group Paging*

```
CME_Voice(config)# ephone-dn 80
CME_Voice(config-ephone-dn)# number 5555
CME_Voice(config-ephone-dn)# paging
CME_Voice(config-ephone-dn)# exit
```

```
CME_Voice(config)# ephone-dn 81
CME_Voice(config-ephone-dn)# number 5556
CME_Voice(config-ephone-dn)# paging
CME_Voice(config-ephone-dn)# exit
CME_Voice(config)# ephone-dn 82
CME_Voice(config-ephone-dn)# number 5557
CME_Voice(config-ephone-dn)# paging group 80,81
CME_Voice(config-ephone-dn)# exit
CME_Voice(config)# ephone 1
CME_Voice(config-ephone)# paging-dn 80
CME_Voice(config-ephone)# exit
CME_Voice(config)# ephone 2
CME_Voice(config-ephone)# paging-dn 80
CME_Voice(config-ephone)# exit
CME_Voice(config)# ephone 3
CME_Voice(config-ephone)# paging-dn 81
CME_Voice(config-ephone)# exit
CME_Voice(config)# ephone 4
CME_Voice(config-ephone)# paging-dn 81
```

With the configuration shown in Example 7-9, a call to DN 5555 pages ephones 1 and 2, a call to DN 5556 pages ephones 3 and 4, and a call to DN 5557 pages all ephones. You do not need to assign any ephones to paging-dn 82 because this ephone-dn represents a group of both paging-dns 80 and 81.

Note CME allows you to list up to 10 paging numbers using the **paging group** command.

If you choose to use CCP to configure paging, navigate to **Unified Communications > Telephony Features > Paging Numbers**. Clicking the **Create** button allows you to define numbers and associate phones, as shown in Figure 7-17. Think of this as the single-group paging configuration.

CCP also allows the configuration of multiple-group paging. By navigating to **Unified Communications > Telephony Features > Paging Groups**, you can create paging group numbers that associate with other paging groups rather than individual extensions, as shown in Figure 7-18.

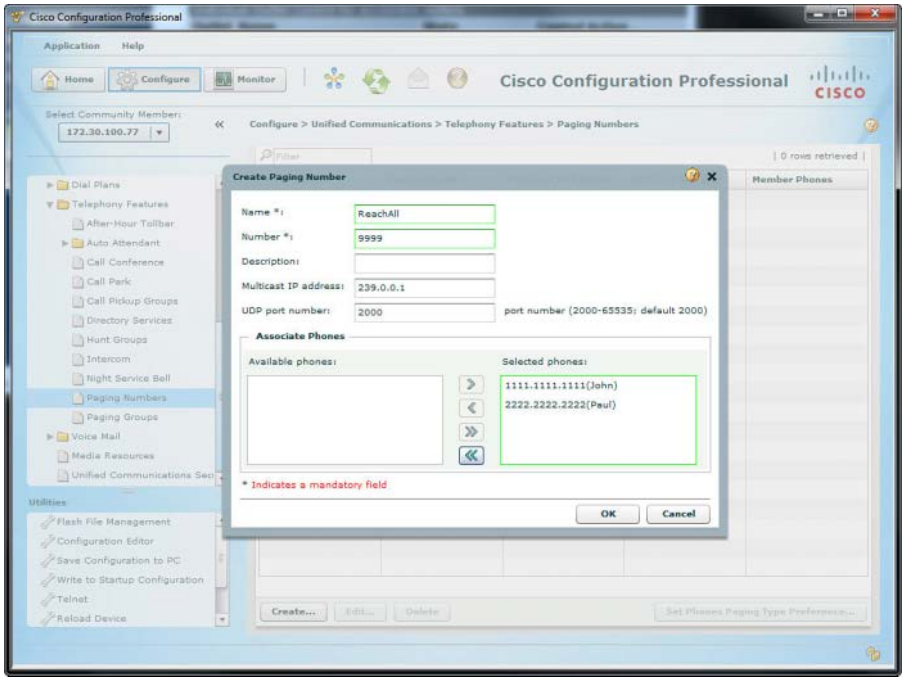


Figure 7-17 *Configuring Single-Group Paging in CCP*

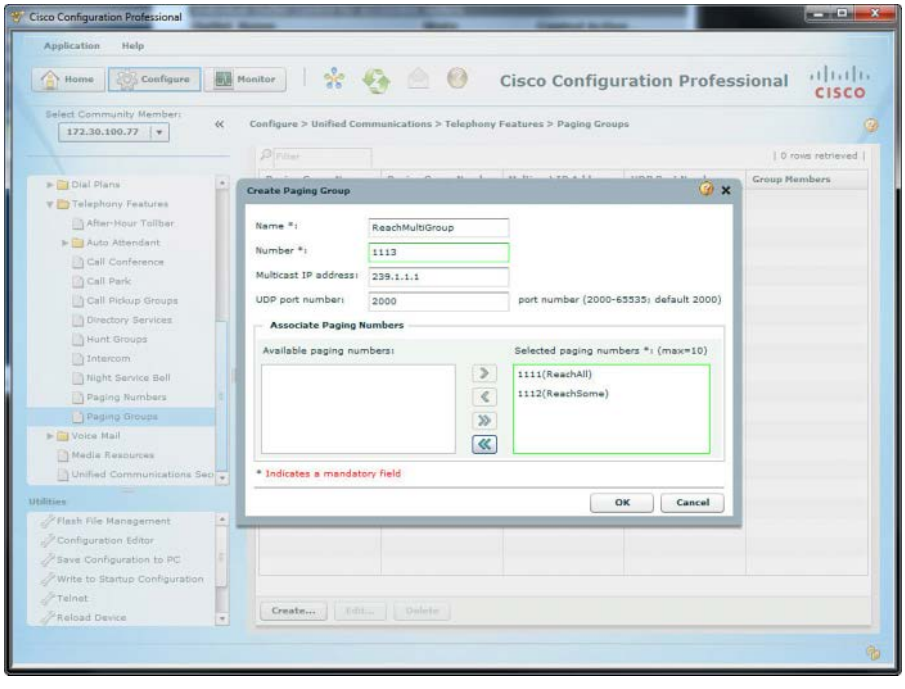


Figure 7-18 *Configuring Multiple-Group Paging in CCP*

Configuring After-Hours Call Blocking

In the traditional telephony realm, there have been many recorded incidents of unauthorized phone calls being placed after-hours, when most, if not all, staff has left for the evening. To prevent this, you can implement after-hours call blocking on CME.

After-hours call blocking allows you to define ranges of times specified as after-hours intervals. You can then list number patterns that are disallowed during those intervals. If a user places a call during the after-hours time range that matches one of the defined patterns, CME will play a reorder tone and disconnect the call.

Of course, there are exceptions to every rule. You may want to have some phones completely exempt from the policy, or give users a "back door" around the restrictions if they are working late and need to make business-related calls that CME would typically restrict. The after-hours call blocking configuration on CME provides for both of these scenarios. You have the option to completely exempt certain IP phones from the after-hours restrictions or provide users with a PIN they can enter into the IP phone. If they enter the PIN correctly, CME exempts the IP phone from the after-hours policy for a configurable amount of time.

Note There are some patterns that may be beneficial to block all the time. For example, 1-900 numbers in the United States often represent high-cost, less-than-reputable businesses that are typically banned from all corporate environments. CME also allows you to create a 24/7, no exemptible pattern that is disallowed at all times, using the after-hours call blocking system.

After-hours call blocking has three major steps of configuration:

Step 1. Define days and/or hours of the day that your company considers off-hours.

Step 2. Specify patterns that you want to block during the times specified in Step 1.

Step 3. Create exemptions to the policy, if needed.

You will perform most of the configuration for the after-hours call blocking restrictions from telephony service configuration mode. Example 7-10 demonstrates the configuration of after-hours time intervals.

Example 7-10 *Configuring After-Hours Time Ranges and Dates*

Key Topic

```
CME_Voice(config)# telephony-service
CME_Voice(config-telephony)# after-hours ?
  block  define after-hours block pattern
  date   define month and day
  day    define day in week
CME_Voice(config-telephony)# after-hours day ?
  DAY  day of week (Mon, Tue, Wed, etc)
CME_Voice(config-telephony)# after-hours day mon ?
  hh:mm  Time to start (hh:mm)
```

```
CME_Voice(config-telephony)# after-hours day mon 17:00 ?
  hh:mm  Time to stop (hh:mm)
CME_Voice(config-telephony)# after-hours day mon 17:00 8:00
CME_Voice(config-telephony)# after-hours day tue 17:00 8:00
CME_Voice(config-telephony)# after-hours day wed 17:00 8:00
CME_Voice(config-telephony)# after-hours day thu 17:00 8:00
CME_Voice(config-telephony)# after-hours day fri 17:00 8:00
CME_Voice(config-telephony)# after-hours date ?
  MONTH  Month (Jan, Feb, Mar, etc)
CME_Voice(config-telephony)# after-hours date dec ?
  <1-31>  day of month in date
CME_Voice(config-telephony)# after-hours date dec 25 ?
  hh:mm  Time to start (hh:mm)
CME_Voice(config-telephony)# after-hours date dec 25 00:00 ?
  hh:mm  Time to stop (hh:mm)
CME_Voice(config-telephony)# after-hours date dec 25 00:00 00:00
CME_Voice(config-telephony)# after-hours date jan 1 00:00 00:00
```

The configuration in Example 7-10 defines weekdays, from 5:00 p.m. to 8:00 a.m. the next day, as after-hours, along with the entire day on December 25 (Christmas) and January 1 (New Year's Day).

In the next step of the after-hours configuration, you define the patterns that CME should block during the after-hours time slots you have configured (see Example 7-11).

Note Chapter 8, "Administrator and End-User Interfaces," and Chapter 9, "Managing Endpoints and End Users in CUCM," discuss the patterns you can use for matching fully. For now, examples in this chapter use the "." wildcard, which matches any digit dialed, and the T wildcard, which matches any number of digits.

Key Topic

Example 7-11 *Configuring After-Hours Block Patterns*

```
CME_Voice(config)# telephony-service
CME_Voice(config-telephony)# after-hours block ?
  pattern  block pattern
CME_Voice(config-telephony)# after-hours block pattern ?
  <1-32>  index of patterns
CME_Voice(config-telephony)# after-hours block pattern 1 ?
  WORD  digits string for after hour block pattern
CME_Voice(config-telephony)# after-hours block pattern 1 91.........
CME_Voice(config-telephony)# after-hours block pattern 2 9011T
CME_Voice(config-telephony)# after-hours block pattern 3 91900..... ?
  7-24  block pattern works for 7 * 24
  <cr>
CME_Voice(config-telephony)# after-hours block pattern 3 91900..... 7-24
```

You might have noticed based on the context-sensitive help output in Example 7-11 that the CME router allows you to configure up to 32 indexes of block patterns. The initial block pattern 1 matches and blocks long distance numbers; block pattern 2 matches and blocks international numbers; block pattern 3 matches and blocks 1-900 toll calls. Notice that block pattern 3 is followed by the 7-24 keyword. This additional syntax tells the CME router to block calls to this pattern at all times. If you enter block patterns with this keyword, phones exempted from other after-hours blocked numbers are not exempt from these patterns.

Note If you need more flexibility than after-hours blocking provides, you can also use class of restriction (COR) features with CME.

The final step in the configuration of after-hours blocking is to allow any necessary exemptions to the policy, as shown in Example 7-12. You can add exemptions on a per-IP phone basis or by using one or more PIN numbers to allow on-demand access to block patterns (with the exception of the patterns defined with the **7-24** keyword) from any IP phone. Example 7-12 configures ephone 1 to be exempt from the after-hours call-blocking policy. Ephones 2 and 3 are configured with PIN numbers. To become exempt from the after-hours call blocking policy, the user using the phone must enter the necessary PIN number.

Example 7-12 *Configuring After-Hours Exemptions*

```
CME_Voice(config)# ephone 1
CME_Voice(config-ephone)# after-hour exempt
CME_Voice(config-ephone)# exit
CME_Voice(config)# ephone 2
CME_Voice(config-ephone)# pin ?
  WORD  A sequence of digits - representing personal identification number
CME_Voice(config-ephone)# pin 1234
CME_Voice(config-ephone)# exit
CME_Voice(config)# ephone 3
CME_Voice(config-ephone)# pin 4321
CME_Voice(config-ephone)# exit
CME_Voice(config)# telephony-service
CME_Voice(config-telephony)# login timeout 120 clear 23:00
```

Note The PIN number can be any number between four and eight digits.

The last line in Example 7-12 is a key to allowing the PINs to function properly. By default, all the CME-supported Cisco IP phones have a Login softkey on the LCD display. This softkey is dimmed and unusable until you enter the **login** command from telephony service configuration mode. The timeout value that follows this command represents the amount of idle time before the phone automatically revokes the last PIN number entered. The clear value is an absolute time at which the last-entered PIN becomes invalid. In the case of Example 7-12, the PIN will clear at 11:00 p.m., regardless of the last time it was entered.

This does not prevent users from logging back in by entering their PIN a second time after 11:00 p.m.

Note The default timeout for the login command is 60 minutes. Also, you need to restart or reset all phones before the **login** command takes effect.

CCP provides a fairly spectacular interface for configuring after-hours call blocking. When navigating to **Unified Communications > Telephony Features > After-Hour Toolbar**, CCP greets you with a window allowing you to define the specific patterns you want to block (shown in Figure 7-19). You can create schedules and PIN overrides by clicking the Weekly Schedule, Holiday Schedule, or Override (Softkey Login) window panes at the bottom of the After-Hour Toolbar configuration window.

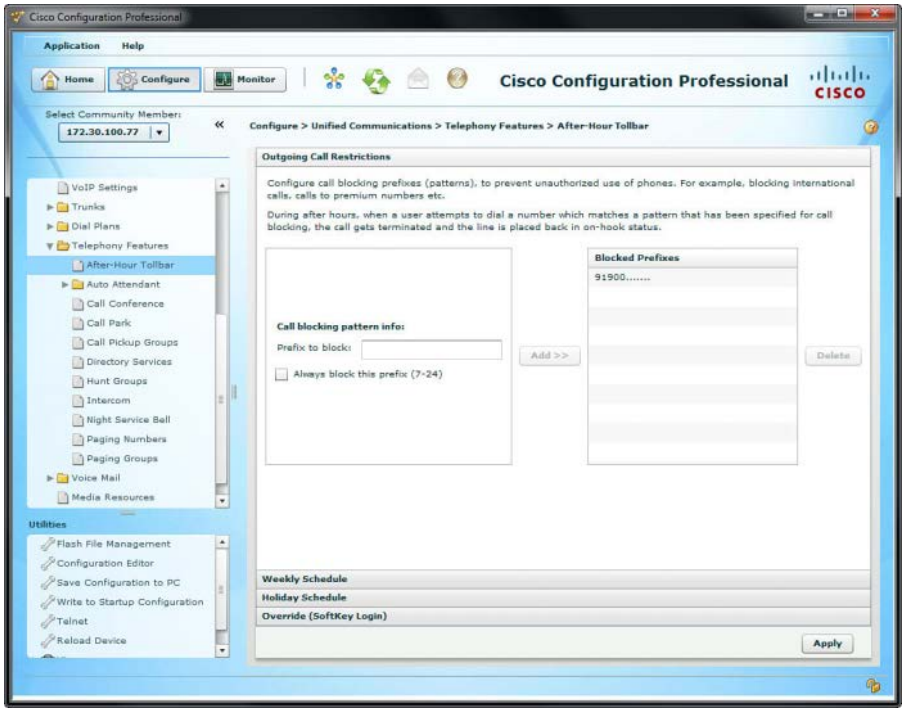


Figure 7-19 *Configuring After-Hours Restrictions Using CCP*

Configuring CDRs and Call Accounting

"Who made that call?" That question could arise for many reasons. Perhaps the entire police and fire departments arrive at the front door of your company because of an emergency call originating from your business. Perhaps management is reviewing the recent long-distance bill and came across an international call to Aruba that was four hours in length. Whatever the reason, you can find the answer by looking through the archived call detail records (CDRs), as long as you have configured the CME router to support them.

CDRs contain valuable information about the calls coming into, going out of, and between the IP phones on your network. These records contain all the information you need to find who called whom and how long they were talking. The CME router can log CDRs to the buffered memory (RAM) of the router, to a syslog server, or to both. Storing the CDRs in the RAM of the router is better than nothing, but not very effective. If the CME router ever loses power, all the CDRs will be lost. Likewise, the RAM of the router has limited storage and is not an effective solution. Viewing CDRs from the log file on the CME router is very cryptic and tedious to understand. Example 7-13 demonstrates the syntax you can use to enable logging of CDRs to the buffered memory of the router.

Example 7-13 *Configuring CDR Logging to Buffered Memory*

```
CME_Voice(config)# logging buffered 512000
CME_Voice(config)# dial-control-mib ?
  max-size      Specify the maximum size of the dial control history table
  retain-timer  Specify timer for entries in dial control history table
CME_Voice(config)# dial-control-mib retain-timer ?
  <0-35791>  Time (in minutes) for removing an entry
CME_Voice(config)# dial-control-mib retain-timer 10080
CME_Voice(config)# dial-control-mib max-size ?
  <0-1200>  Number of entries in the dial control history table
CME_Voice(config)# dial-control-mib max-size 700
```

Example 7-13 specifies the following parameters for CDR buffered logging:

- 512,000 bytes of memory dedicated to the logging functions of the router.
- CDRs are kept for 10,080 minutes (7 days).
- The CME router keeps a maximum of 700 CDRs in memory.

To view the CDRs recorded by CME, use the **show logging** command, as shown in Example 7-14.

Example 7-14 **show logging** *Command Output*

```
CME_Voice# show logging
Syslog logging: enabled (12 messages dropped, 1 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
   Console logging: level debugging, 168 messages logged, xml disabled,
                    filtering disabled
<...output omitted>
Log Buffer (512000 bytes):
*Jun 18 01:57:08.987: %SYS-5-CONFIG_I: Configured from console by     CCMAdmin on vty0
  (172.30.3.28)
*Jun 18 01:57:48.640: %VOIPAAA-5-VOIP_CALL_HISTORY: CallLegType 1, ConnectionId
  B71427FB3C1011DD80EEB6A01B061E9, SetupTime *18:57:17.970 ARIZONA Tue   Jun 17
  2008, PeerAddress 1503, PeerSubAddress , DisconnectCause 1   ,
  DisconnectText
  unassigned number (1), ConnectTime *18:57:48.640 ARIZONA Tue Jun 17   2008, Discon-
nectTime *18:57:48.640 ARIZONA Tue Jun 17 2008,   CallOrigin 2, ChargedUnits
```

```
  0, InfoType 2, TransmitPackets 0, TransmitBytes 0, ReceivePackets 0, ReceiveBytes
  0
*Jun 18 01:57:48.640: %VOIPAAA-5-VOIP_FEAT_HISTORY: FEAT_VSA=fn:CFBY,ft:06/17/2008
  18:57:18.623,frs:0,fid:129,fcid:B77841E83C1011DD80F3B6A01B061E9,legID:0,frson:2,
fdcnt:1,fwder:1501,fwdee:1503,fwdto:1599,frm:1501,bguid:B71427FB3C1011DD80EEB6A
  001B061E9
*Jun 18 01:57:48.640: %VOIPAAA-5-VOIP_FEAT_HISTORY: FEAT_VSA=fn:TWC,ft:06/17/2008
  18:57:17.967,cgn:1503,cdn:,frs:0,fid:126,fcid:B71427FB3C1011DD80EEB6A01B061E9,
  legID:4B,bguid:B71427FB3C1011DD80EEB6A001B061E9
<...output omitted>
```

What you see here are three CDR entries that record a call from x1503 to x1501. If you are able to decode most of what is displayed in that log, you are definitely ahead of the game.

Sending messages to a syslog server is better than sending them to the RAM of the CME router. A syslog server is a PC or server running a dedicated application that receives and stores logging messages from one or more devices. There are many syslog server platforms available for download on the Internet.

Note The Kiwi Syslog Daemon (http://www.kiwisyslog.com) is one of the more popular syslog platforms available. The fact that it is free helps, but it is also easy to install and manage.

After you set up a syslog server, you can direct the CME router to send CDR records to it by using the following syntax:

```
CME_Voice(config)# gw-accounting syslog
CME_Voice(config)# logging 172.30.100.101
```

The initial command in this syntax directs the CDR records to the syslog server. The second command tells the CME router where the syslog server is located; in this case, 172.30.100.101. Figure 7-20 shows the CDR records being received by the Kiwi Syslog application.

The output shown on the syslog server is the same messages received in the buffered logging. Although it is easier to read than scrolling through wrapped terminal output, the messages are just as cryptic. For this reason, many third-party vendors created CDR interpreters that format the syslog data into easy-to-understand spreadsheets and HTML pages.

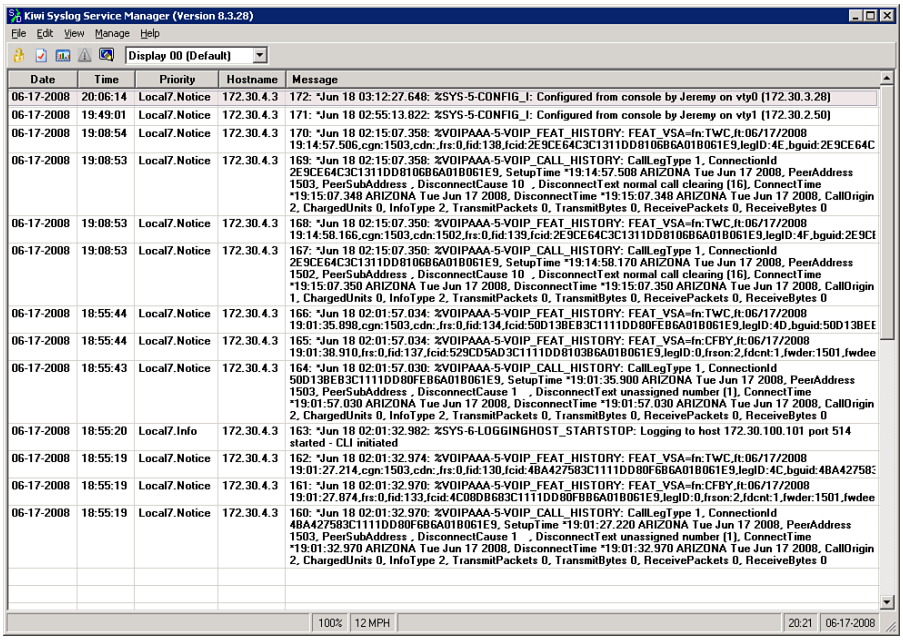


Figure 7-20 *CDR Records Logged to a Kiwi Syslog Server*

It is common for an organization to use these CDRs for billing purposes. Businesses track the long-distance and international calls to the department level to assist in budget accounting. Although it is possible to keep track of the extension numbers that are in each department and the calls they make, the call data is easier to manage if CME can flag the CDR with an account code.

Businesses can distribute account codes to each department in the organization. For example, the East Coast sales group might get account code 1850, the West Coast sales group 1851, management 1852, and so on. You could then train the users in each department to enter this account code each time they make a long distance or international call by pressing the Acct softkey on the phone. This softkey appears when the IP phone is in the ring out or connected state, as shown in Figure 7-21.

After the user presses the Acct softkey, an Acct prompt appears at the bottom of the phone, where the user can enter their department account number followed by the pound key (#). Entering this number during the ring out or connected call state does not interrupt the call in any way. After the user enters the account number, CME flags the CDR records with the account number dialed. This allows for easy filtering and accurate billing to each department.

Figure 7-21 *Acct Softkey in the Ring Out State*

Configuring Music on Hold

What voice network would be complete without the sound of music coming through handsets on hold everywhere? CME has the ability to stream Music on Hold (MoH) from specified WAV or AU audio files that you copy to the flash memory of the router. CME can stream this audio either in multiple unicast streams (which is more resource intensive) or in a single multicast stream (which is less resource intensive but requires a multicast network configuration). In addition, CME can stream the MoH using G.711 or G.729 codecs.

Note Because the G.729 audio codec is designed for human voice, the quality of MoH streamed using G.729 is significantly lower than MoH streamed using G.711. In addition, CME uses transcoding DSP resources to convert the MoH to the G.729 codec. With all these factors, using G.711 for your MoH, if at all possible, is highly recommended.

Example 7-15 configures a CME router to support multicast MoH, streaming music from a file in flash called subdivisions.wav.

Example 7-15 *Configuring MoH Support*

```
CME_Voice(config)# telephony-service
CME_Voice(config-telephony)# moh ?
  WORD  music-on-hold filename containing G.711 A-law or u-law 8KHz encoded audio
    file (.wav or .au format). The file must be loaded into the routers flash
    memory.
CME_Voice(config-telephony)# moh subdivisions.wav
CME_Voice(config-telephony)# multicast moh ?
  A.B.C.D  Define music-on-hold IP multicast address from flash
CME_Voice(config-telephony)# multicast moh 239.1.1.55 ?
  port  Define media port for multicast moh
```

```
CME_Voice(config-telephony)# multicast moh 239.1.1.55 port ?
  <2000-65535>  Specify the RTP port: 2000 - 65535
CME_Voice(config-telephony)# multicast moh 239.1.1.55 port 2123
```

Note Because most governments see MoH as a type of broadcasting, you must pay royalties if you intend to play any songs covered by a copyright (such as music by one of the greatest Canadian bands ever) over MoH. With that in mind, there are thousands of royalty-free songs available on the Internet that you can use for MoH. They are mostly terrible, but they are free.

Configuring Single Number Reach

Wouldn't it be convenient if you were reachable anywhere at a single phone number? A call to your single phone number could make your office desk phone ring in the middle of the day, your cell phone ring in the middle of dinner, or your home phone ring in the middle of the night. Single Number Reach (SNR) allows you to link an additional device to a "parent" number. For example, you could link your mobile phone to your desk extension. When a call comes in for your DN, the office phone begins to ring. After a specified timeout interval, your mobile phone begins to ring along with your office phone. If neither phone answers within a specified timeout, CME transfers the call to the corporate voicemail server.

Tip Single Number Reach in CME is a lightweight version of Mobile Connect, which is a CUCM feature allowing you (or the user) to assign multiple devices to ring simultaneously. The first one to answer receives the call.

In addition to a simultaneous-ring feature, Single Number Reach also allows a mid-call transfer. For example, you could be sitting at your desk speaking on a Cisco VoIP phone with a valued customer when you suddenly realize that you're late for your daughter's birthday party. You can simply press the **Mobility** softkey on your office phone and CME transfers the call to your preconfigured Single Number Reach destination. CME can always transfer the call back by pressing the Resume softkey.

Note Using Single Number Reach might make you want additional voice trunks to the PSTN. For example, if a user received a call on his desk phone and then pressed the mobility button to send it to his cell phone, there will be two PSTN trunks active: one for the incoming call to the office phone and one for the outgoing call to the cell phone.

You can configure Single Number Reach from the command line or using CCP. If using CCP, navigate to the Extension configuration window (**Unified Communications > Users, Phones, and Extensions > Extensions**). You can then edit any extension where you want to enable Single Number Reach. After bringing up the Edit Extension window, click the **Advanced** tab and choose the **Single Number Reach** menu option (see Figure 7-22).

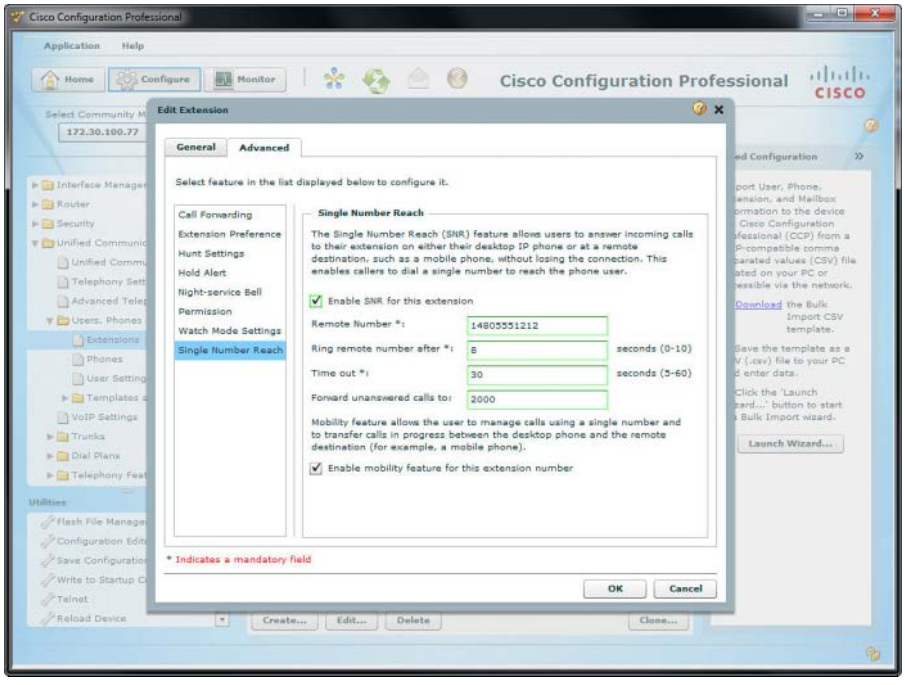


Figure 7-22 *Configuring SNR Using CCP*

From here, you can define the following options:

- **Enable SNR for This Extension:** Enables the feature and allows you to configure the following fields.
- **Remote Number:** This required field defines the remote number CME should ring after a specified timeout. Remember to enter the number accordingly if your CME dial plan requires an access code (such as 9) for an outside line.
- **Ring Remote Number After:** How long (in seconds) CME should wait before ringing the remote number defined in the previous field.
- **Timeout:** The amount of time (in seconds) CME should wait before considering the call unanswered.
- **Forward Unanswered Calls To:** This optional field allows calls to forward to an additional number (such as an operator or hunt group) when the timeout value is reached.

Note Keep in mind the amount of time the phone rings in your country when defining the "remote ring number after" and "timeout" values. For example, in the United States, phones ring for 2 seconds and then remain silent for 4 seconds. Defining a "ring remote number after" value of 8 allows two full rings and then immediately begins ringing the remote cell phone.

Selecting the options shown in Figure 7-22 generates the following command-line syntax:

```
ephone-dn 2 dual-line
 snr 14805551212 delay 8 timeout 30 cfwd-noan 2000
 mobility
 exit
```

Notice that CME applies the configuration on an ephone-dn basis (allowing you to enable this feature only for select users). Also, notice that you can configure the mobility feature (allowing transfers of active calls to and from the Single Number Reach device) separately from the Single Number Reach feature (allowing calls to ring another device after a specified amount of time).

Configuring Ephone Hunt Groups

A hunt group allows you to call a specific number but have multiple different phones ring in a particular desired sequence. The incoming call is extended to the first phone to pick up the call. This feature is widely used for Helpdesk or other team environments in which callers are trying to reach a service or department as opposed to an individual.

Key Topic

In CME, hunt groups have been around for a long time. The structure is really simple: First, we create special number called a pilot number (but configured in the CLI as ephone-hunt with a pilot subcommand). That is the number people call to reach the help desk, in our example. Our three help desk people are Gord, Alex, and Neil, so we set up their extensions as members of the hunt group. The order of that list may or may not be important; it depends on the type of hunt group we define. The choices (and their meanings) are as follows:

- **Longest Idle**: This is a round-robin call distribution type; the extensions are rung in their listed order, starting with the one that has been on-hook the longest.
- **Peer**: Also a round-robin type; the extensions are rung in their listed order, but this time the starting point is the number after the last one that answered a call.
- **Parallel**: All the extensions in the group ring simultaneously.
- **Sequential**: Strict top-down order as listed. The first extension in the list gets every new call, unless it is already busy or does not answer within the timeout, at which point the second extension rings, and so forth. That first extension will get really busy. I wouldn't want to be them.

Let's say we want to make things pretty fair on the help desk people and use longest idle as the hunt group type. In CCP, navigate to **Unified Communications > Telephony Features > Hunt Groups**. Click the **Create** button, and set up the hunt group as shown in Figure 7-23.

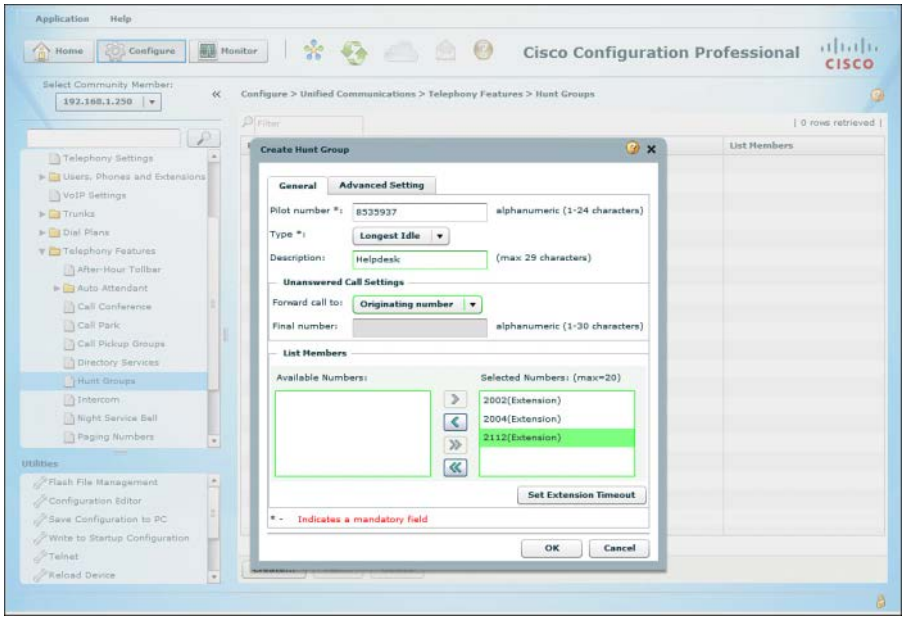


Figure 7-23 *Using CCP to Create Hunt Groups*

The commands generated by the settings in Figure 7-23 look like this:

```
ephone-hunt 1 longest-idle
 pilot 8535937
 list 2002,2004,2112
 fwd-final orig-phone
 description Helpdesk
 no-reg both
 exit
```

Final Forwarding Options for Hunt Groups

Suppose that the call has hunted through the list and that no phone was able to answer it. What do you want to happen then? You can configure CME with a final forwarding instruction to any of the following:

- The pilot number of another hunt group
- A voicemail pilot
- Any ephone-dn
- Back to the extension that transferred the call to the hunt pilot.

The choices shown in CCP are a bit confusing because they do not match up with that list exactly. In CCP, the available settings in the Forward Call To drop-down are as follows:

- **Originating Number**: Forwards the call to the directory number of the phone that transferred the call into the hunt group
- **Final Number**: Forwards the call to the final number in the hunt group

Use the Final Number selection, and enter an extension, voicemail pilot, or hunt pilot number to send the call to a specific number. Use **Originating Number** to return the call back to the extension that transferred or forwarded the call into the hunt system in the first place. Set the timeout value to determine how long the call will ring each extension in the hunt group before moving on to the next extension in the list. Something like 10 seconds is usually pretty good; longer than that and the caller might be annoyed at waiting while the extensions ring out; too short and the users might not be able to stop what they are doing and pick up the phone before it moves on to the next extension.

Tip In your labs, you can save yourself the tedium of watching your phones hunt by setting the timeout to 2 seconds or so!

Key Topic

Configuring Night Service Using CCP

Many businesses have a requirement for a specialized after-hours call forwarding system known as Night Service Bell. This is actually quite an old feature commonly found on legacy PBX systems. The story here is that after regular business hours, or perhaps during a reduced-staffing shift late at night, there is no receptionist and all the calls that person would normally handle are unanswered. Night Service defines one or more extensions that are eligible for Night Service and a set of phones that will ring with a special burst ringer when a Night Service extension receives a call. Night Service-enabled phones display a screen message when Night Service is in effect. Then, any staff person who hears the special ring can use Call Pickup to take the call on a Night Service phone. Alternatively, you could configure Night Service to forward those calls to a specified number. The system incorporates a scheduler to define when Night Service hours should be in effect on a daily, weekly, or annual basis. You can also define a code to manually activate Night Service on demand.

Configuring Night Service from CCP is straightforward:

Step 1. Configure Night Service hours by navigating to **Unified Communications > Telephony Features > Night Service Bell** (as shown in Figure 7-24).

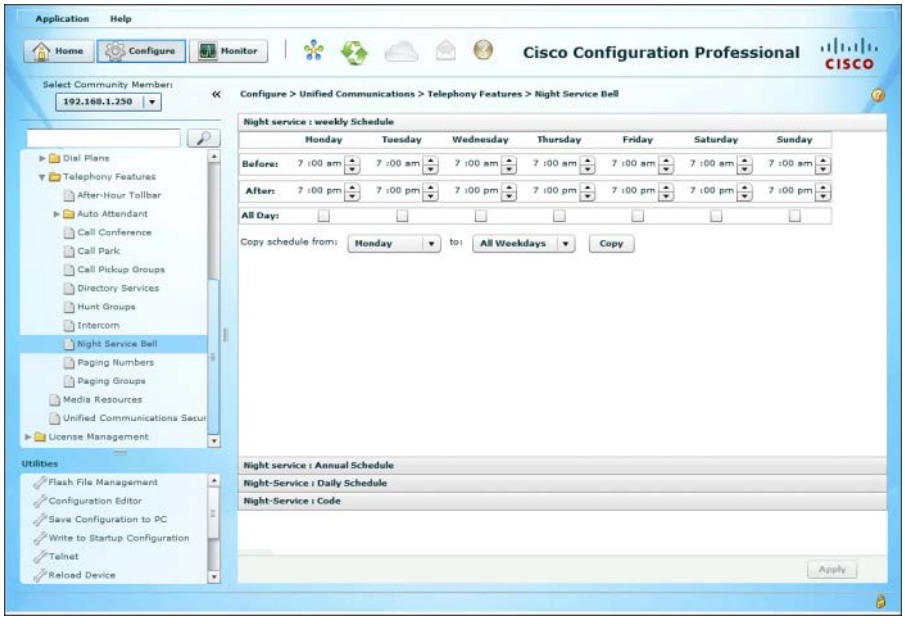


Figure 7-24 *Configuring Night Service Hours*

Step 2. [Optional] Configure the Night Service manual activation code from the Night Service: Code section.

Step 3. Click **Apply** and **Deliver**.

Step 4. Navigate to **Unified Communications > Users, Phones and Extensions > Extensions**, and select an extension that will participate in Night Service.

Step 5. Switch to the Night Service entry to the left, and check the **Enable Night Service** box, as shown in Fig. 7-25.

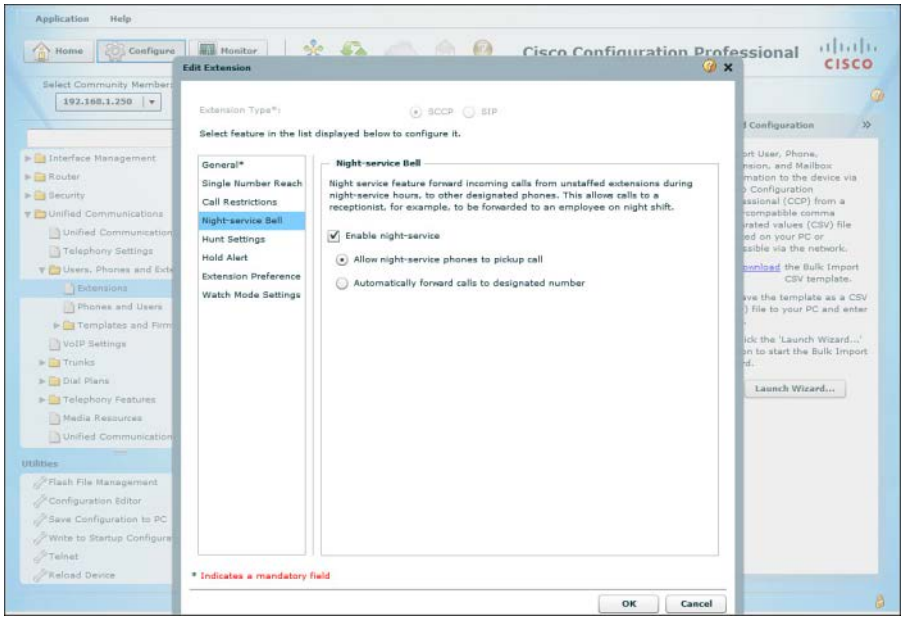


Figure 7-25 *Configuring an Extension for Night Service*

Step 6. Choose either **Allow Night Service Phones to Pick Up Call** or **Automatically Forward Calls to Designated Number**.

Step 7. Click **OK** and **Deliver**.

Step 8. Repeat Steps 5 through 7 for all other Night Service extensions.

Step 9. Next, define which IP phones should ring during Night Service. Navigate to **Unified Communications > User, Phones and Extensions > Phones and Users**, and select a phone.

Step 10. Open the phone configuration window, switch to the **Phone Settings** tab, and in the Night Service section check the box for **Enable This Phone to Receive Calls to Unstaffed Extensions**, as shown in Figure 7-26.

Step 11. Click **OK** and **Deliver**.

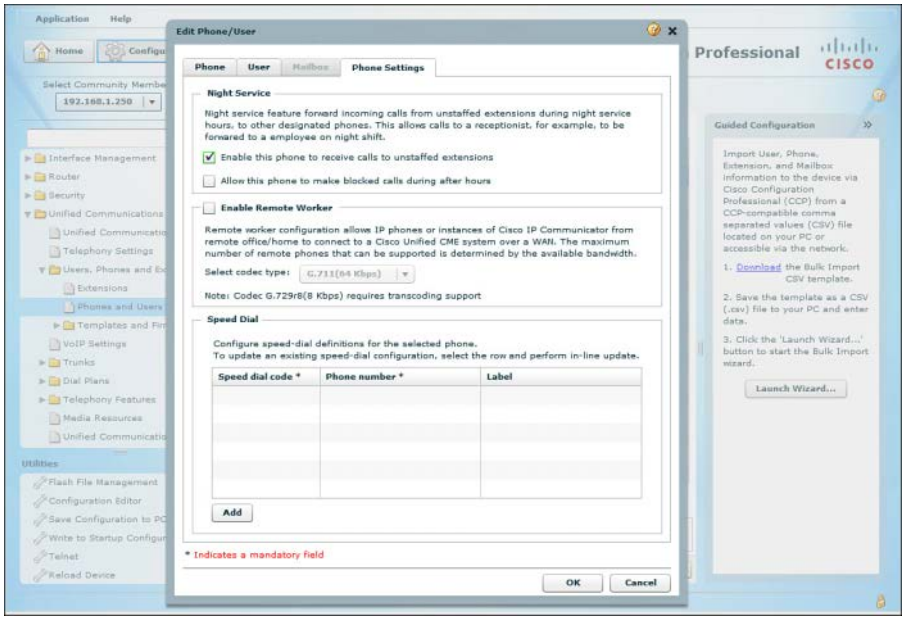


Figure 7-26 *Configuring an Ephone for Night Service*

Configuring Shared Ephone-dn Using CCP

Shared ephone-dn (otherwise known as shared line) is one of the simplest call coverage features available. It simply means putting the same ephone-dn on more than one ephone. When someone calls the shared ephone-dn, all the phones ring at the same time. The first phone that picks up answers the call; if the call is then put on hold, any of the other shared-line phones can pick it up. In CCP, follow these steps; they are actually the same steps as we used for adding the primary extension to a phone, except that now we are putting the same extension on multiple phones. Figure 7-27 shows the phone configuration window with a second extension added.

Step 1. Navigate to **Unified Communications > Users, Phones and Extensions > Phones and Users.**

Step 2. Select one of the phones you want to configure for shared-line use, and then click **Edit.**

Step 3. Under the Phone tab, select the extension you wish to add to multiple phones, and move it to a button entry on the right using the arrow. The next available button will be used by default, but if you first click on the button you want to use and then click the arrow, the shared extension will be assigned there.

Step 4. Click **OK** and then **Deliver.**

Step 5. Repeat these steps on the other phones, assigning the same extension.

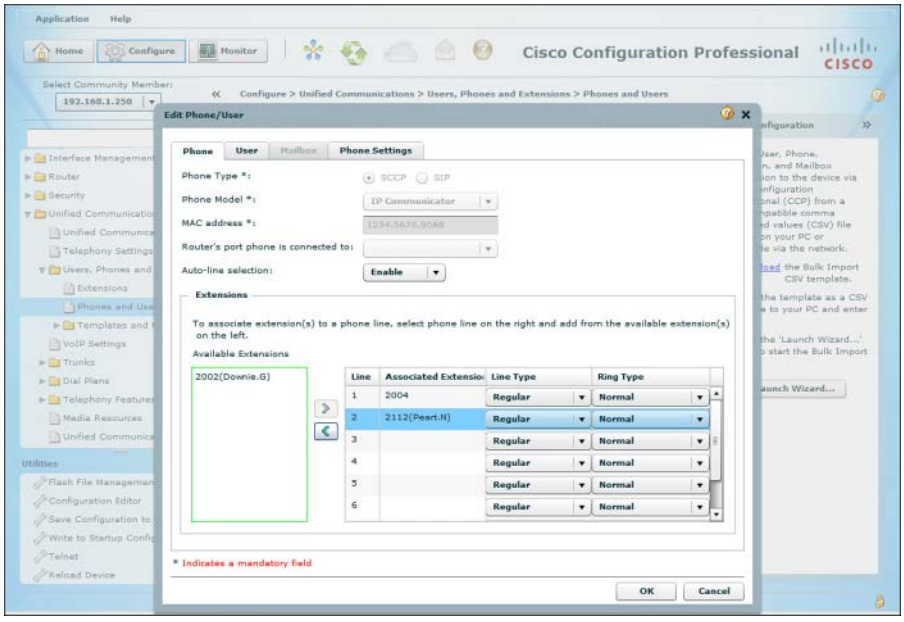


Figure 7-27 *Configuring Shared Ephone-dn Using CCP*

7

Describe Extension Mobility in CME

Extension Mobility (EM) allows a user to log in on any IP phone configured for EM. This is very useful if an employee has two desks in different places, or in any situation where an individual moves from phone to phone and wants his own extension, name for caller ID, speed dials, and other customizations to follow him.

In CME, EM is configured by creating logout profiles. These define what extension and other capabilities a phone will have when a user is not logged in. For example, it is common to provide basic calling capabilities for emergency and internal calls so that any phone remains useful even if nobody is logged in to it. Without a logout profile, the phone is effectively useless; it just sits there consuming power.

For each user that needs EM, we define a user profile that includes their own extension, the user's caller ID name, the user's speed dials, and any other special capabilities. Each phone that must provide EM capability is subscribed to the EM service. The user accesses the service like any other IP phone service; the EM service prompts users for their username and password, which they enter using the phone keypad. (This is a bit like text messaging in the old days—pressing the 2 key can enter A, B, C, a, b, c, or 2, and so forth for the other keys. It takes a little getting used to, but it is not bad, especially as the phone displays the character choices, moving a cursor to show you where you are.) EM is one of those features where if you need it, your users will treat it like some kind of fantastic magic and hail you as a hero for implementing it, but if you do not need it, nobody is interested.

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 7-3 lists a reference of these key topics and the page numbers on which each is found.

Table 7-3 Key Topics for Chapter 7

Key Topic Element	Description	Page Number
Example 7-2	Configuration of busy and no answer call forwarding	172
Figure 7-7	Illustrates the concept of call hairpinning	174
List	Differentiation between blind and consult call transfer methods	175
Example 7-4	Allowing outside call transfers using the **transfer-pattern** command	177
Example 7-6	Configuration of call pickup	182
List	Three types of call pickup methods	183
Example 7-7	Configuration of intercom	185
Note	Key note regarding the number of paging groups to which a Cisco IP phone can belong	187
Example 7-8	Configuring unicast paging	188
Example 7-10	Configuring after-hours time designations	191
Example 7-11	Configuring after-hours block pattern	192
Section	Configuring ephone hunt groups	201
Section	Configuring Night Service using CCP	203

Definitions of Key Terms

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

local directory, H.450.3, H.450.2, hairpinning, call park, call pickup, directed pickup, local group pickup, other group pickup, Single Number Reach, Extension Mobility, Night Service, hunt groups

This page intentionally left blank

This chapter covers the following topics:

- **Describe the CUCM Administration Interfaces:** This section provides an overview of the graphical and command-line administration interfaces for CUCM.
- **Describe the CUC Administration Interfaces:** The section reviews the GUI and CLI administration interfaces for CUC.
- **Describe the CM-IMP Administration Interfaces:** This section discusses the GUI and CLI administration interfaces for CM-IMP.
- **Describe the End-User Interface for CUCM:** This section provides an overview of the end-user interface for CUCM.

CHAPTER 8

Administrator and End-User Interfaces

Each Unified Communications application has several different administration interfaces to provide configuration and maintenance functionality. End users also have an interface to allow them to customize their own environment. This chapter introduces the Administrator interfaces for the Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUC), and Cisco Unified Communications Manager IM and Presence (CM-IMP) products, and the end-user interface (called the Self-Care Portal) for CUCM.

"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 8-1 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 8-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions Covered in This Section
Describe the CUCM GUI and CLI	1–4
Describe the CUC GUI and CLI	5–7
Describe the CM-IMP GUI and CLI	8–10

1. How many administration web interfaces does CUCM v.10.6 provide?
   a. 3
   b. 4
   c. 5
   d. 6
2. The account named CMMasterAdmin was created at install as the Application administration account. The account named CMPlatformAdmin was created as the Platform administration account. Which two CUCM interfaces can CMMasterAdmin not log in to?
   a. Unified CM Administration
   b. Unified Serviceability
   c. Unified OS Administration
   d. Disaster Recovery System

3. Which of the following best describes the interaction between CUCM users, access control groups, and roles?
   a. User accounts can be assigned a role, which defines the user's administrative role in the company. Users may be placed into access control groups to allow simpler directory searches.
   b. Access control groups are associated with one or more roles that define a level of privilege to an application's resources. The user inherits those privileges when they are added to the access control group.
   c. Of the 46 roles defined by default, only 12 are active. Others must be activated via the Unified Serviceability interface.
   d. One group and one role are defined by default (the standard CCM super users group and the standard CCM admin users role). Other custom access control groups and roles can be defined by the administrator.
4. Bob needs to restart the TFTP service on a CUCM server. Where can he do this?
   a. Unified Serviceability > Tools > Service Activation
   b. Unified Serviceability > Tools > Control Center > Feature Services
   c. Unified Serviceability > Tools > Control Center > Network Services
   d. Only at the command line
5. Cisco Unity Connection provides five web-based administration interfaces. Which one of the following is not one of them?
   a. Cisco Unified Serviceability
   b. Disaster Recovery System
   c. Cisco Unity Connection Serviceability
   d. Cisco Unified OS Administration
   e. Cisco Unity Connection Administration
   f. Cisco Unified Messaging Administration
6. Which of the following are valid call-handler types in CUC 8.x? (Choose three.)
   a. System call handlers
   b. Holiday call handlers
   c. Directory call handlers
   d. Interactive voice response call handlers
   e. Interview call handlers

7. Which of the following is true of the Cisco Unified Serviceability application in Cisco Unity Connection?
   a. It is identical to the Cisco Unified Serviceability application in CUCM.
   b. It is also known as Cisco Unity Connection Serviceability.
   c. It is reached via the same URL (with a different IP) as the CUCM Unified Serviceability.
   d. It is replaced by Cisco Unity Connection Serviceability in CUC 8.x.

8. Cisco Unified Communications Manager IM and Presence has several administrative components in common with other Unified Communications applications. Which of the following are CM-IMP administration interfaces? (Choose all that apply.)
   a. Cisco Unified Serviceability
   b. Cisco Unified CM IM and Presence Serviceability
   c. Cisco Unified CM IM and Presence OS Administration
   d. Cisco Unified OS Administration
   e. Cisco Unified CM IM and Presence Disaster Recovery System
   f. Command-Line Interface

9. CM-IMP uses two different protocols for integration with Microsoft Office Communicator and third-party services, such as Google Voice. Under which administrative menu are they configured?
   a. CM-IMP Administration > System
   b. CM-IMP Administration > Messaging
   c. CM-IMP Administration > Presence
   d. CM-IMP Administration > Application

10. CM-IMP can be configured for regulatory compliance for IM retention. Under which administrative menu can this be done?
    a. CM-IMP Administration > System
    b. CM-IMP Administration > Messaging
    c. CM-IMP Administration > Presence
    d. CM-IMP Administration > Application

Foundation Topics

Describe the CUCM Administration Interfaces

Administrative web access to CUCM is possible only via HTTPS (or Secure Shell [SSH] for the command line). There are seven separate interfaces:

- Cisco Unified CM Administration (https://<node_ip>/ccmadmin)
- Cisco Unified Serviceability (https://<node_ip>/ccmservice)
- Disaster Recovery System (https://<node_ip>/drf)
- Cisco Unified OS Administration (https://<node-ip>/cmplatform)
- Cisco Unified Reporting (https://<node-ip>/cucreports)
- Cisco Unified IM and Presence Reporting (https://<node-ip>/cucreports)
- Command-line interface (CLI)

Each of these (with the exception of the CLI) is accessible via its own URL or by using the navigation drop-down at the top right of the page and clicking the **Go** button next to it.

The account and password defined at install for platform administration are used to access the Disaster Recovery System and the Operating System Administration pages. Likewise, the application administration account and password defined during install is used to access the CM Administration, Serviceability, and Unified Reporting interfaces. Additional accounts can be created and assigned administrative privileges so that they may also access these interfaces.

During install, an additional password is defined as the security password. This password is needed to connect to the Publisher database (for Subscriber servers or other Unified Communications applications that use the Publisher database).

Cisco Unified Communications Manager Administration Interface

The CM Administration interface (as shown in Figure 8-1) includes nine menus as described in the list that follows (a brief description is given for the tasks that each menu can perform; this is by no means an exhaustive list, and there are many tasks not listed):

- **System menu:** Includes tasks for the configuration of CM groups, Presence groups, device mobility groups, device pools, regions, locations, enterprise and service parameters, Survivable Remote Site Telephony (SRST), and others.
- **Call Routing menu:** Includes tasks to define the call routing system; call hunting; class of control; intercom; and features such as call park, call pickup, and many more.
- **Media Resources menu:** Under this menu, resources such as Music on Hold (MOH), annunciator, media termination points, and transcoders can be defined and hold-music files managed.

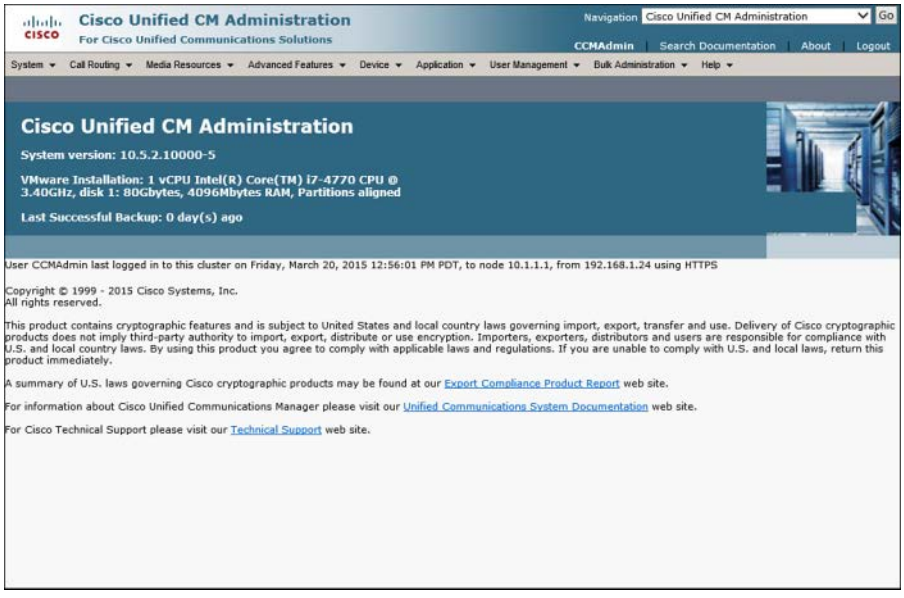


Figure 8-1 *CUCM Administration Home Page*

- **Advanced Features menu:** Under this menu, voicemail integrations, inter-company media engine configuration, Extension Mobility cross-cluster, and VPN features are configured.
- **Device menu:** Provides configuration pages for gateways, gatekeepers, trunks, IP phones, and remote destinations, plus many device settings, including phone button and softkey templates.
- **Application menu:** Accesses the CUCM Assistant Configuration Wizard and the Plug-Ins menu.
- **User Management menu:** Accesses the Application User, End User, Access Control Group, and Role configuration pages.
- **Bulk Administration menu:** Provides many options to perform repetitive configuration tasks (such as adding many users or phones) in an automated way. There are many additional and powerful capabilities of the BAT tool not listed here.
- **Help menu:** Provides access to the local searchable help files, the This Page help, and the About information page.

Cisco Unified Serviceability Administration Interface

The Cisco Unified Serviceability interface (shown in Figure 8-2) provides six menus, each with submenus, as summarized in the list that follows.

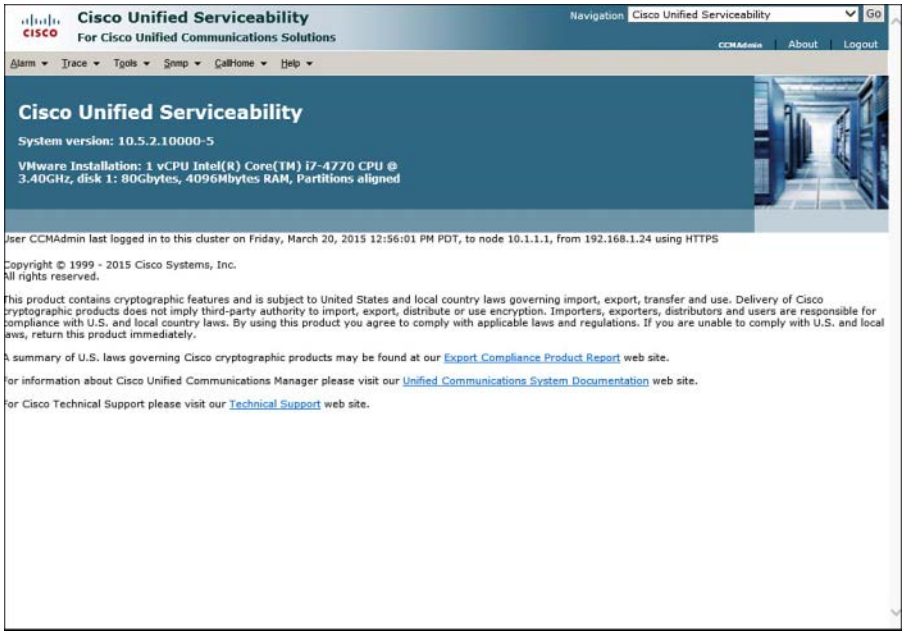


Figure 8-2 *Cisco Unified Serviceability Interface for CUCM*

- **Alarm menu:** Provides Configuration and Definition options for alarms to monitor system performance and health.
- **Trace menu:** Provides the Configuration and Troubleshooting Trace Settings submenus, which monitor the system and troubleshoot.
- **Tools menu:** Under this menu, the CDR Analysis and Reporting submenu provides an interface to gather call logs and report on calls made using the system. The Service Activation screen provides the interface to activate installed services for the first time (or deactivate them later). There are two Service Control Centers: Network and Feature (see the following Note). Using this interface, administrators can stop, start, or restart activated services. The Serviceability Reports Archive provides access to the reporting interface for system and trend analysis. The CDR Management interface allows administrators to configure and check call detail record (CDR) storage disk utilization. The Audit Log Configuration page provides settings for what will be included in audit logs.
- **SNMP menu:** The submenus (V1/V2c, V3, and SystemGroup) control Simple Network Management Protocol (SNMP) connectivity and authentication to network management applications.
- **CallHome menu:** Using the CallHome Configuration submenu, administrators can set up an automated, proactive problem reporting to internal messaging and monitoring systems, and direct case generation capability with Cisco TAC.
- **Help menu:** Provides access to the searchable Contents help, This Page help, and About information.

Note What is the difference between feature services and network services? Network services are automatically activated and required for server operation (such as Cisco CallManager Admin Service, DB Replicator, and CDP). Network services cannot be deactivated but can be started, stopped, and restarted.

Feature services are optional services that can be activated using the Service Activation page. These services might or might not be activated on a particular server in a large cluster where the design calls for assigning a particular role to a server. For example, the Cisco CallManager, TFTP, or IP Voice Media Streaming App services might be active or inactive depending on the server's job(s) in the cluster.

Cisco Unified Operating System Administration Interface

The Unified Operating System interface (shown in Figure 8-3) allows an administrator to monitor and interact with the Linux-based operating system platform. Administrative tasks that can be performed here include those in the list that follows.

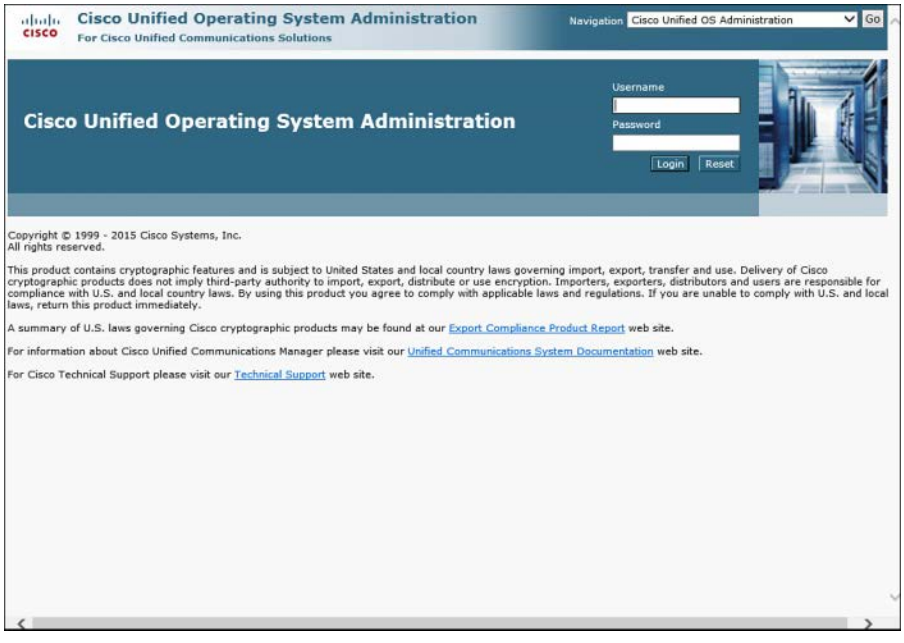


Figure 8-3 *Cisco Unified OS Administration Interface for CUCM*

- Monitor hardware-resource utilization (CPU, disk space)
- Check and upgrade software versions
- Verify and change IP address information
- Manage Network Time Protocol (NTP) server IP addresses
- Manage server security including IPsec and digital certificates

- Create a TAC remote assistance account
- Ping other IP devices

Disaster Recovery System Interface

The Disaster Recovery System (DRS) provides a backup (with scheduler) and restore capability. Access to this interface uses the Platform Administration account defined at install (as does the OS Admin interface). Additional accounts can be created for access by other individuals.

Backups must be written to a networked SFTP server. (DLT tape drive support is discontinued as of v9.x.) A scheduler is provided for automated backups, or an immediate start to the backup can be selected. Individual server or full cluster backups may be performed.

Cisco Unified Reporting Interface

The Cisco Unified Reporting interface provides a simplified method to access system reports. These reports gather information from existing logs and format the data into simple, useful, one-click reports. Data is collected from logs across the cluster (Publisher and Subscribers) to provide summarized information and highlight issues or irregularities that might impact operation of the cluster. The interface also warns if running a particular report could adversely impact server operation and affect performance or take excessive time.

CLI

The CLI is typically accessed using SSH, although it is possible to directly connect a keyboard and monitor. Initially, the only account that can log on using the CLI is the Platform Administration account defined during install, although additional accounts can be created to allow access.

The commands and functionalities of the CLI include all those found in the OS Administration interface, plus the following (not a comprehensive list):

- Shut down or restart the system
- Change versions after an upgrade
- Start, stop, and restart services
- Modify network settings (IP address, mask, gateway, and so on)
- Use network tools such as ping, traceroute, and packet capture
- Use the DRS (backup and restore)
- Add and modify Platform Administration accounts
- Display server load and process information
- Check server status, including software versions, CPU, memory and disk utilization, hardware platform, serial numbers, and so on

Inline help is available for the CLI using the question mark (?) in a similar fashion to the Cisco router IOS.

Caution The CLI is a powerful interface. The Enter key commits the command immediately, and you are very rarely asked to confirm your intent. This effectively means the CLI will do exactly what you just told it to do, including the possibility of negatively impacting the operation of the server. Review the CLI Administration Guide and be certain of the commands you are entering before using the CLI.

User Management in CUCM: Roles and Access Control Groups

The CUCM application defines a consistent and simple method of assigning (and limiting) administrative privilege to users. Users are assigned to access control groups, access control groups are assigned roles, and roles define privileges to applications. The following sections provide some detail on this structure.

Roles

Key Topic

Roles define a set of privileges to the resources in an application. Resources may be a CUCM administration web page, a report tool, or a feature section within a CUCM web page.

The privilege assigned for each resource can be one of the following:

- **No Access:** The role denies access to the resource; for example, a web page will not load, and an error appears instead.
- **Read:** The role allows the resource to be displayed but not edited: for example, a web page may load, but none of the fields or settings can be modified. Buttons such as Add, Insert, Delete, or Update do not appear.
- **Update:** The role allows full access to the resource, including editing and modification (and deletion where applicable).

Other applications (for example, Cisco Unified Serviceability or Cisco Extension Mobility) define access privileges that are relevant and specific to the application.

There are 46 standard roles defined by default in CUCM 10.6; in most cases, 1 of these roles provide the administrative functions required. If a standard role is not exactly correct for a particular scenario, custom roles can be defined that exactly define the administrative privilege required in any context. Custom roles can be defined for any of the following applications:

- CUCM Administration
- CUCM Serviceability
- Cisco Computer Telephone Interface (CTI)
- CUCM Administrative XML (AXL) database
- Cisco Extension Mobility
- CUCM End User
- Cisco Unified Reporting
- Cisco Call Manager Dialed Number Analyzer
- Cisco Unified CM IM and Presence Administration
- Cisco Unified CM IM and Presence Reporting

Figure 8-4 shows the Find and List Roles page.

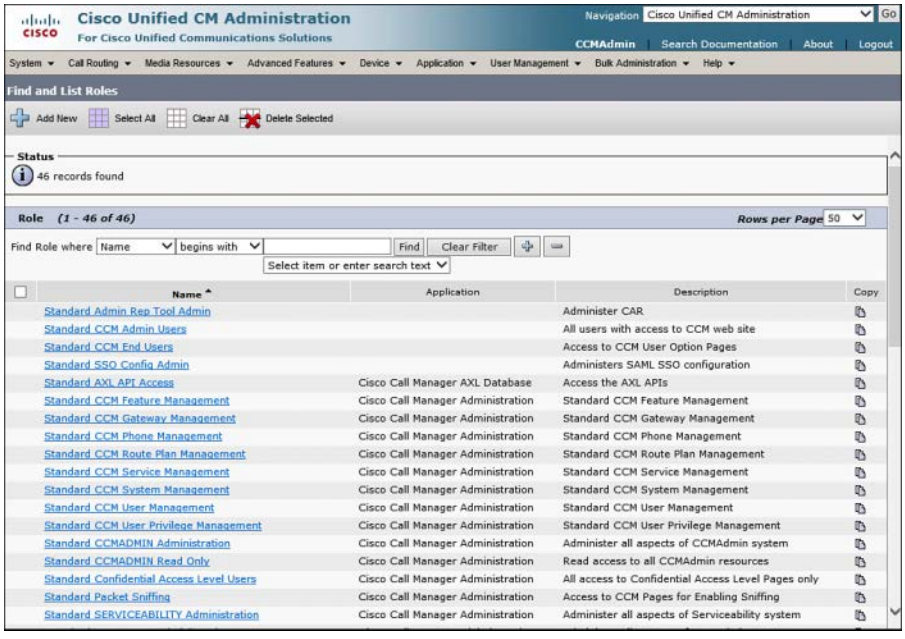


Figure 8-4 *Roles List in CUCM*

Access Control Groups

The CUCM 10.6 application defines 28 standard access control groups by default. These access control groups are each associated with 1 or more standard role(s) that provide various levels of privilege to the various applications accessible via CUCM Administration pages. Most access control groups have no members by default; when end users are created or imported in CUCM, these accounts may be added to 1 or more access control groups. The privileges defined by the role are inherited by the user account by way of their membership in the group.

As with roles, it is likely that the administrative requirements in most scenarios will be met by using the standard access control groups and role associations. If this is not the case, custom access control groups can be created and associated with standard or custom roles to exactly meet administrative requirements.

Because a user account can be a member of multiple access control groups and therefore inherit multiple levels of privilege, it is important to understand the effect of conflicting role privileges. Consider this scenario:

> Bob is a member of two user access control groups, called A and B. Group A is associated with Role X, which provides update privilege to an application resource. Group B is associated with Role Z, which provides read privilege to the same resource. The question is: What are Bob's effective privileges for the resource?
>
> The answer is determined by the enterprise parameter Effective Access Privileges for Overlapping User Access Control Groups and Roles. The default setting is Maximum, meaning that, by default, Bob has update privileges. The parameter can be changed to Minimum, changing Bob's effective privilege to read.

Note Changing the enterprise parameter as described affects all access control groups except the standard CCM super users group (the maximum-privilege group, the only default member of which is the CUCM application administrator defined at install [for example, CCMAdministrator]).

Interestingly, the default setting of Maximum privilege is the opposite of the default security settings of most network applications and operating systems. This fact is not an issue as long as the administrator is aware of the impact and significance of the setting, regardless of what setting is chosen.

Figure 8-5 shows the Find and List User Access Control Groups page in CUCM.

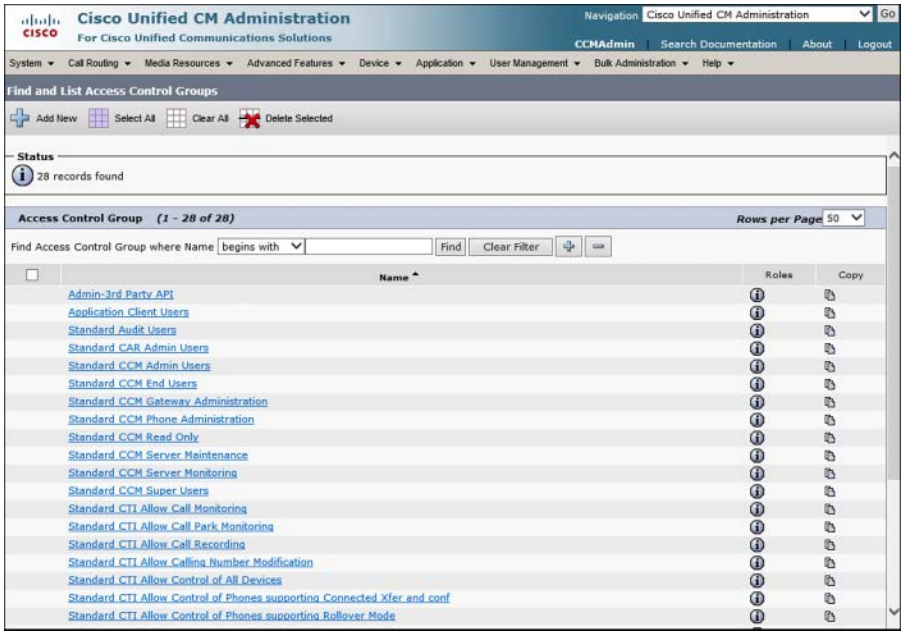


Figure 8-5 *Access Control Groups List in CUCM*

Describe the CUC Administration Interfaces

CUC provides the following six administration interfaces:

- Cisco Unity Connection Administration (https://<ip-address>/cuadmin)
- Cisco Unified Serviceability (https://<ip-address>/ccmservice)
- Cisco Unity Connection Serviceability (https://<ip-address>/cuservice)
- Cisco Unified Operating System Administration (https://<ip-address>/cmplatform)
- Disaster Recovery System (https://<ip-address>/drf)
- Command-line interface

Cisco Unity Connection Administration

The CUC Administration interface uses a tree structure similar to the Windows Explorer, making finding and navigating to the desired page easy. The main menu items are described in the following sections. You can find more detailed information in Chapter 13, "Voice Messaging Integration with Cisco Unity Connection."

- **Users:** Provides access to the local user database to create or edit users. User import and synchronization menu options are also listed here.
- **Class of Service:** Defines the features available to the user, including licensed and advanced features, and may apply other user interaction limits. Class of service is a flexible and powerful method of controlling users' interaction with CUC, particularly for licensed features. There is no limit to the number of classes of service that can be created, making it possible to build a diverse and specific range of classes of service to cover any combination of requirements.
- **Templates:** Provide a way to define common settings for users, contacts, or call handlers. When creating a new one of these three types of object, selecting the appropriate template applies all but the individually specific information for each object, making the process faster and more accurate.
- **Contacts:** A system contact is an account that provides interaction with CUC without an associated mailbox. Perhaps a consultant works in a customer office and interacts with customer team members on a daily basis but has a mailbox on the system at his consulting firm's corporate office. A system contact can provide a directory entry for CUC users to send messages to, with the messages being relayed to the consultant's mailbox at the corporate office.
- **Distribution Lists:** Allow one message to be delivered to multiple users. As many distribution lists as needed can be created. A class of service setting can prevent users from sending to system distribution lists.
- **Call Management:** Defines call handlers. There are three types of call handler in CUC: System call handlers are the foundation structures of CUC and can be configured to answer calls, play greetings, route calls, and take messages. Specialized call handlers include directory handlers, which allow a caller to search the directory and either call or leave a message for the selected user, and interview handlers, which interact with caller by playing a series of recorded questions, then collecting the answers in a single message.
- **Message Storage:** Allows mailbox quotas to be set, enforcing limits on mailbox size to prevent running out of disk space.
- **Networking:** Configures multiple CUC systems in either a digital networking or VPIM environment.
- **Dial Plan:** Provides for the creation of additional partitions and search spaces to control visibility and access to messaging components. It is useful to "hide" part of the CUC system from certain users or functions.
- **System Settings:** The System Settings submenus provide global configuration settings. Some of the submenus are summarized here:
  - **Licenses:** Tracks and displays the licenses available to the system. Licenses are tied to the MAC address of the network interface card (NIC) on the server.

- **Holiday Schedules:** The three system schedules (All Hours, Weekdays, and Voice Recognition Update Schedule) can be modified but not deleted; new schedules can be added to customize the system.
- **External Services:** CUC can be configured to access user calendar and contact information held by Microsoft Exchange. This information can then be incorporated into Personal Call Routing Rules. Likewise, if Cisco Unified MeetingPlace is available in the network, CUC can pull conference information from the server so that users can view and join meetings from their Personal Communications Assistant or from the phone.
- **LDAP:** The submenus allow the configuration of Lightweight Directory Access Protocol (LDAP) synchronization (user import) and LDAP authentication (redirection of password authentication to LDAP).
- **SMTP:** CUC can notify users of new messages via email; the submenus configure details for the integral SMTP server.
- **Advanced:** Several configuration submenus are found under the Advanced submenu, including the SMPP entry, in which CUC can be configured to send Short Message Peer to Peer/Short Message Service text message notifications to mobile phones.

- **Telephony Integrations:** Lists and configures the phone systems with which CUC is integrated, port groups, and ports.
- **Tools:** Includes the Bulk Administration interface and the Task Management (automated maintenance and troubleshooting) system.

Figure 8-6 shows the CUC Administration home page.

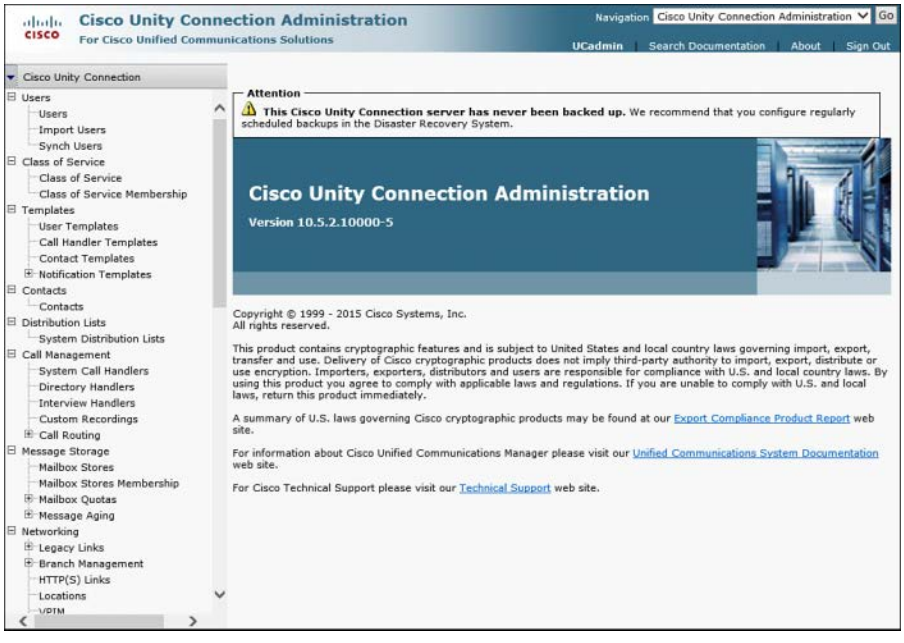


Figure 8-6 *CUC Administration Home Page*

Cisco Unity Connection Serviceability

The CUC Unified Serviceability application is similar to the app of the same name in CUCM. CUC provides an additional application called Cisco Unity Connection Serviceability, which despite the similar name provides a very different functionality. CUC Serviceability is primarily a troubleshooting tool, with tools to define alarms, traces and logs, plus service controls (activate/deactivate, start/stop/restart) for CUC-specific feature services. If an active-active redundant cluster pair is in use, the tools to manage the cluster are provided here. A reports interface is also available.

Describe the Cisco Unified CM IM and Presence Server Administration Interfaces

CM-IMP provides seven administration interfaces:

- Cisco Unified CM IM and Presence Administration (https://<ip-address>/cupadmin)
- IM and Presence Serviceability (https://<ip-address>/ccmservice)
- Cisco Unified IM and Presence OS Administration (https://<ip-address>/cmplatform)
- Disaster Recovery System (https://<ip-address>/drf)
- IM and Presence Reporting (https://<ip-address>/cucreports)
- Cisco Unified Reporting (https://<ip-address>/cucreports)
- Command-line interface

As with CUCM and CUC, the account defined at install as the platform administrator is, by default, the only one that can log in to the OS Administration, DRS, and CLI interfaces. The application administration account is the only one, by default, that can log in to the CM-IMP Administration and Unified Serviceability interfaces. Additional application and platform administration accounts can be created as required.

Cisco CM-IM and Presence Administration Interface

The CM-IMP Administration menus include the following:

- **System:** Provides integration configuration for CUCM, definition of inbound and outbound access control lists, and licensing status and management.
- **Presence:** Provides definition of gateways providing Presence information from CUCM or calendar integration with Microsoft Outlook. Interdomain federation across different presence domains using Session Initiation Protocol (SIP) or Extensible Messaging and Presence Protocol (XMPP) can be configured. SIP is commonly used with Microsoft Office Communications Server (OCS), and XMPP is typically used with Google Talk.
- **Messaging:** CM-IMP can be used with external databases (PostgreSQL compliant) or third-party servers to enable IM retention regulatory compliance (persistent messaging).
- **Application:** CM-IMP applications, such as Desk Phone Control and IP Phone Messenger, are configured here.

- **Bulk Administration:** A similar interface to CUCM provides bulk configuration of repetitive tasks, with scheduler capability.
- **Diagnostics:** Accesses system status and troubleshooting tools, plus a system dashboard for quick review of system configurations.

Help: Links to the Help Contents, Help for This Page, and About pages.

Figure 8-7 shows the CM-IMP Administration page.

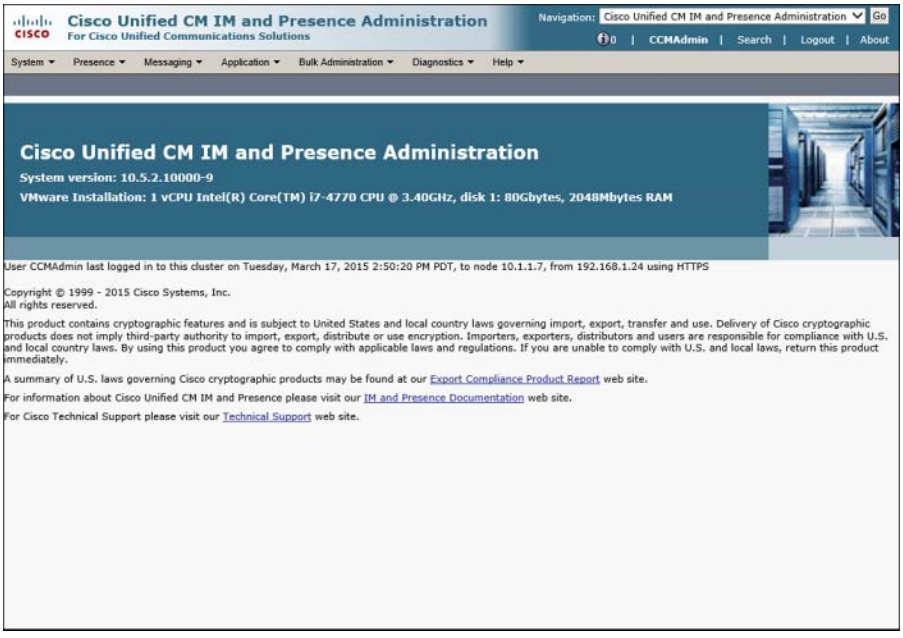


Figure 8-7 *CM-IMP Administration Page*

Cisco Unified IM and Presence Serviceability

The Cisco Unified Presence Serviceability interface provides similar functionality to the CUC Serviceability interface, including the following:

- Alarms and events monitoring for troubleshooting purposes
- Access to CM-IMP service trace logs
- Monitor real-time CM-IMP component behavior via CUCM RTMT
- Feature service activation, deactivation, and control; network service control
- Reports archive
- SNMP configuration
- Disk usage monitoring for log partition on local and cluster servers

Figure 8-8 shows the CM-IMP Serviceability page.

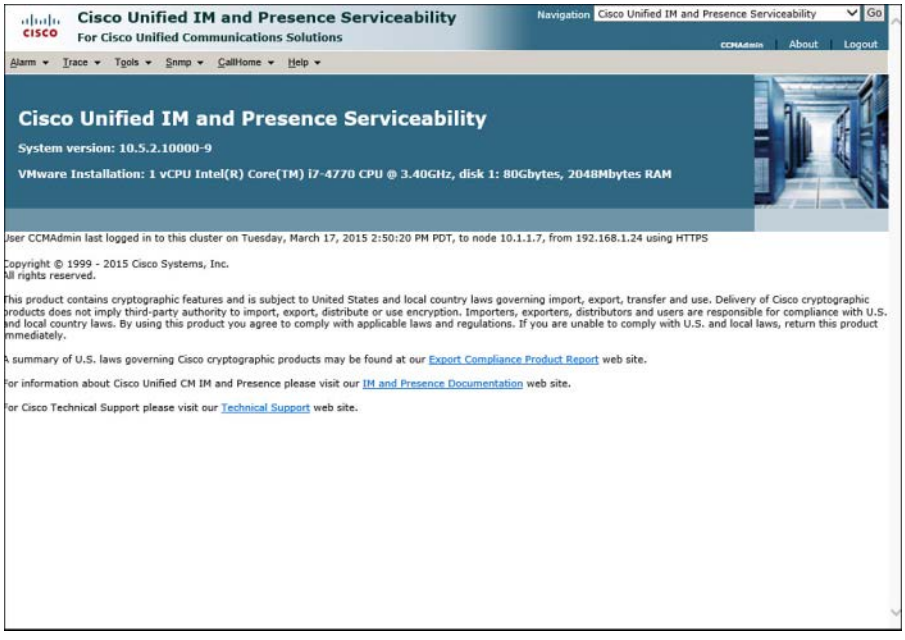


Figure 8-8 *CM-IMP Serviceability page*

Describe the End-User Interface for CUCM

CUCM provides a robust and easy-to-use end user web interface. After user accounts have been provisioned and associated to the correct IP phones, end users who are members of the standard CCM end user access control group can log in to the Self-Care Portal at https://<publisher_IP>/ccmuser and perform tasks, including the following:

- Change their own password or PIN
- Add, edit, or remove speed dials
- Download the user guide for their phone
- Access the Directory and click to dial an entry
- Subscribe or unsubscribe their IP phone from an IP phone service

Figure 8-9 shows the login screen for the Self-Care Portal. We explore the Self-Care Portal and its capabilities in more detail in Chapter 9, "Managing Endpoints and End Users in CUCM."

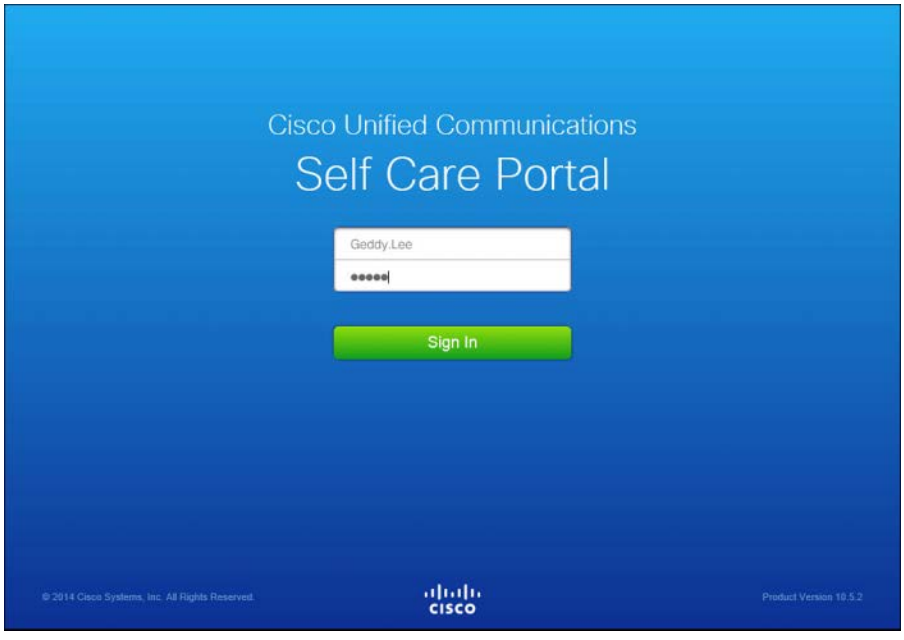


Figure 8-9 *The Self-Care Portal Login Screen*

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 8-2 describes these key topics and identifies the page number on which each is found.

Table 8-2 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Paragraph	Default accounts' access to administration interfaces	214
Section	Roles in CUCM	219
Section	Access control groups in CUCM	220

Definitions of Key Terms

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

role (CUCM), access control group (CUCM), application (CUCM), resource

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

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.

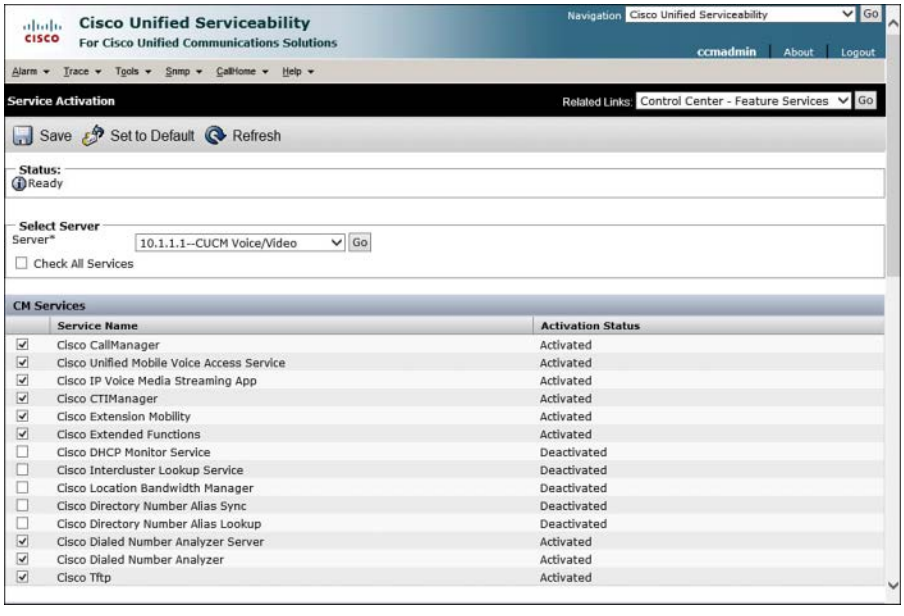


Figure 9-1 *Activating Required Services*

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.

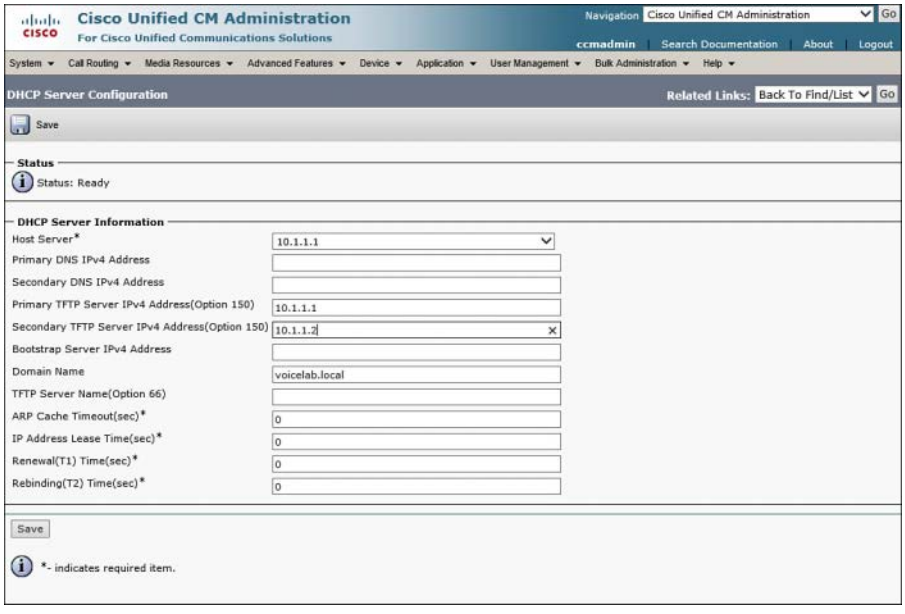


Figure 9-2 *DHCP Server Configuration*

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.

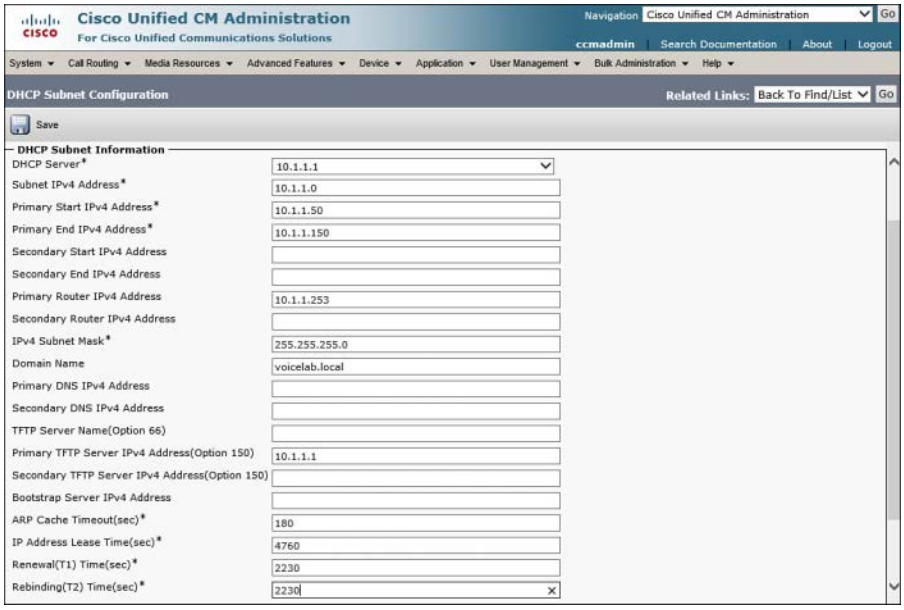


Figure 9-3 *DHCP Subnet Configuration*

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.

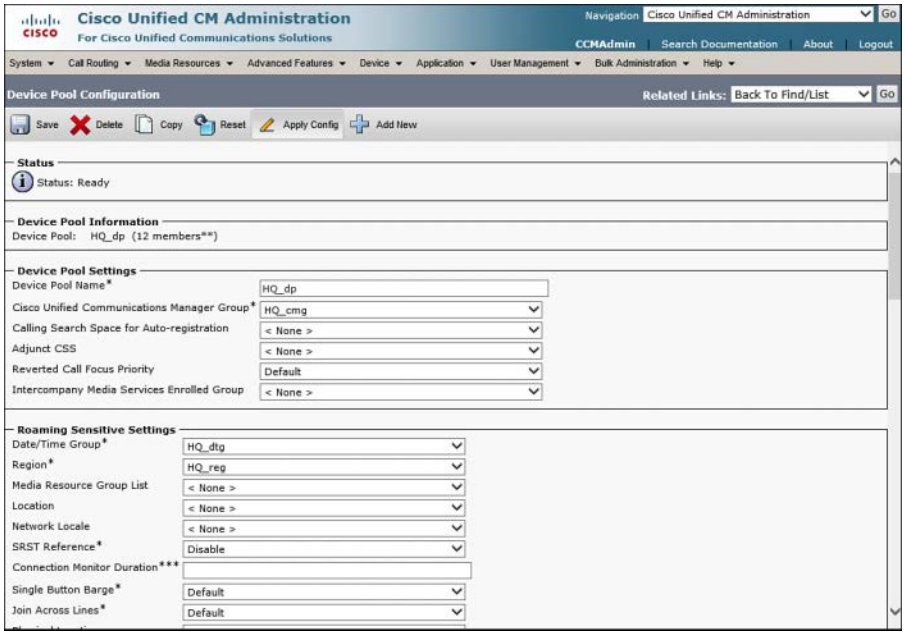


Figure 9-4 *Device Pool*

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.

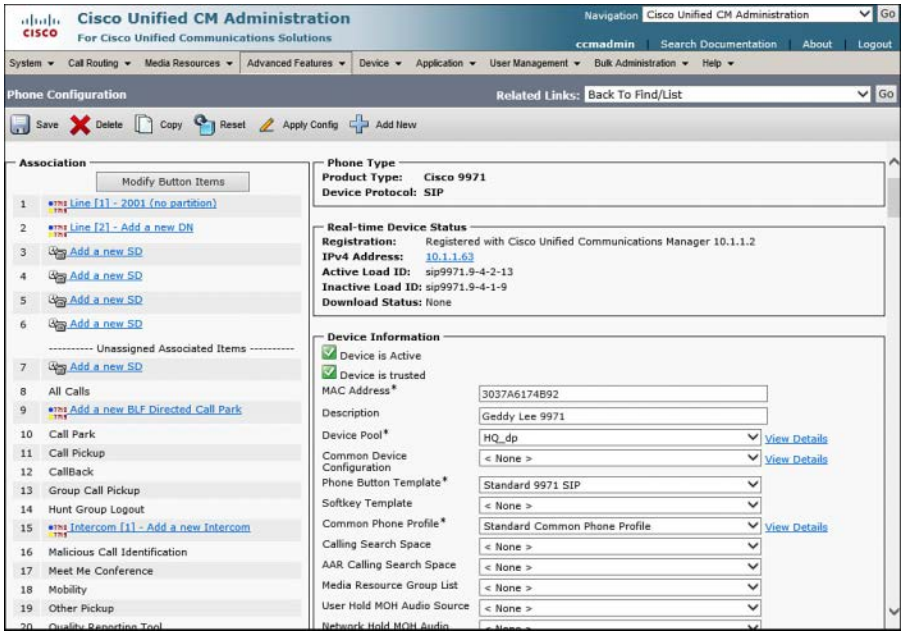


Figure 9-5 *The Phone Configuration Page*

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.

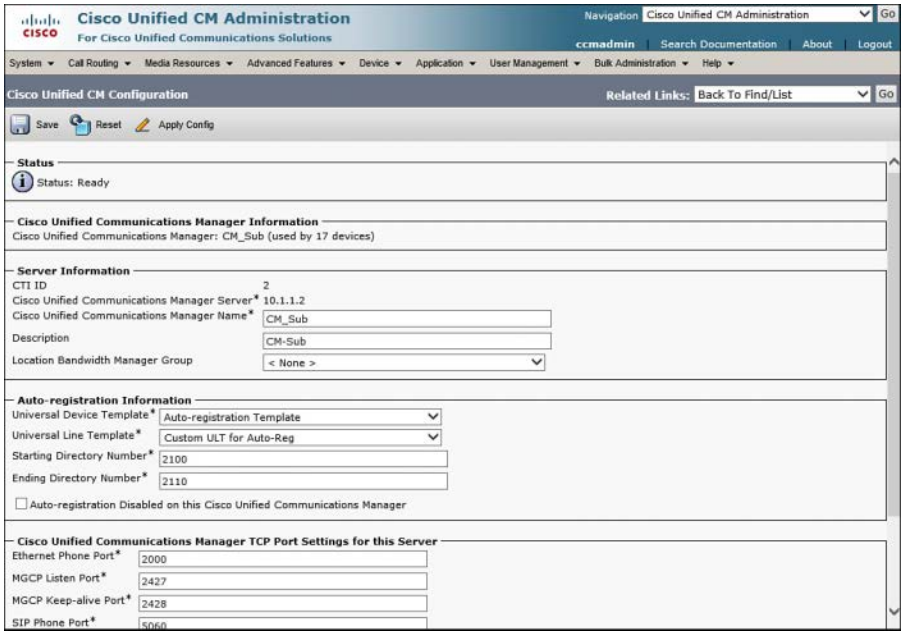


Figure 9-6 *Auto-Registration Configuration*

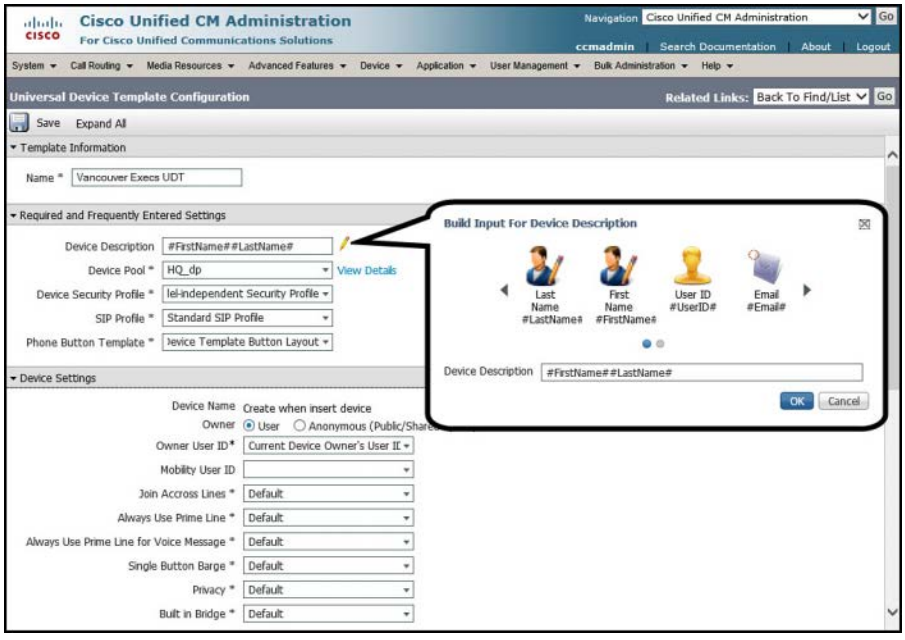


Figure 9-7 *Building a Universal Device Template*

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.

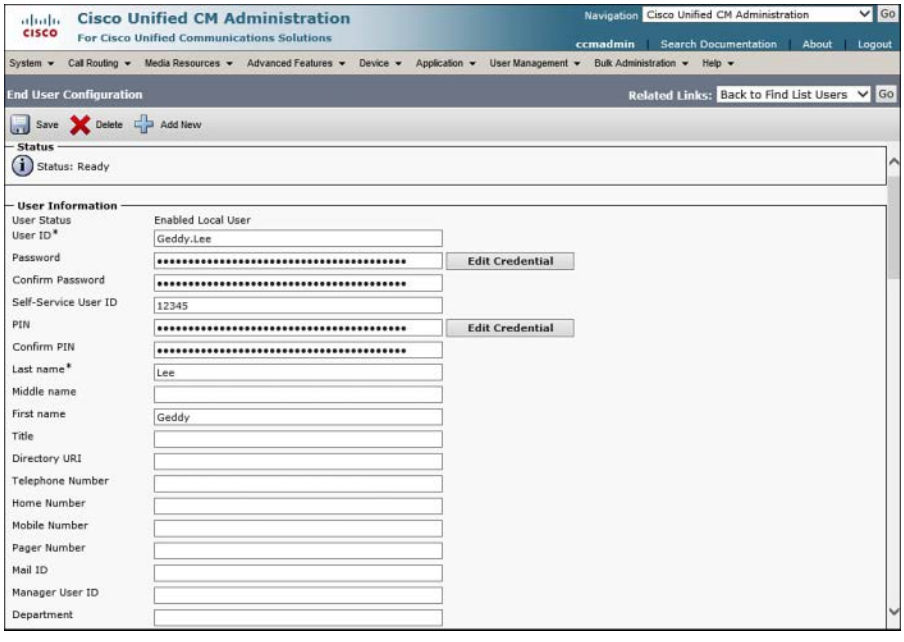


Figure 9-8 *End User Configuration Page*

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

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.

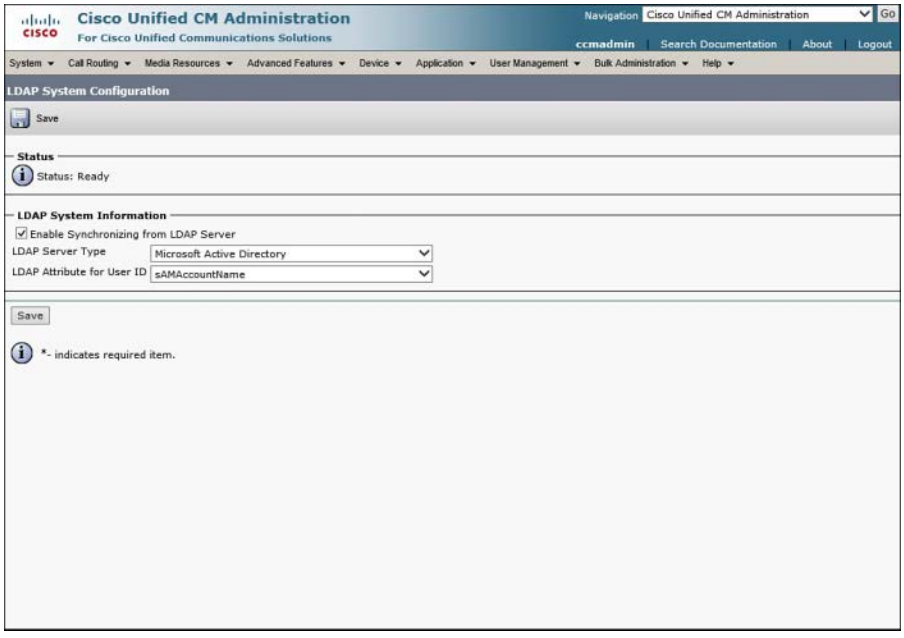


Figure 9-9 *LDAP System Configuration*

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.

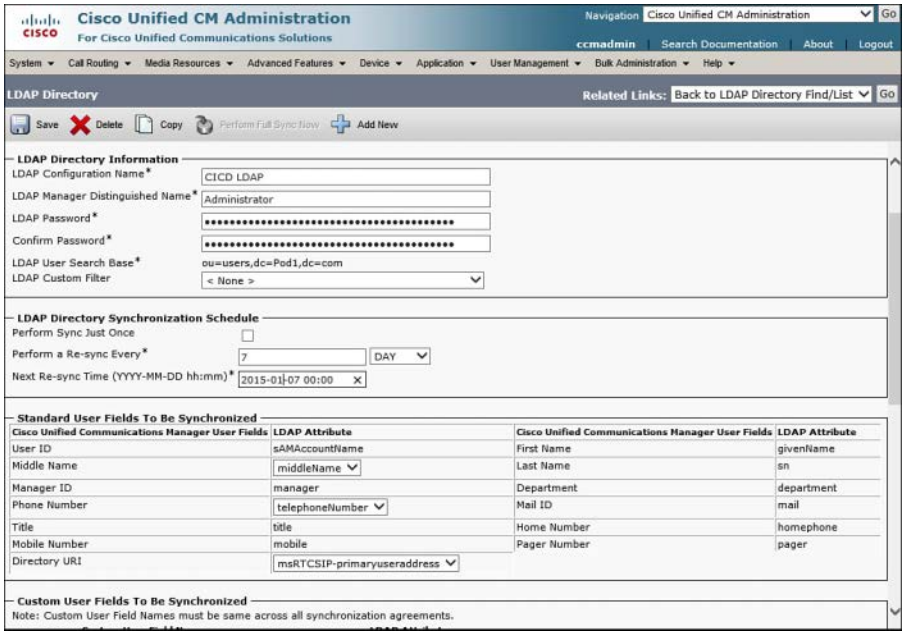


Figure 9-10 *LDAP Directory Configuration Page*

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

This chapter covers the following topics:

- **Call Flows in CUCM:** This section describes how call signaling and audio traffic flow in a CUCM system.
- **CAC and AAR:** This section explains CAC and the use of AAR.
- **Call Routing Components:** This section discusses the sources, destinations, and interaction of the various call routing components in CUCM.
- **Class of Control:** This section discusses the capabilities and configuration of class of control elements in CUCM

CHAPTER 10

Understanding CUCM Dial Plan Elements and Interactions

Chapter 9, "Managing Endpoints and End Users in CUCM," discussed the administration of IP Telephony endpoints and users in Cisco Unified Communications Manager (CUCM). This chapter reviews the components, behaviors, and interactions of the CUCM dial plan.

"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 10-1 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 10-1 Understanding CUCM Dial-Plan Components

Foundation Topics Section	Questions Covered in This Section
CUCM Call Flows	1–3, 6–9
CAC and AAR	4–5
Class of Control	10–12

1. Which two of the following are reasons to eliminate IP phone reliance on DNS?
   a. Elimination of additional licensing costs for Cisco Unified DNS server
   b. Elimination of single point of failure
   c. Reduce delay caused by name resolution lookups
   d. Eliminate delays caused by ARP resolution
2. Which of the following is true regarding call flows in CUCM? (Choose two.)
   a. Signaling traffic using RTP is sent directly to the CUCM from the IP phone.
   b. Signaling traffic using SCCP/SIP is sent directly to the CUCM from the IP phone.
   c. Voice bearer stream traffic flows through the CUCM server to maintain QoS policy.
   d. Voice bearer stream traffic flows direct from phone to phone.

3. Which of the following is true of SRST?
   a. SRST allows IP phones in a branch to be controlled by the local router in the event that WAN failure causes a loss of connectivity to the CUCM.
   b. SRST performs dynamic gateway services, allowing keepalives and signaling to be sent over the backup PSTN link.
   c. The NM-SRST module is supported on the 2900 and 3900 series ISR platforms only.
   d. SRST is a legacy feature; the replacement feature set is called Service Advertisement Framework.
4. Call admission control serves what purpose?
   a. Limiting user access to toll calls (for example, preventing unauthorized long-distance calling)
   b. Throttling the number of concurrent call attempts to prevent Code Yellow events
   c. Rerouting calls over the PSTN in the event of WAN failure
   d. Tracing malicious calls received from the PSTN to verify their origin
   e. Preventing oversubscription of IP WAN voice bandwidth by dropping calls that exceed the configured voice queue size
5. Which of the following is the only event that will trigger AAR?
   a. WAN failure
   b. CFUR rejection
   c. SRST registration
   d. Local route group failure
   e. CAC call rejection
   f. International Talk Like a Pirate Day
6. Which of the following is the correct order of configuration of call routing components?
   a. Device, route group, route list, route pattern
   b. Route pattern, route list, route group, device
   c. Route pattern, route group, route list, device
   d. Route group, device, route pattern, route list
7. Which of the following route patterns is the closest match for the dialed number 98675308?
   a. 9.1[2-9]XXXXXX
   b. 9.[2-9]XXXXXX
   c. 9.@
   d. 9.8[67][67]XXXX
   e. 9.8XXXXXX
   f. 9.86[^012345689]5308

8. Which two of the following signaling methods provide digit-by-digit analysis?
   a. SIP en-bloc
   b. MGCP en-bloc
   c. SIP using station dial rules
   d. SIP using CUCM dial rules
   e. SCCP
   f. SIP using KPML

9. Which of the following are line group distribution algorithms? (Choose all that apply.)
   a. First-in, first-out
   b. Broadcast
   c. Directed broadcast
   d. Top-down
   e. Longest idle
   f. Circular

10. Which of the following is true?
    a. No partitions or search spaces exist by default in a CUCM installation.
    b. One partition exists by default; it is named default.
    c. Only the default CSS has access to the default partition.
    d. All CSSs have access to the default partition.

11. Which statement is correct regarding calling search spaces?
    a. If a CSS is applied to the phone, it overrides the CSS on the line.
    b. If a CSS is applied to the line, it invalidates the CSS on the phone.
    c. If a CSS is applied to the line, it overrides the CSS applied to the phone.
    d. If a CSS is applied to the phone, a CSS cannot be applied to the line.

12. A partition is linked with a schedule that is in effect every day from 8:00 a.m. to 5:00 p.m. The partition contains a translation pattern that causes the dialed number of 5555309 to ring extension 2112. The partition is listed last in the CSS applied to a gateway. Another translation pattern is created that causes the dialed number 5555309 to ring the Auto-Attendant pilot. The translation pattern is not assigned to a partition. What happens when a PSTN phone calls 5555309 at 7:00 p.m. on Saturday?
    a. Extension 2112 rings.
    b. The caller gets an error message.
    c. The Auto-Attendant answers.
    d. None of the options are correct.

Foundation Topics

CUCM Call Flows

Chapter 6, "Understanding the CME Dial Plan," discussed how Cisco Unified Communications Manager Express (CME) selects call routing targets. The dial plan in Cisco Unified Communications Manager (CUCM) is more complex because it is a distributed system that uses remote components such as gateways to route calls. CUCM is intended to scale to large-enterprise environments, and consequently has a greater capacity for call routing complexity and redundancy. This chapter introduces and discusses call signaling and voice traffic flow in different scenarios; the components of the call routing system; and the call routing decision process, component configuration, redundancy, and restriction.

Call Flow in CUCM If DNS Is Used

Generally speaking, Domain Name System (DNS) is not recommended for use with Cisco IP phones. If DNS is used, the IP phones must complete a DNS name resolution lookup to learn the IP address of the CUCM server before any signaling can occur. At best, doing so introduces delay; at worst, it allows the possibility of a misconfiguration or failure of the DNS system that could cause the phones to stop working.

When the DNS lookup has completed successfully, the call flow consists of signaling (using either Skinny Call Control Protocol [SCCP] or Session Initiation Protocol [SIP]) between the phone and the CUCM, and the voice bearer streams (using Real-Time Transport Protocol [RTP]) directly between the phones. Note that the phones do not signal each other directly, nor does any voice traffic usually flow through the CUCM. Figure 10-1 illustrates call flow when DNS is used by the phones.

Note The exception to the last statement is if the CUCM is hosting a voice conference; in that case, the voice streams from all conference participants flow into the CUCM and the combined streams (minus the listener's own stream) flow out of the CUCM back to the participants.

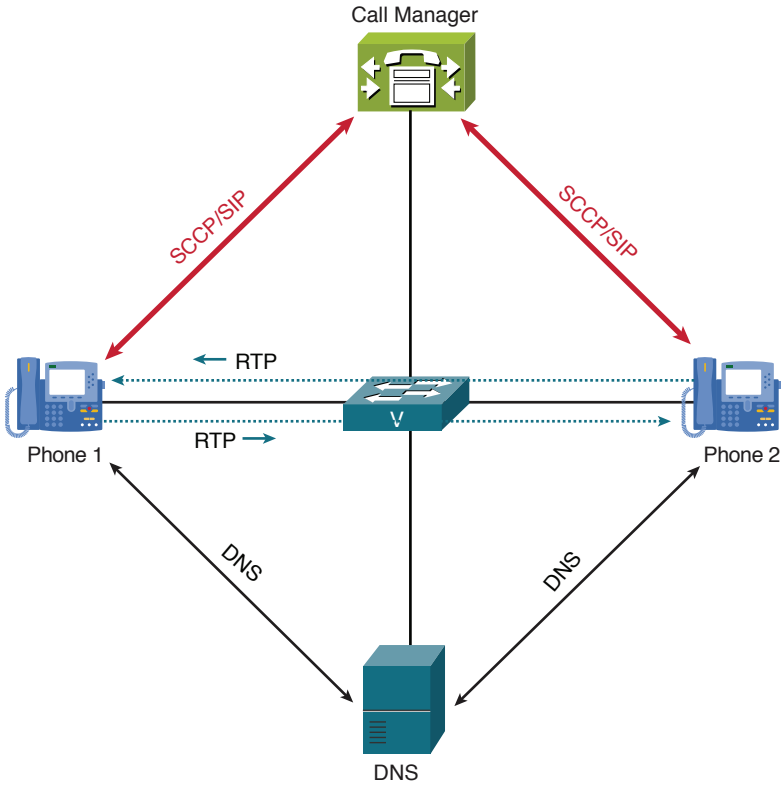


Figure 10-1 *Call Flow with DNS*

Call Flow in CUCM If DNS Is Not Used

Eliminating IP phone reliance on DNS is recommended to eliminate unnecessary delay and potential points of failure. If DNS is not used, the call flow is similar, except that the initial DNS lookup is eliminated, there remains only the signaling flow between the phones and the CUCM, and the voice bearer streams directly between the phones. Figure 10-2 illustrates call flow without DNS in use by the phones.

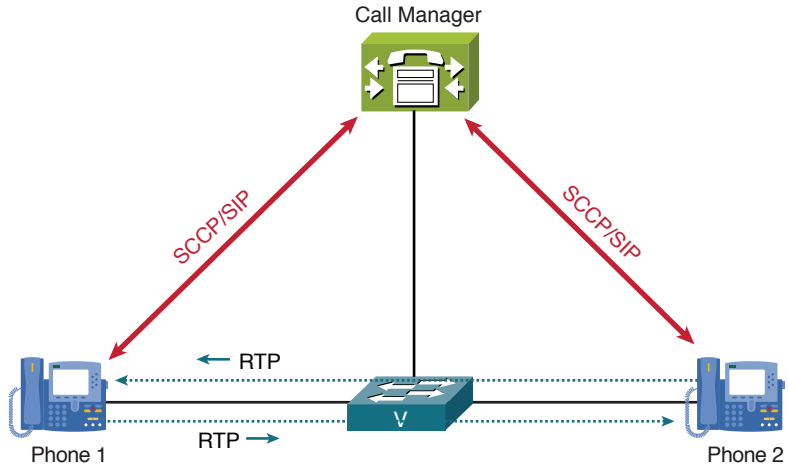


Figure 10-2 *CUCM Call Flow Without DNS*

The elimination of DNS reliance is simple to configure. The default installation of CUCM lists the hostname in the database field used by the phone configuration file to identify the CUCM server(s) the phone should use for registration. To change the value in this field, follow these steps:

Step 1. In CUCM Administration, navigate to **System > Server**.

Step 2. Select a server and, in the Server Configuration page, change the value of the Hostname/IP Address field from the hostname to the host's IP address, as shown in Figure 10-3.

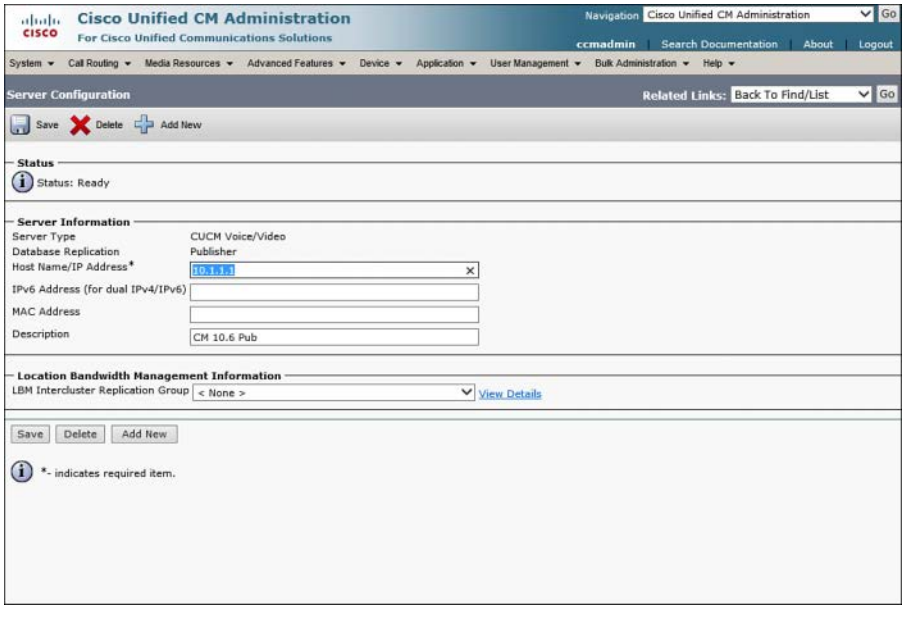


Figure 10-3 *Hostname Changed to IP Address in Server Configuration Page*

Step 3. Click **Save**.

Step 4. Repeat the previous steps for each server.

The next configuration task is similar but carried out under System > Enterprise Parameters. Scroll to the section titled Phone URL Parameters (shown in Figure 10-4), and in each field you change the URL to use the host IP address instead of the hostname.

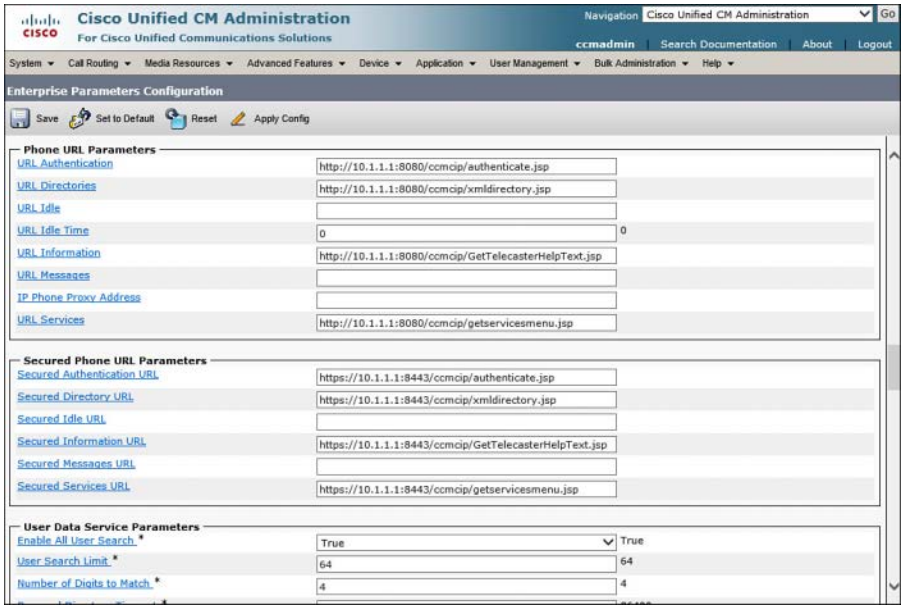


Figure 10-4 *Phone URLs Changed from Hostnames to Host IP Addresses*

Note The elimination of DNS reliance is recommended for IP phones, but there are some circumstances where it is useful, including when changing IP address schemes (when the DNS name stays stable, but the IP address it represents changes). The integration of Cisco Unified Presence Server (CUPS) with CUCM may require DNS service, but this might not affect the hardware IP phones. If DNS is used, it must be correctly managed and maintained so that it does not cause failures.

Centralized Remote Branch Call Flow

In a centralized deployment, the CUCM servers are located at the main location, with one or more locations at remote branches, connected by an IP WAN. The branch office IP phones use the IP WAN for both signaling and on-net voice traffic. Off-net calls from branch IP phones might be routed out the branch gateway or the main location gateway, depending on design.

The signaling and voice bearer stream paths are the same as in the single-site deployment; the difference is simply that the branch phones send all signaling traffic over the WAN to

the CUCM server, along with on-net RTP voice streams to IP phones at other locations. However, if a branch phone calls another branch phone, both phones signal to the CUCM across the WAN, but the RTP voice streams stay local to the branch—direct from phone to phone, as always. Figure 10-5 illustrates centralized remote branch call flow.

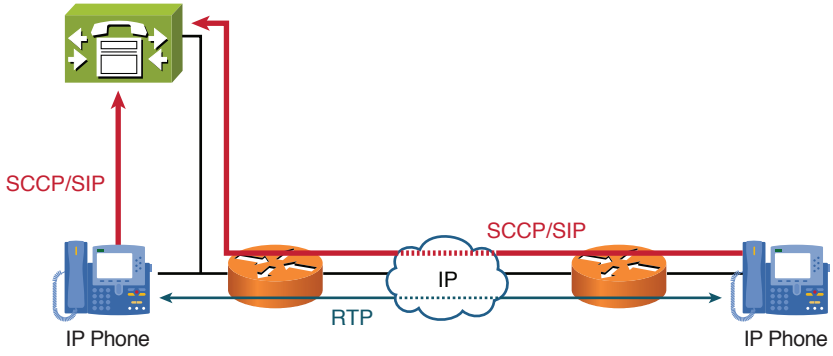


Figure 10-5 *Centralized Remote Branch Call Flow*

Centralized Deployment PSTN Backup Call Flow

Key Topic

If the IP WAN fails, all phones in the branch lose connectivity to the CUCM at the main location and no longer function. In this event, Survivable Remote Site Telephony (SRST) is recommended to provide registration and call control signaling local to the branch phones. SRST provides on-net IP-to-IP calling between branch phones, but if calls from branch phones to other locations are placed (whether on-net or off-net), they will fail. This is because of a lack of call routing configuration on the branch gateway router. Typically, the branch gateway is configured with a subset of CUCME capabilities to provide public switched telephone network (PSTN) access to branch phones. If the SRST router dial plan is configured properly, the branch users can still dial the same on-net extensions for calls to other locations, and the SRST router transparently modifies the dialed digits for PSTN routing. Most users will not be aware of the WAN failure.

From the main location CUCM perspective, the branch phones have de-registered and are considered unreachable. This is not entirely accurate (because they are reachable via the PSTN) and is an undesirable failure of the system. To provide continuity of service, call routing options and settings are configured on the CUCM that provide an alternate path to the branch via the PSTN:

1. The call routing table has a second option added to provide a PSTN gateway and appropriate digit manipulation to provide the required PSTN dialed digits.
2. The Call Forward UnRegistered (CFUR) option is configured on each branch phone to specify the full PSTN number needed to reach the branch phone.

These two configurations, in combination with the appropriate SRST configuration, ensure that branch phones can both reach and be reached by the main location in the event of WAN failure.

When the WAN recovers, the branch phones de-register from the SRST router, re-register with the CUCM, and the normal WAN-based signaling and calling patterns resume.

Centralized Deployment Considerations and Limitations

Deploying CUCM in a centralized call processing environment is one of the most popular choices, providing full features and capabilities to branch offices while centralizing equipment and management efforts at the headquarters. The following points should be considered during the design and planning of a centralized deployment:

- CUCM v10.x supports a maximum of 2000 locations and a maximum of 2100 H.323 or Media Gateway Control Protocol (MGCP) devices per cluster.

  Although there is no limit to the number of phones at a branch, the number of phones supported by the SRST router will be limited based on the router hardware model and the configuration applied to it. The maximum number of phones supported in SRST mode is 1500 on a 3945E branch router. The correct configuration to allocate resources to support that many phones must be applied, and the appropriate amount of RAM must be installed.

  The WAN must be properly provisioned and QoS enabled to allocate the priority queue bandwidth appropriate to the number of concurrent calls, and to limit delay for both RTP voice and signaling traffic.

- Call admission control (CAC), as explained in the next section, should be implemented, either CUCM location-based or Resource Reservation Protocol (RSVP) based. Regardless of the CAC method used, the goal is to prevent more calls than the design specifies from being extended across the WAN, thereby protecting call quality for all IP calls.

PSTN Backup Using CAC

CAC prevents IP calls from being extended across a WAN link, if the additional WAN bandwidth required would exceed the quality of service (QoS)-allocated bandwidth for concurrent calls. For example, if the design specifies a maximum of 10 calls using G.729, the QoS engineer would create a priority queue (low-latency queuing [LLQ]) sized to serve those 10 calls. (The QoS configurations are beyond the scope of the CCNA Collaboration Exam.) If an eleventh call were extended to the gateway, the additional bandwidth would overrun the input buffer for the LLQ, and packets from all 11 calls would start to drop, causing unacceptable packet loss and resultant deterioration of voice quality for all 11 calls.

With location-based CAC implemented, CUCM tracks how many calls are extended to a given location, subtracting the bandwidth used for each concurrent call from the bandwidth specified for that location. When the remaining bandwidth is less than the amount used by a single call (which varies based on the codec used for the call, which is in turn defined by the Region setting), the default behavior of CAC is to drop the call. Users get a reorder tone or an annunciator message indicating that the call has failed.

In most cases, dropping the call is not desirable, and automated alternate routing (AAR) is implemented to reroute the call across the PSTN. AAR is exclusively triggered by CAC; when CAC prevents the call from extending across the WAN, CUCM checks to see whether an AAR group is configured for the calling phone. If an AAR group is configured, it specifies what digit manipulation is required to retry the call with a full PSTN Dialed Number Information Service (DNIS). The operation is transparent to the user (although it is possible that he might notice a difference in call quality using the PSTN instead of the WAN).

If the call is extended over the PSTN, the call signaling path includes the PSTN gateways at the main and branch locations, and the RTP voice streams are converted to the appropriate PSTN transport.

Note Be clear about the difference between PSTN rerouting due to WAN failure versus CAC and AAR being triggered by a lack of available WAN bandwidth for calls. If the WAN fails, calls may be rerouted to the PSTN using the hierarchical design of the dial plan and CFUR on the CUCM side, and SRST on the branch side. If the WAN has no available bandwidth, CAC triggers AAR, which will redial the call with a full PSTN number, but only if it is correctly configured to do so. Figure 10-6 summarizes the sequence of events if the WAN fails.

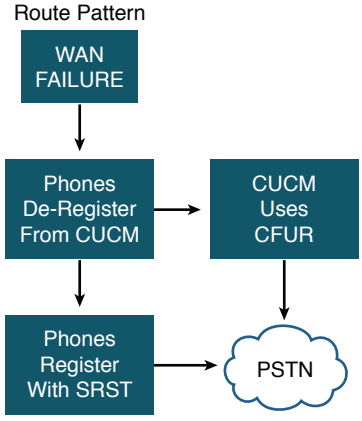


Figure 10-6 *WAN Failure to SRST/CFUR*

Distributed Deployment Call Flow

In a distributed deployment, one CUCM cluster signals another CUCM cluster across a WAN. The signaling flows from the calling phone to the local CUCM, then from the local CUCM across the WAN to the remote CUCM, then from the remote CUCM to the remote (called) phone. The RTP voice streams extend from each phone across the WAN to the other phone. Figure 10-7 illustrates call flow in a distributed deployment.

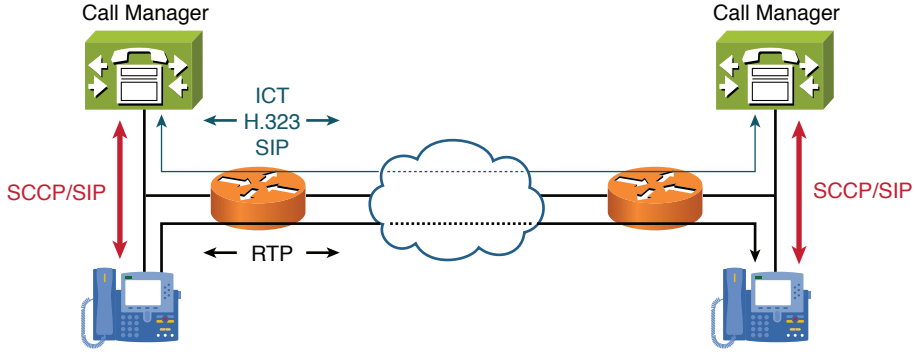


Figure 10-7 *Distributed Deployment Call Flow CUCM Call Routing Components*

The signaling protocols available include Inter-Cluster Trunk (ICT), H.323, and Session Initiation Protocol (SIP). The CUCM clusters at each site control their local phones using Skinny Client Control Protocol (SCCP) or SIP. The use of gatekeepers (along with a well-designed dial plan) allow scalability to thousands of sites, with either a full CUCM cluster for large sites or a CUCME for smaller sites (third-party solutions may also be integrated). PSTN backup for WAN failure is achieved using a hierarchical dial plan, and CAC should be used when WAN bandwidth for calls is not available.

Note As of CUCM v9.x, locations-based CAC is now available in a distributed (multi-cluster) deployment, although this topic is well outside the scope of CICD. Gatekeeper CAC could be implemented instead to provide a centralized service to track available bandwidth between clusters and trigger AAR when necessary. Gatekeeper is a router IOS feature set that may be configured on one or more gateway routers in the system. RSVP-enabled CAC is another possible option for distributed deployments.

The building blocks of the CUCM dial plan are simple and consistent. The potential for complexity exists when multiple hierarchical paths are implemented, with different features and capabilities enabled. This section identifies the core elements and explains their interactions.

Call Routing Sources in CUCM

A call routing request (including but not limited to a simple phone call) can originate from any of the following:

- **IP phone:** Places a routing request using one of its configured lines. This may be a manually dialed number, speed dial, feature button, or softkey.
- **Trunk:** Signals inbound calls from another CUCM cluster, CUCME, or other call agent.
- **Gateway:** Signals inbound calls from the PSTN or another call agent, such as a private branch exchange (PBX).
- **Translation pattern:** Matches the original called digits and immediately transforms them to a new dialed string. The new string is resubmitted to digit analysis for routing.
- **Voicemail port:** Can be the source of a call routing request if the application attempts a call, transfer, or message notification on behalf of a user's mailbox.

A call routing request is simply one of the previous entities signaling CUCM with a string of dialed digits. These digits can be manually dialed by a user on their phone, automatically by an application such as Cisco Unity Connection, or by another system via a trunk or gateway.

Call Routing Destinations in CUCM

The following are possible call routing destinations in CUCM:

- **Directory number (DN):** Each button on an IP phone can be assigned a unique on-net extension.
- **Translation pattern:** Matches a string of dialed digits and transforms them to a new dialed string, which is in turn resubmitted to digit analysis and routed to a different target.

- **Route pattern:** Matches a set of dialed digits and triggers a call routing process that can include one or more potential paths, providing a hierarchical set of call routing options.
- **Hunt pilot:** A specific pattern of digits that, when matched, triggers a customizable call-coverage system.
- **Call park number:** A pattern or range of patterns that CUCM can use to temporarily hold a call until a user dials the call park number to pick it up from any IP phone.
- **Meet-Me number:** The conference call initiator dials into the Meet-Me number to begin the conference, and one or more other users dial into the same number to join the conference.

All the previous destinations are represented by strings of dialable digits, or as of CUCM v9.x potentially a SIP Uniform Resource Identifier (URI).

Note A SIP URI is an alphanumeric string (for example: sip:1-999-123-4567@voip-provider.example.net). CUCM has the ability to route calls using this addressing method, but that topic is also out of scope for CICD. It is a very cool and potentially very important capability that you might want to learn more about (once you pass your CICD).

The dial plan must allocate ranges of numbers for all these targets, and CUCM must be configured to route to them appropriately (including *not* routing to them, if necessary).

Call Routing Configuration Elements

The primary components of the CUCM call routing system are the following:

- Route patterns
- Route lists
- Route groups
- Gateways/trunks

Route Pattern

A route pattern matches a string of dialed digits. The pattern may be specific, matching a single dialable number, or it may be general, matching hundreds of thousands of possible numbers. This variable precision is configured using wildcard digits in the pattern. Route patterns allow the administrator to specify the target of any given string of dialed digits.

Route patterns are necessary to provide PSTN dial access. They may also be used to integrate the CUCM dial plan with an existing PBX dial plan; in this instance, the route pattern would match all the DNs (extensions) controlled by the PBX. In fact, a route pattern may be customized to allow users to dial any number and reach any desired end station.

Route patterns are associated with either a route list or a specific gateway.

Note If a route pattern is directly associated with a gateway (as opposed to a route list), the selected gateway can no longer be referenced by a route group; the gateway is "locked in" to the route pattern. In small deployments, this may not be problematic, but in large deployments, doing so limits the flexibility of the system.

Route List

A route list is an ordered list of route groups. The first entry in the list is the preferred call routing path; if that path is unavailable (due to failure or no circuit/channel available), if a second choice is configured, it will be used instead. There may be several choices in the list; each new call uses the choices in top-down order.

The hierarchical order of the route list entries allows the administrator to provide depth of coverage for call routing paths while controlling which resources are used for each call. For example, if the route pattern that matches a national long-distance number is associated with a route list that lists its first choice as a route group providing access to an inexpensive inter-exchange carrier (IXC) PRI circuit, the call is routed to that IXC circuit. Subsequent calls matching the same route pattern are also routed to the IXC circuit until no channels are available.

At that point, the routing request to the IXC is rejected and the route list's second choice is tried. If the second choice is a local exchange carrier (LEC) PSTN PRI circuit, the call is dialed over the LEC PSTN link, as long as a channel is available. This call costs more than using the IXC circuit, but it works; the call does not fail, and business continuity is maintained.

In this example, cost is the design driver: The IXC is less expensive than the LEC circuit, so the IXC is the desired target for all long-distance calls. However, if the IXC is busy (or has failed), it is acceptable that long-distance calls be placed out the LEC circuit so that service is not interrupted.

Route Group

A route group is a list of devices (gateways or trunks) that are configured to support circuits to the PSTN or to remote CUCM clusters in distributed designs. Route groups are commonly configured to contain devices with common signaling characteristics (for example, a set of PSTN PRI gateways in one group and a set of WAN IP trunks to a remote cluster in another).

The distribution algorithm of a route group is configurable; selecting Top-Down causes the devices in the group to be used in top-down order for each new call, and selecting Circular uses the devices in round-robin order. The specific context and requirements of the system determines which algorithm is appropriate.

Note The local route group feature allows the administrator to define a route group in the device pool and reference that local route group in the route list. Doing so effectively decouples the location of a PSTN gateway from the route patterns that target the gateway. This feature greatly reduces the complexity of dial plan design in systems with many locations and makes much more complex environments and feature implementation much simpler. You really like the local route group feature, even if you do not know it yet.

Gateways and Trunks

Gateways and trunks are the devices that physically terminate and support circuits to the PSTN, to digital or analog PBXs, and to IP WAN circuits to remote clusters or IP-TSP circuits to service providers.

CUCM supports various gateway devices and interfaces, controlling them with either peer-to-peer gateway protocols (H.323 and SIP) or gateway control protocols (Media Gateway Control Protocol [MGCP] and SCCP).

Figure 10-8 shows the call routing elements previously described.

Key Topic

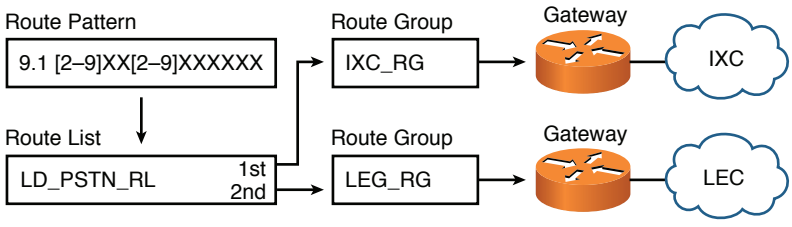


Figure 10-8 *Call Routing Elements*

Note The configuration order of the call routing elements is as follows: devices, route groups, route lists, route patterns. The call flow is the reverse: The dialed digits match a route pattern, which points to a route list, which points to a route group, which references devices.

Call Routing Behavior

Digit analysis is the process by which CUCM matches dialed digits to possible targets for call routing. Different protocols and devices perform digit analysis in different ways: Dialed digits are collected digit-by-digit on SCCP phones and SIP phones that use Keypad Markup Language (KPML), and en-bloc (all at once as a set of digits) on basic SIP phones, trunks, and most gateways.

Digit Analysis

The digit analysis logic that CUCM uses to select the target for the call routing request is based on the closest match. Consider the following set of route patterns:

- 1111
- 1211
- 1[23]XX
- 131
- 13[0-4]X
- 13!

With these route patterns in mind (these are not intended to be realistic; they just illustrate the pattern-matching logic), let's look at three examples of how CUCM will process different dialed strings:

Example 1: If User A dials 1111, there is an exact match with the pattern 1111. No other patterns match, and the call is extended to that target.

Example 2: If User B dials 1211, CUCM has two possible matches:

- **1211:** Matches 1 digit string
- **1[23]XX:** Matches 200 digit strings

CUCM selects the closest match target (the one that matches the fewest possible strings) (in this case, 1211).

Example 3: If User C dials 131, CUCM has four possible matches:

- **1[23]XX:** Matches 200 digit strings
- **131:** Matches 1 digit string
- **13[0-4]X:** Matches 50 digit strings
- **13!:** Matches almost 10,000 quintillion digit strings (For our purposes, that is practically an unlimited number.)

The pattern 131 matches exactly, but other patterns match, too; these other patterns are longer, so CUCM has to wait to see whether User C dials another digit. If she does, 131 no longer matches and is discarded as a possible target. The wait time is set by the T.302 Inter-Digit Timeout value, which defaults to 15 seconds. If User C dials a fourth digit, the T.302 timer starts again because there is still a longer pattern that might match (13!). If User C stops dialing after 4 digits, after 15 seconds (the T.302 timer wait), the call is extended to the target of the 13[0-4]X pattern. If she dials another digit within the T.302 timer count, the 13[0-4]X pattern is discarded because it no longer matches. When User C finishes dialing, the T.302 timer must exhaust before the call is routed.

Key Topic

Note Digit-by-digit analysis means that CUCM collects digits one at a time as they are dialed. As digits are collected, patterns that no longer match the string are discarded as possible routing targets.

The closest match logic will choose a pattern target according to the following criteria:

- The pattern matches the dialed string.
- Among all the potential matches, it matches the fewest strings other than the actual dialed string.

10

Hunt Groups

A hunt group is a set of IP phones (technically, the directory numbers [DNs] on the phones) that are able to be reached by calling a common number. The classic example is the help desk; users dial 7777, and all the DNs of the help desk staff ring in sequence until one of them picks up the call.

The components of a hunt group are as follows:

- **Line groups:** Contain the DNs that will be rung sequentially. The line group settings allow the selection of the call distribution algorithm: top-down, circular, longest idle, or broadcast. The settings also control when, or if, to proceed to the next available line group in the hunt list.
- **Hunt lists:** Contain a top-down ordered list of line groups. Each new call is routed to the first line group in the list; if that group cannot provide call coverage, the next line group in the hunt list is tried until the list is exhausted.
- **Hunt pilot:** This is a call routing entry (much like a route pattern) that matches a dialed string and targets a hunt list (which in turn targets a line group). Hunt pilot numbers may be on-net, E.164, or any format as required.

Class of Control

Class of control is defined as the ability to apply calling restrictions to devices. Typical examples include the following:

- Preventing certain individuals from placing long-distance calls
- Routing the same called number to different targets at different times of day
- Routing the same called number to different targets at different locations

Class of control is configured using partitions and calling search spaces (discussed in the following sections).

Partition

A partition is a grouping of things with similar reachability characteristics. In general, you can think of a partition as being assigned to things you can dial, such as the following:

- DNs
- Route patterns
- Translation patterns
- Voicemail ports
- Meet-Me conference numbers

By default, one partition exists; it is called the null partition, although it is listed in the CUCM web pages as <none>. Up to 75 additional partitions can be created at once.

Calling Search Space

A calling search space is a top-down ordered list of partitions. A calling search space can be applied to a device (such as an IP phone or gateway) or to a line on the IP phone. One CSS exists by default, and by default, it contains only the null partition. You can think of a CSS as being assigned to things that can place calls.

Interaction of Partitions and Calling Search Spaces

The essential thing to understand is this: If the target that is being dialed does not exist in one of the partitions in the CSS of the caller, the call will fail. This behavior allows us

to design specific calling privilege schemes and apply them to different calling devices or lines. Consider the following example: A company wants to implement call restriction such that the lobby phones cannot place long-distance calls. A new partition is created called PSTN_Local_PTN. The route patterns that match 7-digit and 10-digit (toll-free) PSTN calls are assigned to the PSTN_Local_PTN partition.

A new CSS is created called Lobby_CSS. The PSTN_Local_PTN partition is added to the Lobby_CSS.

The Lobby CSS is applied to the lobby phones configuration. As soon as that change is made, the lobby phones will get the reorder tone when they try to dial any number that does not match the 7- or 10-digit patterns in the Lobby_CSS. Thus, no one can abuse the lobby phones and cost the company toll fees by making long-distance calls.

A few related points:

- If a user tries to call 911 from the lobby phone, that call will fail too, unless the emergency call patterns are also added to the PSTN_Local_PTN partition or to another partition that is in turn added to the Lobby_CSS. It is generally a good idea to ensure that every phone can place emergency calls.
- When a route pattern is moved from the default partition <none>, it is no longer accessible to the default CSS. This means that calls matching the Route Pattern will fail until a new, functional CSS/partition structure is completed. For this reason, it is best to plan and implement class of service (CoS) configurations before phones are in use to avoid service interruption.
- Every CSS includes the default partition <none>, at the end of the list of custom partitions. This means that any target that is left in the default partition <none> is reachable by every calling device.

Line Device Configuration

Key Topic

So far, we have assumed that the CSS is applied only to the device (that is, the IP phone). It is also possible to apply a CSS to the line on the phone; the line CSS may be very different and include other partitions, which in turn contain different route patterns, and so on.

If both a device and a line CSS are applied, the partitions in both CSS are concatenated in sequential top-down order, with the line CSS partitions listed first, and the device CSS partitions second.

CUCM will analyze the list of partitions in that order, looking for a match to the dialed digits among the patterns in the list. If a match is found, the call is routed to the target. If more than one identical match is found, the partition containing the match that is first in the concatenated list will be the target. In other words, the line CSS overrides the device CSS.

There are several benefits to using the line/device method. In general, best practices suggest setting up the device CSS to allow full calling privilege to all patterns, with the call routing appropriate to the device's location (for example, PSTN calls placed out the local gateway). The calling restrictions are then applied using the line CSS, which can contain route patterns that match long-distance numbers but are configured to block those calls. The result is that fewer total CSS need to be configured, which makes it simpler to manage and scale the dial plan.

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 10-2 lists and describes these key topics and identifies the page number on which each is found.

Table 10-2 Key Topics for Chapter 10

Key Topic Element	Description	Page Number
Section	Call routing behavior and features in the event of WAN failure	274
Section	Call routing behavior in the event of a lack of WAN bandwidth for voice	275
Section	Describes the configuration and use of route patterns, route lists, route groups, and devices	278
Figure 10-8	Illustrates call routing components	280
Note	Explains the logic CUCM uses in dialed digit analysis for call routing	281
Section	Explains the structure and behavior of partitions and calling search spaces	282
Section	Explains interaction of CSS applied to both phone and line	283

Definitions of Key Terms

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

SRST,CAC, AAR, route pattern, route list, route group, hunt group, partition, search space, CFUR

This page intentionally left blank

This chapter covers the following topics:

- **Describe Extension Mobility in CUCM:** This section describes the Extension Mobility feature, its advantages, its disadvantages, and its integration into the CUCM cluster.
- **Enable Extension Mobility in CUCM:** This section describes how to enable the Extension Mobility feature.
- **Describe Telephony Features in CUCM:** This section describes CUCM telephony features, including call coverage, intercom, and Presence.
- **Enable Telephony Features in CUCM:** This section describes how to enable the telephony features described in earlier sections in this chapter.

CHAPTER 11

Enabling Telephony and Mobility Features with CUCM

Getting Cisco Unified Communications Manager (CUCM) to the point where it will ring phones is only part of the fun. Users of a contemporary business phone system expect it to have a comprehensive feature set. This chapter explores just a few of the features available in CUCM 10.x and the basics of implementing them.

"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 11-1 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 11-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Extension Mobility in CUCM	1–2
Enable Telephony Features in CUCM	3–10

1. Which of the following defines Cisco Extension Mobility?
   a. A user can log in to any IP phone in the cluster; that phone is dynamically configured with the user's DN, speed dials, and other custom configurations.
   b. A user can move his phone anywhere within the cluster, and its calls will be routed out the local gateway.
   c. A user can define several remote destinations so that a call to his IP phone rings his mobile and home destinations simultaneously.
   d. Users can log in to any phone in the cluster and receive a DN from a predefined range.
   e. Users can choose one of several wireless IP phone models for mobile IP communication throughout the WLAN coverage area.
2. Which of the following is not an administrative option when a user attempts to log in to multiple devices using Cisco Extension Mobility?
   a. Allow Multiple Logins
   b. Prompt User
   c. Deny Login
   d. Auto Logout

3. How can call forwarding options be configured in CUCM? (Choose all that apply.)
   a. Administratively, using the CM Administration pages
   b. Automatically, using device defaults
   c. By the user from the IP phone
   d. By the user from the user web pages
   e. By the user using Cisco Unified Call Forward Central
4. A user hears another phone ringing, presses a softkey, enters a number, and the call is extended to his phone. What feature did the user just invoke?
   a. Call pickup
   b. Group call pickup
   c. Other group pickup
   d. Call intercept
5. Which of the following is the correct order of call flow through a call hunting system?
   a. Hunt Pilot > Hunt Group > Hunt List > DN
   b. Hunt Pilot > Hunt List > Hunt Group > DN
   c. Hunt Group > Hunt List > Line Group > DN
   d. Hunt Pilot > Hunt List > Line Group > DN
6. Which of the following are distribution algorithm choices for hunt lists? (Choose all that apply.)
   a. Top-down
   b. Round-robin
   c. Simultaneous
   d. Broadcast
   e. Longest idle
   f. Circular
   g. Multicast
7. Which two of the following are options for intercom functionality? (Choose two.)
   a. A softkey with the intercom DN preprogrammed
   b. A phone button with the intercom DN preprogrammed
   c. An intercom button which when pressed allows you to dial the intercom DN manually
   d. An IP phone service that when accessed allows you to dial the intercom DN manually

8. John is on the phone with Guy. Lesley uses the whisper intercom feature to speak to John. What happens?
   a. John and Guy hear Lesley.
   b. John hears Lesley and Guy does not.
   c. John hears Lesley, Guy does not, and Lesley hears John.
   d. John hears Lesley, Guy does not, and Lesley does not hear John.
9. CUCM includes a native Presence capability. What three IP phone states is CUCM Native Presence able to monitor?
   a. On-hook
   b. Logged out
   c. Off-hook
   d. Unregistered
10. Which of the following describes the interaction of presence groups and Subscribe calling search space?
   a. BLF speed dials depend on both to function.
   b. The Subscribe CSS overrides the Presence group subscription permission.
   c. The Presence group subscription permission overrides the Subscribe CSS.
   d. Both the Subscribe CSS and the Presence group subscription permission must allow subscription in order to allow presence indications to work properly.

Foundation Topics

Describe Extension Mobility in CUCM

Key Topic

Cisco Extension Mobility (EM) allows a user to log in to any phone in the CUCM cluster (and as of version 8.x, cross-cluster). In environments where workers move from desk to desk, this allows their personal configurations, such as directory numbers (DNs) and speed dials, to be dynamically set up on the IP phones they are currently using, making them reachable at the same extension number regardless of which phone they are using.

EM operates as an IP phone service, applying user-specific device profiles to the phone the user logs in to. Once the phones are subscribed to the Extension Mobility service, the user selects that service on the phone and enters his user ID and PIN when prompted (using the phone keypad in alphanumeric mode, similar to texting on an old cell phone). CUCM then applies the user device profile settings and resets the phone. Separate device profiles must be created for each phone model a user might log in to. For example, suppose the user's primary phone is a 7965 with six buttons set up for two DNs and four speed dials. When the user logs in to a 7942 with only two buttons, the device profile defines what to configure on the two buttons: one DN and a speed dial, two DNs, or whatever the user needs. The user must select the correct profile from a list if multiple profiles exist.

If a user logs in to multiple phones concurrently, administrators have three options to determine how the system behaves:

- **Allow multiple logins:** The user can be logged in to multiple phones at the same time. When this happens, the effect is that of a shared line: All the phones will ring when the DN configured on each of them is called.
- **Deny login:** The user can only be logged in to one device at a time. When he attempts to log in to a second device, he receives an error message. He must log out of the first device before the second login will succeed.
- **Auto-logout:** The user can only be logged into one device at a time. When he attempts to log in to the second device, the system automatically logs him out of the first device, and the second login succeeds.

When the device is logged out, either another device profile can be applied (typically a logout device profile, perhaps allowing on-net and emergency calls only) or the settings in the phone configuration page are applied.

The device profile settings include the following:

- User Music on Hold (MoH) audio source
- Phone Button template
- Softkey template
- User locale
- Do not disturb (DND)
- Privacy setting
- Service subscriptions
- Dialing name

A default device profile exists to allow users without a user device profile for a particular IP phone type to log in using EM.

Enable EM in CUCM

Key Topic

Enabling EM involves several steps, a few of which may need to be repeated many times depending on the number of phones and users in the system. The basic steps are as follows:

Step 1. Activate the Cisco EM service.

Step 2. Configure EM service parameters.

Step 3. Add the EM service.

Step 4. Create a default device profile for each model of phone in use.

Step 5. Create device profiles and subscribe them to the EM service.

Step 6. Create end users and associate them with device profiles.

Step 7. Enable EM for phones and subscribe phones to the EM service.

The steps are described in more detail in the following sections.

Step 1. Activate the EM service:

- **a.** On the Serviceability web page, navigate to **Tools > Service Activation**.
- **b.** Select **Cisco Extension Mobility**, and then click **Save**.

Step 2. Configure EM service parameters:

- **a.** On the CM Administration web page, navigate to **System > Service Parameters**. Select the servers that you want to configure from the Server drop-down, and then select the **Cisco Extension Mobility Service** from the Service drop-down.
- **b.** Scroll down to the Clusterwide Parameters section. Here, you can select whether to force EM logout after a maximum login time has expired and how long that timer is. This is also where you can set the behavior for multiple logins (Multiple Logins Not Allowed, Multiple Logins Allowed, or Auto Logout), as described earlier. Additional settings here include enabling alphanumeric user IDs (or using numeric only), choosing to remember and display on the phone (or not) the last user ID logged in to the phone, and whether to clear the call lists for the last logged in user on logout.

Step 3. Add the EM service:

- **a.** Navigate to **Device > Device Settings > Phone Services**.
- **b.** Click **Add New**.
- **c.** Give the EM service a name and description, if desired.
- **d.** Type (or copy and paste from an external source) the following URL into the Service URL field: **http://<*IP_address_of_Publisher*>:8080/emapp/EMAppServlet?device=#*DEVICENAME*#**.

e. You may choose to add the Secure Service URL as well; if both are configured, and the IP phone supports HTTPS, the secure URL will be used preferentially.

f. Make sure that the **Enable** check box is selected.

g. You may choose to select the Enterprise Subscription check box as well. Doing so automatically subscribes all IP phones that support service subscription to the EM service; the administrator does not need to add the service manually to each device.

Figure 11-1 shows the EM Service Configuration page.

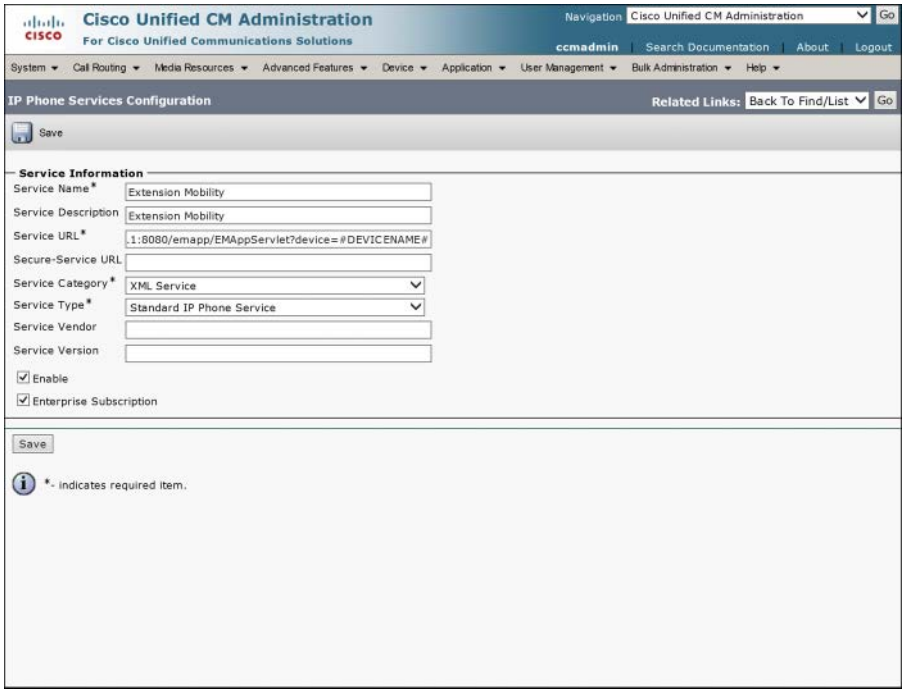


Figure 11-1 *Extension Mobility Service Configuration*

Step 4. Create default device profiles:

a. In the CM Administration web pages, navigate to **Device > Device Settings > Default Device Profile**.

b. Click **Add New**.

c. Select the product type (the phone model) and device protocol.

The available settings depend on the phone model and protocol chosen. You may select the Phone Button and softkey templates, but you are not able to configure DNs or other specific phone button settings. Figure 11-2 shows the Default Device Profile page.

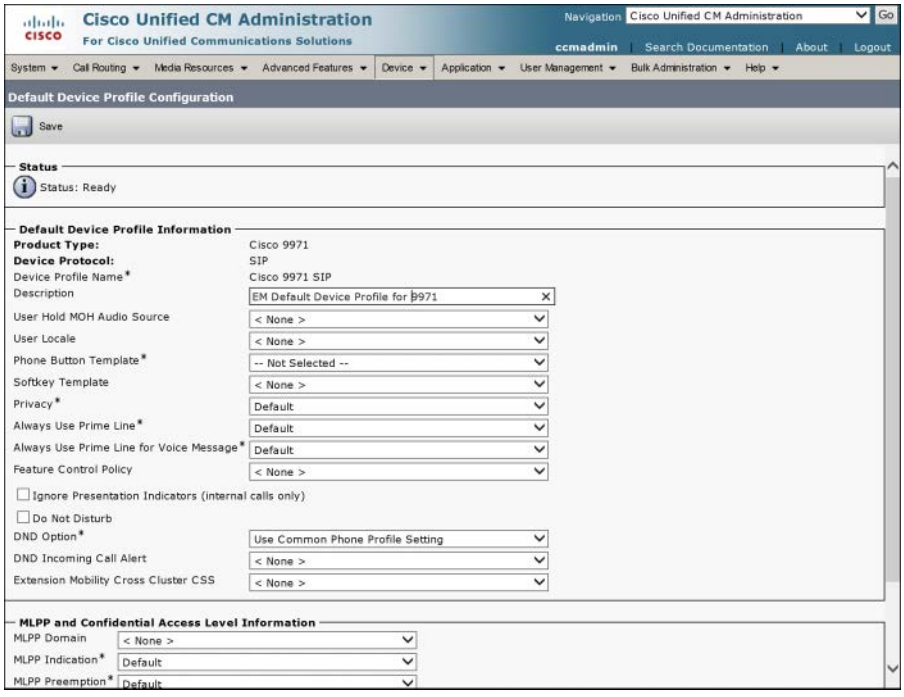


Figure 11-2 *Default Device Profile Configuration*

Step 5a. Create device profiles:

i. Navigate to **Device > Device Settings > Device Profile**.

ii. Click **Add New**.

iii. Select the phone model and protocol for a particular user's phone.

iv. Enter a name for the profile.

v. Configure user-specific settings, including DN, button customizations, and other parameters.

Figure 11-3 shows a Device Profile Configuration page.

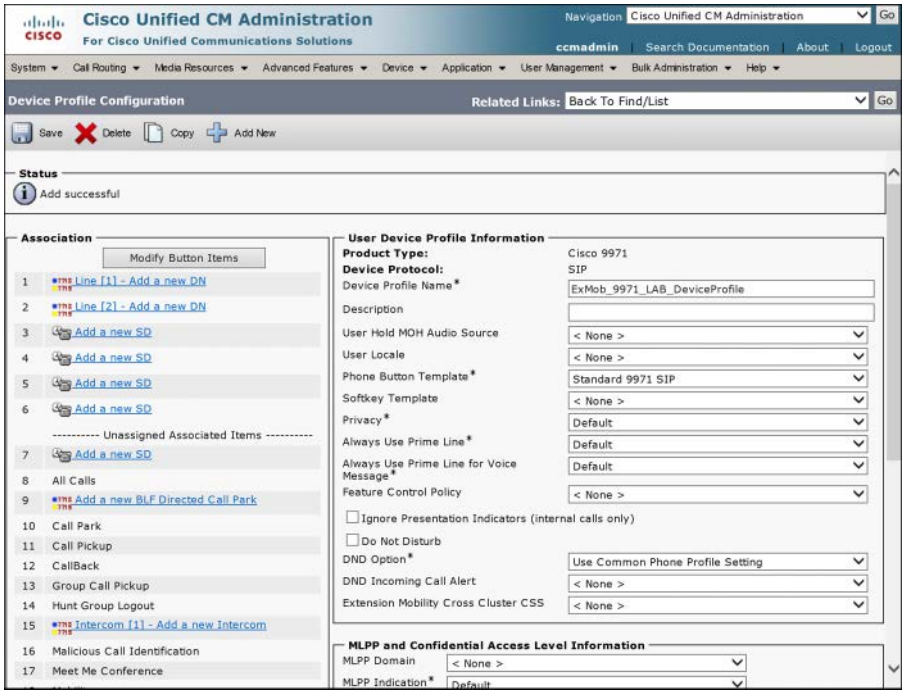


Figure 11-3 *Device Profile Configuration Page*

Step 5b. Subscribe device profiles to the EM service:

i. From the Device Profile page, choose **Subscribe/Unsubscribe Services** from the Related Links pull-down and click **Go**.

ii. Choose the EM service added in Step 3, and click **Next**.

iii. Enter the display name for the EM service and an ASCII version if needed for phones with low-resolution displays.

iv. Click **Subscribe**, and then click **Save**.

Note If the Enterprise Subscription check box was selected in Step 3, Step 5b is not required.

Figure 11-4 illustrates this procedure.

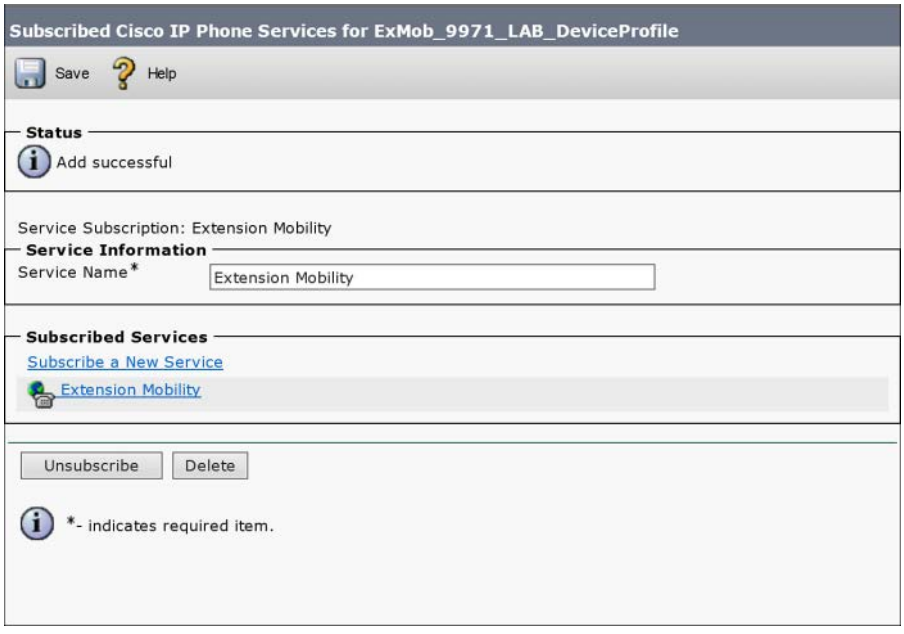


Figure 11-4 *Subscribe Device Profile to EM Service*

Note You must subscribe both the device profiles and the IP phones to the EM service. If you do not, the user will not have access to the EM phone service after she logs in and her device profile is applied—and she will not be able to log out!

Step 6. Associate users with device profiles:

a. Navigate to **User Management > End User**.

b. Select the user for whom you want to create a profile association, or, if necessary, create a new user (see Chapter 9, "Managing Endpoints and End Users in CUCM").

c. In the user configuration, choose the device profiles that should be associated with the user. If more than one is assigned, the user must select the one she wants to use after she logs in to EM. The Default Profile option puts the selected profile at the top of the list of choices.

Figure 11-5 illustrates associating an end user with a device profile.

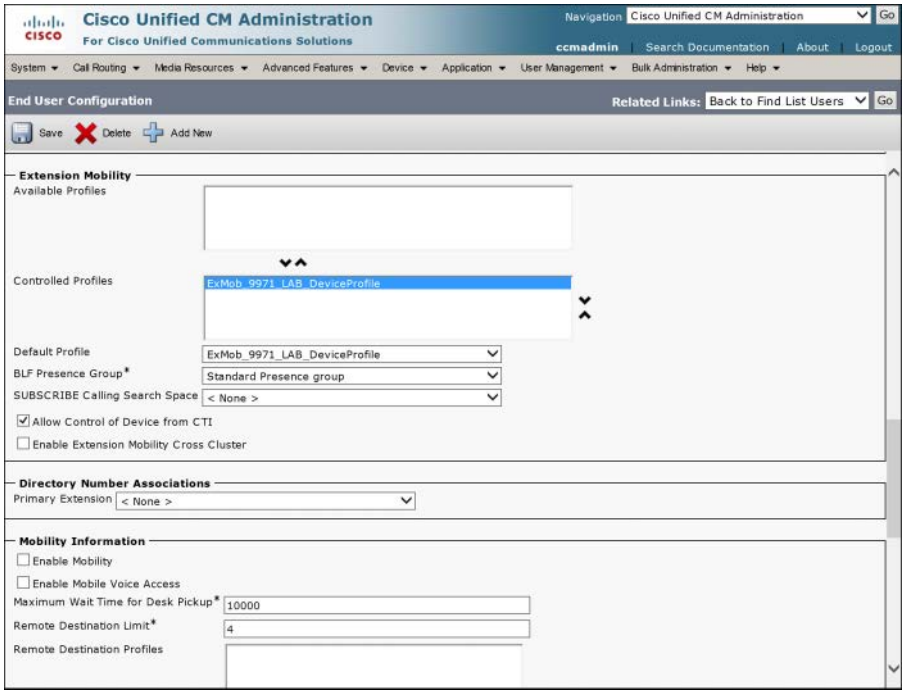


Figure 11-5 *Associating an End User with a Device Profile*

Step 7a. Enable EM for phones:

i. Navigate to **Device > Phone** and select the phone you want to configure for EM.

ii. In the Extension Mobility section, check the **Enable Extension Mobility** box.

iii. Choose either a specific device profile or the currently configured device settings (recommended) in the Log Out Profile pull-down.

Note The logout profile is the configuration that is applied to the phone when no one is logged in to it. Often, this profile includes emergency, internal, and sometimes local calling capabilities.

Figure 11-6 shows the phone configuration for EM.

Step 7b. Subscribe phones to the EM service:

i. On the Phone Configuration page, choose **Subscribe/Unsubscribe Services** from the Related Links pull-down to open the Subscribed Cisco IP phone Services window. (This step is not necessary if the Enterprise Subscription check box is selected on the EM Service Parameters page.)

ii. Choose the **EM** service from the Select a Service pull-down.

iii. Enter the name of the service as you want it to appear on the IP phone.

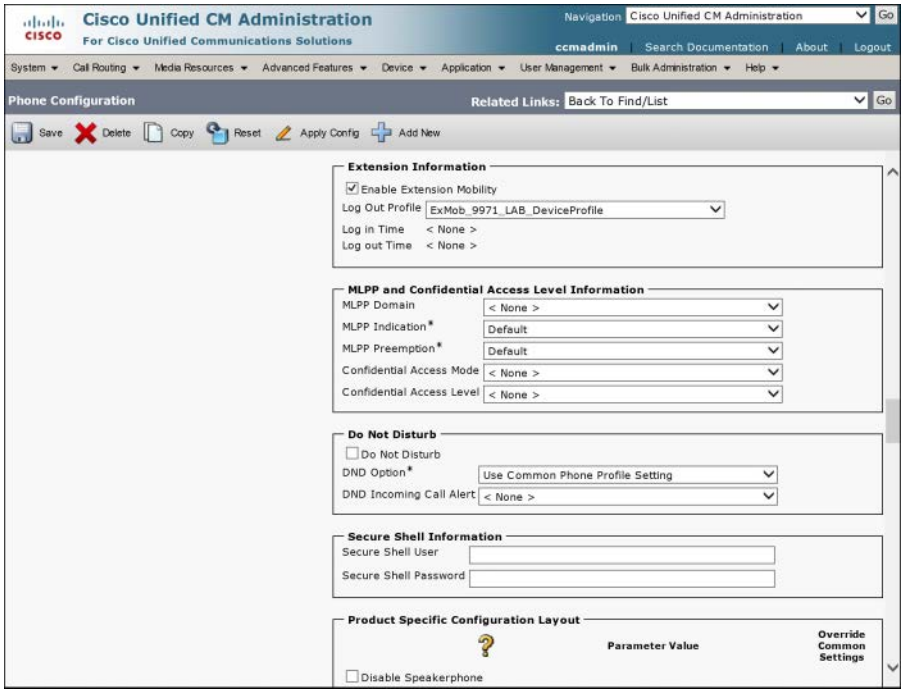


Figure 11-6 *Configuring the Phone for EM*

You should now be able to go any phone that you have subscribed to the EM service and log in as any user you have configured with a device profile for that type of phone.

Figure 11-7 illustrates adding the EM service to a phone.

Figure 11-7 *Subscribing the Phone to the EM Service*

Describe Telephony Features in CUCM

CUCM supports a wide range of telephony features. This section reviews some of the more widely used features, including several call coverage options, intercom, and Presence.

Call Coverage

Call coverage is a general term that references several features and mechanisms used to ensure that calls are answered under almost any foreseeable circumstances. CUCM supports the following call coverage features:

- Call forward
- Shared lines
- Call pickup
- Call hunting
- Call park

Call Forward

Several call forward options are configurable in CUCM:

- **Call Forward All (CFA):** CFA causes all calls to be forwarded to the destination number specified by the user or administrator, either at the phone itself or on the CUCM user or administrative web pages, without ringing the original dialed number. When CFA is enabled, the call forward search space is used and line/device search spaces are ignored. For this reason, the call forward search spaces should be configured to avoid call failures in a system that uses custom partitions and search spaces.

- **Call Forward Busy (CFB) Internal / External:** When the phone is off-hook, calls to the line are forwarded to the specified number or to the voicemail pilot. The Internal or External designation refers to calls that are identified as coming from On-Net or Off-Net, respectively, and can be configured separately.
- **Call Forward No Answer (CFNA) (Internal / External):** When a call to the DN is not answered after the Ring No Answer Reversion timer has expired, the call is forwarded to the specified number or the voicemail pilot. The Internal and External configurations are the same as described earlier.
- **Call Forward No Coverage (CFNC) (Internal / External):** This setting takes effect when the DN has been forwarded to a Hunt Pilot. If the hunt system cannot provide coverage for the call (that is, the hunt system timed out with no answer or all stations were busy or unavailable), and if the Use Personal Preference check box was selected on the hunt pilot, the call is forwarded to the number specified in the CFNC setting or to the voicemail pilot. The Internal and External configurations are the same as described earlier.
- **Call Forward Unregistered (CFUR) (Internal / External):** This setting is most commonly used in conjunction with Survivable Remote Site Telephony (SRST) during a WAN failure. Assuming a typical centralized call processing model, when SRST is in operation due to WAN failure, branch phones are fully functional within the branch thanks to SRST, but they appear as unregistered on the CUCM at the HQ (because they no longer have the WAN available for keepalives and signaling) and are therefore unreachable. The CFUR setting forwards all calls to the specified number or voicemail pilot. The number specified could be the DID of the DN, routed to the branch SRST router by the public switched telephone network (PSTN), or an attendant number. The Internal and External configurations are the same as described earlier.

Note If the Voice Mail check box is selected, CUCM ignores the destination in the forward setting and calling search space fields and forwards the call to the voicemail pilot number specified in the configured voicemail profile.

Shared Lines

If two (or more) IP phones have the same DN configured on one of their lines, calling the DN causes both phones to ring. The first phone to be picked up takes the call; the second phone cannot also pick up the call without invoking the Barge feature (if configured). If the first phone places the call on hold, the second phone can pick up the held call.

Barge and Privacy

If two phones have a shared line configured and one of the phones is using that line, the second phone can force a three-way conference with the first phone by using the Barge feature. The conference is hosted on the first phone's built-in conference bridge. (For IP phone models not supporting a built-in bridge, an external conference bridge can be configured.) When the second phone barges in on the call, all parties hear a beep (by default). If the barge fails (typically because of a lack of conference resources), the barging phone displays an error message.

A Privacy softkey can be configured that, when enabled, prevents barging into a call in progress. Both the barge and privacy capabilities can be enabled and disabled both cluster-wide and at the individual phone configuration pages.

Call Pickup

A DN can be made a member of a call pickup group, which is simply a numbered assignment. Three types of call pickup can be configured using these pickup group assignments:

- **Call Pickup:** If multiple DNs have the same group number and one of them is ringing, another phone with a DN in the same pickup group can invoke the Call Pickup softkey and the call is immediately extended to that phone instead.
- **Group Call Pickup:** If two phones have DNs in different call pickup groups and one of them is ringing, the other phone can invoke the GPickup (Group Call Pickup) softkey, dial the group number of the ringing DN, and the call is immediately extended to that phone instead. A variant of this feature called Directed Call Pickup allows a user to enter a specific DN that is ringing to pick up that specific call, rather than the first call that started ringing in the group.
- **Other Group Pickup:** Introduced in CUCM v.7, Other Group Pickup allows the administrator to set up group associations between call pickup groups. This allows a phone to pick up a call ringing in a different associated group without having to enter the other group's number. The OGroup softkey accesses this feature.

For all call pickup implementations, the administrator can configure audio/visual/both notifications on group member phones to indicate that a phone in one of their pickup groups is ringing. This is particularly useful if the phones are not within earshot of each other.

Call Hunting

A more advanced call coverage system can be built in CUCM using a call hunting structure. Call hunting allows a single dialed DN (or PSTN number) to distribute calls to several phones in sequence. This is typically set up for help desk or customer service groups that are not very large; large implementations would be better served by a dedicated call center application. Call hunting consists of the following components and configurations:

- **DNs and voicemail ports:** The ultimate targets of the call hunting system. These are assigned to Line Groups.
- **Line groups:** Assigned to hunt lists; one or more can be assigned to a single hunt list. The line group configuration provides for different hunt algorithms (specifically, top-down, circular, longest idle, and broadcast) and other hunt options.
- **Hunt lists:** A hunt list is a top-down ordered list of line groups. Calls flowing through the call hunting system are sent to the first line group in the hunt list. If no member of that line group can answer the call, it may be returned to the hunt list, which then tries the second line group. This process may repeat until the call is answered, the list of line groups is exhausted, or the caller hangs up.
- **Hunt pilots:** A hunt pilot is associated with a hunt list. The hunt pilot may be a unique DN, a shared line, or a PSTN number.

During the hunting process, the call forwarding configuration of line group members is ignored; for example, if the DN is busy, the next DN in the line group would be chosen rather than using the CFB setting for that DN.

Call Park

Call park allows a user to temporarily attach a call to a call park slot (effectively a DN). Any user can pick up the call by dialing the call park number. For example, if Mark is on the phone with a customer, and the customer asks about the HayBailer 9000 series product, Mark can say, "That's LuAnn's product line. Let me find LuAnn for you." Mark presses the Call Park softkey, and CUCM displays a message on the phone indicating the call park slot number at which it parked the call. Mark then has to contact LuAnn (perhaps using a paging system or just yelling across the showroom) and tell her the call park number, and LuAnn simply dials that number to pick up the call.

A variation of this feature, called directed call park, requires LuAnn to enter a prefix code (effectively a password) to retrieve the call.

Intercom

Key Topic

The intercom feature allows a button to be configured that calls an intercom line on another phone. The recipient phone auto-answers in speakerphone mode, with the microphone muted. A one-way audio stream now exists from the caller to the recipient; the recipient can hear the caller, but the caller cannot hear the recipient. This is known as Whisper intercom.

When the recipient presses their Intercom button, a second one-way audio stream is established back to the caller and they can each hear the other. For both these intercom calls, an auto-answer tone is heard when the recipient phone answers the call.

If the recipient is in a call when the Whisper intercom call is made, the recipient hears the one-way audio from the intercom caller, but the other party does not.

Intercom lines are different from normal DNs. Intercom lines cannot call DNs, and DNs cannot call intercom lines. Intercom lines have their own dial plan and permissions (intercom partitions and CSS). An Intercom button can be a speed dial (with one preconfigured target intercom line), or you can configure an Intercom button that requires the user to dial the target intercom line.

CUCM Native Presence

Key Topic

Presence can be defined as "signaling one's capability and willingness to communicate." Presence indications can include instant messaging status indications, such as online, offline, busy, out to lunch, in a call, and so on, or in a telephone system, simply on-hook or off-hook. CUCM supports a built-in capability to track the on or off hook status of a DN.

Presence status can be monitored using either a Busy Lamp Field (BLF) speed dial or Presence-enabled call and directory lists. A BLF speed dial is a speed dial button that lights up when the target of the speed dial is off-hook. Presence-enabled call lists display an icon that indicates that the entry in the list is one of the following:

- **Unregistered:** The entry is not being watched, or the device displaying the list does not have permission to watch the target's presence status. The icon displayed is a blank phone keypad.
- **On Hook:** The entry is on hook. The icon displayed is a telephone over a blank keypad.
- **Off Hook:** The entry is off hook. The icon displayed is two handsets over a blank keypad.

Figure 11-8 shows an IP phone displaying a Presence-enabled call list with each of the three icons showing the current status of the targets of recent placed calls. In the figure, 85122001 and 3001 display unregistered status, 2002 is off-hook, and 2001 is on-hook.

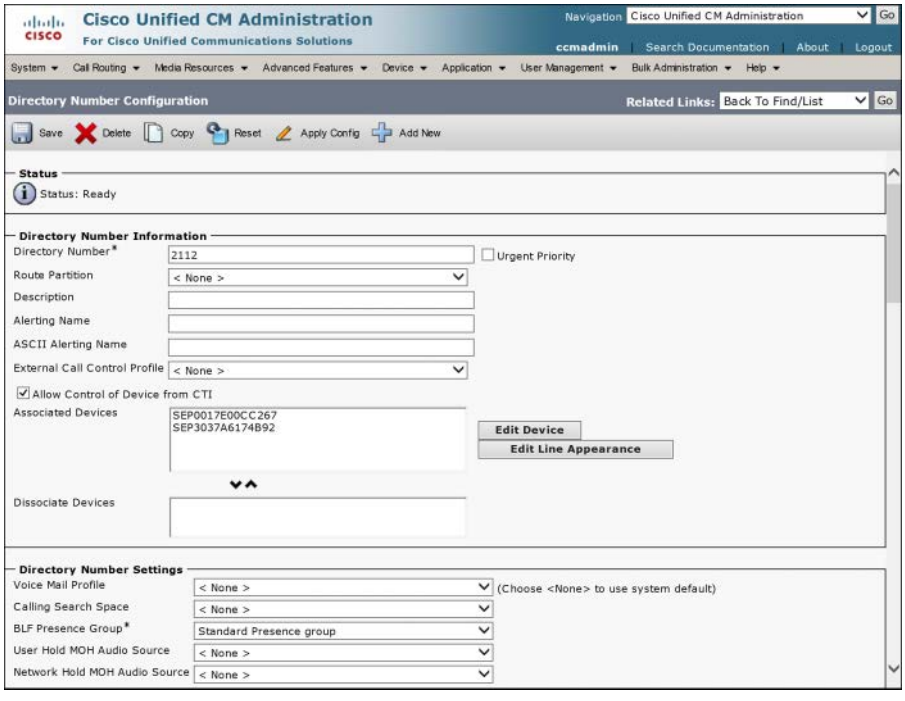


Figure 11-8 *Presence Indications*

Presence Architecture

Key Topic

In some cases, it may not be desirable to have every phone watch every DN in the system. Presence visibility can be controlled in the following ways:

- BLF speed dials can be configured only by an administrator; users cannot create or edit their own.
- Visibility for Presence-enabled call and directory lists can be limited through the use of partitions and Subscribe calling search spaces. A Subscribe CSS is specific to a Presence monitoring system: If the DN to be watched is in the watcher's Subscribe CSS, presence indications are visible; if it is not, the DNs appear as unregistered status to the watcher.

- Presence groups allow different sets of watchers to be assigned (or denied) permission to watch the Presence status of DNs in other Presence groups. Phones, DNs, and users can be assigned to Presence groups. All users are in the standard Presence group by default but can be assigned to custom Presence groups as desired. The enterprise parameter configuration page Inter-Presence Group Subscribe Policy setting defines the default setting for whether Presence groups have permission to watch each other's Presence status; this setting may be overridden in the Presence group settings. Members of a Presence group are always able to watch other members of the same group, unless the Subscribe CSS prevents the subscription. The Subscribe CSS and Presence group settings may be used independently of one another or together. If both are used, both must allow a subscription in order for a watcher to monitor the Presence status of a DN.
- Inter-Presence group settings apply only to BLF call lists and directories and do not affect BLF speed dials.

Enable Telephony Features in CUCM

The following sections detail the necessary steps to configure the telephony features outlined earlier, including call coverage, intercom, and Presence.

Enabling Call Coverage

This section describes the configuration steps to enable the following call coverage features:

- Shared lines
- Barge and CBarge
- Call pickup
- Call park and directed call park
- Call hunting

Configuring Shared Lines

When two or more devices are configured with the same DN, it is called a shared line. The configuration is straightforward: Simply add the same DN to multiple phones, either from the DN Configuration page or the Phone Configuration page via the Phone Button configuration. Figure 11-9 shows the DN configuration page, with two devices associated with the same DN.

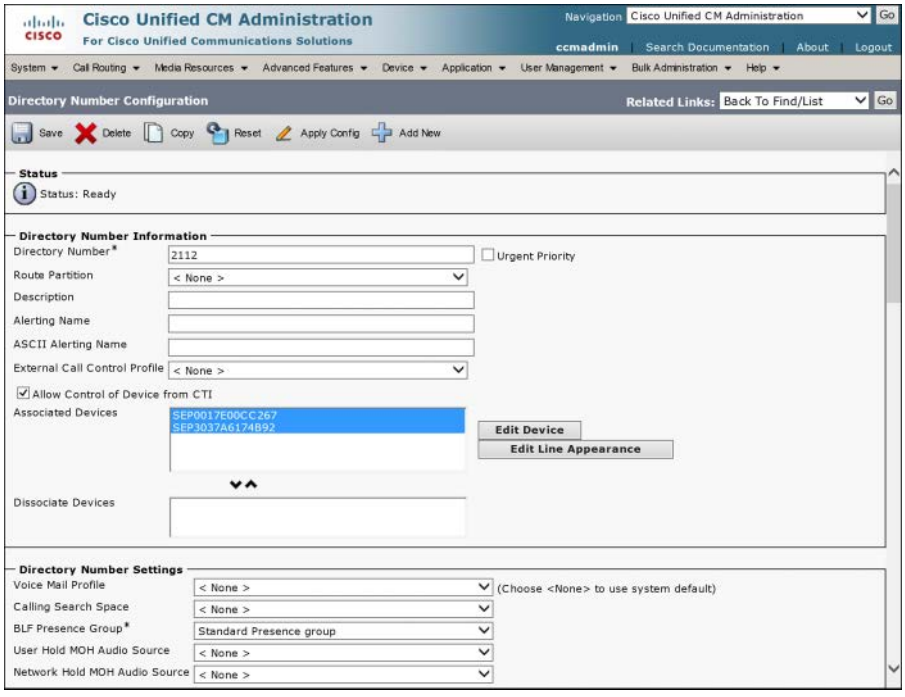


Figure 11-9 *DN Configuration for Shared Line*

Configuring Barge

The Barge feature (as described earlier) allows a user with a shared line to force a three-way conference with another user of that shared line. To enable the feature, the built-in conference bridge (available on most IP phone models) must be activated. The Privacy feature removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. The following steps describe how to configure Barge and Privacy:

Step 1. In CM Administration, navigate to **System > Service Parameters**. Select the server you want to configure from the Server drop-down.

Step 2. Select the **Cisco CallManager** service from the Service drop-down.

Step 3. Scroll down to the Clusterwide Parameters (Device-Phone) section. Set **Built-In Bridge Enable** to **On**.

Step 4. Set the **Privacy** setting to **True** (the default).

Note The Built-In Bridge, Privacy, and Single Button Barge settings can be overridden at the device pool or the individual phone if desired.

Step 5. Scroll down to Clusterwide Parameters (Feature-Join Across Lines And Single Button Barge Feature Set) and set the **Single Button Barge/CBarge Policy**.

Your choices are **Off**, **Barge**, or **CBarge**. This setting allows pressing the shared line button to cause a Barge onto the shared line when it is in use (instead of using the Barge softkey). Setting the value to Barge uses the built-in bridge on the target phone, while setting it to CBarge forces the Barge operation to use an external conference resource. Figure 11-10 shows the Clusterwide Parameters section where Barge is configured.

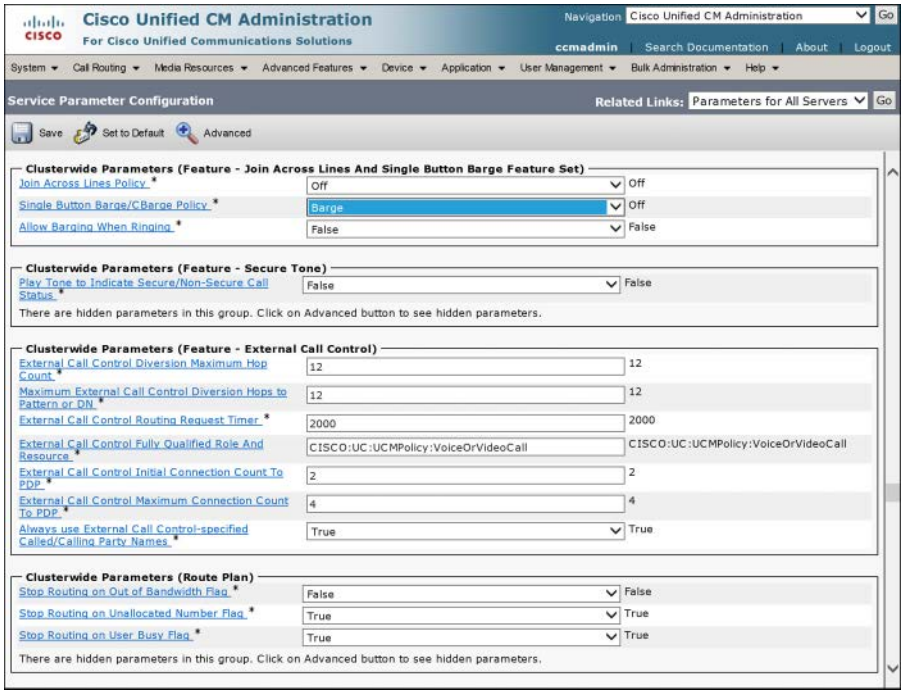


Figure 11-10 *Service Parameter Configuration for Barge*

Note Using the Barge softkey method requires that you configure the softkey template to include the Barge softkey for the phones involved with the Barge operation. Using the Single Button Barge method does not.

If CBarge is required, an external conference resource must be configured and made available to the phones.

Configuring Call Pickup

To configure call pickup, you must create and apply call pickup groups to DNs that must pick up each other's calls. Follow these steps:

Step 1. In CM Administration, navigate to **Call Routing > Call Pickup Group**.

Step 2. Click **Add New**.

Step 3. Enter a name and a unique number. (The number cannot contain wildcards.)

Step 4. Select a partition (normally the same as the DN partition; however, selecting a different partition allows the administrator to restrict access to the pickup group by modifying the CSS of the phones if desired).

It is possible to preconfigure associated call pickup groups so that the Other Group Pickup feature (described earlier) can be used if desired; this option is only available during the initial configuration of the Pickup Group. Figure 11-11 shows the Call Pickup Group Configuration page.

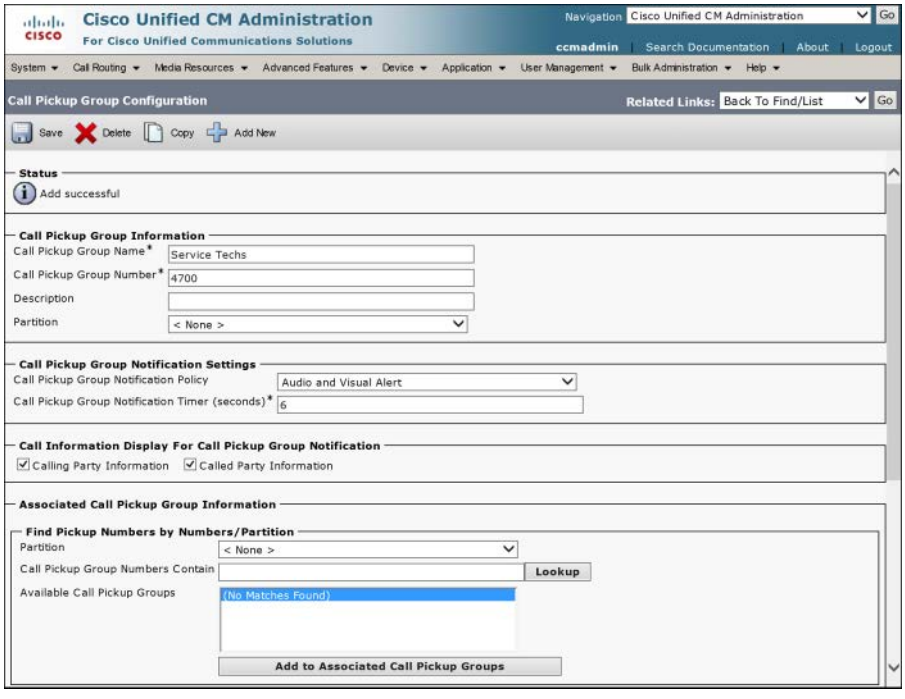


Figure 11-11 *Call Pickup Group Configuration*

To use the pickup feature, a softkey must be added to the phone(s). The following steps outline the process of modifying and adding a softkey template to enable call pickup:

Step 1. To configure the softkey template, navigate to **Device > Device Settings > Softkey Template**.

Step 2. Select, add, or copy a softkey template.

Step 3. From the Related Tasks pull-down, select **Configure Softkey Layout**.

Step 4. Add the **Pickup**, **Group Pickup**, or **Other Group Pickup** softkeys as desired. (These keys can be selected in the off-hook or on-hook call states.)

Step 5. Click **Save**.

Step 6. Apply the modified softkey template to phones or device profiles as desired.

Figure 11-12 Shows the Softkey Template Configuration page with the On Hook call state template options being configured.

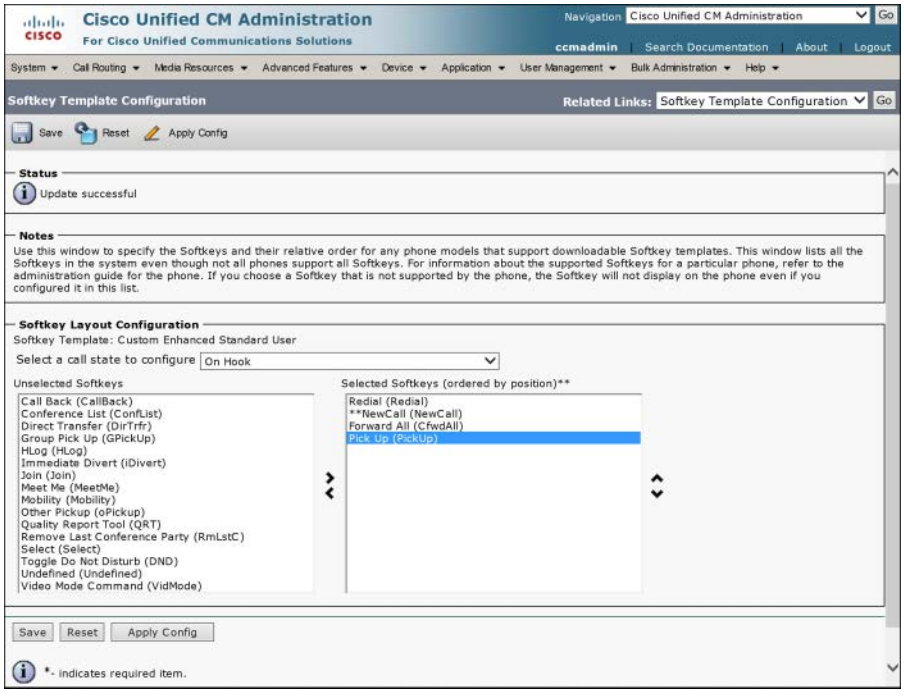


Figure 11-12 *Configuring a Softkey Template for Pickup*

To use the call pickup feature, the individual DNs must be associated with the call pickup groups we just configured. DNs with the same call pickup group configured can use the pickup feature to answer each other's calls; those with different call pickup groups can use Group Pickup or Other Group Pickup if their call pickup groups are pre-associated. Figure 11-13 illustrates the association of a DN with a call pickup group.

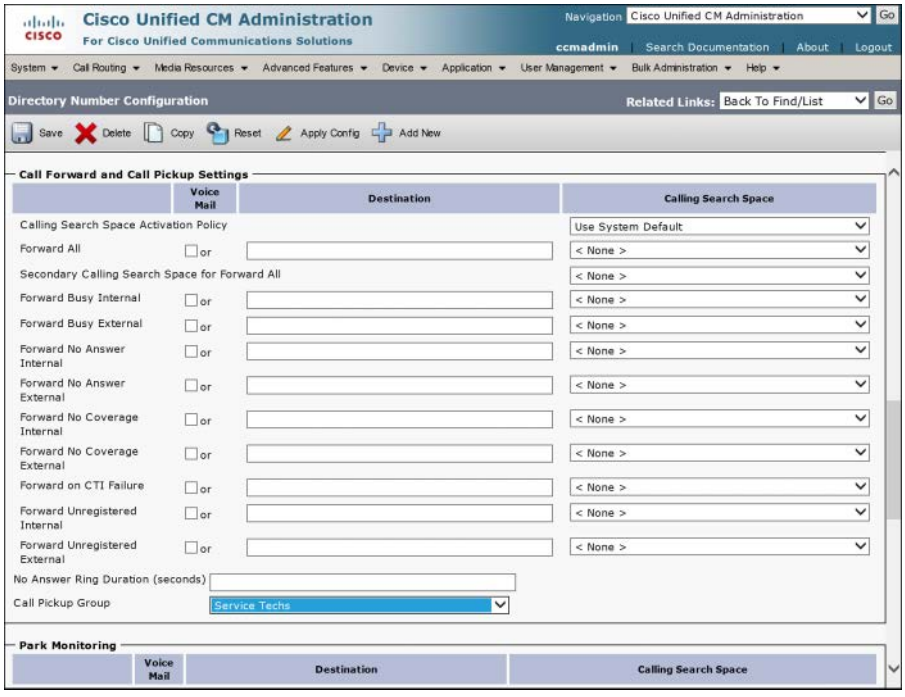


Figure 11-13 *Call Pickup Group Association with a DN*

Configuring Call Park and Directed Call Park

The call park feature allows a user to park a call at a reserved DN and retrieve it from any IP phone. Directed call park is similar, with the added features of requiring a prefix code to retrieve the call and the ability to specify a different reversion number. The following steps configure the call park and directed call park features:

Step 1. In CM Administration, navigate to **Call Routing > Call Park**.

Step 2. Click **Add New**.

Step 3. Specify either an individual DN or a range of DNs to be used for call park. The number can be partitioned if desired by selecting a custom partition. A number or range is associated with the CUCM server you select from the pull-down; if you are associating call park slots to multiple servers, ensure that the number ranges do not overlap between servers.

Step 4. Click **Save**.

Note A call park number range is defined with the same wildcard used in route patterns; for example, the range of 880X defines 10 call park slots, numbered 8800 through 8809.

Figure 11-14 shows call park configuration.

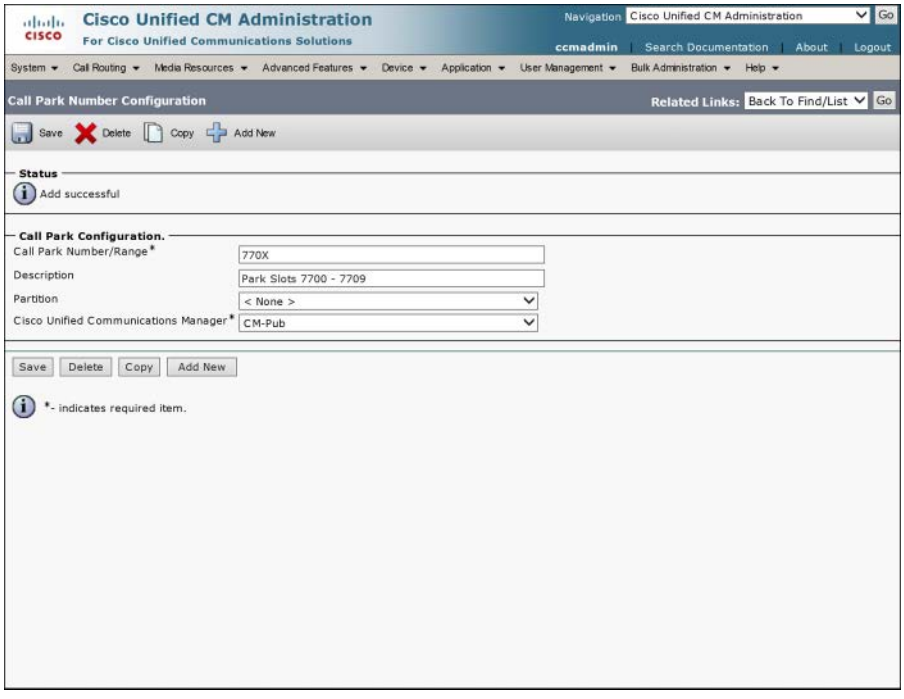


Figure 11-14 *Call Park Configuration*

Configuring directed call park is similar. Follow these steps:

Step 1. In CM Administration, navigate to **Call Routing > Directed Call Park**.

Step 2. Click **Add New**.

Step 3. Enter a unique number or range and specify a partition if desired.

Step 4. Specify the reversion number (the DN to which a call will be forwarded if not picked up from the park slot before the Call Park Reversion timer [60 seconds by default] expires).

Step 5. Specify the reversion calling search space to allow the phone to find the reversion number specified previously, if it is not in the normal CSS of the phone or line.

Step 6. Specify the retrieval prefix, which is the code the person picking up the parked call must dial in order to retrieve it.

Step 7. Click **Save**.

Figure 11-15 shows directed call park configuration.

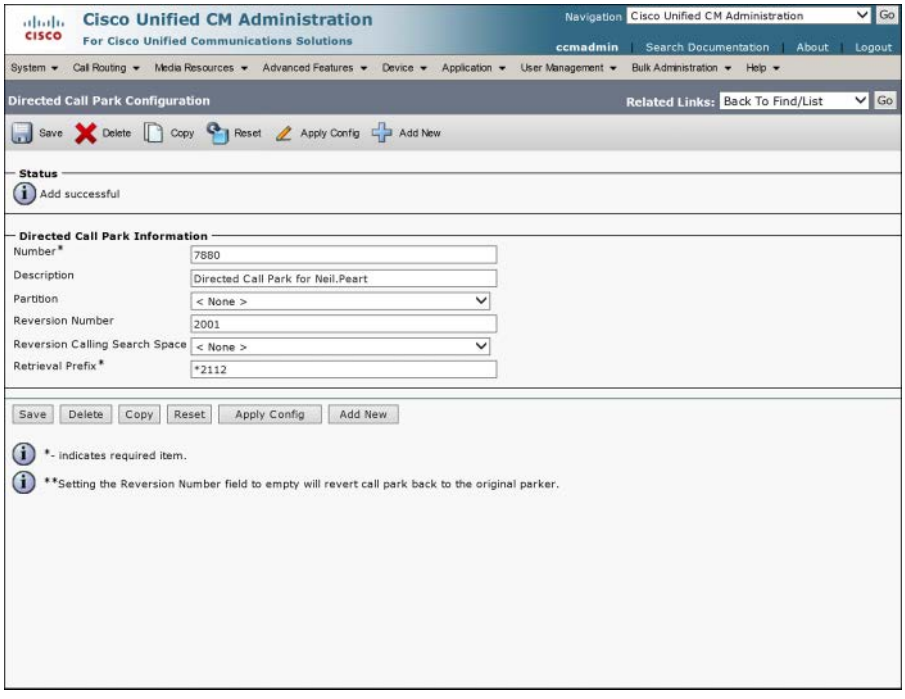


Figure 11-15 *Directed Call Park Configuration*

Configuring Call Hunting

Key Topic

To configure call hunting, groups of DNs are associated with line groups that specify the hunting behavior. Line groups are added to hunt lists, which select the order of hunting through the line groups. A hunt pilot number is associated with a hunt list and serves as the dialed number trigger of the hunting system. To configure call hunting, follow these steps:

Create line groups:

Step 1. Create DNs and associate them with phones.

Step 2. In CM Administration, navigate to **Call Routing > Route/Hunt > Line Group**.

Step 3. Click **Add New**.

Step 4. Enter a line group name.

Step 5. Specify the RNA reversion timeout (the number of seconds each DN in the line group will ring before the No Answer trigger is reached).

Step 6. Select **Distribution Algorithm: Top Down** (each new call starts with the DN at the top of the list), **Circular** (each new call begins starts at the next DN in the last after the one used by the previous call), **Broadcast** (all DNS in the line group ring simultaneously), or **Longest Idle Time** (the DN that has been in the on-hook state for the longest rings).

Step 7. Select the hunt option for each call state (No Answer, Busy, and Not Available) from the pull-down. The hunt options determine whether and when the call will move from the current line group to the next line group in the hunt list.

Step 8. Add DNs to the line group. The order in which the DNs are listed may be important depending on the earlier choice of distribution algorithm.

Step 9. Click **Save**.

Figure 11-16 shows the Line Group Configuration page.

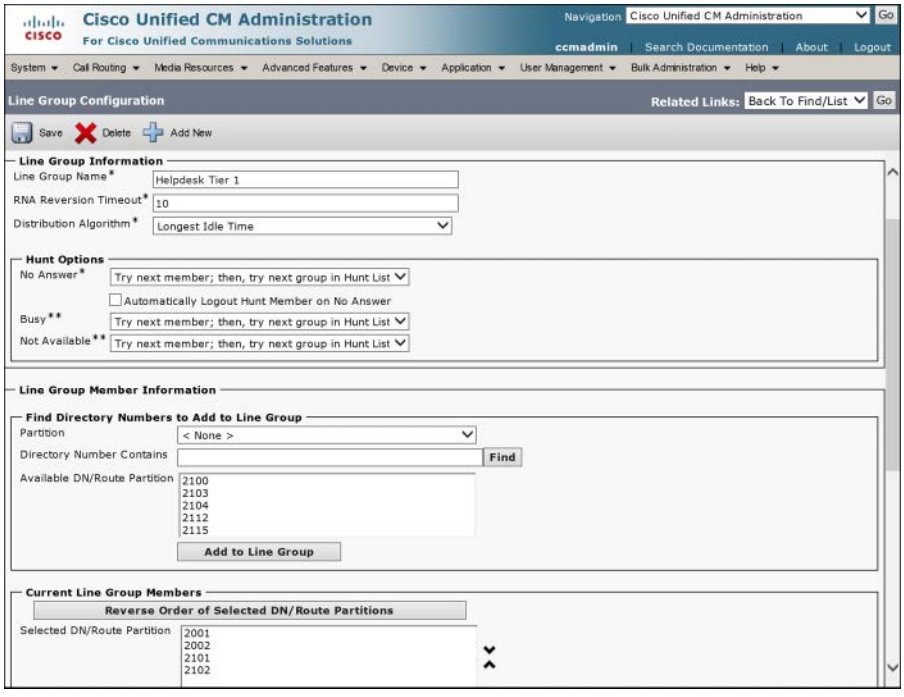


Figure 11-16 *Line Group Configuration*

Create hunt lists:

Step 1. Navigate to **Call Routing > Route/Hunt > Hunt List**.

Step 2. Click **Add New**.

Step 3. Specify a **Name**.

Step 4. Set the CUCM group in order to provide CUCM redundancy for the hunt list.

Step 5. Click **Save**. The hunt list configurations now appear on the page.

Step 6. Add line groups to the hunt list. The hunt list is always top-down processed, so the order of the line groups is important; use the arrows to adjust the order if needed.

Step 7. Click **Save** when the desired line groups appear in the correct order.

Create a hunt pilot:

Step 1. Navigate to **Call Routing > Route/Hunt > Hunt Pilot**.

Step 2. Click **Add New**.

Step 3. Enter a hunt pilot number. This behaves the same way as a route pattern; you can specify any string you like, including a valid PSTN or DID number.

Step 4. Set a partition, if desired, to control access to the hunt pilot.

Step 5. In the Hunt List field, select the hunt list that should be accessed by dialing this hunt pilot number.

Step 6. Specify an alerting name, which displays on phones receiving calls as part of the hunting system.

Step 7. Set hunt forwarding options to control where calls that cannot be handled by the hunting system are sent. The Use Personal Preferences check box ignores the configured settings, instead using the CFNC setting of the station that forwarded the call to the hunt pilot.

Step 8. Click **Save**.

Figure 11-17 shows the Hunt Pilot Configuration page.

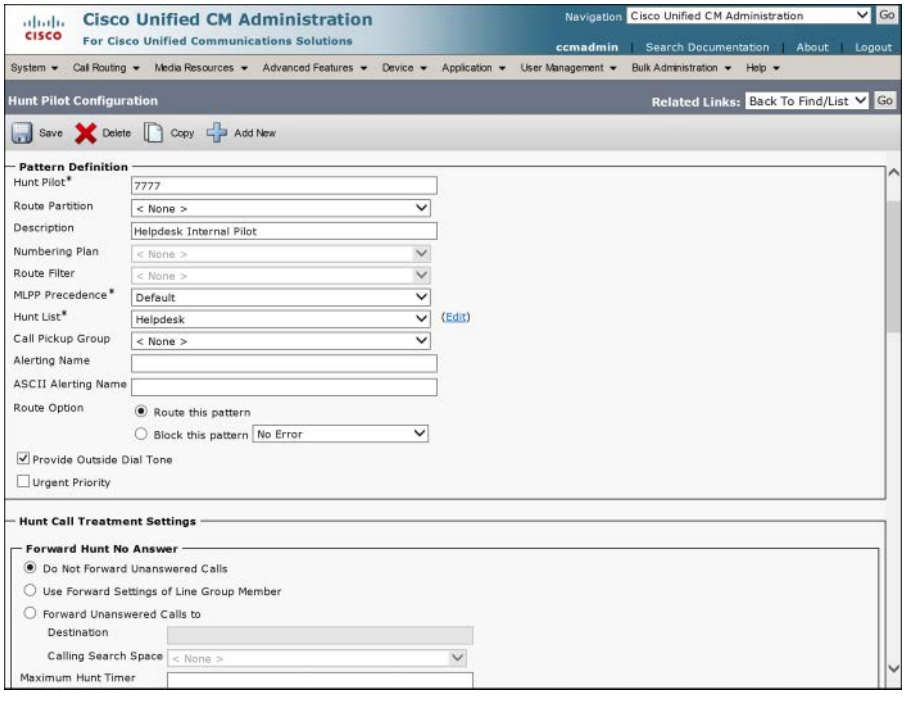


Figure 11-17 *Hunt Pilot Configuration*

Note The Phone Button template and/or softkey template can be configured to include the HLog key, which allows a user to log in to or out of a hunt group. The CallManager Service parameter Hunt Group Logoff Notification specifies a ringtone that plays to alert a user that there is an incoming call that would ring their phone if it were not logged out of the hunting system. This is useful as a reminder to users that they are logged out if they return to their desk after an absence.

Configuring Intercom Features

Key Topic

As previously discussed, the intercom feature uses special intercom DNs, partitions, and calling search spaces. The following steps walk through setting up the intercom feature:

Step 1. Navigate to **Call Routing > Intercom > Intercom Route Partition**.

Step 2. Click **Add New**. On the Configuration page, enter the name and comma-separated description of the new Intercom partition. You can create up to 75 partitions at once on this page.

Step 3. Click **Save**.

Step 4. Navigate to **Call Routing > Intercom > Intercom Calling Search Space**. Click **Find**, and note that an Intercom CSS has been automatically created as a result of creating the Intercom Partition (the auto-named entry will be <partition_name>_GEN). The auto-generated CSS automatically includes the Intercom Partition just created. You may use the auto-generated CSS, modify it or create custom Intercom CSSs as desired.

Note A custom Intercom CSS is really only necessary if an Intercom button needs to support multiple (dialed instead of speed dialed) targets, and access to some of those targets must be limited. If you are creating point-to-point intercom lines, there is no need to customize the Intercom CSS.

Step 5. Navigate to **Call Routing > Intercom > Intercom Directory Number**.

Step 6. Click **Add New** to create an Intercom DN. You must create at least two because of the one-way nature of Intercom DNs and the fact that an Intercom DN cannot call an ordinary DN.

Step 7. Assign an intercom partition and intercom calling search space to the intercom DNs according to your call control design.

To configure a phone with an Intercom button, the Phone Button template must be modified. (Alternatively, you could modify the button directly from the Phone Configuration page, but this kind of one-off configuration is more difficult to administer and does not scale well.) To set up and apply the Phone Button template, follow these steps:

Step 1. Navigate to **Device > Device Settings > Phone Button Template.**

Step 2. Select the Phone Button template that corresponds to the phone/protocol for which you want to configure intercom. You may modify the stock profile, copy it and modify the copy, or create a new one from scratch. Copyincg and modifying the copy is the recommended action.

Step 3. In the Phone Button Template configuration window, add the intercom feature to the desired button appearance.

Step 4. Click **Save.**

Figure 11-18 shows the Phone Button template Configuration page.

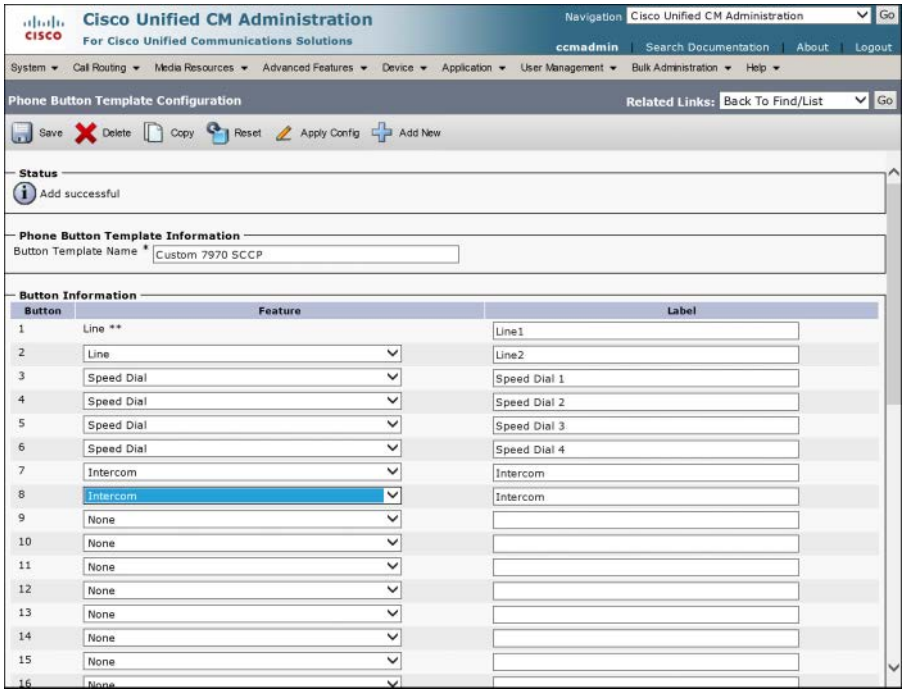


Figure 11-18 *Adding Intercom Button to a Phone Button Template*

Now that we have the DNs and template set up, we can assign the template to the phones:

Step 1. Apply the template to a phone by selecting the modified template from the pull-down in the phone's configuration page.

Step 2. Configure a button on the phone with an intercom DN, intercom partition, and Intercom CSS.

Figure 11-19 illustrates the Intercom button configuration.

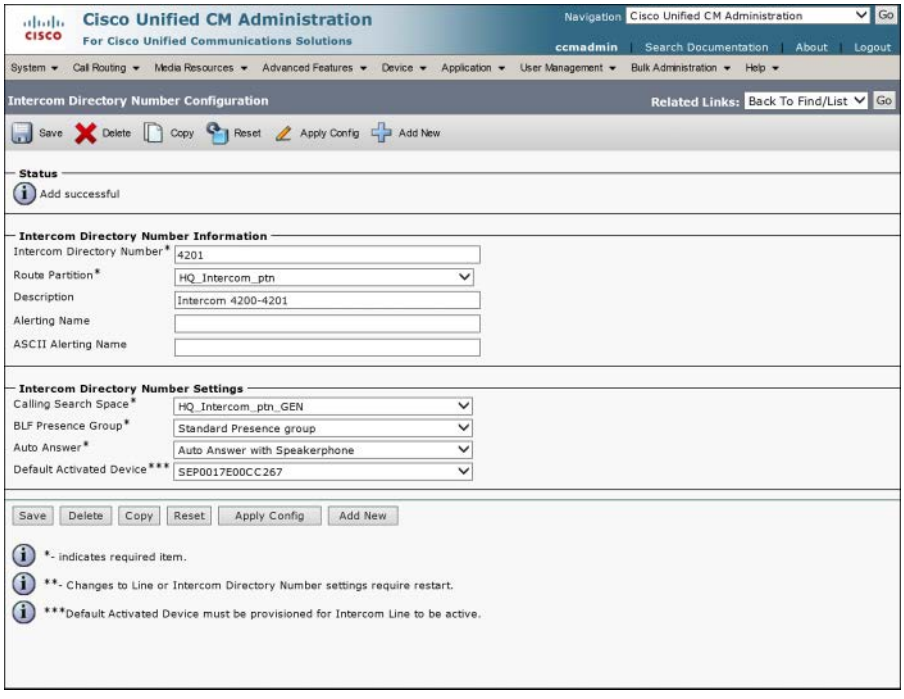


Figure 11-19 *Intercom Button Configuration*

Configure CUCM Native Presence

As previously described, there are two implementations of CUCM native Presence. The first, simplest implementation is BLF speed dial; the second, more involved implementation is Presence-enabled call lists, which uses presence groups and a special Subscribe CSS.

Configuring BLF Speed Dials

To add a BLF speed dial to a phone, it is recommended that you modify the Phone Button template; it is possible to modify the individual phone's buttons, but doing so creates administrative burden and does not scale well. To set up BLF speed dial, follow these steps:

Step 1. Navigate to **Device > Device Settings > Phone Button Template**.

Step 2. Select, copy, or create the appropriate template for the phone model/protocol.

Step 3. Add the Speed Dial BLF feature to one or more of the available buttons.

Step 4. Apply the template to the phones.

Step 5. On the Phone Configuration page, select an available Add a new BLF SD button and configure the destination DN and display label.

Figure 11-20 illustrates the configuration of a BLF speed dial.

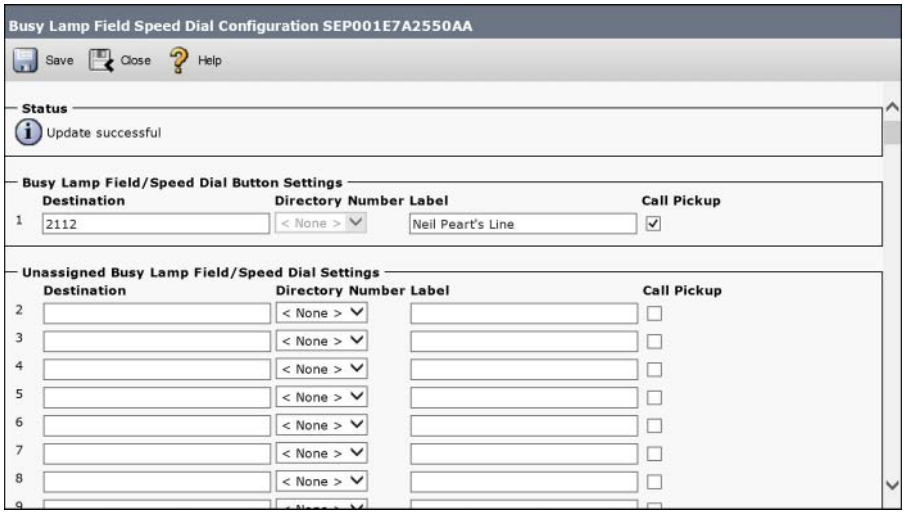


Figure 11-20 *Configuring a BLF Speed Dial*

Configuring Presence-Enabled Call Lists

Key Topic

As described earlier, the CUCM system can track the on-hook status of phones both through BLF Speed dials and Presence-enabled call lists. Presence-enabled call lists use the device's configured Subscribe CSS and/or Presence group subscription policies to determine whether a device can watch a DN's Presence status:

- If the Subscribe CSS applied does not include the partition of the DN being watched, Presence status is unavailable.
- If the Inter-Presence Group Subscription setting is denied between the two groups, Presence status information is unavailable.
- If both the Subscribe CSS and Presence groups are used together, both must allow the subscription in order for Presence status to be watched.

Configuring Presence-enabled call lists is somewhat more complex than BLF speed dials, but it allows a greater flexibility, precision, and scalability when large numbers of devices need to watch large numbers of DNs. To configure Presence-enabled call lists, follow these steps:

Step 1. Navigate to **System > Enterprise Parameters**. Scroll down to Enterprise Parameters Configuration.

Step 2. Set Enable BLF for Call Lists to **Enabled**.

Figure 11-21 illustrates the Enterprise BLF for call lists configuration.

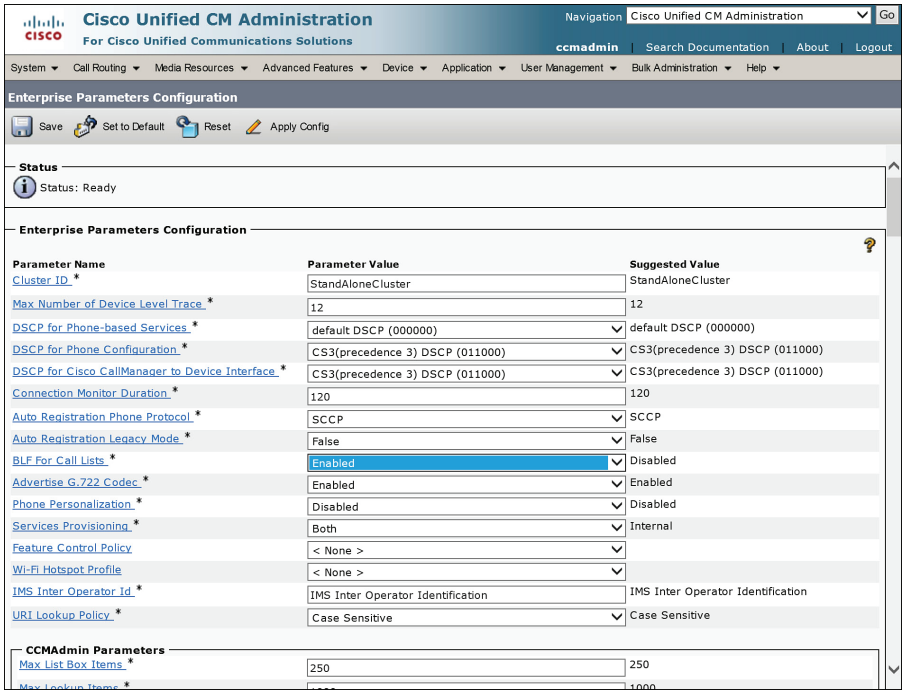


Figure 11-21 *BLF for Call Lists Enterprise Parameter*

Step 3. If using a custom Subscribe CSS is desired, create new Subscribe CSSs. It is generally recommended to create custom Subscribe CSSs and use existing partitions; the overall class of control plan should be well thought out prior to making these changes.

Step 4. Apply the appropriate CSS to phones and Session Initiation Protocol (SIP) trunks as required.

Configuring Custom Presence Groups

Because all devices and DNs are part of the standard Presence group by default and all devices can watch all DNs within the same Presence group, the configured Subscribe CSS and existing partitions may provide adequate control over Presence subscriptions. If a more complex design is required, it may be necessary to set up custom Presence groups and define custom inter-Presence group subscriptions, as follows:

Step 1. Navigate to **System > BLF Presence Group**.

Step 2. Click **Add New** and configure a name.

Step 3. Set the Presence Group Relationship to each other Presence group **(Allow Subscription** or **Disallow Subscription**) to control whether this group can watch the Presence status of other groups. Setting it to **System Default** references the Default Inter-Presence Group Subscription Service Parameter

discussed next. Each subscription is one-way: For example, executives may be allowed to watch employee Presence status, but employees may not be allowed to watch executive status. Figure 11-22 shows a Presence Group Configuration page.

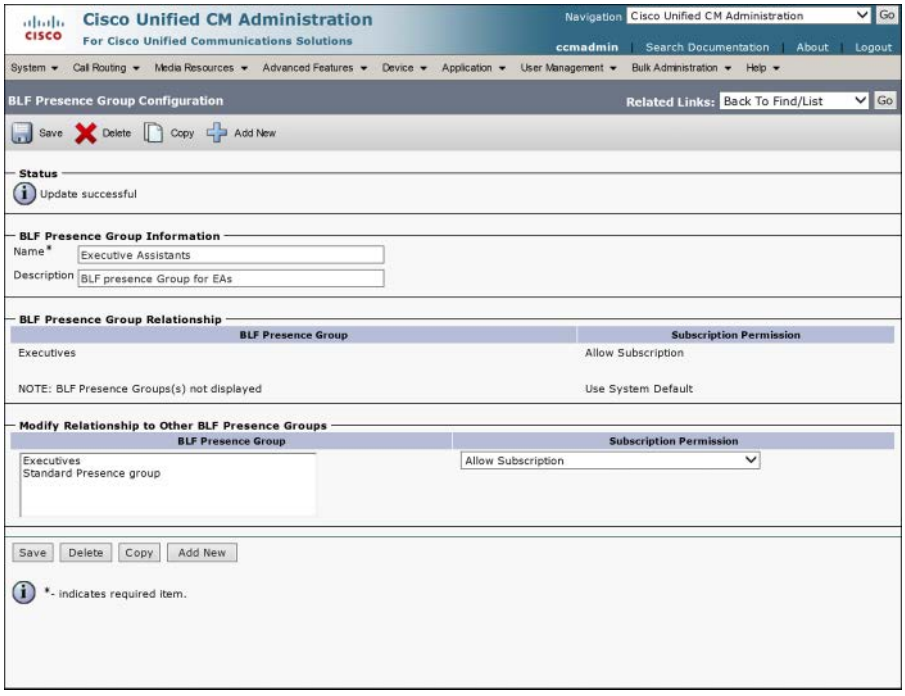


Figure 11-22 *Presence Group Configuration*

Step 4. Navigate to **System > Service Parameters**. Select the server you want to configure and then the **Cisco CallManager Service**. Scroll down to Clusterwide Parameters (System-Presence).

Step 5. Set the default Inter-Presence Group Subscription policy to either **Allow** or **Disallow**, as desired. (The Use System Default setting mentioned references this parameter setting.)

Step 6. Assign Presence groups to DNs and phones. Remember that phones watch DNs. The Presence groups assigned to the phone and the DN, the Inter-Presence Group Subscription Setting, the Subscribe CSS of the watcher, and the partition of the DN all interact to determine whether Presence information is available to the watcher.

Figures 11-23 through 11-25 show the Presence group configuration for a phone, a DN, and a SIP trunk.

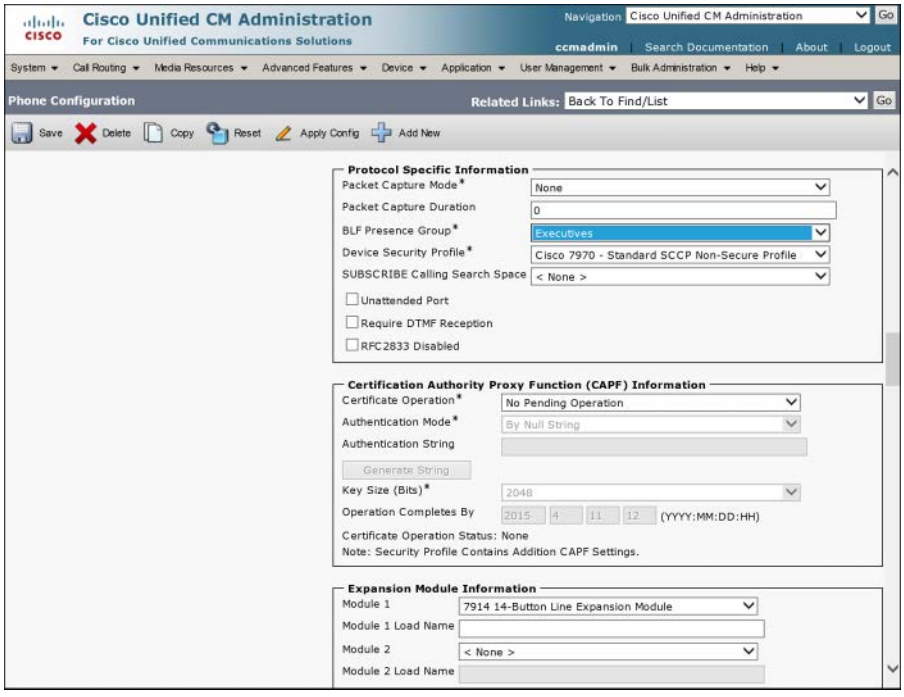


Figure 11-23 *IP Phone Presence Group Configuration*

Key Topic

Note Phones are watchers that monitor the Presence status of Presence entities (such as DNs and SIP trunks). The Presence group assignment and Inter-Presence Group Subscription setting control whether the watcher can see the Presence status of the Presence entity. A SIP trunk, however, is both a watcher and a Presence entity, but only one Presence group can be assigned to a SIP trunk. This single Presence group is applied to both sending and receiving Presence subscriptions. Keeping that in mind, make sure that the Presence group assigned to a SIP trunk has the correct permissions to watch and be watched by (or not) the other Presence groups in the system.

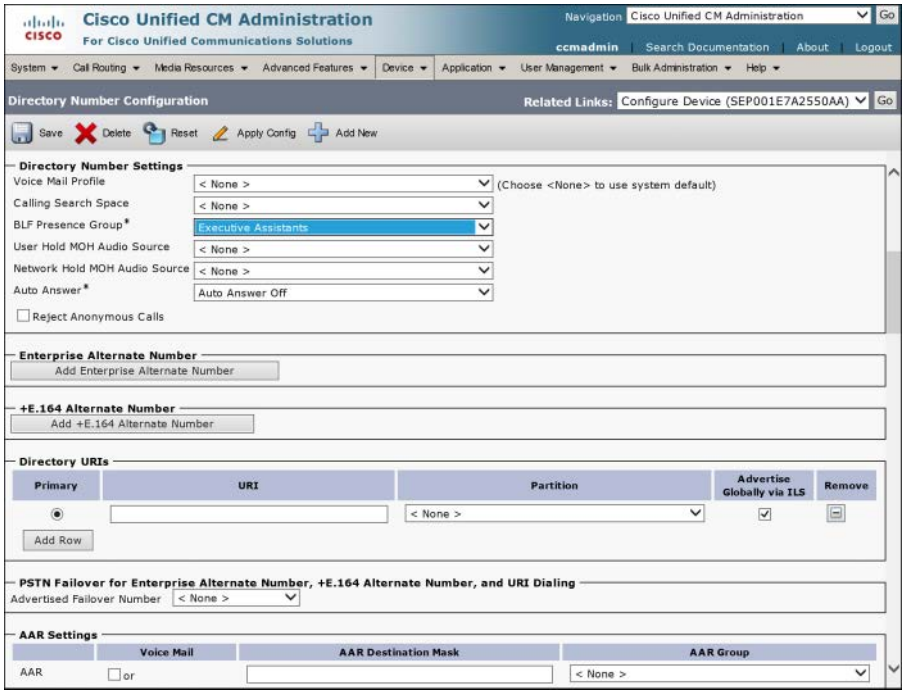


Figure 11-24 *DN Presence Group Configuration*

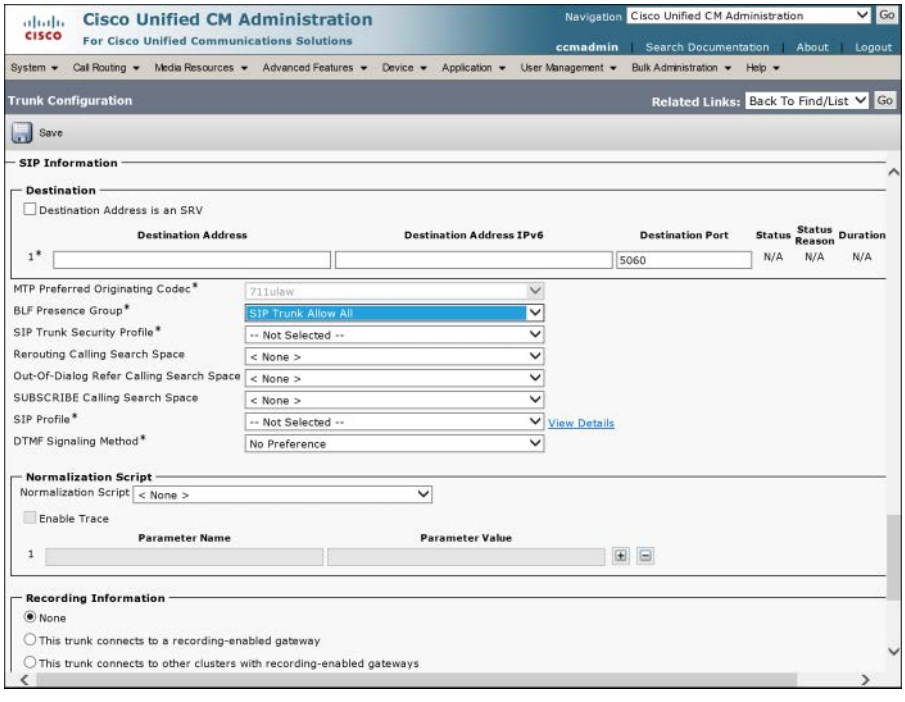


Figure 11-25 *SIP Trunk Presence Group Configuration*

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 11-2 lists and describes these key topics and identifies the page number on which each is found.

Key Topic

Table 11-2 Key Topics for Chapter 11

Key Topic Element	Description	Page Number
Paragraph	Extension Mobility in CUCM	290
Paragraph	Enable Extension Mobility in CUCM	291
Paragraph	Intercom	301
Paragraph	Native Presence	301
Paragraph	Presence architecture	302
Paragraph	Configure call hunting	310
Paragraph	Configure Intercom	313
Paragraph	Configure Presence-enabled call lists	316
Note	Presence configuration for SIP trunks	319

Definitions of Key Terms

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

Extension Mobility, call coverage, call forward, shared line, pickup, hunt, call park, intercom, native Presence

This chapter covers the following topics:

- **Understanding CUCM Mobility Features:** This section describes the Mobile Connect and MVA features in CUCM.
- **Implementing Mobility Features in CUCM:** This section outlines the procedures for implementing Mobile Connect and MVA.

CHAPTER 12

Enabling Mobility Features in CUCM

The explosion in mobile technology has made communication possible from a huge array of devices, including home phones, cellular phones, WiFi-enabled smartphones, tablets, laptops, desktops, and specialized wireless IP phones. It has never been easier to stay in touch. But all this has created its own set of problems: Managing all the different methods of communication and all the phone numbers and voicemail boxes takes increasingly more time and creates more confusion.

In a business environment (and increasingly in a personal context), this confusion creates inefficiencies that actually impair communications instead of facilitating them. That might mean a loss of valuable business or simply missing an important call. The Unified Mobility feature set allows a person to be reached at a single number and to place calls from any device and have all calls appear to come from that same number, creating a consistent point of voice contact and greatly simplifying the management of voice communications with an individual.

This chapter defines, describes, and reviews the implementation steps for both of these mobility features, explaining the advantages, drawbacks, and integration of each with the Cisco Unified Communications Manager (CUCM) architecture.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter or simply jump to the "Exam Preparation Tasks" section for review. If you are in doubt, read the entire chapter. Table 12-1 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 12-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions Covered in This Section
Mobile Connect	1–3, 6
Mobility (General)	4–5
Mobile Voice Access	7–9

1. Which of the following best describes Mobile Connect?
   a. It has the capability to have multiple IP phones ring when a single DN is called.
   b. It has the capability to enable users to dial in from the PSTN and be greeted by an auto-attendant that allows them to enter the extension of the person they are trying to reach.
   c. It has the capability for IP phone users to forward calls to their mobile phones.
   d. It has the capability to have multiple remote PSTN devices ring simultaneously with their enterprise IP phone.
2. Which of the following are valid steps in the configuration of Mobile Connect? (Choose all that apply.)
   a. Add the Mobility softkey to softkey templates.
   b. Activate mobility for end users.
   c. Associate users to their IP phones.
   d. Configure remote destination profiles.
   e. Associate remote destinations with remote destination profiles.
   f. Configure and apply access lists.
3. Which of the following is true of the access lists used with Mobile Connect?
   a. Access lists are required for mobility features to function.
   b. Access lists are configured on the IOS gateways to filter calls at the interface.
   c. Access lists cannot be empty.
   d. An empty access list applied to an allowed calls filter allows no calls.
   e. An empty access list applied to a disallowed calls filter allows no calls.
4. What is the maximum number of remote destination profiles that can be configured for a user?
   a. 1
   b. 5
   c. 10
   d. Unlimited
5. What is the maximum number of remote destinations that can be configured for a user?
   a. 1
   b. 5
   c. 10
   d. Unlimited

6. What is the correct order of processing during a Mobile Connect call if the caller has dialed the user's IP phone number?
   a. Remote destination, remote destination profile, ring schedule, access list
   b. Remote destination profile, remote destination, ring schedule, access list
   c. Access list, ring schedule, remote destination profile, remote destination
   d. Ring schedule, access list, remote destination, remote destination profile
7. Which component is not part of a Mobile Voice Access configuration?
   a. Cisco Unity Connection Auto-Attendant
   b. Cisco IOS H.323 VXML gateway
   c. Mobile Voice Access Media Resource
   d. End user configured for Mobile Voice Access
8. How does an H.323 gateway route calls inbound for the MVA service to the CUCM server hosting the service?
   a. One dial peer matching the MVA access PSTN number pointing to the CUCM server.
   b. Two dial peers: One matching the MVA access PSTN number with incoming called-number configured, and one matching the MVA access PSTN number pointing to the CUCM server.
   c. A static route redirecting all HTTP calls to the CUCM server.
   d. All H.323 configuration is dynamically created by the CUCM server via TFTP download.
9. Which IOS dial peer configuration command associates the dial peer matching the MVA access PSTN number with the VXML application hosted by the CUCM server running the MVA service?
   a. **incoming called-number 4085555000**
   b. **session target ipv4:10.1.1.1**
   c. **service mva**
   d. **service mva http://10.1.1.1:8080/ccmivr/pages/IVRMainpage.vxml**

Foundation Topics

Understanding CUCM Mobility Features

CUCM incorporates a range of mobility features that allow a user to interact with their Unified Communications devices and applications regardless of where they happen to be. The goal is to extend the ability to communicate with customers or colleagues using their enterprise IP phone number, both for inbound and outbound calls, in a seamless and flexible way. The following sections describe the features and configuration of some of the mobility capabilities of CUCM.

Describe Mobile Connect

Mobile Connect is often called single number reach: A user's IP phone number becomes the single number by which all the various other devices that person uses can be reached, including home phones, mobile phones, Internet-based Voice over IP (VoIP) numbers, and so on. The benefit is that a single point of voice contact is published for simplicity and consistency, whereas a range of devices can actually take calls, which provides maximum flexibility and reachability for the person almost regardless of where they may be or which communication method they may have available to them.

The user experience is simple but powerful; if he receives a call at his business number, his IP phone rings. In addition, all the other devices configured for Mobile Connect ring at the same time. Whichever device is answered receives the extended call, and all other devices stop ringing.

Suppose the user answers the call on his mobile phone while on the way to his office. When he gets to his desk, he has the option of picking up the call at his IP phone by pressing a softkey. The call is seamlessly transferred to the desk phone, and the caller may not even realize it has happened.

Likewise, the user can be in a call on his IP phone and redirect it to his mobile device as he leaves the office, again without the other party knowing that it has happened (except, of course, the possibility of a change in background noise or voice quality on a cell phone).

If the user calls a colleague's IP phone by dialing his direct inward dial (DID) from his mobile phone, CUCM recognizes the automatic number identification (ANI) (the caller ID) of the user as matching a remote destination profile, which has a shared line with the user's directory number (DN). The call to the colleague's IP phone is presented as being from the DN of the user's IP phone. This functionality also allows the user to call in to the Cisco Unity Connection voice-messaging system and have Easy Message Access to his personal mailbox (which is associated with the DN on his IP phone).

Note Most implementations of Mobile Connect use access codes for remote destinations. If this is the case, some digit manipulation of the incoming ANI may be necessary to match the entire remote destination profile number pattern. Alternatively, the CallManager Service Parameter Matching Call ID with Remote Destination can be set to Partial Match, which causes CUCM to make the closest match with a remote destination profile, starting with the least-significant digit of the ANI.

Unified Mobility Architecture

Key Topic

Mobile Connect uses remote destination profiles to configure virtual phones that share several configuration settings with the user's primary IP phone. In effect, the remote destination profiles act as phones with shared lines; when the primary number rings, the shared lines also ring, but the system configuration redirects the call out to the public switched telephone network (PSTN) to ring the other devices.

Remote destination profiles are configured with many of the same settings as the physical IP phone, including a partition, device pool, calling search space (CSS), user and network Music on Hold (MoH), and of course the same DN. The profile also includes a rerouting calling search space to allow the system to route calls to the device, even if that call would normally be restricted by the CSS of the IP phone.

Up to 10 remote destinations can be defined per user. Immediate complexities emerge with respect to the behavior of the Mobile Connect feature: How long should the system wait before ringing the remote destination profile phones? How long should the remote devices be made to ring? How long must the remote device ring before the call can be picked up on it? The adjustment of these timers can greatly improve the utility of the Mobile Connect feature, as well as avoid unwanted behavior, such as calls going to voicemail too soon or possibly going to some other voicemail (such as the personal voicemail at the user's home phone).

Access Lists

Not to be confused with IOS router access control lists, these access lists give both administrators and users control over which calls will ring which remote destination profile devices and at what time of day.

Access lists filter calls based on the caller ID; they can be configured to allow certain number patterns (called a white list) or to block certain number patterns (called a black list). The callers are identified using three types of match:

- **Not available:** The caller ID is not provided.
- **Private:** The caller ID is not displayed.
- **Directory number:** The caller ID matches a specific number or a wildcard-defined range of numbers (using the digits 0 through 9, *, #, and the wildcards of X and !).

Time-of-Day Access

Each remote destination profile can be configured with a schedule that controls when it should be included in the set of remote devices that will ring. By default, all remote devices ring. The time zone of the actual remote device should be specified so that the time-of-day rules apply correctly.

For incoming calls, the time-of-day rules are processed first. If the time-of-day rule allows the call to be extended to the remote destination profile, any configured access lists are processed next. If the access list allows the call, it is extended to the remote destination device.

> **Note** Avoid using empty access lists. An empty access list selected in a white list causes no calls to be routed; an empty access list in a black list causes all calls to be routed to the remote destination device.

Mobile Voice Access

Key Topic

Mobile Voice Access (MVA) provides the same single-number consistency and flexibility for outbound calls from users: By accessing the CUCM system from their mobile device, they can instruct the system to place calls and have the call appear to be from their IP phone using their primary IP phone number (assumed to be a DID, but could be the main business number). As a result, their physical location has no impact on their voice communication consistency. Whether they are sitting in front of their IP phone or using their mobile phone from the golf course, the calls they place all appear to come from their primary business number.

To use the feature, the user dials in to a specific PSTN DID to access the MVA service. A specially configured VoiceXML gateway routes calls to an interactive voice response (IVR) application that guides the user through his MVA session. The IVR app provides security by prompting the user to authenticate with their user ID (optional) and PIN. Once successfully authenticated, the IVR prompts the user for the number they want to dial. The user enters the PSTN number and the system places the call, using the ANI of the user's IP phone. The user can switch between his mobile device and his IP phone during the call. The called party sees the caller ID as that of the user's IP phone, providing the single-number consistency and recognition, as well as ease of callback from a call list.

Figure 12-1 shows the basic call flow in MVA.

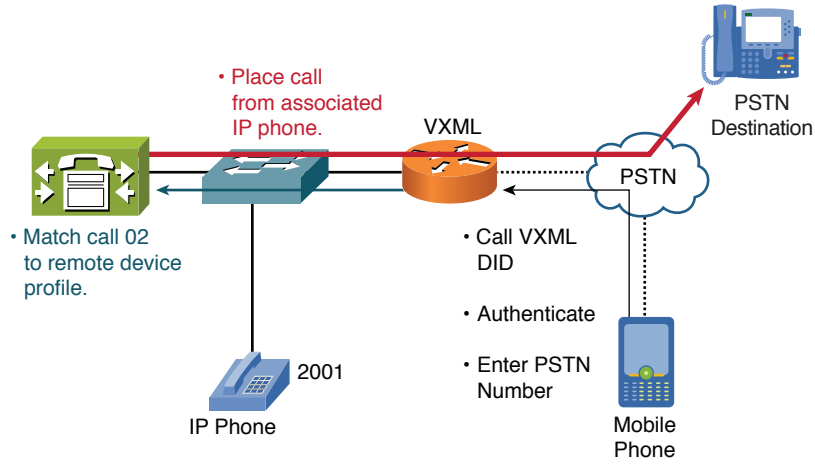


Figure 12-1 *Mobile Voice Access Basic Call Flow*

Implementing Mobility Features in CUCM

The configuration of the various mobility features in CUCM is not difficult, but it is repetitive and potentially time-consuming, especially when many users need to be configured. This section outlines the configuration tasks for the mobility features described earlier.

Configuring Mobile Connect

Key Topic

Many different components interact to allow Mobile Connect to function. The basic steps to configure Mobile Connect are as follows:

Step 1. Configure softkey templates to include the Mobility key.

Step 2. Configure user accounts for mobility.

Step 3. Configure IP phones to support mobility features.

Step 4. Create remote destination profiles and assign them to each user.

Step 5. Add remote destinations to remote destination profiles .

Step 6. Configure ring schedules for each remote destination.

Step 7. Configure access lists.

Step 8. Apply access lists to remote destinations.

Step 9. Configure service parameters.

Each of the following sections describes these configuration steps in detail.

Step 1: Configure Softkey Templates

To use Mobile Connect, the user activates a softkey on his IP phone. Complete the following tasks to add the softkey to the phone(s) that will use this feature:

1. Navigate to **Device > Device Settings > Softkey Template**.
2. Select, copy and modify, or add a new template.
3. In the Related Tasks pull-down, select **Configure Softkey Layout** and click **Go**.
4. Move the Mobility softkey to the OnHook and Connected call states lists. Click **Save** after each move.

Figure 12-2 shows the Softkey template with the Mobility key added.

Step 2: Configure User Accounts for Mobility

Individual user accounts must be enabled for mobility and some settings tuned for optimal functionality. Complete the following steps to set up the user accounts for mobility:

1. Navigate to **User Management > End User** and select a user.
2. Check the **Enable Mobility** check box.
3. Set the Remote Destination Limit (maximum 10).
4. Set the Maximum Wait Time for Desk Pickup timer. This is how much time (in milliseconds) is allowed for the user to pick up a call that was redirected from the remote device to the IP phone. The default is 10,000 ms (10 sec) with a maximum of 30,000 ms (30 sec).

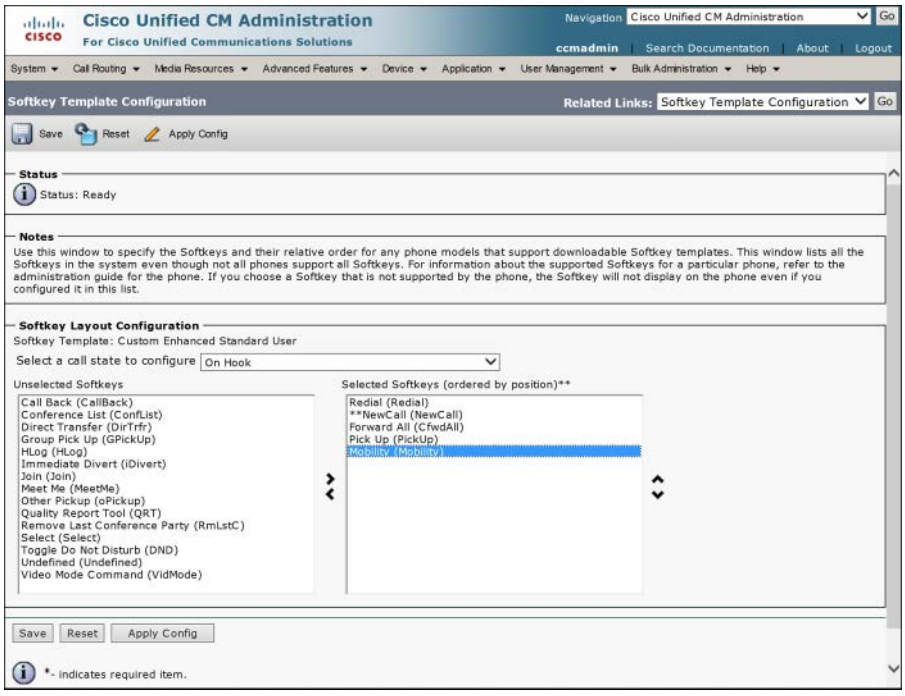


Figure 12-2 *Softkey Template with Mobility Key Added*

Figure 12-3 shows the End User Configuration page for Mobile Connect.

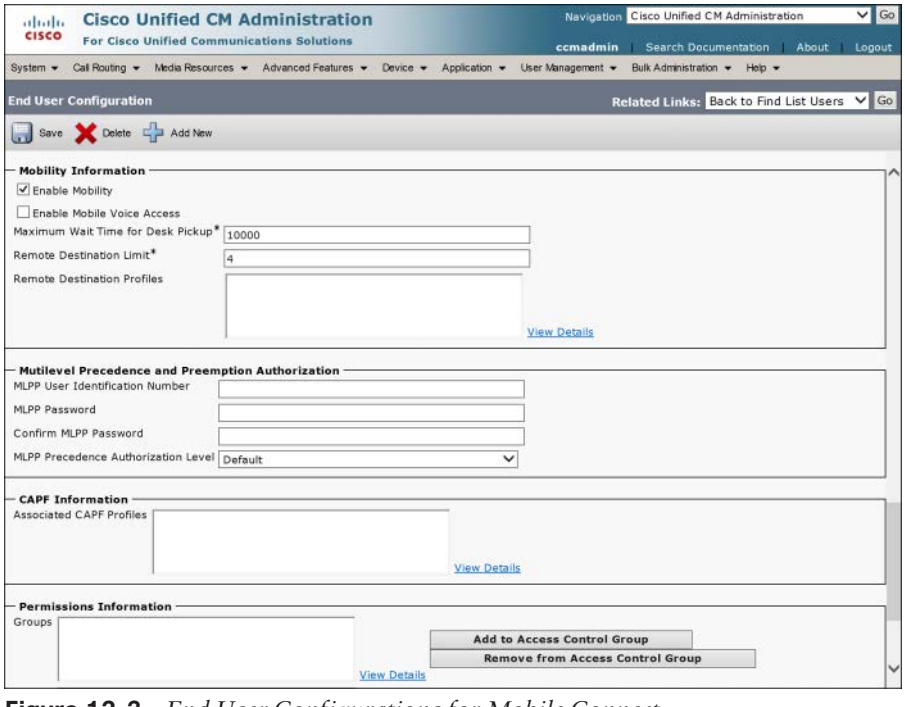


Figure 12-3 *End User Configurations for Mobile Connect*

Step 3: Configure the IP Phone to Support Mobility Features

The users' IP phones must be configured to link the user configuration and softkey template. To do this, complete the following steps:

1. Assign the Softkey template to which you previously added the Mobility key.
2. Set the Owner User ID to the appropriate mobility-configured user.

Step 4: Create Remote Destination Profiles

The following steps create the remote destination profiles, link them to the user accounts, and ensure that calls can reach the remote numbers:

1. Navigate to **Device > Device Settings > Remote Destination Profile**.
2. Click **Add New** and configure a name.
3. Select the User ID to be associated with this profile.
4. Select the **Rerouting Calling Search Space**. This CSS will redirect calls to remote devices and, therefore, must provide access to the remote devices' phone numbers.

Figure 12-4 illustrates a remote destination profile configuration.

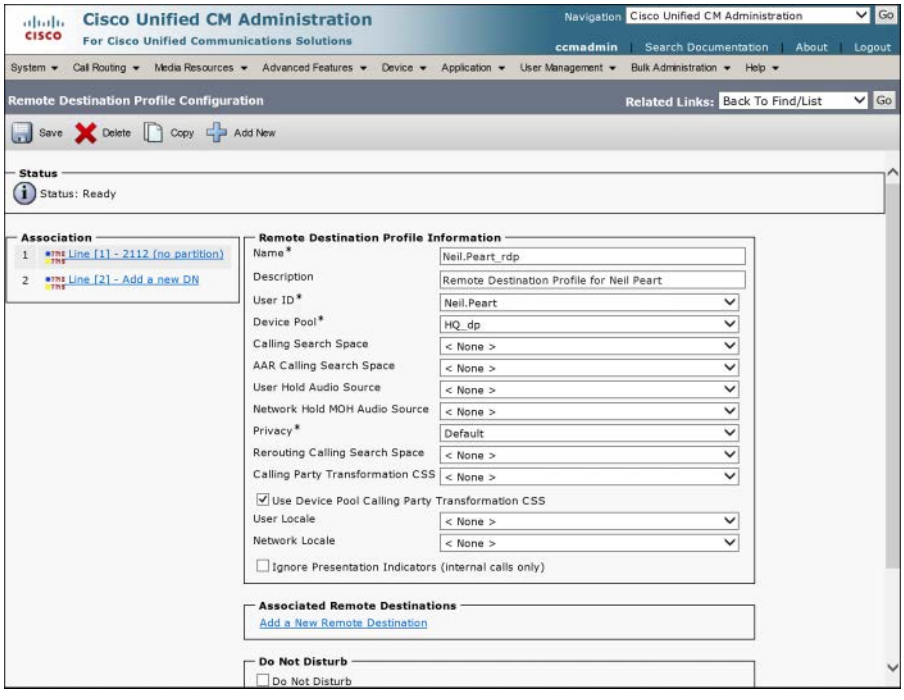


Figure 12-4 *Remote Destination Profile Configuration*

Step 5: Add Remote Destinations to Remote Destination Profiles

These steps link the remote destinations to the remote destination profiles:

1. Navigate to **Device > Remote Destination**.

2. Click **Add New**.
3. Enter a **Name**.
4. Set the Destination Number, just as it would be dialed from an IP phone, including any access codes. This entry must be a PSTN number.
5. Associate the appropriate remote destination profile for the user. Once configured, this cannot be changed; to change it, delete the remote destination and re-create it with the desired setting.
6. Check the **Enable Single Number Reach** check box to include this remote destination in the set of those that will ring when the IP phone shared line rings.
7. Check the **Enable Move To Mobile** check box to allow manual handoff of calls from the IP phone using the Mobility softkey.
8. In the Association Information area, select one or more of the shared lines on the remote destination profile.

Figure 12-5 illustrates adding a remote destination to a remote destination profile.

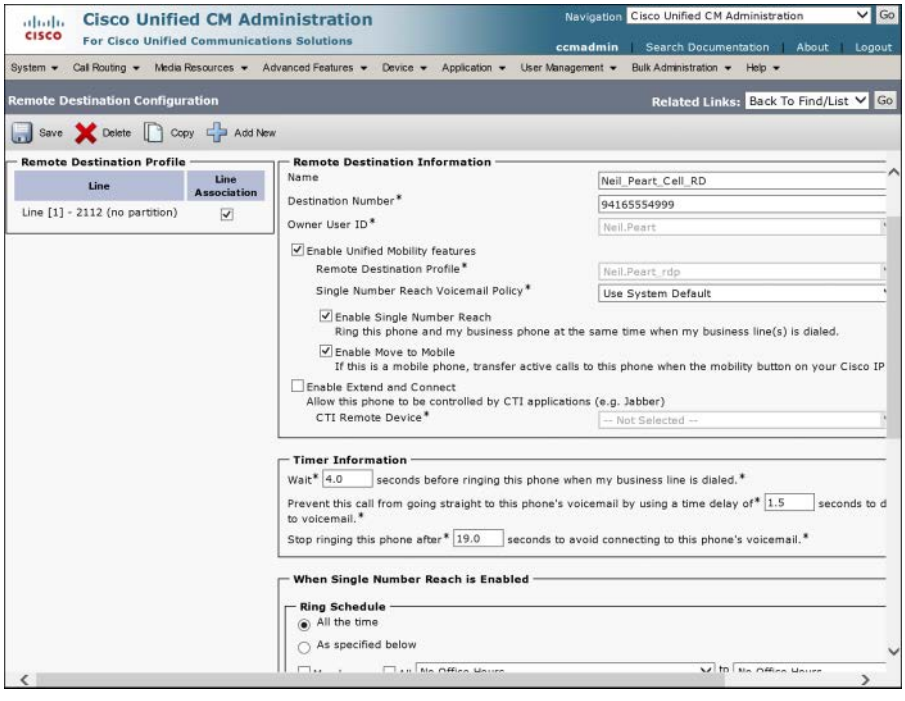


Figure 12-5 *Adding Remote Destinations to a Remote Destination Profile*

Step 6: Configure Ring Schedules for Each Remote Destination

The next steps tune the functionality of the remote destinations by limiting the times of day when they will ring:

1. Set the days and times when this remote device should ring.
2. Select the correct time zone of the remote device.

Step 7: Configure Access Lists

These steps configure access lists to limit which numbers can or cannot ring remote destinations:

1. Navigate to **Call Routing > Class of Control > Access List**.
2. Click **Add New**.
3. Configure a name for the list.
4. Set the owner user ID from the pull-down. This entry should be the Mobile Connect user to whom the access list applies.
5. Choose either **Allowed** or **Blocked** to set the function of the list.
6. Click **Save**.

When the screen refreshes, in the Access List Member area, click **Add Member**.

Figure 12-6 shows an access list configuration to block certain calls (a disallowed list or blacklist).

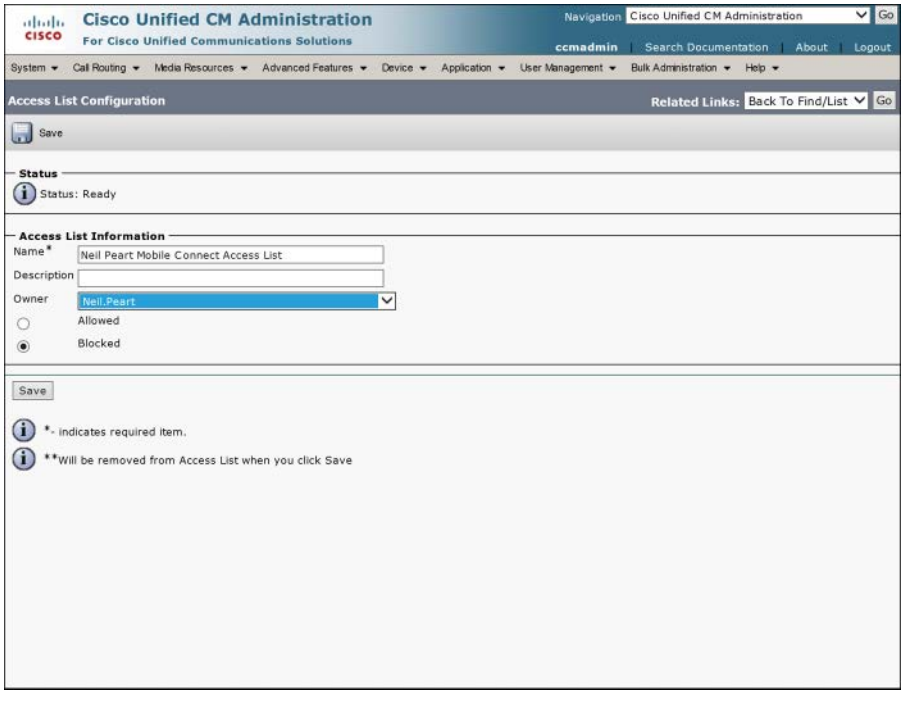


Figure 12-6 *Access List Configuration*

- On the Access List Member Detail page, select **Filter Mask:**
  - **Directory Number:** To enter a specific ANI number or wildcard pattern
  - **Private:** To filter based on calls with caller ID not displayed
  - **Not Available:** To filter based on calls without caller ID

- In the DN Mask field, you can enter a specific digit string (for example, 5558675309) or use the wildcards X (matching a single dialed digit) and ! (matching any number of digits) to represent multiple strings in one entry (much like route patterns).

Figure 12-7 illustrates a filter mask configuration to block a specific caller ID number.

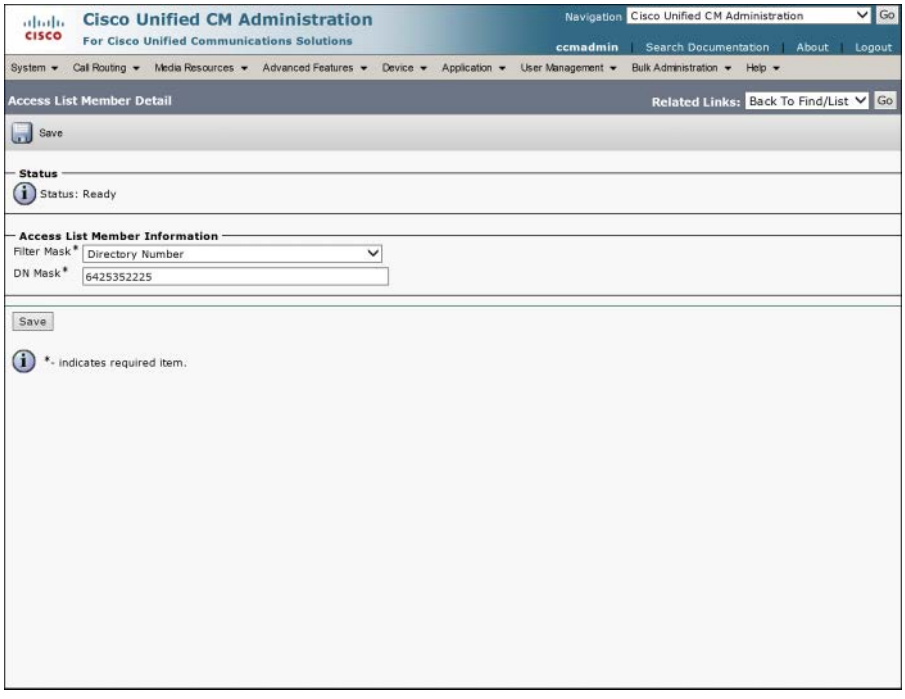


Figure 12-7 *Configuring a Filter Mask for an Access List*

Step 8: Apply Access Lists

These access lists configured previously must be applied to the remote destinations, as described in the following steps:

1. Navigate to **Device > Remote Destination** and select a remote destination.
2. Select either the **Always Ring This Destination** or one of the **Ring This Destination If the Caller Is in (Allowed)** or **Do Not Ring This Destination If The caller Is in (Blocked)** radio buttons. You must select one or the other; selecting both is not an option.
3. In the pull-down next to the ring selection, select the access list that provides the desired filter.
4. Click **Save**.

Figure 12-8 shows an access list applied to a remote destination.

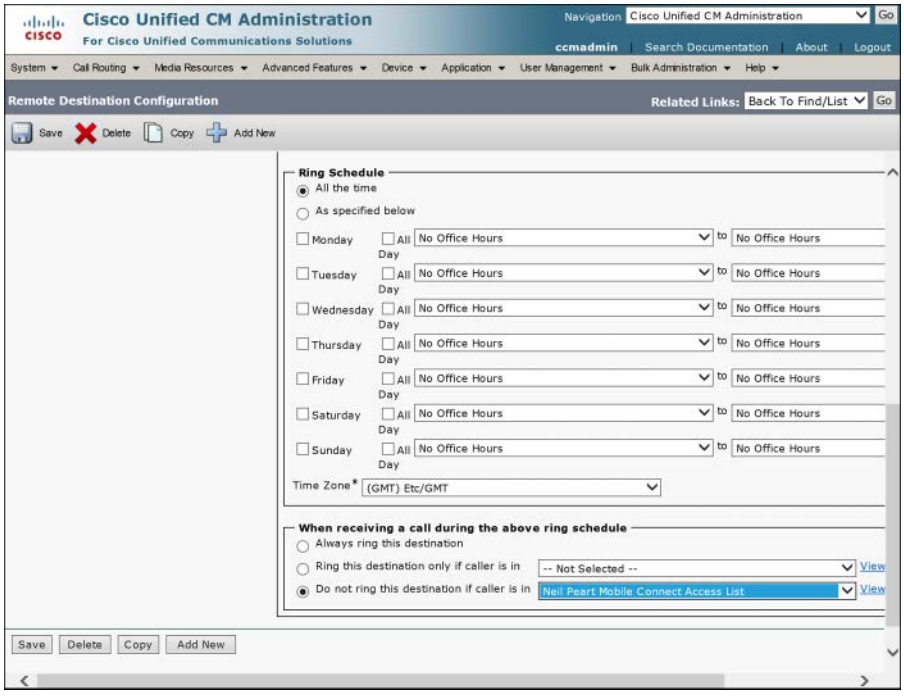


Figure 12-8 *Applying an Access List to a Remote Destination*

Step 9: Configure Service Parameters

Certain service parameters can be tuned to customize the behavior of the Mobility features, as discussed in these steps:

1. Navigate to **System > Service Parameters**. Select the **Server** you want to configure from the pull-down.
2. Select the **Cisco CallManager** service from the Service pull-down.
3. Scroll down to the Clusterwide Parameters (System - Mobility) section.
4. In the Inbound Calling Search Space for Remote Destination field, choose either **Trunk or Gateway Inbound Calling Search Space** (the default, which uses the CSS of the trunk or gateway that is routing the inbound call from the remote destination) or **Remote Destination Profile + Line Calling Search Space** (which uses the combined line and remote destination profile CSS).
5. In the Matching Caller ID with Remote Destination field, select either **Complete Match** (the default, which requires the incoming Caller ID to exactly match the Remote Destination number) or **Partial Match**, which allows you to specify how many digits of the Caller ID to match, starting with the least significant digit.
6. Scroll down to the Clusterwide Parameters (Feature - Reroute Remote Destination Calls to Enterprise Number) section.

7. Set Reroute Remote Destination Calls to Enterprise Number to **True** (the default is False) to cause direct calls to a Remote Destination number to be extended to the IP phone number, allowing the user to take advantage of Mobility features.
8. Set Ignore Call Forward All on Enterprise DN to **True** to route calls to remote destinations, even if the IP phone has CFA active.

Figure 12-9 shows some of the service parameter configurations for mobility.

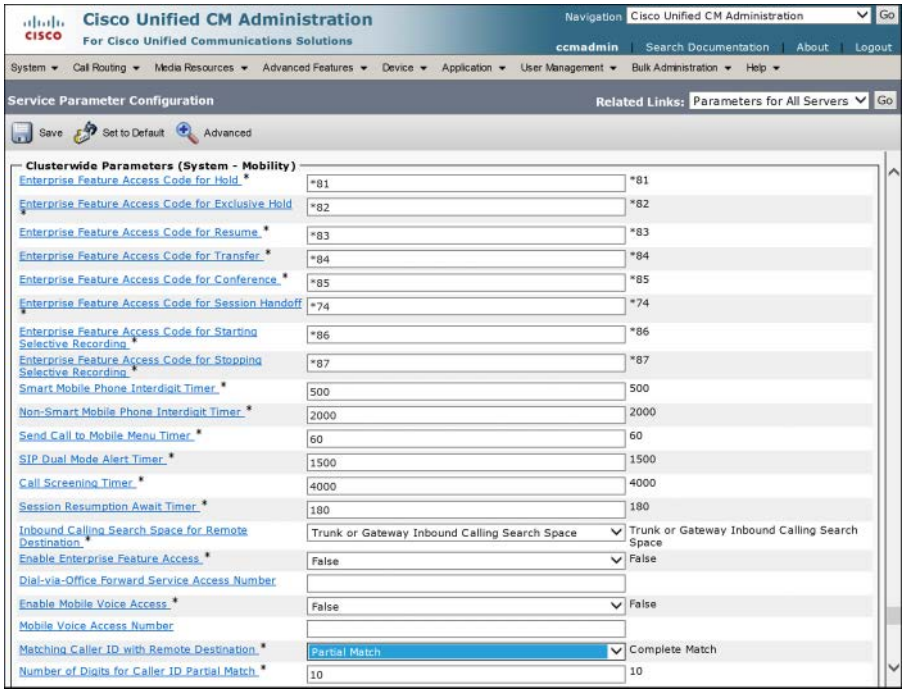


Figure 12-9 *Service Parameters Configuration for Mobility*

Configuring MVA

Key Topic

The basic steps to configure MVA are as follows:

Step 1. Activate the MVA service.

Step 2. Configure service parameters.

Step 3. Enable MVA for each user.

Step 4. Configure the MVA media resource.

Step 5. Configure the MVA VXML application at the IOS gateway.

These steps are described in more detail in the following sections.

Step 1: Activate the MVA Service

Before the MVA feature can function, the service must be activated, as described in the following:

1. Navigate **to Unified Serviceability > Tools > Service Activation.**
2. Select the **Cisco Unified Mobile Voice Access Service.**
3. Click **Save.**

Step 2: Configure Service Parameters

With the MVA service active, you can now enable it for the cluster, as shown in the following steps.

1. Navigate to **Unified CM Administration > System > Service Parameters.**
2. Select the server you want to configure, and select the **Cisco CallManager Service.**
3. Scroll down to Clusterwide Parameters (System - Mobility).
4. Set the Enable Mobile Voice Access value to **True.**
5. Modify other system parameters, such as access codes, if desired.

Figure 12-10 shows the Cisco Unified Mobile Voice Access Service activated.

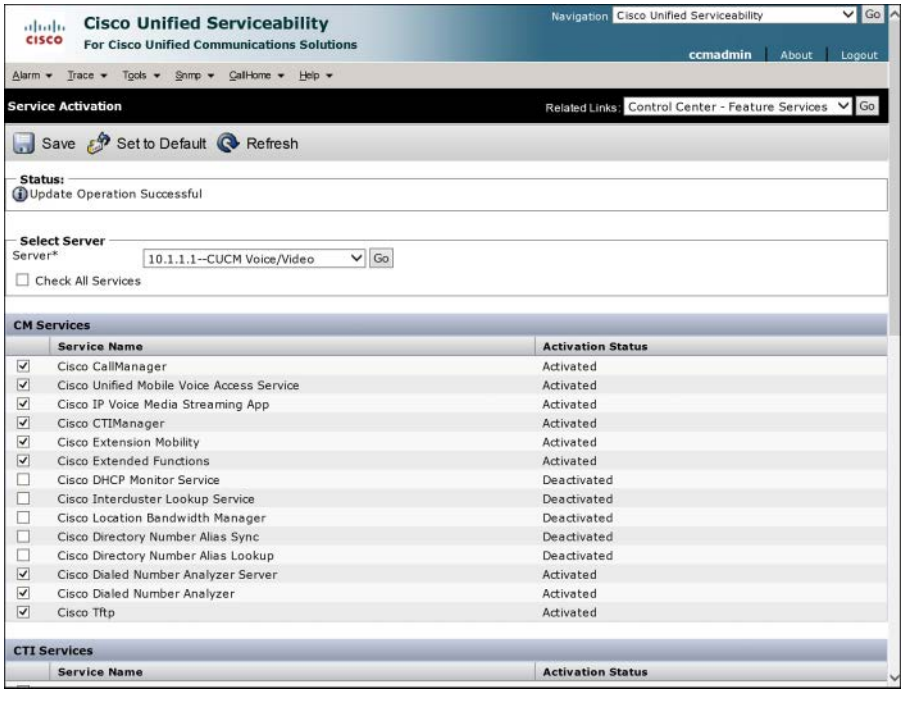


Figure 12-10 *Activating the MVA Service*

Note Enabling the MVA service is required to enable MVA globally, but it is also necessary to activate MVA for each user for it to actually function.

Step 3: Enable MVA for Each User

As noted previously, it is not sufficient to activate the MVA service and enable MVA for the cluster; you must now enable MVA for each user, as described in the following steps:

1. Navigate to the user configuration page for the user(s) for whom you want to enable MVA.
2. Scroll down to the Mobility Information section.
3. Check the **Enable Mobile Voice Access** box.
4. Verify that the remote destination profile listed is configured correctly to provide authentication.

Figure 12-11 shows the End User Configuration page for MVA.

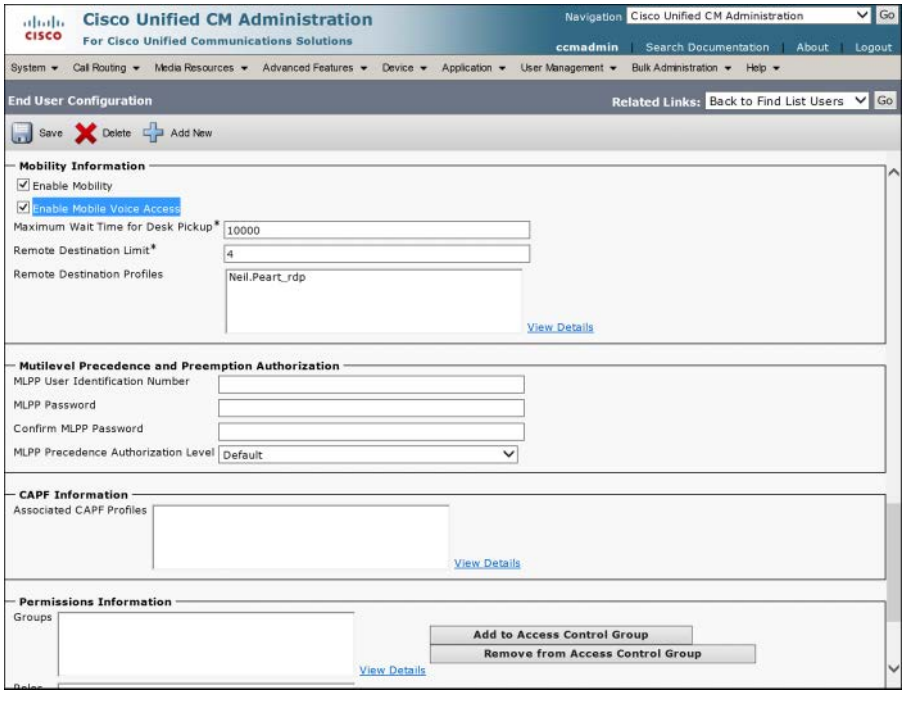


Figure 12-11 *Configuring the End User for MVA*

Note Other mobility-related parameters were discussed and configured in the Mobile Connect sections of this chapter.

Step 4: Configure the MVA Media Resource

The MVA media resource is automatically created when the MVA service is activated. To configure options, follow these steps:

1. Navigate to **Media Resources > Mobile Voice Access.**
2. Enter a number for the Mobile Voice Access directory number. This number is the internal number to which the H.323 MVA gateway will forward calls it receives on the PSTN number for MVA access. On the gateway, a dial peer must be configured that matches the PSTN MVA number to the MVA CUCM server.
3. Assign a partition if desired. This partition must be in the CSS of the MVA gateway.
4. Move the English, United States locale to the Selected Locales list. Set additional locales, if desired, to provide users with MVA IVR service in multiple languages. (Additional locales may be purchased and installed.)

Figure 12-12 shows the MVA media resource configuration page.

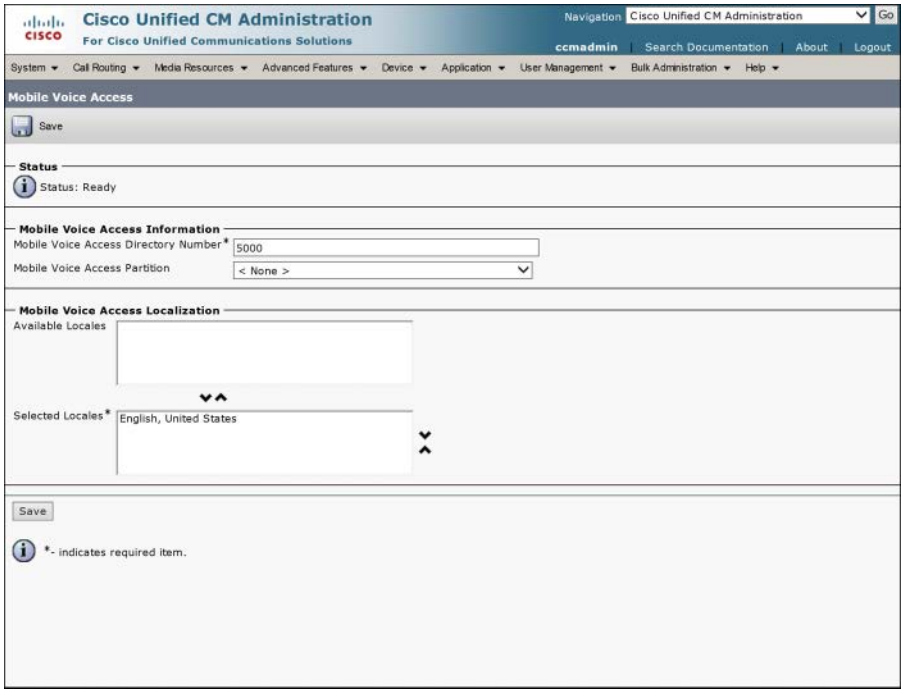


Figure 12-12 *MVA Media Resource Configuration*

Step 5: Configure the MVA VXML Application at the IOS Gateway

The H.323 gateway configuration must include the following statements. The output shown here is annotated to explain what the commands do:

```
! Define the MVA Application and URL
application
 service mva http://10.1.1.1:8080/ccmivr/pages/IVRMainpage.vxml
dial-peer voice 50001 pots
! Associate the MVA application to this dial peer
 service mva
! Match the PSTN MVA access number to this inbound dial peer
 incoming called-number 4085555000
 direct-inward-dial
dial-peer voice 50002 voip
! Match the PSTN MVA access number to this outbound dial peer
 destination-pattern 4085555000
! Identify the CUCM server running the MVA service VXML app referenced above
 session target ipv4:10.1.1.1
 dtmf-relay h245-alphanumeric
  codec g711ulaw
 no vad
```

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 12-2 describes these key topics and identifies the page number on which each is found.

Key Topic

Table 12-2 Key Topics for Chapter 12

Key Topic Element	Description	Page Number
Section	Understanding the components of Mobile Connect and MVA	327
Section	Understanding MVA	328
List	Steps required to configure Mobile Connect	329
List	Steps required to configure MVA	336
CLI output	IOS configuration to support MVA	340

Definitions of Key Terms

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

Mobile Connect, Mobile Voice Access (MVA)

This chapter covers the following topics:

- **Describe Cisco Unity Connection:** This section describes the capabilities and features of the CUC application with CUCM integration.
- **Describe Cisco Unity Connection Users and Mailboxes:** This section describes the core components and related configuration requirements of the CUC system.
- **Implement Cisco Unity Connection Users and Mailboxes:** This section reviews the implementation of users and mailboxes in CUC.

CHAPTER 13

Voice Messaging Integration with Cisco Unity Connection

Voicemail (which we are encouraged to call *voice nessaging* these days) is a ubiquitous feature of a modern business phone system. The Cisco Unity Connection (CUC) product certainly qualifies as voicemail but has so many related and advanced features that calling it simply voicemail is at least inaccurate and probably an injustice. This chapter reviews the features and capability of the CUC application, the core components and systems, and the configuration and implementation of basic services for voice messaging.

"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 13-1 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 13-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Describe Cisco Unity Connection	1–6
Describe Cisco Unity Users and Mailboxes	7–8
Implement Cisco Unity Connection Users and Mailboxes	9–10

1. What is the maximum number of mailboxes supported on a single CUC 10.x virtual machine?
   - **a.** 3000
   - **b.** 7500
   - **c.** 10,000
   - **d.** 20,000
2. Which of the following is not deployed as a Linux appliance?
   - **a.** Cisco Unity Connection 10.x
   - **b.** Cisco Unified Contact Center 8.x
   - **c.** Cisco Unified Communications Manager 10.x
   - **d.** Cisco Emergency Responder 10.x
   - **e.** Cisco Unified Communications Manager IM and Presence 10.x

3. Which of the following are supported phone system integrations in CUC? (Choose all that apply.)
   a. CUCM using SCCP
   b. IP PBX using SIP
   c. Digital PBX using PIMG
   d. PBX using AMIS
   e. PBX using analog DTMF
4. Which of the following represents the correct order of processing of components when a user presses his Messages button?
   a. Voicemail pilot, voicemail profile, hunt group, hunt list, line group, voicemail port
   b. Voicemail profile, voicemail pilot, hunt pilot, hunt list, line group, voicemail port
   c. Voicemail profile, voicemail port, voicemail pilot, hunt pilot, hunt list, line group
   d. Hunt pilot, hunt list, line group, voicemail profile, voicemail pilot, voicemail port
5. Which of the following is not a call handler type in CUC?
   a. System call handler
   b. Directory call handler
   c. Interview call handler
   d. Holiday call handler
6. Which of the following would be processed by direct routing rules in CUC? (Choose two.)
   a. Bill dials Max's phone, but Max is on the phone, so it goes to voicemail.
   b. Max dial's Keisa's phone, but Keisa is away from her desk, so it goes to voicemail.
   c. Keisa dials Angie's phone, which is forwarded to Angie's cell phone, and Keisa gets Angie's cell phone voicemail.
   d. Max sees his message lamp and presses the Messages button to check his voicemail.
   e. Bill calls the company number from home and hears the auto-attendant opening greeting.
7. Where can the maximum message length be set? (Choose three.)
   a. Class of service
   b. User template
   c. User account settings
   d. Mailbox quotas
   e. Message store settings

8. Guy is the CUC administrator. He uses AXL to import user accounts from the CUCM database into CUC. What is the result?
   a. Usernames and aliases of users imported via AXL cannot be changed in CUC.
   b. User passwords cannot be changed in CUC.
   c. Active Directory regularly syncs users to CUC.
   d. User accounts can no longer be created in the local CUC database.

9. Guy notices that some of the user accounts he wants to import from CUCM into CUC using AXL do not appear in the list of users found via AXL. What might be the problem?
   a. The LDAP Manager account password is incorrect.
   b. The DirSync Service is not activated.
   c. The missing user accounts are not configured with a primary extension in the CUCM database.
   d. The missing user accounts had the Do Not List In Directory setting checked.

10. Pete wants to be able to call into the CUC auto-attendant number from his mobile phone and be prompted to enter his PIN for quick access to his mailbox. What should he ask the CUC administrator to do for him?
   a. Configure a special dial peer on the gateway router to send calls from Pete's number to an Attempt Sign-In conversation on CUC.
   b. Tell Pete about the hidden key press during the Opening Greeting that will send him to the Attempt Sign-In conversation.
   c. Buy a different voicemail system because CUC cannot do this.
   d. Add an alternate extension with the correct ANI of Pete's mobile phone.

Foundation Topics

Describe Cisco Unity Connection

Cisco Unity Connection (CUC) is a full-featured voice-messaging, auto-attendant, and voice-recognition system providing universal access to calls and messages as part of a Unified Communications solution. Up to 20,000 mailboxes can be hosted by a single CUC v10.x server (assuming the most powerful OVA template). Voice recognition capabilities allow speech-activated commands to be used by both internal and external callers. A built-in IMAP server allows email access to voice messages, and a clientless, web-based interface provides the same capability from any compatible browser with web access to the CUC server. The following sections discuss CUC.

Overview of Cisco Unity Connection

CUC is installed as a Linux appliance just as other Unified Communications applications (including CUCM, CM-IMP, UCCX, and CER) are. The data and message store databases are held locally on the server, both using an instance of the Informix Database Service application. The recommended deployment of CUC is as a VMware guest on a Unified Computing System hardware platform. Third-party hardware may also be supported in some environments.

CUC supports integration with a variety of traditional PBX systems that support either native IP functionality or a digital TDM circuit that can be connected via PBX or T1 IP Media Gateway (PBX IP Media Gateway [PIMG] or T1 IP Media Gateway [TIMG]). CUC users can be manually configured, bulk imported from a Comma-Separated Values (CSV) file, imported from a CUCM server database using the Administrative XML Web Service (AXL), or synchronized directly from a Lightweight Directory Access Protocol (LDAP) system. Password authentication can also be redirected to the LDAP system.

CUC can integrate with a Microsoft Exchange server, using Web-Based Distributed Authoring and Versioning (WebDAV) to provide calendar and journal information for integration with Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express, Microsoft Exchange 2003, and personal call routing rules within CUC itself. Calendar integration services for Microsoft Exchange 2007 are handled using the web service's application programming interface (API).

CUC provides a traditional Telephone User Interface (TUI) for interaction over Dual-Tone Multi-Frequency (DTMF) phones, a Voice User Interface (VUI) for hands-free interaction, and the IP phone application Phone View (Visual Voicemail) to see voice-message headers on the IP phone screen or in the Cisco Jabber client.

Single-Site and Multisite Deployment Considerations

The simplest deployment of the CUC application is as a single-site model, with one building or campus accessing a single CUC server (or active-active redundant server pair). The advantages of design simplicity, a single codec for all calls, and a greatly simplified implementation task list make this an attractive option.

If there are multiple locations (or will be in the future), a multisite deployment may be a better choice; although users can call across the IP WAN to check or leave voice messages (or use other features) in a single-site deployment, doing so can put a significant extra load on WAN bandwidth and transcoder resources. This is especially true as the number of users in the system increases. Locating additional servers in branch locations can greatly reduce the impact of these problems while providing the same seamless functionality as in a single-site model.

CUC Integration Overview

Integration in this context refers to interoperation with a PBX- or IP-based telephone system. CUC supports a variety of integrations using SCCP, SIP, or PIMG/TIMG. Multiple phone systems are supported concurrently; CUCM and CME can be supported using SCCP or SIP, a SIP-capable PBX will integrate using SIP, and a variety of digital PBX products can be supported using a PIMG or TIMG device that provides gateway services between a digital TDM circuit and a SIP trunk.

CUC Integration with CUCM Using SCCP

Key Topic

A Voicemail Port Wizard is available in CUCM that simplifies the integration of CUC with CUCM. The wizard requests user input to correctly set up the system and then generates voicemail ports in CUCM and adds them to a Line Group. The administrator must manually configure a hunt list and hunt pilot to support the line group.

The hunt pilot is referenced by a voicemail pilot, which is itself referenced by a voicemail profile. Figure 13-1 illustrates the architecture of the voicemail integration on the CUCM side.

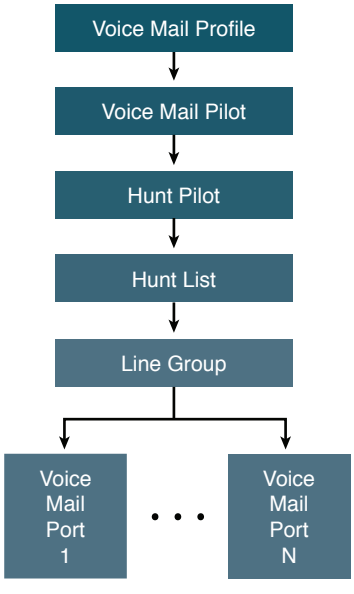


Figure 13-1 *SCCP Voicemail Integration Components in CUCM*

Default entries for the voicemail profile and voicemail pilot exist, which are used by all users of the CUCM system; these may be used and customized, or others may be added for other integrations and used by different subsets of users. The Voicemail Port Wizard has all but eliminated a common problem in CUCM-to-CUC integrations with SCCP: Often, administrators would forget one or more of the critical steps of creating the voicemail pilot and linking it to the hunt pilot, and creating the voicemail profile and linking it to the voicemail pilot. Miss one of these, and the Messages button on the phones won't work, even though you can dial the CUC hunt pilot number directly and reach CUC.

On the CUC server, a set of ports is defined (the number of available ports being limited by the server hardware capacity), and each port is configured for various call behavior options, including whether the port should answer calls, perform message waiting indicator (MWI) or message notification, and other settings. Call routing within CUC can be controlled by (among other things) the phone system or the port group.

In a SCCP integration, MWI uses a separate and unique directory number (DN) for MWI On and MWI Off. The DNs must be configured (and match) in both CUCM and CUC. One of the tricks you can play on your coworkers is to dial the MWI On DN from their phone; their MWI light will come on (dial MWI Off and it turns off, too). This practical joke is also an effective way to test MWI functionality.

An integration using Skinny Client Control Protocol (SCCP) may be secured using digital certificates and SCCP over port 2448. (Nonsecure SCCP uses port 2000.)

CUC Integration Using SIP

The Session Initiation Protocol (SIP) integration components are slightly different from SCCP: Instead of the voicemail pilot pointing to a hunt pilot, it points to a route pattern, which in turn points to a SIP trunk. The SIP trunk is configured to connect to CUC. The number of ports is not defined on the CUCM server as it is for SCCP integration; rather, they are only defined in CUC. Each port is configured to register with a SIP server (which is the CUCM server). A significant difference with a SIP integration is that there are no separate DNs for MWI On/Off; instead, SIP itself handles the signaling of the MWI lamp state. SIP can also be secured using port 5061. (Nonsecure SIP uses port 5060.) Figure 13-2 illustrates the SIP integration components on CUCM.

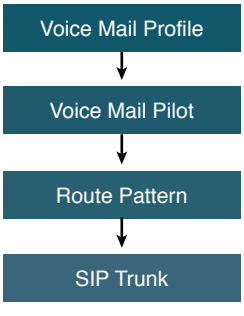


Figure 13-2 *SIP Voicemail Integration Components in CUCM*

CUC Features

This section describes many of the system-level features and settings of CUC.

System Settings

The installation and configuration of CUC includes many system settings. Because the CICD exam scope is relatively limited, we describe only a few here.

General Configuration

The General Configuration page includes the defaults for the system time zone, language, and maximum greeting length.

Roles

The Roles page lists the nine administrative roles defined in the CUC 10.x application. An administrative role gives (and limits) administrative capability to users. Table 13-2 lists these roles and brief descriptions of their functions.

Table 13-2 CUC Roles and Descriptions

Role	Description
Audio Text Administrator	This role allows an administrator to manage call handlers, directory handlers, and interview handlers.
Audit Administrator	This role allows an administrator to enable or disable Unity Connection application and database auditing, to configure audit settings, and to view or delete audit logs.
Greeting Administrator	This role allows an administrator to access the Cisco Unity Greetings Administrator, a Unity Connection phone conversation that allows users to manage the recorded greetings for call handlers by phone. **Note** You need to assign this role to a user with voice mailbox account because the administrator must be able to access Unity Connection by phone.
Help Desk Administrator	This role allows an administrator to reset user passwords and PINs, unlock user accounts, and view user setting pages. **Note** The "Manage Call Handlers Belonging to Users Only - View Only" privilege refers to the primary call handler assigned to a user that include all greetings, transfer rules, and menu entries that you see on the User's page under the Roles section.
Mailbox Access Delegate Account	A user with this role has access to all messages. Remote applications, for example, Cisco Unified Mobility Advantage use the username and password of a user with this role for the purposes of retrieving messages on behalf of other users. Typically, this role is assigned to only one user account, which does not represent a real user but exists to access mailboxes on behalf of other users.
Remote Administrator	This role allows an administrator to administer the database using remote tools.

Role	Description
System Administrator	This is the top-level Unity Connection administration role. This role allows access to all Unity Connection administrative functions, including all user and system settings, all reports, and all administration and diagnostic tools. The default administrator account that the installer specified during initial setup of Unity Connection is set to this role. A system administrator is the only role that has permission to create administrative accounts.
Technician	This role allows an administrator access to all functions that enable management of the Unity Connection server and phone system integration settings; administrators with this role can also run all reports, use diagnostic tools, and view all system and user settings pages.
User Administrator	This role allows an administrator to manage user accounts and access all user administration functions and user administration tools.

Enterprise Parameters and Service Parameters

Equivalent to the pages of the same name in CUCM, these pages define and tune system and service parameters, such as what users can see and configure on the user web pages, quality of service (QoS) settings for CUC-generated traffic, and so on.

LDAP

These pages define the integration with an LDAP system to provide user synchronization and optional authentication.

Call Handlers

All inbound calls to CUC are handled by a series of call handlers. The three basic types of call handlers are as follows:

- **System call handlers** are used for greetings and can be customized to offer user input options ("For Sales, press 2...") and automation, such as playing a different greeting when the business is closed.
- **Directory handlers** allow callers to search the CUC directory for the user they want to contact. Different directories can be defined based on location, distribution list membership, and so on.
- **Interview handlers** provide the caller with recorded information and then ask questions and record the caller's answers in a single message. Interview handlers can be used for telephone-based reporting for almost any purpose, such as automating job applications.

Three system call handlers are defined by default: goodbye call handler, opening greeting, and operator call handler. Opening greeting is what outside callers (those without a voicemail box on the CUC server) hear; it is expected, of course, that the greeting will be customized by the business.

Call Routing

Key Topic

Two primary call routing criteria are built in to CUC: The application identifies direct calls and forwarded calls. A direct call is when the caller dials the CUC system directly, either by pressing the Messages button on the IP phone (or dialing the voicemail pilot manually) or by dialing the public switched telephone network (PSTN) Direct Inward Dial (DID) of the CUC auto-attendant.

The system examines the information presented in the call as it is routed to the CUC port that answers it. The information available to CUC for its decision making includes the following:

- Calling number
- Called number
- Forwarding station
- Phone system/port
- Schedule

Two rules are defined under each category of call routing rule. The following sections describe these rules.

Figure 13-3 illustrates the call routing actions and rule criteria within CUC.

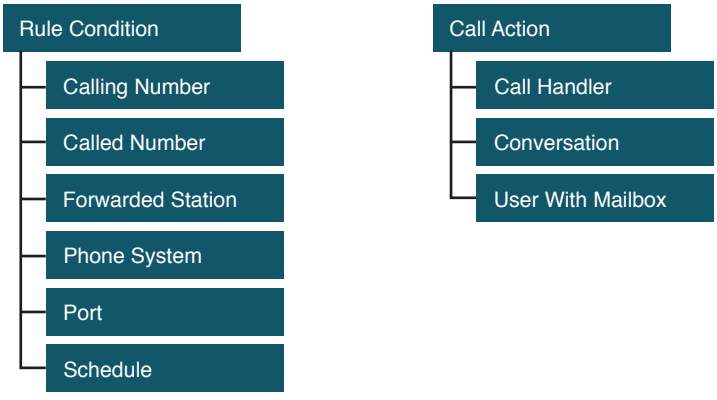


Figure 13-3 *Call Routing Actions and Rule Criteria*

Direct Routing Rules

For calls placed directly to CUC, the following two default rules apply:

- **Attempt sign-in:** If the calling number is recognized as the extension associated with a voicemail box, the call is sent to the attempt sign-in conversation and the caller is prompted to enter the correct PIN to log in to the voicemail box.
- **Opening greeting:** If the calling number is not associated with a voicemail box on the CUC server, the call is sent to the opening greeting.

Additional rules can be defined administratively (for example, routing calls to the business' customer help number to a specific call handler); the rules are processed top-down for each call, so the order of the rules is critical to their behavior.

Forwarded Routing Rules

For calls that are forwarded to CUC (typically because the user was on the phone or did not answer her phone), the following two default rules apply:

- **Attempt forward:** If the forwarding station is associated with a voicemail box on the CUC system, the forwarding phone user's personal greeting is played.
- **Opening greeting:** If the forwarding station is not associated with a voicemail box on the CUC system, the opening greeting is played.

Call Routing Rule Filters

When defining custom call routing rules (whether for direct or forwarded calls), you can apply the following filters (singly or combined within a single rule):

- Calling number
- Called number
- Voicemail port
- Phone system
- Forwarding station (applies only to forwarded calls)
- Schedule

The use of these rule capabilities provides administrators with a powerful customized call routing capability.

Note CUC call routing rules only apply if the call has been answered by CUC; for example, a PSTN call to a user's IP phone DID will not be answered by CUC unless the IP phone forwards it because of a busy or no answer condition.

Distribution Lists

Distribution lists (DLs) provide a simple way to send a voice message to a group of users. Two types of DL can be configured: System DLs are managed by the administrator and can be made available to all users or a subset of users as required. Private DLs are managed and maintained by an individual user and are usable only by the user who made them. The administrator can limit how many private lists a user can create and how many members can be in each.

Authentication Rules

To set the security level for access to the CUC system, authentication rules for voicemail (for TUI access via PIN) and web application (for access to the user web pages, called the Personal Communications Assistant [PCA]) can be customized. Authentication rules specify how many failed login attempts can occur before the account is locked out, how long the account is locked out, the minimum number of characters in a password, how often the password must be changed, and so on. The default authentication rules apply to all users. You can create new authentication rules with customized settings, and apply them to user

templates or even individual users. In this way, you could allow a four-digit password for a new user template while keeping a five-digit password for another.

Dial Plan

CUC incorporates the concepts of partitions and search spaces in a similar way to CUCM. Objects that can receive calls, such as a user mailbox or call handler, are assigned a partition; objects that can place or transfer calls are assigned a search space. The object being called must be in one of the partitions listed in the search space of the object making the call. A default search space, containing the default partition, allows all objects to reach all other objects until the administrator customizes the system as needed.

Using this mechanism, it is possible to create a directory handler for the Vancouver office and limit the search space of the directory handler to include only the Vancouver partition. In this way, searching the Vancouver directory would list only users assigned to the Vancouver partition.

Note that the partitions and search spaces used in the CUC application are in no way related to those configured in the CUCM application; they are not linked, replicated, or related in any way.

Describe Cisco Unity Connection Users and Mailboxes

The system components identified previously are important, but without users and mailboxes, system functionality would be pretty boring. The following sections outline the basics of adding users and mailboxes to the system.

User Templates

User templates, as the name implies, provide a pattern used in the creation of new user accounts. Most of the required configuration information common to all the new users can be entered in the template, and then the individual user-specific information is combined with the template to create (potentially many) new user accounts with speed and accuracy. The template settings are applied as the user is created; changing the template does not retroactively change the user accounts that were created using that template.

Two default user templates are created at install: one for administrators and one for users. These can be modified if desired, and as many custom templates as needed can be created.

The following sections highlight some of the settings on the user template pages (of which there are many, so not all settings are discussed).

User Template Basics

The basic elements of user template configuration are summarized in the following sections:

- **Name:** The name of the template, such as Managers. The alias and display name generation for user accounts can also be specified; the default is first name followed by last name.
- **Phone:** In this section, the dial plan (partition/search space), class of service (CoS), and schedule are defined.
- **Location:** Geographic location information, language localization, and time zone are set here.

Key Topic

Key Point CoS in CUC (not to be confused with Layer 2 quality of service [QoS] marking or CUCM class of control) is a simple and powerful method of assigning and restricting user privilege. The CoS defines greeting and message length timers, licensed feature access, advanced feature access, alternate extension definition, private DL number, membership limits, and call transfer abilities.

An unlimited number of CoS can be defined, providing exactly the combination of abilities and features for as many sets of users as needed.

Figure 13-4 illustrates the basic components of a CoS.

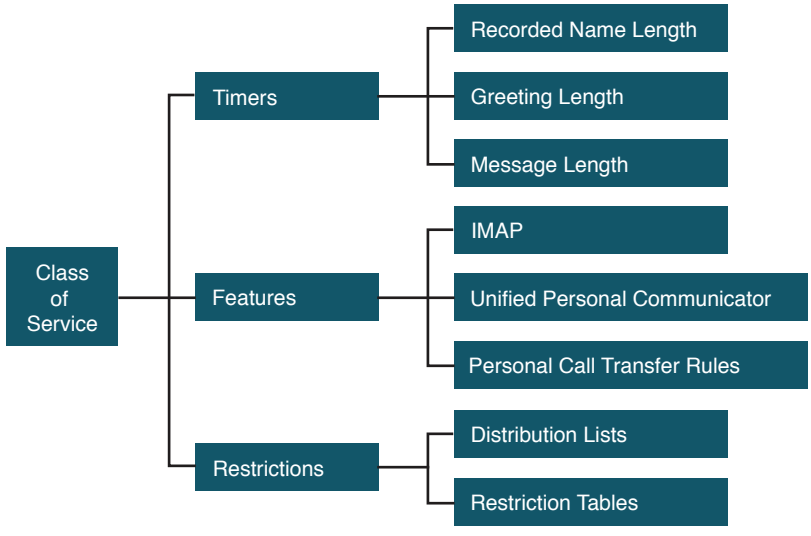


Figure 13-4 *CoS Components*

Password Settings

On this page, the administrator can lock and unlock the account, control when and if the password must be changed, and set the authentication rule. All these can be set for both the voicemail password and the web application password.

Roles

Roles define one of the default administrative capability assignments, as described in Table 13-2.

Transfer Rules and Greetings

Three transfer rules are defined by default. The standard rule cannot be modified and is active by default. The alternate rule can be modified to be active according to a different schedule or a specific end date. The closed rule takes effect during defined closed hours.

These rules are applied to determine the behavior of the user's mailbox, including which greeting is played to callers. The available greetings are the following:

- **Alternate:** Used for personalization of the voicemail box with a custom greeting
- **Busy:** Plays when the user's extension is busy
- **Error:** Plays when the user or caller enters an invalid choice
- **Internal:** Plays only to internal (On-Net) callers
- **Closed:** Plays when the closed schedule is in effect
- **Standard:** Plays the default <*username*> is not available" greeting
- **Holiday:** Plays when the Holiday schedule is in effect

Call Actions

The administrator can select what action the system takes after the greeting has played. Typically, Take Message would be selected, but hang up and Restart Greeting are available options.

Other call actions include sending the call to any configured call handler or to a user mailbox.

Message Settings, Message Actions, and Caller Input

When the caller leaves a message, he can be allowed to edit it or not, allowed to mark it as urgent, or have the system set all messages as urgent or normal. Messages can also be marked as secure, which can be used to limit where the message can be delivered. (For example, a secure message can be restricted from delivery to an IMAP client.)

After the message has been left, the administrator can set what action the system takes, with the default being say goodbye and hang up. Other options include sending the caller to any configured call handler or to a user mailbox.

During the conversation with CUC, the caller may be allowed to press a key to perform a configured action (such as logging in to the greetings administrator TUI). The default key presses are zero (0) for the operator and asterisk (*) to log in to the mailbox.

TUI Settings

The TUI user experience can be customized to speed up or slow down the conversation with CUC, make it louder or quieter, change how long the system will wait for key presses, and customize the order of playback of different message types, among others.

CUC End Users

Creating a new end user requires very few configuration parameters because most of the hundreds of user configuration settings are pulled from the user template chosen as we create the user. The unique individual settings that must be explicitly configured include the alias (the unique user ID), name, mailbox store, extension, and alternate extensions.

Extension and Call Forward Options

Key Topic

The extension number is a required entry. This number should be the primary DN on the user's IP phone; when she presses the Messages button, it is the caller ID that CUC uses to determine whether she is a mailbox owner, and if so, prompts her to log in. Likewise, if a call to a user's phone is forwarded to CUC because the user was on the phone or did not answer, CUC uses the caller ID to determine which mailbox greeting to play to the caller.

The call forward options on the IP phone (discussed earlier in this book) can change the behavior of CUC; for example, a different greeting can be played for internal versus external callers.

Voice Messaging with SRST and AAR

In the event that calling over the IP WAN is not possible due to WAN failure or congestion, calls can be rerouted over the PSTN. If the CUC server is normally reached over the WAN from by branch user, in the event of an outage, these systems reroute the call to CUC over the PSTN, too. When the call arrives at CUC, the 10-digit PSTN caller ID will not be recognized as a mailbox owner unless it is added as an alternate extension for the user. (The same goes for each other user on the system as well.)

Voicemail Box

When creating the user mailboxes, the administrator can choose whether to list the user in the directory or not, record the voice name (the spoken version of the username; CUC speaks the name in the configuration page if the name is not recorded), and record a greeting. The administrator can also require the user to go through these steps at his next login.

Private Distribution Lists

Each user is permitted to create up to 99 private DLs, each with a maximum of 999 members. Lower limits can be set in the CoS or individually per user. Private DLs are visible only to the user who created them (and to administrators).

Notification Devices

In addition to the MWI lamp on the IP phone, users can be notified of new messages by way of up to three PSTN numbers (mobile phone, home phone, and pager) and email. Toll call control is handled by restriction tables that define what numbers CUC can call for message notification. When CUC calls the configured number, it informs the user that there is a new voice message and prompts the user to authenticate before playing the message.

User Creation Options

Key Topic

There are several ways to create or import user accounts into CUC:

- **Manual creation:** Creates users one at a time. All user data is maintained locally in the CUC database.
- **Bulk administration:** Creates many users at once from data in a CSV file. All user data is maintained locally in the CUC database.

- **Migration from Cisco Unity:** Users can be migrated and imported using the Consolidated Object Backup and Restore Application Suite (COBRAS) tool. COBRAS helps administrators migrate users from a Windows server-based Cisco Unity system to a Cisco Unity Connection system. The users can be imported with or without their mailboxes.
- **Import from CUCM via AXL:** Synchronizes the CUC user database with an existing CUCM database. Some user data is maintained in CUCM and copied to CUC, but CUC-specific data is locally maintained in the CUC database.
- **Import from LDAP:** Synchronizes the CUC user database with an existing LDAP user database. Some user data is maintained in LDAP and copied to CUC, but CUC-specific data is locally maintained in the CUC database. Optionally, web password authentication can be redirected to LDAP to provide a single point of administration and single sign-on for user passwords.

CUC Voicemail Boxes

A voicemail box is typically associated with each user (one per user in most scenarios). The mailbox is held in a database store that may be synchronized between two CUC servers in an active-active redundant pair. The user mailbox may be moved to another store if necessary.

Message Aging Policy and Mailbox Quotas

To control disk space utilization by voicemail box storage, administrators can set message aging policies that move read messages to the Deleted Items folder after a specified number of days (disabled by default). Messages in the Deleted Items folder are automatically permanently deleted after 15 days by default (configurable).

User storage quotas can be configured to warn users when their mailbox nears the maximum allowed size (warning at 11 MB by default). Users are prevented from sending new messages when their mailbox reaches 12 MB (configurable to any appropriate value), and they cannot send or receive messages if their mailbox reaches 14 MB by default (also configurable).

12 MB of disk space is approximately 200 minutes of recorded messages using the G.729 codec and about 25 minutes using G.711.

Implement Cisco Unity Connection Users and Mailboxes

In the following sections, the concepts introduced previously are put into action. What follows are the basics of implementation of users and mailboxes in CUC. There are, of course, many other possible steps that are not included here, both for clarity and to stay within the scope of the CICD exam.

Configure End User Templates

Templates are a powerful and useful way to speed up and simplify the creation of users. You may modify an existing template or create a new one to meet requirements. Although many configurations are available, the CICD course is limited in scope and examines primarily the following Edit menu entries:

- User Template Basics
- Password Settings
- Roles
- Message Settings and Actions
- Phone Menu
- Playback Settings
- Message Notification

Remember that all the following sections reference editing a user template and consequently will set configurations for all user accounts created with the template. Some settings obviously need to be unique per user and can either be included as part of the user creation steps or configured after the accounts are created. You can create as many user templates as you need. To begin, navigate to **Templates > User Templates** and select an existing template (or create a new one).

User Template Basics

The following points review most of the elements found on the User Template Basics screen. You may or may not need to change them all; each template will be at least slightly different in your environment:

- **Alias:** This is a required field; in this case, it is the name of the template itself.
- **Display Name:** This is a required field; this is the template name as it appears in the Find/List Templates page.
- **Display Name Generation:** Choose one of First Name, then Last Name or Last Name, then First Name.
- **Outgoing Fax Server:** Select the correct fax server for the users, if any.
- **Partition:** Select the appropriate partition for the users.
- **Search Scope:** Select the appropriate search scope (search space) for the users.
- **Phone System:** Select the phone system for the users. Most deployments will have only one available, but CUC supports multiple integrations so this setting can be important.
- **Class of Service:** The CoS controls what features and capabilities the users can access.
- **Active Schedule:** Select the schedule that will be applied to the users. Schedules can be used to affect when the standard or closed greetings play, as well as what after-greeting actions CUC takes.
- **Set for Self-Enrollment at Next Login:** Check this box to force the user to go through the tutorial and record his voice name and greetings the next time he logs in to CUC.
- **List in Directory:** Select this check box to list the users in the CUC directory; doing so allows outside callers to search for, find, and then call users.
- **Time Zone:** Select **Use System Default Time Zone** or choose the appropriate time zone for the users. Select the time zone with care because it will modify CUC behavior for displaying the time a message was received and for message notification.
- **Language:** Set the language that CUC uses to play instructions to users and for text-to-speech. This setting does not apply to the voice recognition conversation.

Figure 13-5 shows part of the User Template Basics page.

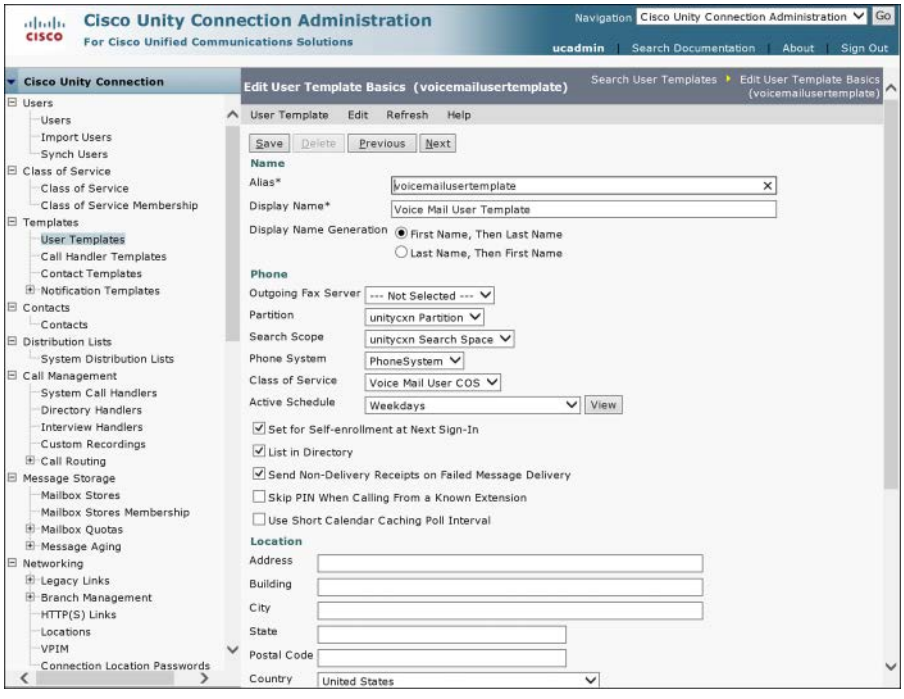


Figure 13-5 *User Templates Basics Page*

Password Settings

CUC uses two separate passwords for each user: The web application password is used for logins to CUC web pages (including the user web pages, and administration pages if the user has the privilege to access them); the voicemail password is actually the PIN, which is used for TUI logins. To begin, select which password you want to configure. On the page that opens, select or modify the following options:

- **Locked by Administrator:** Select this if you want to prevent the user from logging in to CUC.
- **User Cannot Change:** Select this to prevent the user from changing his password. This is recommended if more than one user will access the voicemail box; it is also recommended in this case to select the Does Not Expire check box.
- **User Must Change at Next Login:** Select this to force the user to change his password the next time he logs in to CUC.
- **Authentication Rule:** Set the Authentication Rule that will be applied to the user account's password.

Figure 13-6 shows the Password Settings page.

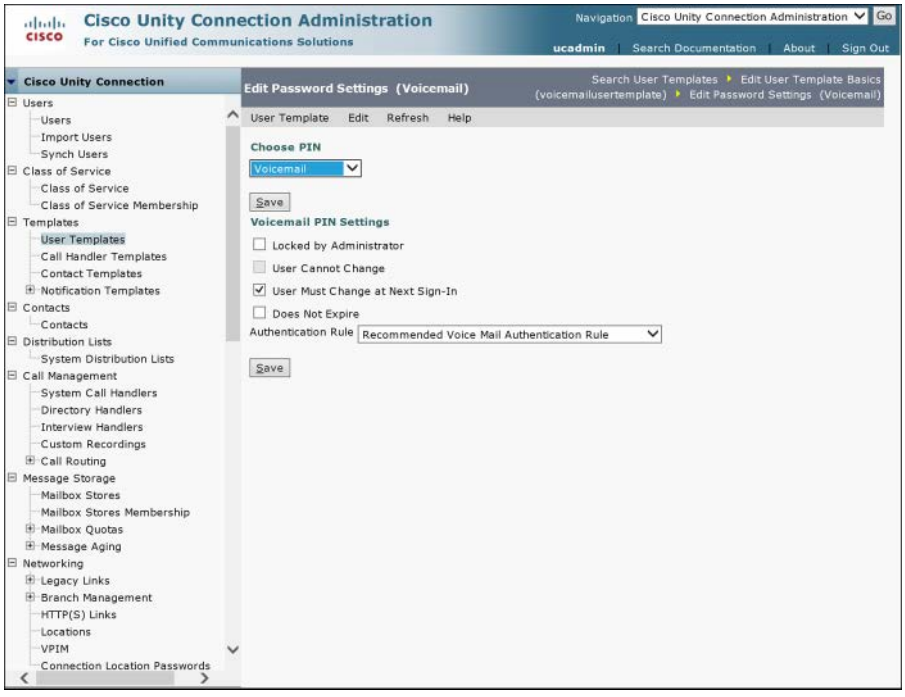


Figure 13-6 *User Template: Password Settings*

Roles

By default, no roles are selected for user accounts. Assign the appropriate roles, if these users need administrative privilege. Table 13-2 described the role functions.

Message Settings

On the Message Settings page, you can select or modify the following as appropriate for your environment:

- **Maximum Message Length:** Limits how long a single message can be. (The default is 300 seconds.)
- **Callers Can Edit Messages:** Select to prompt users to listen to, add to, re-record, or delete a message they have just left.
- **Language That Callers Hear:** Choose one of the installed languages. This setting affects the language of system recordings, such as "Record your message at the tone." If Inherit Language from Caller is selected, when an IP phone calls, the user locale setting (in CUCM) of that phone determines what language will be used (as long as that language is installed on CUC).

- **Message Urgency:** Messages left by callers can all be set to Normal or Urgent, or the system can be set to Ask Callers, giving them the choice. By default, when a user logs in to his mailbox, CUC plays messages marked urgent first. Some organizations use this behavior to improve customer service, by forcing all outside callers' messages to be marked urgent. Setting the Unidentified Callers Message Urgency here (in the User Template) will apply the chosen setting to all users created with this template; you can override this setting at the individual user's account under the Message Settings menu.

Figure 13-7 shows part of the Message Settings page.

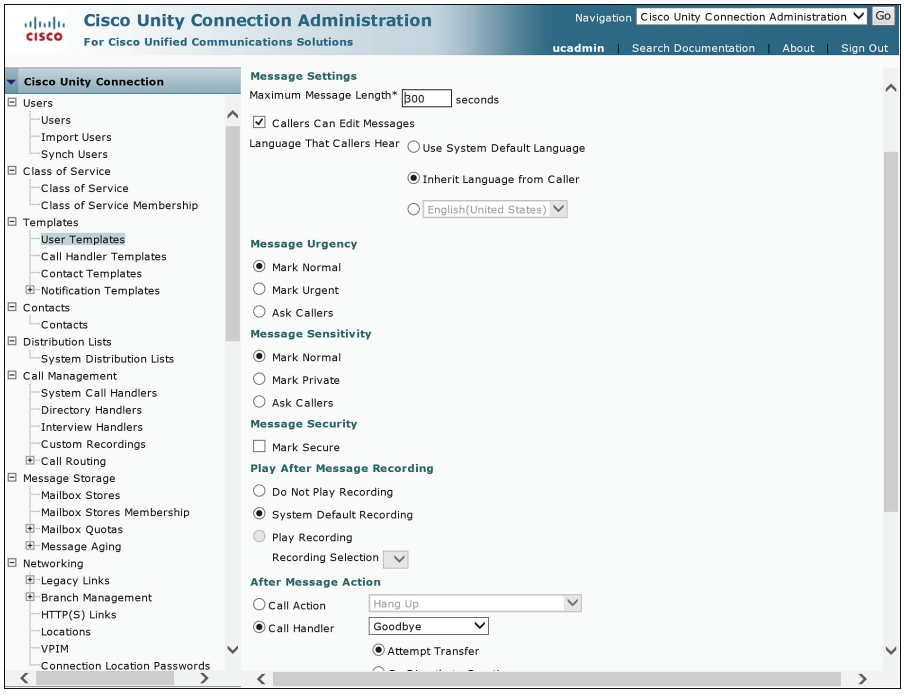


Figure 13-7 *User Template: Message Settings*

Message Actions

For each type of message (voicemail, email, fax, and delivery receipt), set the action CUC will take: accept, reject, relay, or accept and relay.

Figure 13-8 shows the Message Actions page.

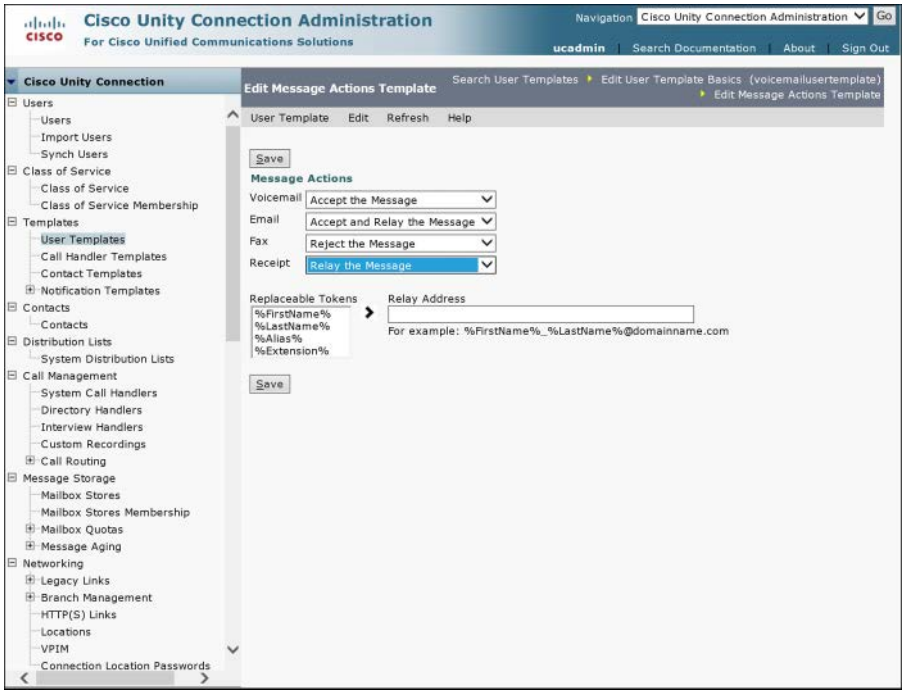


Figure 13-8 *IDS and IPS Operational Differences*

Phone Menu

Under the Phone menu, you can select or modify the following settings (plus others not shown):

- **Touchtone Conversation Menu Style:** Select **Full** to have CUC play detailed instructions for callers or **Brief** for shorter, less-detailed instructions.
- **Conversation Volume:** Adjusts the loudness of CUC conversations.
- **Conversation Speed:** Adjusts the playback speed of CUC conversations.
- **Time Format:** Specify 12-Hour or 24-hour clock to change how CUC expresses the time in conversations with the caller.
- **Use Voice Recognition Input Style:** When selected, CUC uses voice recognition in conversation with the caller, unless voice-recognition resources are unavailable; in which case, CUC reverts to touchtone style. This selection will not be visible if the class of service does not permit the voice recognition feature.
- **Touchtone Conversation Style:** Select the keypad emulation (to make the key press functions the same as other voice-messaging systems); this is normally done if you want to provide a smoother transition for users from a legacy voice-messaging system to CUC.
- **Enable Message Locator:** Enables users to search messages by user name, extension, or caller ID.

Figure 13-9 shows part of the Phone Menu page.

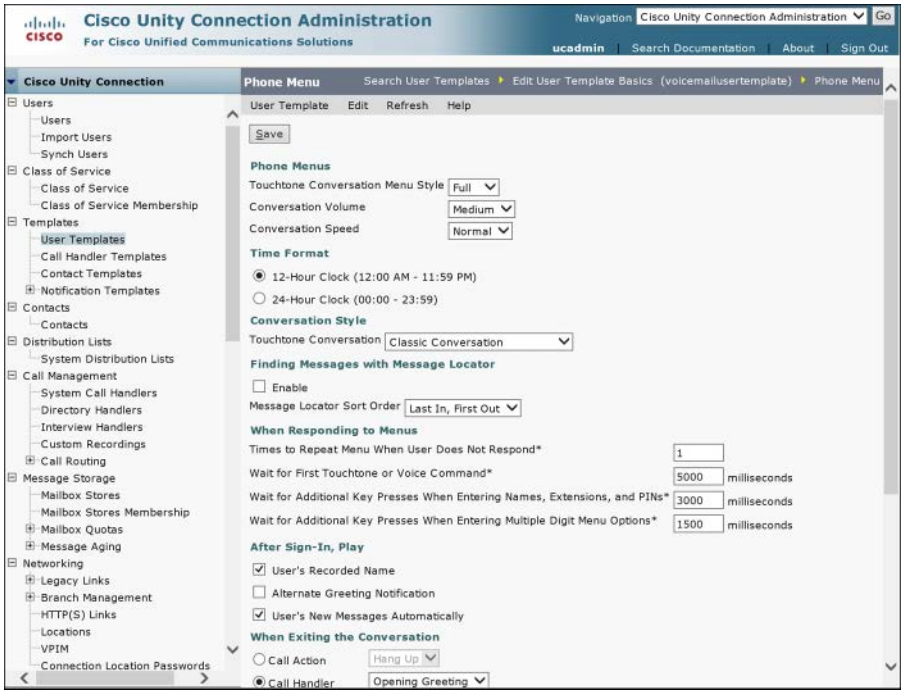


Figure 13-9 *User Template: Phone Menu*

Playback Message Settings

Under the Playback Message Settings menu, you can select or modify the following settings:

- **Message Volume:** Sets the volume for message playback.
- **Message Speed:** Sets the speed at which messages are played back.
- **For New Messages, Play:** Check each box as desired to hear message counts for totals (all new messages), emails, faxes, and receipts.
- **For Saved Messages, Play:** Check this box to have CUC announce the number of saved messages.
- **Before Playing Messages, Play:** Check the **Message Type Menu** box to hear a menu of key press options to hear messages of each type.
- **New Message Play Order and Saved Message Play Order:** Use this set of preference lists to set the order in which CUC plays messages to the users. To hear emails and faxes, the user must be assigned a CoS that has the Access to Email in Third-Party Message Stores and Fax features enabled. If there are fax messages, CUC announces just the sender, date, and time. (It does not read the fax body.)
- **Before Playing Each Message, Play:** Check each box as desired to hear any (or all) of the following:
  - **Sender's Information:** Recorded name or ANI for internal callers; ANI for outside callers is not played.

- **Include Extension:** In conjunction with the Sender's Information check box, selecting this check box causes CUC to play the extension of an internal caller and the recorded name (if available).
- **Message Number:** CUC announces the sequential number of messages in the mailbox as it plays them.

- **Time the Message Was Sent:** CUC plays the timestamp of each message.
- **Sender's ANI:** CUC plays the ANI for outside caller messages.

Message Duration: CUC announces the length of each message.

Figure 13-10 shows part of the Playback Message Settings page.

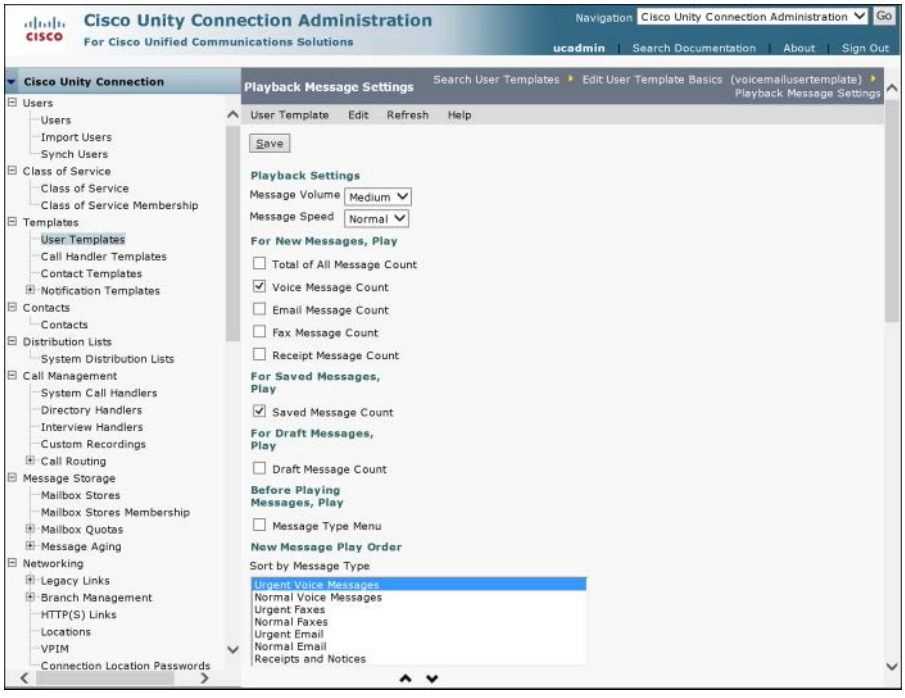


Figure 13-10 *User Template: Playback Message Settings*

Notification Devices

Message notification should not be confused with MWI; notification refers to CUC making a phone call or sending an email to advise a user that he has a new message. CUC supports notification on a pager, work phone, home phone, and mobile phone and via SMTP by default. Additional notification devices may be added.

For each device, set the following as needed:

- **Enable:** Check this box to allow CUC to send notifications to this device.
- **Display Name:** Modifies the name as needed.
- **Delay Before First Notification Event:** Sets the number of minutes CUC waits after a new message is left before it sends a notification using this device.

- **Notification Repeat Interval:** Sets how frequently CUC resends the notification.
- **Notify Me Of:** Select the check boxes to have CUC send notifications for **All Messages**, **All Voice Messages**, **Fax Messages**, **Calendar Appointments**, **Calendar Meetings**, and for each type, whether to send for **Urgent Only**.
- **Pager/Phone Settings:** Sets the phone number CUC should call. Modify the extra settings to add extra digits, wait times, and so on to ensure the call completes correctly. All these settings should be applied at the individual user account rather than at the template.

Configure CUC End Users

Adding users to CUC can be done manually (one at a time), via import from CUCM using AXL, via LDAP, or by using the Bulk Administration Tool (BAT). In each case, the goal is to provide individually specific information per user to complete the common information provided by the user templates previously configured.

In the following sections, some possible configuration steps have been omitted in the interest of relevancy to CICD.

Manual Process

To manually create a new user, navigate to **Users > Users** and create a new user. Select the appropriate user type (typically **User with Mailbox**), and select or enter the following:

Step 1. From the Based on Template drop-down, select the appropriate user template for this user to supply the common configurations.

Step 2. Add the alias (which must be unique), first name, last name, and display name.

Step 3. Choose the appropriate mailbox store, if there is more than one in use.

Step 4. Add the extension of the user, which is typically the primary DN associated with his IP phone.

Step 5. Click **Save**.

Figure 13-11 shows part of the Edit User Basics page.

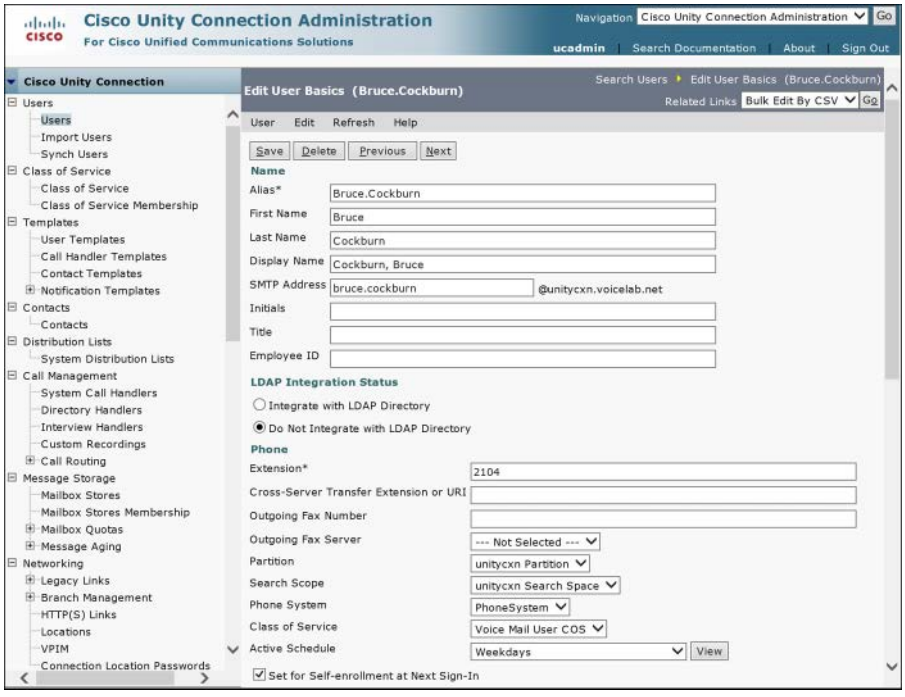


Figure 13-11 *User Configuration Basics*

Alternate Extensions and Names

An alternate extension can be provided to users to allow them to call in to CUC from a number other than their primary extension and gain access to their mailbox without having to go through the opening greeting. The following steps outline the configuration of alternate extensions:

Step 1. On the User Configuration page, from the Edit menu, select **Alternate Extensions** and click **Add New**.

Step 2. Set the type of phone from the drop-down (**Work**, **Home**, **Mobile**).

Step 3. Provide a display name.

Step 4. Set the correct phone number. This is the caller ID (ANI) number of the phone as it will appear to CUC; typically, this is the full PSTN number, but be aware of the possibility that CUCM may be stripping or modifying digits before they are sent to CUC.

Figure 13-12 shows the Alternate Extension page.

Step 5. From the Edit menu, select **Alternate Names**.

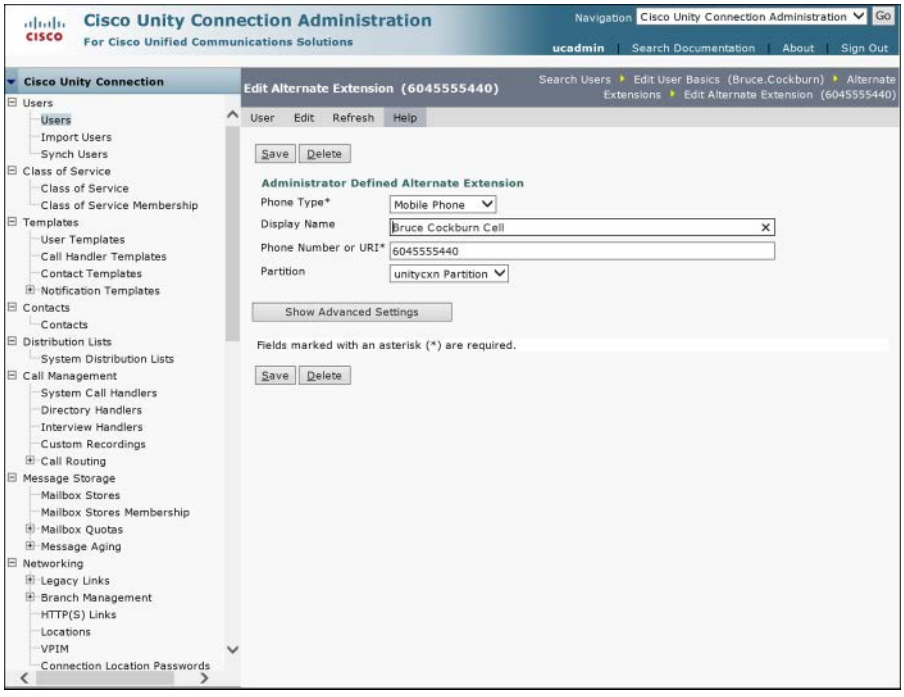


Figure 13-12 *User Configuration: Alternate Extensions*

An alternate name allows the administrator to define nicknames, familiar names, or phonetic name spellings to allow callers to search for users by a name other than the entry in their user page main configuration. For example, if Jedediah is the first name entry but callers search for J.D. because that is his nickname, the administrator can add the alternate name of J.D., or even Jaydee if voice recognition is in use.

Private DLs

The administrator can add private DLs on behalf of the user, or the user can add them from his Personal Communications Assistant (PCA) web pages. (Note that the administrator interface also opens the PCA, logged in as the user.) Each list (up to 99 can be created) needs a unique name and can contain up to 999 members. These maximums can be limited in the CoS.

Figure 13-13 shows the PCA view of private lists.

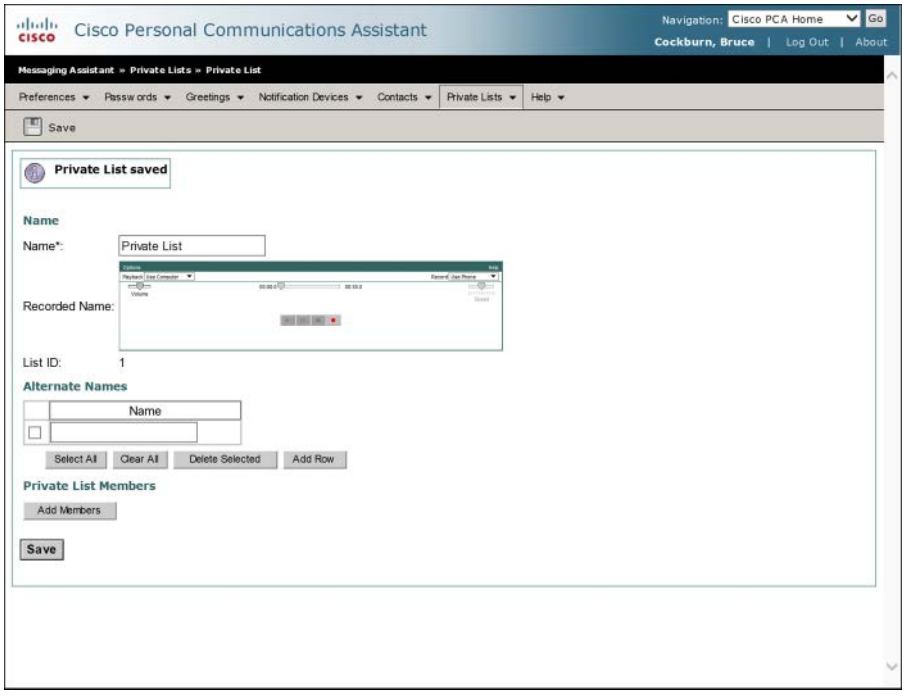


Figure 13-13 *PCA: Private Lists*

Importing End Users into CUC

Key Topic

Performing a user import is one of the quickest and simplest ways to create user accounts in CUC. By using fully configured user templates, the work of creating users is much faster and more accurate. Depending on the implementation, there may be an added benefit if the user accounts are synchronized with another system, which reduces the replication of administrative tasks associated with user maintenance.

Importing Users from CUCM

If the CUCM server already has a fully populated user database, those entries may be easily imported and synchronized in the CUC database. To enable this capability, perform the following actions on CUCM server:

Step 1. From the Cisco Unified Serviceability interface, under the Tools menu, select **Service Activation**.

Step 2. Select the Cisco AXL Web Service and click **Save**.

Step 3. In Cisco Unity Connection Administration, navigate to **Telephony Integrations > Phone System**.

Step 4. Click the name of the CUCM server from which you want to import users.

Step 5. Under the Edit menu, click Cisco **Unified Communications Manager AXL Servers**.

Step 6. On the Edit AXL Servers page, under AXL Server Settings, enter the username and password of the account that CUC will use to log in to the CUCM AXL server.

Step 7. Click **Save**.

Step 8. In the AXL Servers section, click **Add New**.

Step 9. Enter the IP address and port of the CUCM server. (CUCM 8.x supports SSL, so use port 8443 or 443.)

Step 10. Click the **Test** button. "Test message successfully sent to AXL server <*ip_address:Port*>" appears in the Status section.

Step 11. Click **Save** to complete the integration.

Figure 13-14 shows the Edit AXL Servers page with a successful test message.

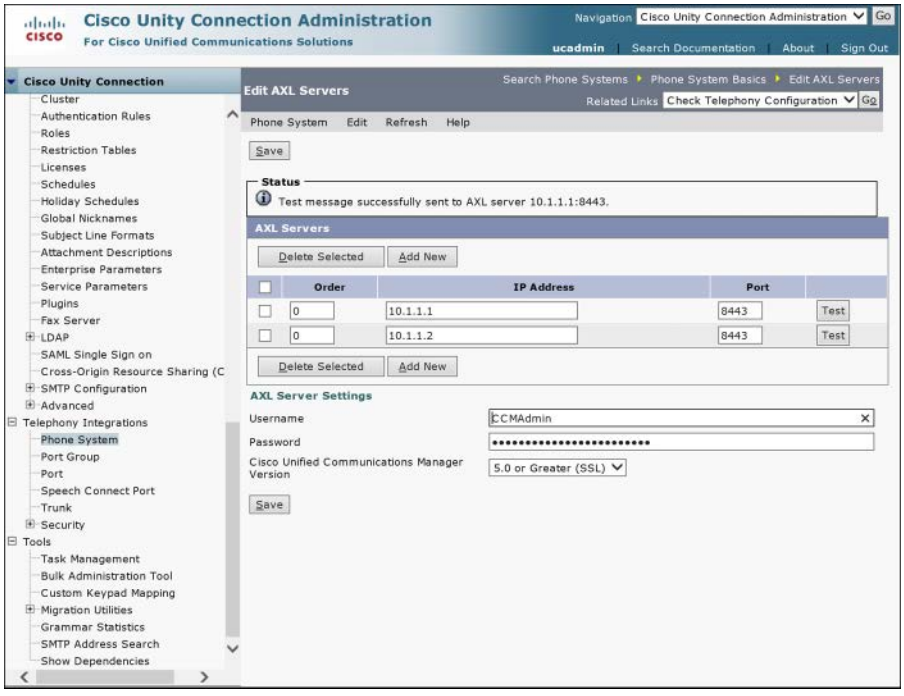


Figure 13-14 *AXL Server Edit Page: Successful Test*

Now that we know AXL is working properly, we can use it to import users, as outlined in the following steps:

Step 1. On the CUC server, from the Cisco Unity Connection Administration interface, navigate to **Users > Import Users**.

Step 2. Select the CUCM server from the Find End Users In drop-down. Filter the search if needed.

Step 3. Choose the appropriate user template from the Based on Template drop-down.

Step 4. Click **Find**.

Step 5. Select the users to import from the list, and then click **Import Selected**.

Note CUCM users must have a primary extension defined; otherwise, the users will not appear on the Import Users page in CUC.

Figure 13-15 shows an import of users from the CUCM AXL server.

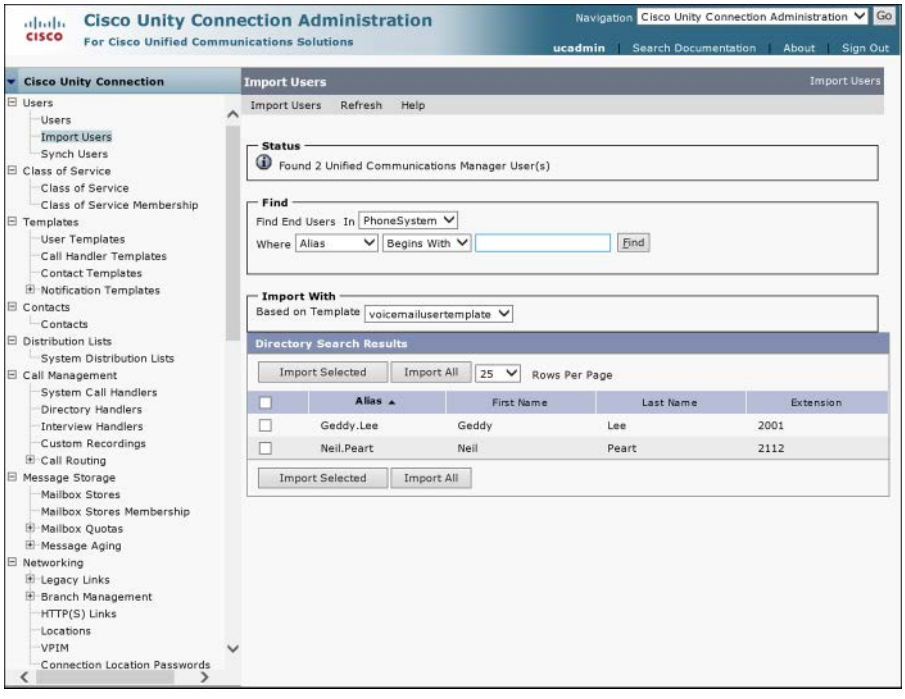


Figure 13-15 *User Import from CUCM Using AXL*

Importing Users from LDAP

Key Topic

LDAP is a standards-based user, password, and privilege database system. Multiple other applications can access a LDAP directory to determine if a particular username and password are valid and have access privileges to a particular resource.

CUC can import users from a number of different vendors' implementations of LDAP. These user accounts are held and maintained in the LDAP system, with certain fields (attributes) copied as read-only entries to the CUC database. User authentication can be optionally redirected from the local CUC database to the LDAP system as well.

To enable LDAP synchronization, follow these steps:

Step 1. In the CUC Cisco Unified Serviceability interface, navigate to **Tools > Services**.

Step 2. Select the **DirSync** service and click **Save**.

Step 3. In the CUC Administration interface, navigate to **System Settings > LDAP > LDAP Setup**.

Step 4. Check the **Enable Synchronizing from LDAP Server** check box.

Step 5. Choose the **LDAP Server Type** from the drop-down.

Step 6. In the LDAP Attribute for User ID drop-down, select the LDAP attribute that will be mapped to the CUC alias attribute. The selected attribute in LDAP must contain data, and the data must be unique. User accounts without data in the selected attribute will not be imported.

Step 7. Navigate to **LDAP > LDAP Directory Configuration**.

Step 8. Enter an LDAP configuration name. It is recommended to use a name that identifies the users are being imported, especially if multiple user search bases are configured.

Step 9. Enter the LDAP manager distinguished name and LDAP password. This is the LDAP account and password that CUC uses to read and import the LDAP database.

Step 10. Enter the LDAP user search base. This entry defines the point at which CUC will begin reading the LDAP database. Most LDAP designs are hierarchical tree structures; CUC starts the LDAP search at the point in the tree specified by the user search base and can read down all branches of the tree. It cannot move up the tree from that point, nor can it cross to other branches. CUC can only integrate with a single LDAP database. If the administrator does not know the LDAP design or the correct syntax for the user search base, he should contact the LDAP administrator to confirm what should be entered. An example search base is cn=Users, DC=cisco, DC=com.

Step 11. In the LDAP Directory Synchronization Schedule section, choose **Perform Sync Just Once** if you do not want to have CUC perform a regular sync. Choosing this option causes CUC to only refresh and update current user information; it will not import any new users created since the agreement was last synchronized. A new user import must be performed to create those users in CUC.

Step 12. To have CUC synchronize on a regular scheduled basis, set the **Perform a Re-Sync Every** *interval* as desired.

Step 13. To configure the mappings between LDAP attributes and CUC user database attributes, set the desired values in the User Fields to Be Synchronized section. Different fields will be changeable, with different field names listed depending on the LDAP type/vendor selected.

Figure 13-16 shows part of the LDAP Directory Configuration page.

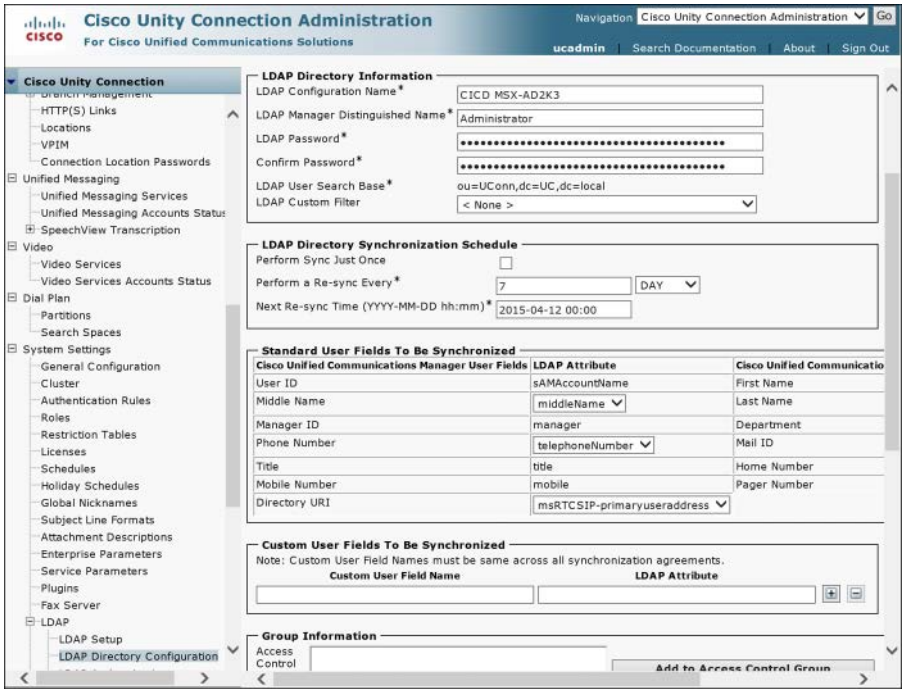


Figure 13-16 *LDAP Directory Configuration Page*

Bulk Administration Import of CUC Users

Key Topic

Importing users using the Bulk Administration Tool is a fast and easy way to create multiple accounts if the required user information can be formatted as a CSV file. To bulk import users, follow these steps:

Step 1. Navigate to **Tools > Bulk Administration Tool**.

Step 2. Under Select Operation, select **Create**. (Note that you can also select Update, Delete, or Export.)

Step 3. Under Select Object Type, choose **Users With Mailbox**.

Step 4. Under Override CSV Fields When Creating User Accounts, select **User Template Yes** and select the desired User Template.

Step 5. Under Select File, browse to the CSV file that contains the user import information.

Step 6. Specify a failed objects filename.

Step 7. Click **Submit**.

Note The formatting of the CSV is critical to the success of the import. The easiest way to get a correctly formatted file is to perform a BAT export of a single user. The CSV file then has all the necessary information you need to create the import file correctly. This is different from the CUCM BAT tool, which includes an Excel template file for download with macros to help to create the file.

Figure 13-17 shows the BAT page set up for user import.

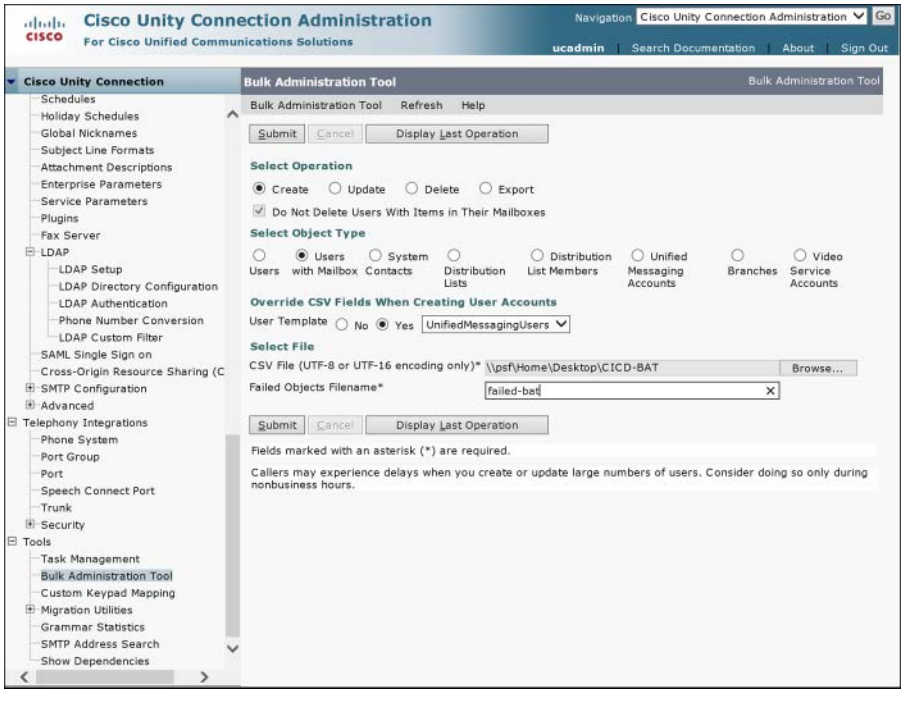


Figure 13-17 *BAT: User Import*

Managing the CUC Message Store

The size and some details of the mailbox store can be checked by navigating to **Message Storage > Mailbox Stores** and selecting the store you want to check. The display page provides information on the size of the store, the number of mailboxes, and when it was created. It also allows you to set the maximum size before warning value to determine when CUC begins sending warnings about the store size. (When 90 percent of the configured value is reached, warnings are logged; at 100 percent, errors are logged.)

Figure 13-18 shows the Edit Mailbox Store page.

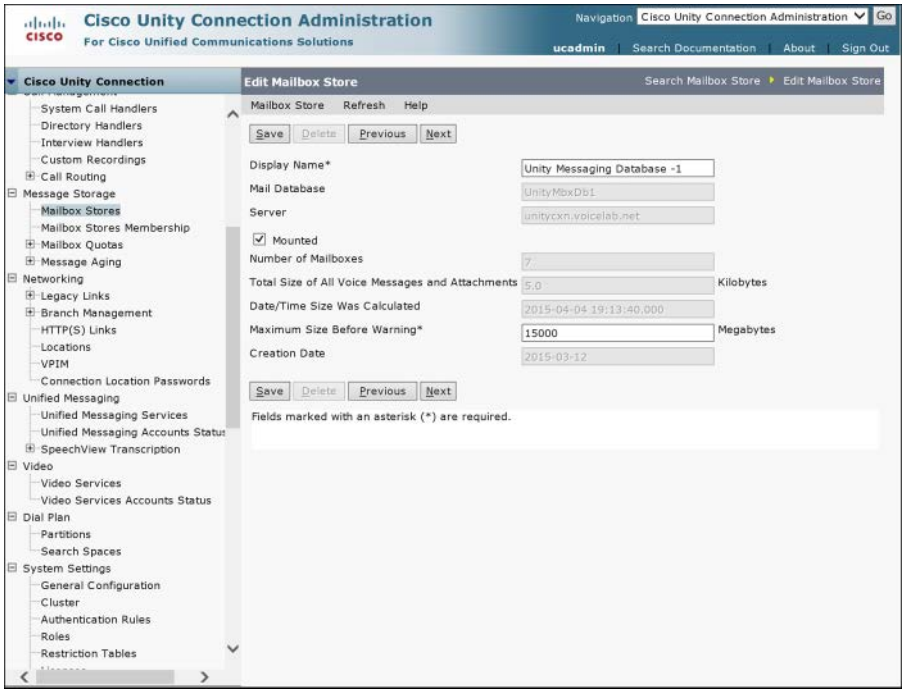


Figure 13-18 *Edit Mailbox Store Page*

Mailbox Stores Membership

Additional message stores can be created if additional space is required. Users can be easily moved to the new store by navigating to **Message Storage > Mailbox Stores Membership**.

Select the user(s) you want to move, select the database to move them to, and click **Move Selected Mailboxes**.

Message Aging Policy

The default message aging policy deletes items in the Deleted Items folder after 15 days. To modify the policy, navigate to **Message Storage > Message Aging Policy**, and then select **Default System Policy**. (Note that you may create custom aging policies if you want.) You may disable the policy by deselecting the **Enabled** check box; the default is enabled. You may also choose to modify the following:

- Under the Message Aging Rules Based on When the Message Was Last Modified heading, you may select whether to move new messages to the Saved folder, saved messages to the Deleted Items folder, and after how many days for each.
- Under the Secure Message Aging Rules Based on When the Message Was Created heading, you may choose to permanently delete secure touched messages or all secure messages that reach a specified age.

Figure 13-19 shows the Message Aging Policy page for the default system policy.

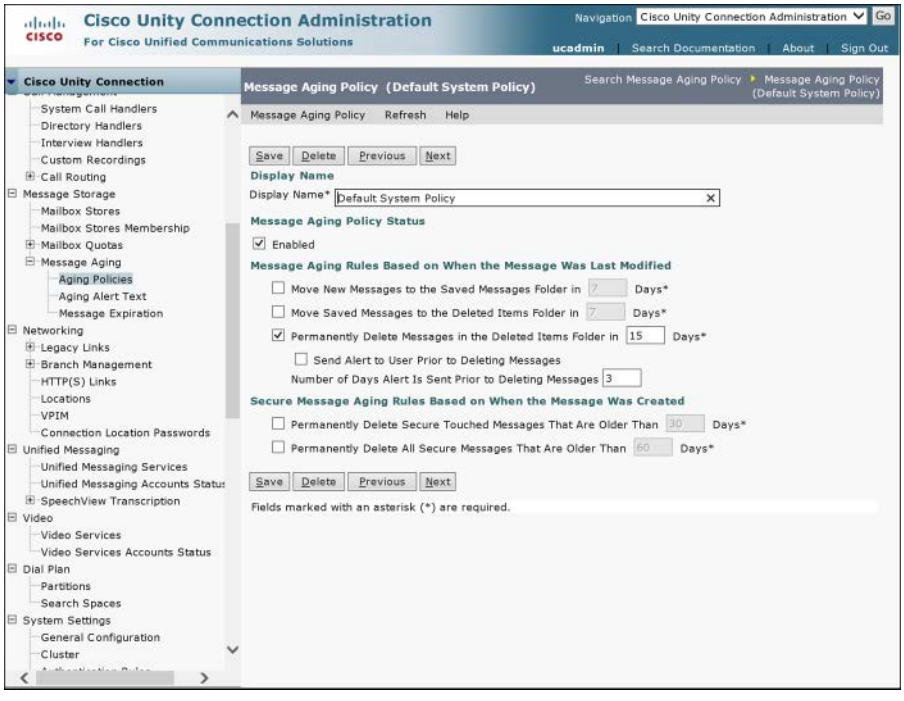


Figure 13-19 *Message Aging Policy Page*

Mailbox Quotas

Setting strict mailbox size limits early in the deployment is a good idea. To begin, navigate to **Message Storage > Mailbox Quotas.** Here, you can change the system-wide mailbox quotas, including the warning, send, and send/receive thresholds. These quotas may be overridden in the user template or individually per user.

Figure 13-20 shows the System-Wide Mailbox Quotas page.

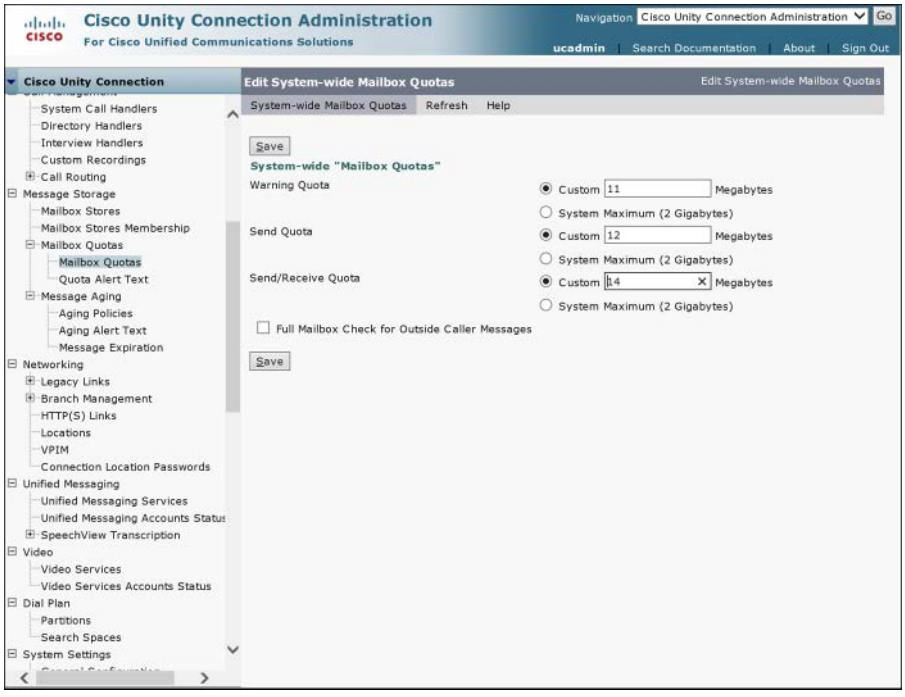


Figure 13-20 *System-Wide Mailbox Quotas Page*

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 13-3 describes these key topics and identifies the page number on which each is found.

Key Topic

Table 13-3 Voicemail Integration with Cisco Unity Connection Key Topics

Key Topic Element	Description	Page Number
Paragraph	CUC integration with CUCM using SCCP	347
Paragraph	Call routing	351
Key Point Box	CoS in CUC	354
Paragraph	Extension and call forward options	356
Paragraph	User creation options	356
Paragraph	Configure CUC end users	365
Paragraph	Importing end users in to CUC	368
Paragraph	Importing users from LDAP	370
Paragraph	Bulk administration import of CUC users	372

Definitions of Key Terms

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

integration, call handler, class of service (CoS), Administrative Extensions for XML (AXL), call routing rules

This chapter covers the following topics:

- **Describe CM IM and Presence Features:** This section discusses the Cisco Jabber client, its features, operating modes, and protocol utilization. The basic capabilities of the Cisco Unified Communications Manager IP phone service and IP phone Messenger are also reviewed.
- **Describe Cisco CM IM and Presence Architecture:** This section identifies the protocols and interactions associated with CM-IMP integrations to other Unified Communications applications and features. Jabber client call flows in both deskphone and softphone mode are described, along with regulatory compliance and QoS considerations.
- **Enabling CM-IMP:** This section reviews the steps required to configure end users so that they can use the Jabber client in either deskphone control mode or softphone mode.

CHAPTER 14

Enabling CM IM and Presence Support

The Cisco Communications Manager IM and Presence Service (CM-IMP) extends the native Presence capabilities of Cisco Unified Communications Manager to include multiple communications methods and status settings, in addition to important enterprise features relating to compliance with legislation regarding retention of communications. This chapter introduces CM-IMP and briefly describes some of the implementation considerations in its deployment.

"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 14-1 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 14-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Describe CM-IMP Features	1–6
Describe CM-IMP Architecture and Call Flows	7–8

1. CM-IMP uses standards-based protocols for call control signaling and instant messaging chat. Which of the following are protocols used by CM-IMP for these purposes? (Choose two.)
   - **a.** SCCP
   - **b.** SSH
   - **c.** SIP/SIMPLE
   - **d.** XMPP
2. Which external communications and presence applications can CM-IMP interact with? (Choose all that apply.)
   - **a.** Cisco Unity Connection
   - **b.** Microsoft Exchange Server
   - **c.** Google Talk
   - **d.** Cisco Unified MeetingPlace
   - **e.** Cisco WebEx

3. Which of the following is not a capability of Jabber?
   a. Voice calling
   b. Video calling
   c. IM chat
   d. Visual voicemail
   e. Persistent Group Chat

4. Jabber can operate in two modes. What are they?
   a. SIMPLE Telephony User Node (STUN) mode
   b. Deskphone mode
   c. Autonomous mode
   d. Softphone mode

5. Which of the following is true of the Client Services Framework?
   a. It is a standards-based communication platform that enables cross-platform Presence signaling.
   b. It is a Windows Server software that enables features and functionality for Cisco Unified Communications.
   c. It is a core component of Jabber and enables integration with multiple call control, messaging, conference, IM, and directory services.
   d. Multiple CSF clients can be installed on a single workstation, enabling simultaneous cross-platform communications.

6. Group Chat is a feature of CM-IMP. If group chat rooms and discussions need to be available for future reference after all participants log off, which two steps are required?
   a. Obtain additional licenses for Persistent Chat.
   b. Install a WebEx server to record group chats.
   c. Install a third-party IM-retention compliance application on the CM-IMP server.
   d. Enable Persistent Chat on the CM-IMP server.
   e. Provision a PostgreSQL-compliant external database.

7. What components are required for Jabber to operate if the user is traveling with his laptop? (Choose three.)
   a. CSF registers as a SIP device with CUCM using SIP.
   b. User account associated with CSF device in CUCM.
   c. Jabber downloads config file from TFTP.
   d. Cisco IP Communicator must be installed on the client workstation.

8. How can calendar information in Microsoft Exchange be integrated into CM-IMP Presence signaling so that Free/Busy status in an Outlook calendar can be mapped to the Available/Away Presence status?
   a. Using WebDAV
   b. Using SIP/SIMPLE
   c. Using CTIQBE
   d. Using XMPP

Foundation Topics

Describe CM-IMP Features

CM-IMP extends the basic Presence capability of Cisco Unified Communications Manager (CUCM) (on-hook, off-hook, or unknown) to include advanced capability and availability signaling. The availability and capability of colleagues and business partners to communicate (Available, Busy, and Away status for various devices) is immediately visible and can be additionally enhanced using their calendar statuses. Enterprise instant message (IM) capability is available both within and extended beyond the enterprise to external contacts, including Group Chat; Persistent Chat; and compliance features, such as IM logging and IM history.

The primary goal of CM-IMP is to reduce communication delays by providing instant and useful information about the capability and availability of the person you are trying to contact. Users can indicate whether they are available, and by which methods, including desk phone, mobile phone, IM, or conferencing application. This signaling capability can be extended to existing applications to allow contact with the right individual to be quickly established. This helps resolve support or customer issues more quickly, eliminating phone tag and the delays associated with email exchanges.

Key Topic

CM-IMP is tightly integrated with CUCM, which provides call control and native Presence signaling (on-/off-hook status). CM-IMP itself provides a central collection point for user capabilities and status by way of standards-based signaling using Session Initiation Protocol (SIP), SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE), and Extensible Messaging and Presence Protocol (XMPP). A variety of client interfaces are available, including the Jabber client, which provides a rich and tightly integrated user experience.

Jabber

Jabber provides a single interface for the most commonly used Cisco Unified Communications tools. From the Jabber application, users can initiate voice calls (either through deskphone control or in softphone mode). Contacts are listed with their enhanced Presence status, providing click-to-communicate functionality by phone call, video call, chat, group, chat, and collaboration interaction with a simple interface to transition from one medium to another. Chat is enabled using the Jabber Extensible Communications Platform (XCP) using XMPP as the chat protocol.

Jabber Operating Modes

Key Topic

Jabber operates in two modes:

- **Deskphone mode:** Jabber can control the user's desk phone to place calls. The IP phone must be registered with CUCM and associated with the user. Jabber uses Computer Telephone Integration Quick Buffer Encoding (CTIQBE) for IP phone control. Figure 14-1 illustrates the protocol interaction when Jabber is in deskphone mode.

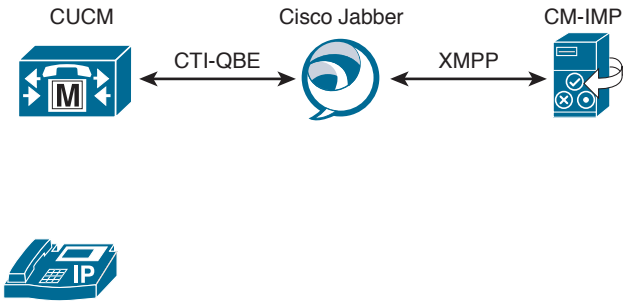


Figure 14-1 *Jabber in Deskphone Mode*

- **Softphone mode:** When the IP phone is not available or the user is away from his desk, Jabber activates the associated softphone based on the Cisco Unified Client Services Framework (CSF), which registers the softphone with CUCM as a SIP device (see Figure 14-2). The CUCM administrator must create the CSF device in order to enable this functionality.

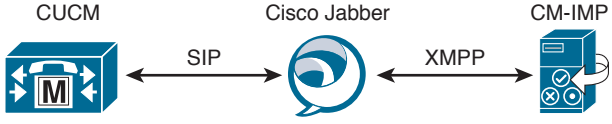


Figure 14-2 *Jabber in Softphone Mode*

Enterprise Instant Messaging

Key Topic

Jabber provides Transport Layer Security (TLS)-secured Chat and Group Chat capability. Ad hoc Group Chat sessions are stored in memory on the Jabber server. The Persistent Chat feature enables group chat rooms where the conversation persists even when all participants have left the chat session. If Persistent Chat is enabled, it requires an external database to store the chat rooms and conversations. Offline IM allows chat messages to be sent to users who are currently offline; these messages are stored in the local IDS database on the CM-IMP server.

The Jabber XCP message routing system has been modified in the CM-IMP implementation to improve functionality when users are available on multiple devices. Messages are routed to all the non-negative priority devices the user is logged into, instead of routing only to the highest-priority device. (Non-negative means devices that are not explicitly blocked from receiving messages.) CM-IMP delivers messages to all the logged-in devices for a user. (This behavior is called IM forking.) When the user replies on a particular device, subsequent messages are sent only to the device used for the reply. Backward compatibility for SIP-only Presence clients (such as Jabber 7.x) is provided via an IM gateway.

Voice Calls

Jabber supports voice calls in deskphone mode or softphone mode. Voice encryption using Secure Real-Time Protocol (SRTP) is supported. Survivable Remote Site Telephony (SRST) is supported in softphone mode with appropriate CUCM/CSF configuration. Jabber supports the following codecs in softphone mode:

- G.711 a-law, mu-law
- G.722, G.722.1
- G.729A

Codec support in deskphone mode depends on the IP phone model.

Video Calls

Jabber supports video calling in either deskphone or softphone mode. In deskphone mode, Jabber uses Cisco Audio Session Tunnel (CAST) and Cisco Discovery Protocol (CDP) for communication between the IP phone and the computer running Jabber. The desk phone must be enabled for video support in CUCM. 7900-series desk phones running SIP firmware are not supported by CAST and cannot be used for deskphone mode video calls form Jabber.

In softphone mode, Jabber uses the CSF device configured on CUCM for video calls. CSF devices are video-enabled by default.

Video conferencing is supported, using a video-conference bridge accessible by the Media Resource Group List (MRGL) assigned to the IP phone or CSF device.

Integration Support

Jabber can integrate with many Cisco Unified Communications applications, providing a wide range of rich features. Jabber can provide visual voicemail when integrated with Cisco Unity Connection. Users can control their mailboxes and listen to, send, and delete messages using Jabber.

Click-to-call functionality is supported from Jabber and other applications, such as Microsoft Outlook, Word, and Excel. Presence indicators for contacts can also be viewed in Outlook. If Cisco Unified MeetingPlace is integrated in the system, a call in Jabber can be easily escalated to a conference.

Cisco Unified Client Services Framework

The Cisco Unified Client Services Framework (CSF) provides the foundation of all Unified Communications client software. It is part of Jabber, but it also extends the functionality of Microsoft Outlook and WebEx Connect. The core functionality of the CSF is voice and video, secure communication with CUCM, and communication with text (IM) servers such as CM-IMP. CSF provides audio and video call control and advanced features, such as visual voicemail support.

Only one CSF client can be installed at one time on a client PC; for example, Jabber and Cisco Unified Communications Integration for Microsoft Office Communicator cannot co-reside on the same client computer.

Cisco Unified Communications Manager IP Phone Service

The Cisco Unified Communication Manager IP Phone (CCMCIP) Service was originally used to provide authentication, directory services, and help for end users. It has been adapted for use by Jabber and CSF clients to retrieve a list of devices on which the user can be reached when they log in. Figure 14-3 illustrates Jabber's use of the CCMCIP service.

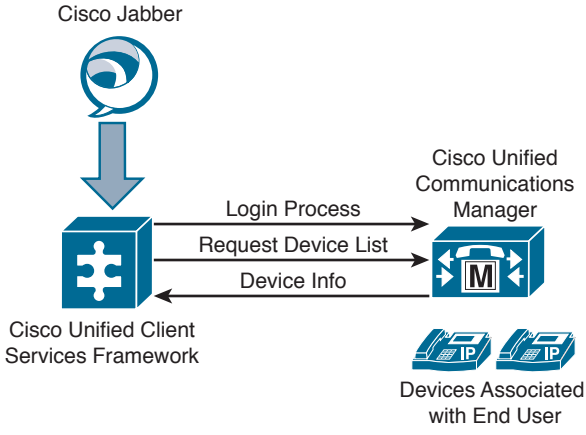


Figure 14-3 *CCMCIP Interaction*

Describe Cisco Unified Presence Architecture

Key Topic

CM-IMP is a standards-based application that uses several protocols to provide functionality and feature richness:

- SIP, SIMPLE, and XMPP to provide generic Presence and federation functionality
- Simple Object Access Protocol (SOAP) to access the CUCM database via Cisco Unified Communications System XML and Jabber configuration profiles
- Computer Telephone Interface Quick Buffer Encoding (CTIQBE) for CTI integration for remote call control with Microsoft Office Communicator

The core components of CM-IMP are as follows:

- **Jabber XCP:** Provides Presence, IM, contacts listing, message and call routing, and policy and federation.
- **Rich Presence service:** Manages Presence state gathering and Presence-enabled routing.
- **Group chat storage:** Ad hoc group chats are normally stored in memory on the CM-IMP server; Persistent Chat and message archiving require an external database.

Integration with Microsoft Office Communications Server

CM-IMP interoperates with Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007 using SIP. The Microsoft Office Communicator client and associated IP phone interoperate to provide click-to-dial, phone control, and Presence capability.

Integration with LDAP

CM-IMP can be integrated with Lightweight Directory Access Protocol (LDAP) (including Microsoft Active Directory), allowing users to log in with their LDAP credentials and synchronize their Presence status with their Outlook/Exchange calendar. The LDAP directory can be searched from the Jabber interface. CM-IMP can communicate with Exchange using Outlook Web Access (a web distributed authoring and versioning interface provided by Exchange). The CM-IMP user database is synchronized with CUCM, which in turn may synchronize its user database with LDAP. CM-IMP can redirect user authentication to LDAP, providing a single sign-on experience for users. Figure 14-4 shows CM-IMP integration with LDAP.

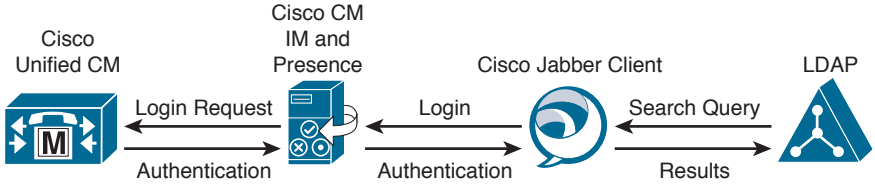


Figure 14-4 *CM-IMP Integration with LDAP*

Integration with Cisco Unity Connection

CM-IMP integration with CUC provide the user with the ability to sort, view, listen to, and delete voicemail messages and call the sender of voicemail messages, all from the Jabber interface. Presence information for the sender is displayed, allowing the user to select how to communicate with the sender or escalate to a call, message, or conference. Interaction with the CUC mailbox is via Internet Message Access Protocol (IMAP) and requires a voicemail profile to be configured on the CM-IMP server. Figure 14-5 illustrates CM-IMP interaction with CUC.

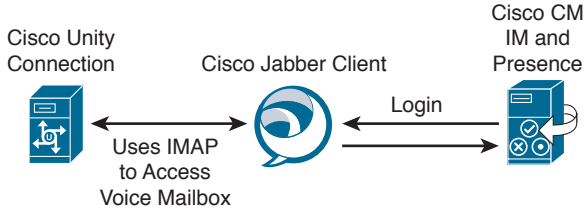


Figure 14-5 *CM-IMP Integration with CUC*

Integration with Conferencing Resources

CM-IMP uses WebEx or MeetingPlace for its conferencing capability. The use of WebEx requires a local Meeting Center server. Communication with conferencing server is via Macromedia Flash using HTTP or HTTPS for transport. Figure 14-6 shows CM-IMP integration with conferencing resources.

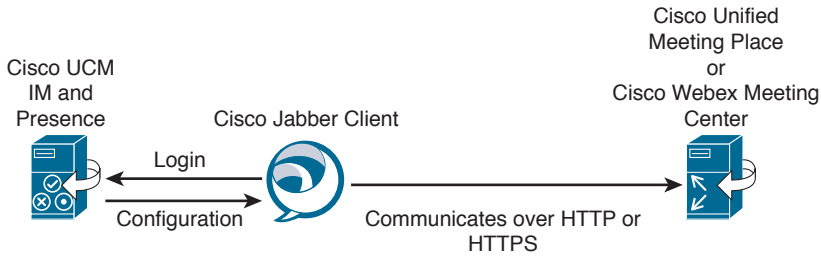


Figure 14-6 *CM-IMP Integration with Conferencing Resources*

Integration with Calendar Resources

CM-IMP can integrate with Microsoft Exchange 2003 or 2007 (Active Directory 2003 or 2008 is required) to provide access to calendar status (Free/Busy/Out of Office) and map that status to a Presence status (Available, Busy, Away). A special Exchange account (with membership in the View-Only Administrators Groups in Exchange and Receive-As permissions on all user mailboxes) must be configured for CM-IMP to inspect user calendars. Figure 14-7 shows CM-IMP interaction with calendar resources.

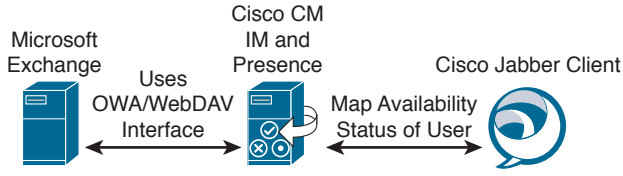


Figure 14-7 *CM-IMP Interaction with Calendar Resources*

Architecture and Call Flow: Softphone Mode

If the user is away from his desk (using a laptop while travelling is a typical scenario) or no IP phone is available, Jabber can operate in softphone mode. In this scenario, the CSF framework uses SIP signaling to register with CUCM as a CSF device. It then downloads the configuration file from CUCM, obtaining a DN, partition, CSS, device pool, and so on. XMPP is used for chat features, sending all IMs to CM-IMP.

Architecture and Call Flow: Deskphone Control Mode

When you are using Jabber in deskphone control mode, Jabber does not register the CSF device; instead, it logs in with the user-provided credentials and uses CCMCIP to obtain the list of user-associated controlled devices. Jabber can then use CTIQBE to control the IP phone. (If the user has multiple phones associated with his account, he can select the phone Jabber should control.) Jabber uses XMPP for chat features, sending all IMs to CM-IMP.

IM/Chat, Compliance, and Persistent Chat

Instant messaging or chat is a core capability of the Jabber/CM-IMP system. Other supported Cisco chat clients include Cisco Unified Personal Communicator (Jabber's predecessor) and Cisco Unified Mobile Communicator (a smartphone application for devices not supported by the Jabber app). CM-IMP uses the Jabber XCP protocol to provide standards-based chat capability between chat clients from different vendors. The Jabber desktop client also supports desktop sharing, which allows users to show their computer desktop to others for easy collaboration.

Persistent Chat refers to group chat messages that are preserved when all group chat participants have left the chat session, so that the information can be referenced later. For ad hoc chats, these messages are preserved in server memory. Persistent Chat requires an external database store; a separate database store is required for each CM-IMP server configured for Persistent Chat. The database instances can run on the same server but do not have to. Interaction with the PostgreSQL database is via Open Database Connectivity (ODBC).

Regulatory compliance may require that IM chats be preserved. CM-IMP can provide this capability by using a PostgreSQL external database. Third-party compliance applications may provide more features than a simple PostgreSQL database store; capabilities such as inline virus scanning of IMs and antispam measures for IM are among the more common features. If a third-party compliance application is in use, all chats are sent through the compliance server; this means that if the server is not available to CM-IMP, no IMs can be sent. Figure 14-8 illustrates CM-IMP integration with an external PostgreSQL server.

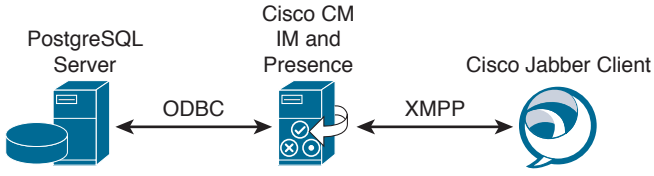


Figure 14-8 *CM-IMP Integration with External Compliance Server*

CM-IMP and QoS Considerations

Because quality of service (QoS) is so vital to successful Unified Communications deployments, some measures must be taken to ensure that Jabber traffic is appropriately processed by QoS mechanisms. Jabber marks traffic outbound from the user workstation with values appropriate for voice, video, and signaling traffic. Normally, all traffic coming from the user workstation is untrusted and marked down to a low QoS value by the first QoS-enabled device that handles it; this behavior must be modified by specifying the port ranges that Jabber uses and applying the appropriate QoS markings to that traffic. This requires that the network device (switch, router, firewall, and so on) have the capability to classify traffic based on port number, mark the traffic as appropriate for the QoS environment, and apply a QoS policy to forward the traffic to specific destination addresses with appropriate bandwidth and delay guarantees.

Table 14-2 lists the protocols transmitted by Jabber, along with their port numbers and a brief description.

Key Topic

Table 14-2 Protocols, Port Numbers, and Descriptions of Jabber Outbound Traffic

Port Number	Protocol	Description
69	UDP	Connects to the TFTP server to download the TFTP file
80	TCP HTTP	Connects to services such as Cisco Unified MeetingPlace for meetings, or Cisco Unity or Cisco Unity Connection for voicemail features
143	IMAP (TCP/TLS)	Connects to Cisco Unity or Cisco Unity Connection to retrieve and manage the list of voice messages for the user, and the voice messages themselves
389	TCP	Connects to the LDAP server for contact searches
443	TCP HTTPS	Connects to services such as Cisco Unified MeetingPlace for meetings, or Cisco Unity or Cisco Unity Connection for voicemail features
636	LDAPS	Connects to the secure LDAP server for contact searches
993	IMAP (SSL)	Connects to Cisco Unity or Cisco Unity Connection to retrieve and manage the list of voice messages for the user, and the voice messages themselves
2748	TCP	Connects to the CTI gateway, which is the CTIManager component of Cisco Unified Communications Manager
5060	UDP/TCP	Provides Session Initiation Protocol (SIP) call signaling
5061	TCP	Provides secure SIP call signaling
5222	TCP (XMPP)	Connects to the Cisco Unified Presence server for availability status and IM features
7993	IMAP (TLS)	Connects to Cisco Unity Connection to retrieve and manage the list of secure voice messages for the user, and the secure voice messages themselves
8191	TCP	Connects to the local port to provide SOAP web services
8443	TCP	Connects to the Cisco Unified Communications Manager IP phone (CCMCIP) server to get a list of currently assigned devices
16384-32766	UDP	Sends RTP media streams for audio and video

Enabling CM-IMP

This section reviews the steps required to configure end users so that they can use Jabber in either deskphone control mode or softphone mode.

Enabling End Users for Cisco Jabber in CUCM

The steps required to enable end users for Jabber must be carried out on CUCM, CM-IMP, and the Jabber client. The steps required for CUCM are summarized in the following list:

Step 1. Configure end users in CUCM.

Assign IM and Presence capabilities to users.

Enable users for CTI control.

Step 2. Associate the directory numbers with the end users in CUCM.

Step 3. Create a Cisco Unified Client Services Framework (CSF) device.

Step 4. Associate the CSF device with the end user in CUCM.

These summary steps are detailed in the following sections.

Step 1: Configure End Users in CUCM

Key Topic

To configure desk phone control for a user, in CUCM Administration, navigate to **User Management > End User** and select the user you want to configure. In the Device Information section on the End User configuration page, click the **Device Association** button and select the user's IP phone so that it appears in the Controlled Devices pane. (You should also verify that the **Allow Control of Device from CTI** check box is selected on that device's configuration page; it is selected by default.) If the user uses Extension Mobility, you must move the appropriate device profile to the CTI Controlled Device Profiles pane.

Key Point If you do not check the **Allow Control of Device from CTI** check box, the user cannot control the desk phone while using Jabber and cannot make any calls!

Because different IP phone models support CTI in different ways, the end user must be added to one or more groups for the CTI functions to work correctly on the various phone models the user might have access to. On the End User Configuration page, scroll down to the Permissions Information section. Use the following guidelines to add the user to the appropriate group or groups:

- **For all IP Phone models:** Add the user to the Standard CTI Enabled group.
- **For IP Phone 69XX series models:** Add the user to the Standard CTI Allow Control of Phones Supporting Rollover Mode group.
- **For IP Phone 89XX and 99XX series models:** Add the user to the Standard CTI Allow Control of Phones Supporting Connected Xfer and conf group.

Step 2: Associate the Directory Numbers with the End Users in CUCM

Navigate to **Device > Phone**, select the user's IP phone, and go to the Directory Number Configuration. Select the **Allow Control of Device from CTI** check box. If using Extension Mobility, click to enable the same box on the appropriate Device Profile configuration page for the user.

Next, scroll down to the Users Associated with Line section, and click the **Associate End Users** button. Select the user associated with this DN, and click **Add Selected**. Click **Apply Config**.

Step 3: Create a Cisco Unified CSF Device

At this point, you need to set up Jabber in softphone mode. Navigate to **Device > Phone** and click **Add New**. Select **Cisco Unified Client Services Framework** as the phone type. Enter a descriptive name (maximum 15 characters, no special characters). Set the device pool, owner user ID, and any other settings as appropriate.

Next, check the **Allow Control of Device from CTI** check box. Then, select a device security profile followed by a SIP profile. Click **Save**.

Under **Association**, select **Line [1]** and configure this new CSF device with the same DN as on the user's primary IP phone. Verify that the user is associated with the line.

Step 4: Associate the CSF Device with the End User in CUCM

On the End User Configuration page, under the Device Information section, add the newly created CSF device to the Controlled Devices list by clicking the **Device Association** button. Click **Save**.

Enabling End Users for Jabber in CUCM

Jabber has a tight integration with both CUCM and CM-IMP. On the CUCM server, there are several configurations called UC Services that must be built to support Jabber features, such as accessing voicemail messages from the Jabber client, deskphone control mode, LDAP directory lookups, and CCMCIP-based user device information. Some features might not be necessary in some deployments. The following list summarizes these features and the CM-IMP configurations required to support them:

- **Access personal voicemail using Jabber:** Jabber can retrieve and process voice messages from a voice messaging server. The CUC server must be configured to allow the user to receive voicemails via IMAP as discussed in Chapter 13, "Voice Messaging Integration with Cisco Unity Connection." There are two steps that must be configured in CUCM to support the feature in Jabber, as follows:

Step 1. **Define the mailstore:** In CUCM, navigate to **User Management > User Settings > UC Service** and select **Add New**.

a. Select **Mailstore** from the UC Service Type drop-down.

b. Enter a name and provide the hostname or IP address of the Unity Connection server.

c. Modify **the** port number and protocol if required. Click **Save**.

Step 2. **Define the voicemail server:**

a. Create a new UC Service by clicking **Add New**.

b. Select **Voicemail** from the UC Service drop-down. Click **Next**.

c. Choose the appropriate product (either **Unity** or **Unity Connection**).

d. Configure a name and IP address for the voice messaging server, optionally modifying the port and protocol as appropriate for the messaging server deployment Click **Save**.

- **Allow desk phone control:** Jabber can control the user's desk phone using CTI. To enable this function, perform the following steps:

Step 1. On the Find and List UC Services page, click **Add New**.

Step 2. Select **CTI** from the drop-down, and then click **Next**.

Step 3. Configure a name and IP address for the CTI server (this would be the CUCM), optionally modifying the port as appropriate for the deployment. Click **Save**.

- **Allow LDAP directory lookups:** Jabber can access the local LDAP directory to provide a list of contacts that can be accessed with click-to-communicate:

Step 1. On the Find and List UC Services page, click **Add New**.

Step 2. Select **Directory** from the drop-down, and then click **Next**.

Step 3. Configure a name and IP address for the directory server (this would be the LDAP server), optionally modifying the port and protocol as appropriate for the deployment. Click **Save**.

- **Define the Presence server:**

Step 1. On the Find and List UC Services page, click **Add New**.

Step 2. Select **Unified CM (IM and Presence)** from the drop-down, and then click **Next**.

Step 3. Configure a name and IP address for the CM-IMP server. Click **Save**.

Key Topic

What you have just done is create a set of UC Services that allows Jabber to connect and communicate with the various resources and applications in the Unified Communications network and to display various types of information in the Jabber interface. (Other UC Services can be created for conferencing or video resources, including WebEx and Telepresence facilities.) The various UC Services you have just defined must be collected into a service profile, which is then assigned to end users. When the end user logs in to their Jabber client, these service profiles configure Jabber with all the correct UC Services for that user. You could have many different UC Services collected into different service profiles designed for different groups of users.

To create a service profile, follow these steps:

Step 1. Navigate to **User Management > User Settings > Service Profile**, and then click **New**.

Step 2. Enter a name and an optional description.

Step 3. If you would like to make this service profile the default for all user on the system, check the box to do so. Remember you can make many different profiles; you might only need one.

Step 4. From the selectors for Voicemail Profile, MailStore Profile, Directory Profile, IM and Presence Profile, and CTI Profile, choose the **UC Services** you previously configured.

Step 5. For the directory profile, specify the **Search Base(s)** using similar syntax to the LDAP configuration described in Chapter 9, "Managing Endpoints and End Users with CUCM." You might also want to specify the account that will log in to LDAP to search for contacts; alternatively, you can set it to use the user's credentials.

Each service profile must be assigned to users for them to be able to use it. You can do this in two ways: The simplest way is to enable the **Make This the Default Service Profile for the System** box on the Service Profile Configuration page. If this is done before any users are synchronized from CUCM, all new user accounts will use these default profiles without requiring that a service profile be explicitly configured for each user. The other way is to associate users individually with the profiles after the profiles are created. You do this from the End User Configuration page in CUCM. This manual method can be used at any time to modify an individual user's application profile set.

Step 6. Each user must be enabled for CM-IMP by checking the box in the Service Settings section of the User Configuration page. Optionally, you can also check the box for **Include Meeting Information in Presence** if you are integrating with a calendaring service such as Microsoft Exchange.

Step 7. Under the Directory Number Associations section, select the correct primary extension for the user using the drop-down.

Enabling CUCM Presence Signaling Integration with CM-IMP

The CM-IMP server is a cluster member; accordingly, much of the information needed for the operation of Presence capabilities is already replicated. However, real-time signaling of on-/off-hook status requires the configuration of a specialized SIP trunk between CUCM and the CM-IMP server, as described in the following steps:

Step 1. Create and configure a customized SIP trunk security profile:

a. In CUCM, navigate to **Cisco Unified CM Administration > System > Security > SIP Trunk Security Profile.**

b. Click **Find.**

c. Click **Non Secure SIP Trunk Profile.**

d. Click **Copy** and enter **CM-IMP Trunk Profile** (or whatever you want to call it) in the Name field.

e. Set Device Security Mode to **Non Secure.**

f. Verify that the incoming transport type is **TCP+UDP.**

g. Verify that the setting for the Outgoing Transport Type is **TCP.**

h. Check to enable these items:

- **Accept Presence Subscription**
- **Accept Out-of-Dialog REFER**
- **Accept Unsolicited Notification**
- **Accept Replaces Header**

i. Click **Save.**

Step 2. Create a SIP trunk:

a. Navigate to **Cisco Unified CM Administration > Device > Trunk.**

b. Click **Add New.**

c. Choose **SIP Trunk** from the Trunk Type menu.

d. Choose **SIP** from the Device Protocol menu.

e. Choose **None** for the Trunk Service Type.

f. Click **Next.**

g. Enter **CM-IMP-SIP-Trunk** (or whatever name you like) for the device name.

h. Choose a device pool from the Device Pool drop-down.

i. In the SIP Information section at the bottom of the window, configure the following values:

- In the Destination Address field, enter the dotted IP address or the fully qualified domain name (FQDN), which can be resolved by DNS and must match the SRV cluster name configured on the IM and Presence node.
- Enter **5060** for the destination port. (This is a required, specific entry.)
- Choose CM-**IMP Trunk Profile** (or whatever you named the profile in the previous steps) from the SIP Trunk Security Profile menu.
- Choose **Standard SIP Profile** from the SIP Profile menu.

j. Click **Save**.

Step 3. Configure the SIP PUBLISH trunk on CM-IMP:

a. Navigate to **Cisco Unified CM IM and Presence Administration > Presence > Settings**.

b. Choose **CM-IMP-SIP-Trunk** (or whatever you named the previously configured SIP Trunk) from the CUCM SIP Publish Trunk drop-down list.

c. Click **Save**.

Enabling End Users for Jabber in CM-IMP

The last configurations needed are on the CM-IMP server itself. We must configure a SIP Publish trunk and define the SIP Presence gateway.

Browse to the CM-IMP Administration page at https://<CM-IMP_ip_address>/cupadmin and follow these steps to configure CM-IMP:

Step 1. Log in with the Application Administration account, and navigate to **Presence > Settings > Standard Configuration**.

Step 2. In the Presence Settings section, verify that the **CUCM IM and Presence Publish Trunk** is set to the SIP Publish trunk configured previously on the CUCM server (**CM-IMP-SIP-Trunk** in this example).

Step 3. Navigate to **Presence > Gateways** and verify that the CUCM gateway is listed.

Troubleshooting Jabber

Table 14-3 provides a few examples of issues that can arise with Jabber, along with things to check to fix the problems.

Table 14-3 Jabber Troubleshooting Quick Reference

Symptom	Things to Check
Error on starting Jabber: "The selected device is not available."	■ Verify that devices are registered in CUCM. ■ Verify that the end user is associated with the IP phone in CUCM. ■ Verify that the CM-IMP profile is associated with the user. ■ Verify that the device and DN can be controlled by CTI in CUCM.
User can't make calls using Jabber in softphone mode.	■ Verify that the user is associated with the CSF device in CUCM. ■ Verify that the CSF device is registered in CUCM. ■ Check for correct DN, partition, and CSS.
Users are not shown as on the phone during an active call.	■ Verify that the SIP trunk between CUCM and CM-IMP exists and is correctly configured. ■ Verify that the user is associated with the line (check the configuration of IP phone, device profile, or CSF as appropriate) in CUCM.
User cannot log in to Jabber.	■ Verify that the user account is not locked. ■ Verify the correct server IP address in Jabber. (The user may have changed it.) ■ If using the hostname instead of the IP address, verify that DNS is available and correctly configured. ■ Verify the license capabilities assignment in CUCM.
User cannot add contacts; search returns no results.	■ Verify that the user is associated with the correct LDAP profile. ■ Verify that the LDAP search context syntax is correct.
User cannot control the IP phone 9971.	■ Verify that the IP phone is associated with the user in CUCM. ■ Verify that the Allow Control of Device from CTI box is checked on the device configuration page in CUCM. ■ Verify that the user is a member of both the Standard CTI Enabled and Standard CTI Allow Control of Phones supporting Connected Xfer and Conf groups.

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 14-4 describes these key topics and identifies the page number on which each is found.

Table 14-4 Key Topics for Chapter 14

Key Topic Element	Description	Page Number
Paragraph	CM-IMP fundamentals	381
Paragraph	Jabber operating modes	381
Paragraph	Enterprise instant messaging	382
Paragraph	Client services framework	383
Paragraph	Presence architecture	384
Table 14-2	Jabber port numbers and descriptions	388
Section	Configure end users in CUCM	389
Paragraph	CM-IMP application profiles	392

Definitions of Key Terms

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

CTIQBE, XMPP, SIMPLE, CSF, Persistent Chat, compliance, IPPM, CCMCIP

This page intentionally left blank

This chapter covers the following topics:

- **Troubleshooting:** This section walks you through a general troubleshooting process you can use to approach almost any network-related issue.
- **Troubleshooting Common CME Registration Issues:** One of the most common issues you will encounter in Cisco VoIP is an IP phone that continually cycles through the boot process. This section discusses these issues and provides an approach to solving them.
- **Troubleshooting Dial-Plan and QoS Issues:** When a phone call fails or starts crackling during a call, people on staff have no problem letting you know that they want you to do something about it.

CHAPTER 15

Common CME Management and Troubleshooting Issues

If it worked right the first time every time, none of us would have jobs! This chapter discusses how to handle questions and troubleshoot Cisco Unified Communication Manager Express (CME). The chapter is divided into the three major areas of troubleshooting typically encountered on production networks: IP phone registration issues, dial plan issues, and quality of service (QoS) issues.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter or simply jump to the "Exam Preparation Tasks" section for review. If you are in doubt, read the entire chapter. Table 15-1 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 15-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions Covered in This Section
Troubleshooting	1–2
Troubleshooting Common CME Registration Issues	3–7
Troubleshooting Common Dial-Plan and QoS Issues	8–10

1. You are planning a structured troubleshooting approach for an IP phone registration issue. You just defined the problem; what is your next step?
   a. Consider the possibilities.
   b. Gather the facts.
   c. Create an action plan.
   d. Implement an action plan.
2. You just finished resolving an outage issue in the voice network. Which of the following should you do as a follow-up measure? (Choose three.)
   a. Reboot the devices to ensure the issue does not reappear.
   b. Document the solution.
   c. Document the root cause of the issue.
   d. Document the changes made to the system.
   e. Document the next change window for follow-up.

3. You are troubleshooting an IP phone registration issue. You verify that the IP phone is receiving an IP address with Option 150 from the DHCP server. What should the phone do next after this point?
   a. Reboot with a new configuration.
   b. Contact the TFTP server.
   c. Register with the CME router.
   d. Update its firmware.
4. A Cisco IP phone is plugged into an Ethernet wall jack. The phone does not respond to the connection. What should your first area of troubleshooting be for this situation?
   a. Verify that the voice VLAN is assigned to the port.
   b. Enable CDP on the interface.
   c. Verify PoE configuration.
   d. Ensure that you are using Category 6 Ethernet cable.
5. You believe one of your Cisco IP phones has not been assigned to the correct voice VLAN. What symptom is typically seen when this occurs?
   a. The IP phone has unforeseen call restrictions or permissions.
   b. The IP phone displays "invalid VLAN" on the screen.
   c. The IP phone continually reboots.
   d. The PC attached to the IP phone loses network connectivity.
6. After a Cisco IP phone determines its voice VLAN configuration via CDP, what does it do?
   a. The phone reboots in the new VLAN.
   b. The phone sends out a DHCP request tagged with the voice VLAN number.
   c. The phone sends out an untagged DHCP request.
   d. The phone queries for a TFTP server in the new VLAN.
7. An IP phone boots and displays "Registration Rejected" on the screen. What is the most likely cause of the issue?
   a. The CME router has no appropriate ephone configuration.
   b. An ACL is blocking access to the CME router.
   c. The TFTP server is not serving the correct files.
   d. The MAC address of the phone is in the disallow list.
8. What command can you enter to watch CME process calls as digits are dialed?
   a. **show dialpeer voice**
   b. **debug dialpeer voice**
   c. **debug voip dialpeer**
   d. **debug voice dialed**

9. What is the one-way delay requirement Cisco recommends to achieve high-quality voice calls?
   a. 100 ms
   b. 150 ms
   c. 200 ms
   d. 250 ms

10. What command can you use to verify QoS operations and packet statistics on a specific interface of your CME router?
   a. **show run**
   b. **show qos interface**
   c. **show service-policy interface**
   d. **show policy-map interface**

Foundation Topics

Troubleshooting

When troubleshooting, employing a consistent and systematic methodology saves time and helps prevent errors that might make the situation worse. The sequence of steps described in this section is supported by Cisco best practices as one model for effective troubleshooting. Figure 15-1 illustrates the troubleshooting sequence. This same model and process is also seen in Chapter 16, "CUCM Monitoring, Maintenance, and Troubleshooting," because it also applies to Cisco Unified Communications Manager (CUCM) troubleshooting.

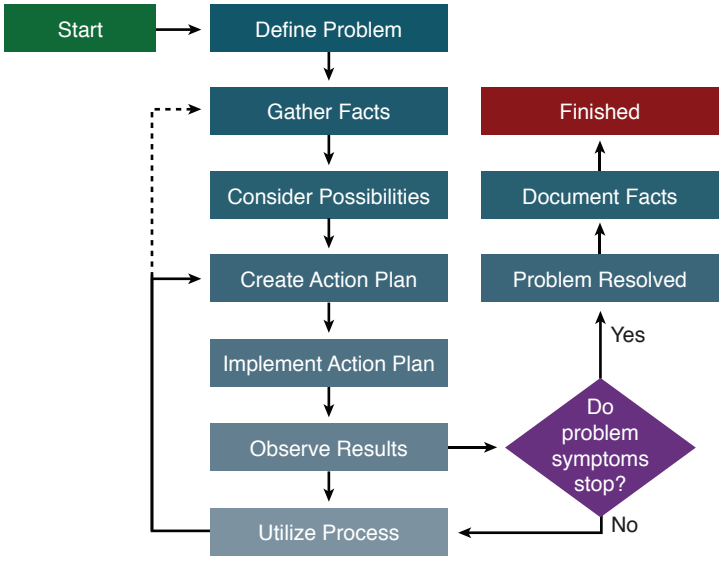


Figure 15-1 *Troubleshooting Methodology*

The steps illustrated in Figure 15-1 are described here:

Key Topic

1. **Define the problem:** Analyze the problem and create a clear problem statement. Define the symptoms and probable causes. Compare current conditions to a baseline "normal" condition.
2. **Gather facts:** Collect and consider command outputs and user statements. Eliminate possible causes to reduce the number of potential issues. Ask: When did this problem occur? What changed before the problem started? It is intermittent or constant? Is there a pattern to the intermittence? Are there any error messages? Does anyone else have the problem?
3. **Consider possibilities:** Based on the facts gathered in Step 2, identify a short list of likely causes. This may be a quick, almost intuitive process, or it might require significant research and discussion.

4. **Create action plan:** Beginning with the most likely cause on the list from Step 3, define a plan of action to correct the problem. The plan should modify only one variable at a time, so that the effect of that one change can be easily evaluated.
5. **Implement an action plan:** Execute the commands or make the changes decided in Step 4. Do not improvise; follow the plan. If new information or ideas come up, you may want to start at Step 3 again. At each step, make sure that the action taken does not make the problem worse; if it does, undo the change. Minimize the impact of changes on production systems, especially limiting the duration of security vulnerabilities, such as temporarily removing access lists to see whether they are the problem.
6. **Observe results:** Has the problem been solved?
   a. **Unsolved:** If the problem is not solved, undo the change implemented in Step 5 and return to Step 4.
   b. **Solved:** If the problem is solved, document the solution, root cause, and the changes made to the system.

Troubleshooting Common CME Registration Issues

I am sure that many of you have had the experience where a friend or family member calls and says, "My computer is not working." Instinctively, your mind begins to try to narrow down this broad statement by asking probing questions, such as, "Are there lights on the PC? Does the monitor display an image? Do applications open? Do you smell smoke?" Based on the answers to these questions, you can begin deducing a plan of action.

In the same sense, troubleshooting IP telephony issues requires you to ask questions to help narrow down the many possible issues to a focused troubleshooting process. For example, imagine you receive a call from a user who states, "My IP phone is not working." You might ask, "How are you talking to me now? Does the IP phone show your extension number on the screen? Is there any dial tone when you lift the handset? What happens when you dial? What messages are on the screen right now? Does it seem like the phone is rebooting? When did you notice the phone stop working?"

All these questions are geared to focus your troubleshooting into one of the following areas:

- Issues relating to the network
- Issues relating to the IP phone configuration
- Issues relating to CME configuration

Just like any data device, an IP phone relies on the network and supporting servers to operate correctly; without them, the IP phone will not function. One of the fundamental things for you to know when troubleshooting network-related issues is the boot process of the Cisco IP phone (see Figure 15-2). This was covered in earlier chapters, but I repeat it here for clarity.

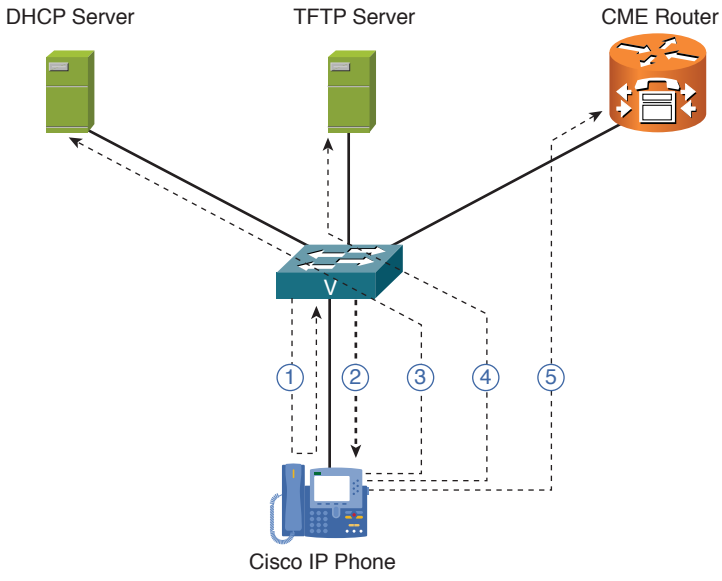


Figure 15-2 *Cisco IP Phone Boot Process*

Key Topic

1. The 802.3af Power over Ethernet (PoE) switch sends a small DC voltage on the Ethernet cable, detects an unpowered 802.3af device, and supplies power to the line.
2. The switch delivers voice VLAN information to the Cisco IP phone using Cisco Discovery Protocol (CDP).
3. The IP phone sends a DHCP request on its voice VLAN. The DHCP server replies with IP addressing information, including DHCP Option 150, which directs the IP phone to the TFTP server.
4. The IP phone contacts the TFTP server and downloads its configuration file and firmware.
5. Based on the IP address listed in the configuration file, the IP phone contacts the call processing server (the CME router, in this case), which supports VoIP functions.

Knowing this boot process almost plans your troubleshooting process for you: Anytime a Cisco IP phone gets stuck in the boot process (for example, it is unable to get a Dynamic Host Configuration Protocol (DHCP)-assigned address, reach a TFTP server, or register with the CME router), it reboots itself and tries again. You can get many clues to how far the phone is getting in the boot process by carefully watching the messages on the screen. The IP phone tells you when it attempts to configure a voice VLAN, obtain an IP address, or contact a TFTP server. By watching the screen, you can identify the step where the phone stops in the boot process and begin your troubleshooting from that point.

Tip Keep in mind that it is normal for a newly installed IP phone to reboot several times because of firmware and configuration updates.

Here is the process you should use for troubleshooting network-related issues:

Issue 1: Verifying PoE

Obviously, if the IP phone does not receive power, nothing is going to work correctly. You can quickly diagnose this issue by asking the user if her phone is displaying anything on the screen. If not, here are your areas of focus:

- **Check the physical connections:** Verify that the IP phone is securely plugged in, verify all patch panel connections, and verify the Ethernet cable used has all eight pins functioning properly (because PoE might use the four pins not used by data).
- **Check the PoE switch:** Ensure that the switch is online and operational, verify that the PoE clients have not maxed-out the switch power supply by using the **show power inline** command, and use a **show run** command to verify that the port does not have the command **power inline never** (which disables PoE).
- **Check the IP phone:** Move the IP phone to a different port to see if it receives power, try a different IP phone on the same port to see if it receives power, and be sure that the IP phone and PoE switch support a compatible PoE standard (Cisco inline power, 802.3af, and 802.3at).

Tip Before you move too far into the troubleshooting process, it is always best to reset the phone's configuration settings to factory default. Although the various IP phone models have different locations to reset the configuration, all of them will have the option. Sometimes, a bogus configuration item will end up stuck in one of the key fields that you may not initially see. Resetting the phone configuration gives you a clean starting ground to work from.

Issue 2: Voice VLAN Assignment

If an IP phone is assigned to the wrong VLAN, it may not be able to contact the necessary supporting servers (DHCP, TFTP, CME, and so on). You can diagnose this and the following issues when you receive a report that the IP phone is continually rebooting:

- **Check the switch configuration:** Ensure that you correctly configured the voice VLAN by viewing the running-configuration (**show run**), verifying the interface operating mode by entering a **show interface** *<interface_name>* **switchport** command, verifying you created the voice VLAN on the switch (**show vlan**), verifying that the voice VLAN is added to all applicable trunk connections (**show interface trunk**), and verifying CDP is enabled on the port connected to the IP phone (because the voice VLAN is sent to the IP phone using CDP).
- **Check the IP phone:** If you have physical access to the IP phone, navigate to the network settings page (using the Settings button on the phone). Verify that the IP phone has received the voice VLAN configuration, verify the IP phone has an IP address, and access the phone IP address in a web browser and view the log files for more clues.

Issue 3: DHCP Server

Receiving an IP address through DHCP goes hand-in-hand with the voice VLAN assignment (Issue 2). If a Cisco IP phone is not assigned to the correct VLAN, it may not receive an IP address from the DHCP server, or if it does, the DHCP options for the pool may not be correct. After you verify the voice VLAN configuration, you can use this process to troubleshoot the DHCP process:

- **Check the DHCP helper address:** If you are using a centralized DHCP server, ensure a router (or L3 switch) supporting the voice VLAN is forwarding DHCP requests to a proper server. (You can find the **helper-address** command under the router interface connected to the VLAN.)
- **Check the DHCP server:** Verify that the DHCP server has an IP address pool created for the voice VLAN devices, ensure that the pool has not run out of IP addresses, verify that DHCP Option 150 (TFTP server) is properly configured and assigned to the pool, connect other test devices (laptop or PC) in the voice VLAN, and ensure these devices receive IP addresses.
- **Check the IP phone:** If you have physical access to the IP phone, navigate to the network settings page (using the Settings button on the phone). Verify that the IP phone received an IP address from the appropriate subnet, verify all applicable DHCP options (subnet mask, default gateway, TFTP server) are filled in, and attempt to ping the phone from another subnet to ensure routing works (assuming no access control lists [ACLs] block this communication).

Keep in mind that it is easy to mix up DHCP-related troubleshooting with other phone system issues. Because a phone experiencing communication issues constantly reboots, there are times when the phone does not have an IP address (which can send you down a wrong track of troubleshooting). Before you pull your hair out focusing on DHCP issues, try statically assigning an IP configuration to the phone and see if the phone registers successfully with CME. If it does register successfully, the problem is most likely related to DHCP or VLAN issues. If not, the problem is more likely related to routing, TFTP, or CME issues.

Issue 4: TFTP Server

The TFTP server is a critical part of the IP phone boot process because it supplies the phone firmware and configuration file with the base settings the phone should use for operation (and the IP address of the CME server for registration). Although CME supports using an external TFTP server to store all this data, most CME deployments simply use the flash memory and dynamic RAM of the router to store these files. Take the following steps to troubleshoot TFTP communication:

- **Check routing configuration:** If the TFTP server is on a different subnet than the IP phone, validate that data is able to route between the two subnets by placing a test device (such as a laptop or PC) in the voice VLAN and testing connectivity to the TFTP server (by transferring files via TFTP).
- **Check the TFTP server:** Verify that the TFTP server is operational and serving files, validate the firmware for the IP phone model in question exists on the TFTP server as well as a specific configuration file for the phone (the configuration file should have the

MAC address of the IP phone in the filename), and verify that you entered the **create cnf-files** command from telephony-service configuration mode to generate the necessary configuration files on the TFTP server. Remember that filenames in the IOS command-line interface (CLI) are case sensitive!

- **Check the IP phone:** If you have physical access to the IP phone, navigate to the network settings page (using the Settings button on the phone). Verify that the IP phone is configured (either statically or via DHCP) for the appropriate TFTP server IP address.

Issue 5: CME Server

The final troubleshooting step is to investigate the CME server itself. The most common CME issue encountered is a "Registration Rejected" error message on the IP phone. Seeing this error is actually good news: It means that the IP phone is moving through the entire boot process but fails when trying to register with the CME router. If this is the case, you can focus on the ephone settings. A registration rejected message almost always appears because the IP phone has not been properly configured in CME. First, validate that an ephone entry exists in your CME configuration for the IP phone in question. If so, verify that the MAC address entered for the ephone matches the MAC address of the IP phone. Do not blindly trust the sticker on the outside of the IP phone. Instead, verify the MAC address directly from the phone settings or the Cisco switch (viewing the dynamic MAC addresses learned on the port connecting to the IP phone).

If the MAC address appears correct in the CME configuration, try enabling auto-registration in CME. (Type **auto-reg-ephone** under the telephony-service configuration.) This should allow the phone to register without any extension assignment. You can then validate the MAC address of the IP phone by entering the **show ephone** command. If you want to get into the nitty-gritty, issue a **debug ephone detail** command, and you will be able to watch the IP phone registration process line by line. Be careful with this command because it might become overwhelming (to both you and your CME router) if you have many phones registering at the same time.

Troubleshooting Dial Plan and QoS Issues

Although this topic is a bit outside the current scope of the CICD exam, it is helpful if you are able to troubleshoot basic dial plan and QoS issues. These issues occur after the IP phone successfully registers with the CME router and attempts to place calls. Symptoms that arise range from call failure when dialing (fast busy/reorder tone) to static, distortion, or dropped calls after the call is connected. The former issue is typically related to a misconfigured dial plan, and the latter issue is typically related to QoS.

Dial Plan Issues

To troubleshoot issues related to the dial plan on the CME router, you must first focus on the dial peers. Remember, the dial-peer configuration builds the routing table for your voice calls. If you configured it inaccurately or incompletely, calls will not complete. Although you can use many commands to troubleshoot calls, two key commands rise to the surface: **show dial-peer voice summary** and **debug voip dialpeer**.

Similar to the **show ip interface brief** command, using **show dial-peer voice summary** enables you to see a table view of all the dial peers that exist on your voice gateway. If calls fail as they are dialed, this is usually the best place to start. Use this command to verify that the expected dial peers exist, have the correct destination pattern configured, and point to a port or IP address that is reachable from the CME router. Example 15-1 shows the output of this command.

Example 15-1 **show dial-peer voice summary** *Command Output*

```
CME_A# show dial-peer voice summary
dial-peer hunt 0
TAG    TYPE   AD  OPER PREFIX  DEST-PATTERN     PRE   PASS                  OUT   PORT
              MIN                              FER   THRU   SESS-TARGET    STAT
20005  pots   up   up           1500$            0                         50/0/20
20006  pots   up   up           1501$            0                         50/0/21
20007  pots   up   up           1502$            0                         50/0/22
20008  pots   up   up           1503$            0                         50/0/23
20009  pots   up   up           1504$            0                         50/0/24
20010  pots   up   up           1505$            0                         50/0/25
20011  pots   up   up           1506$            0                         50/0/26
20012  pots   up   up           1507$            0                         50/0/27
20013  pots   up   up           1508$            0                         50/0/28
20014  pots   up   up           1509$            0                         50/0/29
1101   pots   up   up           1101             0                    up   0/0/0
1102  pots     up up            1102             0                    up   0/0/1
1200   voip   Up   up           91.........      0    Syst   ipv4:67.215.241.250
1201    Voip  up   up           9[^1]..[2-9]....  0    syst   ipv4:67.215.241.250
```

In this example, if you tried to call the destination 916025551212, you could identify a match on dial peer 1200.

Now, verifying that a dial peer matches a dialed string and actually completing a call can be two different things. If you verify the dial peer and still receive reorder tones, you can use the **debug voip dialpeer** command. This command shows digits as they are dialed, as shown in Example 15-2.

Example 15-2 **debug voip dialpeer** *Command Output*

```
CME_A# debug voip dialpeer
Mar 31 16:07:13.195: //-1/xxxxxxxxxxxx/DPM/dpAssociateIncomingPeerCore:
   Calling Number=1500, Called Number=, Voice-Interface=0x8905DD70,
   Timeout=TRUE, Peer Encap Type=ENCAP_VOICE, Peer Search Type=PEER_TYPE_VOICE,
   Peer Info Type=DIALPEER_INFO_SPEECH
Mar 31 16:07:13.195: //-1/xxxxxxxxxxxx/DPM/dpAssociateIncomingPeerCore:
   Result=Success(0) after DP_MATCH_ORIGINATE; Incoming Dial-peer=20005
Mar 31 16:07:13.195: //-1/xxxxxxxxxxxx/DPM/dpMatchSafModulePlugin:
   dialstring=NULL, saf_enabled=0, saf_dndb_lookup=0, dp_result=0
Mar 31 16:07:16.047: //-1/C64C50C58929/DPM/dpMatchPeersCore:
```

```
   Calling Number=, Called Number=9, Peer Info Type=DIALPEER_INFO_SPEECH
Mar 31 16:07:16.047: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=9
Mar 31 16:07:16.047: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Result=Partial Matches(1) after DP_MATCH_DEST
Mar 31 16:07:16.051: //-1/C64C50C58929/DPM/dpMatchSafModulePlugin:
   dialstring=9, saf_enabled=1, saf_dndb_lookup=0, dp_result=1
Mar 31 16:07:16.051: //-1/C64C50C58929/DPM/dpMatchPeersMoreArg:
   Result=MORE_DIGITS_NEEDED(1)
Mar 31 16:07:19.551: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=91, Peer Info Type=DIALPEER_INFO_SPEECH
Mar 31 16:07:19.551: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=91
Mar 31 16:07:19.551: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Result=Partial Matches(1) after DP_MATCH_DEST
Mar 31 16:07:19.551: //-1/C64C50C58929/DPM/dpMatchSafModulePlugin:
   dialstring=91, saf_enabled=1, saf_dndb_lookup=0, dp_result=1
Mar 31 16:07:19.551: //-1/C64C50C58929/DPM/dpMatchPeersMoreArg:
   Result=MORE_DIGITS_NEEDED(1)
Mar 31 16:07:21.159: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=916, Peer Info Type=DIALPEER_INFO_SPEECH
Mar 31 16:07:21.159: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=916
Mar 31 16:07:21.159: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Result=Partial Matches(1) after DP_MATCH_DEST
Mar 31 16:07:21.159: //-1/C64C50C58929/DPM/dpMatchSafModulePlugin:
   dialstring=916, saf_enabled=1, saf_dndb_lookup=0, dp_result=1
Mar 31 16:07:21.159: //-1/C64C50C58929/DPM/dpMatchPeersMoreArg:
   Result=MORE_DIGITS_NEEDED(1) DPM/dpMatchPeersCore:
Mar 31 16:07:21.359: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=9160, Peer Info Type=DIALPEER_INFO_SPEECH
Mar 31 16:07:21.359: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=9160
Mar 31 16:07:21.359: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Result=Partial Matches(1) after DP_MATCH_DEST
Mar 31 16:07:21.359: //-1/C64C50C58929/DPM/dpMatchSafModulePlugin:
   dialstring=9160, saf_enabled=1, saf_dndb_lookup=0, dp_result=1
Mar 31 16:07:21.359: //-1/C64C50C58929/DPM/dpMatchPeersMoreArg:
   Result=MORE_DIGITS_NEEDED(1)
<...output omitted...>
Mar 31 16:07:23.843: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=916025551212, Peer Info Type=DIALPEER_INFO_SPEECH
Mar 31 16:07:23.843: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=916025551212
Mar 31 16:07:23.843: //-1/C64C50C58929/DPM/dpMatchPeersCore:
   Result=Success(0) after DP_MATCH_DEST
```

```
Mar 31 16:07:23.843: //-1/C64C50C58929/DPM/dpMatchSafModulePlugin:
   dialstring=916025551212, saf_enabled=1, saf_dndb_lookup=0, dp_result=0
Mar 31 16:07:23.843: //-1/C64C50C58929/DPM/dpMatchPeersMoreArg:
   Result=SUCCESS(0)
   List of Matched Outgoing Dial-peer(s):
     1: Dial-peer Tag=1200
```

The key areas in Example 15-2 are highlighted. Notice at the beginning of the debug output that the CME router matches an incoming dial peer when the IP phone with extension 1500 goes off-hook (incoming dial peer 20005 matched). Then, CME analyzes each digit as it is dialed from the IP phone. The first digit dialed is a 9. The debug output shows Partial Matches(1), indicating this dialed string partially matches one or more dial peers. The output then continues along this path until the IP phone has dialed a complete string (916025551212). At this point, CME realizes it has a full match on outgoing dial peer 1200.

This **debug** command can be useful to watch the CME router go through the dial peer matching process in real time. This is where you might talk a user through dialing a number that is failing and watch how CME handles the digits as the user dials them.

QoS Issues

Troubleshooting QoS is a different skill set and strategy than troubleshooting dial plan issues. Instead of working with the routing table for voice, you work with the voice traffic itself.

You might have heard the saying before, "If you have no goal, you will hit it every time." Before we can troubleshoot voice quality issues, we need to have a goal we're shooting for. Table 15-2 shows the Cisco recommended parameters for high-quality voice calls.

Key Topic

Table 15-2 Requirements for High-Quality VoIP Calls

Parameter	Requirement
End-to-end (one-way) delay	150 ms or less
Jitter	30 ms or less
Packet loss	1% or less

Key Topic

The full definition of each of these parameters was discussed in Chapter 6, "Understanding the CME Dial Plan." This is half of the puzzle: We know how fast and how consistently our voice traffic must travel across the network. The other half of the puzzle is how *much* voice traffic must travel across the network. You can find this out based on two factors: the voice CODEC you are using for the calls and how many concurrent calls you plan to support. Table 15-3 shows the average bandwidth usage for the two most popular codecs used in a Cisco Voice over IP (VoIP) network.

Table 15-3 Average Bandwidth Utilization for G.711 and G.729A

Codec	Packetization Interval	Bandwidth per Call
G.711	20 ms	80 kbps
G.711	30 ms	74 kbps
G.729A	20 ms	24 kbps
G.729A	30 ms	19 kbps

Keep in mind that these are simply average values. After you develop the advanced skills needed for CCNP Voice, you can calculate these values down to the bit-level for your specific environment.

Tip The packetization interval represents how much audio is included per packet. The larger your packetization interval, the more audio data you put into each packet. The more audio data you put in each packet, the less packets you send (thus, the slight bandwidth savings by choosing 30 ms packetization intervals). The downside, of course, is that losing a single packet has a much bigger negative impact on audio quality. The default packetization interval on Cisco routers is 20 ms.

Now, we can put the two puzzle pieces together. We know the requirements for high-quality audio, and we know how much bandwidth each call consumes. Now, we need to provision QoS to ensure that our switches and routers can guarantee priority queuing for our voice call bandwidth.

After you configure QoS, keep a proactive eye on the network to ensure that it meets quality standards. Although there are many sophisticated (and expensive!) tools available to help measure and monitor the voice traffic crossing the network, you actually get a basic monitoring utility each time you purchase a Cisco IP phone. Whenever a phone is on an active call, you can press the question mark button (help menu) twice to retrieve call statistics, as shown in Figure 15-3.

Figure 15-3 *Gathering Call Statistics*

The call statistics include the following:

- Codec
- Packet size
- Received and transmitted packets
- Average and maximum jitter
- Lost packets

You can also retrieve these statistics by accessing the built-in web server of the IP phone (by entering the phone's IP address into a web browser while it is on an active call).

Although plenty of QoS troubleshooting techniques are available, we highlight only one of them here. When you deploy QoS on a router, you can use a variety of methods and configurations. However, when it comes time to apply these methods to your router, you use an interface command known as service-policy. This command applies a policy map to your interface and engages QoS similar to the **ip access-group** command applying an access list to an interface and engaging security. You can verify your QoS statistics by using the **show policy-map interface** command. Example 15-3 shows the output of this command.

Example 15-3 show policy-map interface *Command Output*

```
Router# show policy-map interface serial3/1 output
 Serial3/1
  Service-policy output: VoicePriority
    Class-map: voice (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 5
      Weighted Fair Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 128 (kbps) Burst 3200 (Bytes)
        (pkts matched/bytes matched) 14231/3903582
        (total drops/bytes drops) 1253/391292
```

This output allows you to see the success or failure of the QoS policy applied to the outbound direction of Serial 3/1. Notice the QoS policy is named VoicePriority. It grants strict priority to the first 128 kbps of voice traffic. Notice the number of packets dropped (1253). This indicates a problem; this is roughly 8 percent of your voice packets. On an actual network, this could cause audio quality degradation issues for active calls.

The drops are most likely caused by one of two things: a congested WAN link or voice traffic exceeding the provisioned amount. A congested WAN link simply means that there is not enough bandwidth to send the calls in the time required, so the packets are dropped. The latter issue seems almost identical to the first. That is, if you have too many voice calls, won't you congest the WAN and not be able to get all the packets through? Although this might be true, the more likely cause is the strict priority queuing configuration. Strict priority ensures that the VoIP traffic gets the first and fastest 128 kbps available. However, once the voice traffic tries to exceed this amount, the router begins dropping the traffic (even if there is bandwidth available on the WAN link). This ensures that you know exactly how much voice traffic is going over your WAN connections. The data traffic will not have to fight for the scraps of bandwidth left over.

Note All these troubleshooting guidelines also apply to phones registering with CUCM.

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 15-4 describes the key topics and the page numbers on which each is found.

Key Topic

Table 15-4 Key Topics for Chapter 15

Key Topic Element	Description	Page Number
List	Cisco best practice troubleshooting guidelines	402
List	Boot process for Cisco IP phones registering with CME	404
Table 15-2	QoS requirements for high-quality voice calls	410
Table 15-3	Average bandwidth utilization for popular Cisco codecs	411

Definitions of Key Terms

Define the following key term from this chapter, and check your answer in the Glossary:

packetization interval

This page intentionally left blank

This chapter covers the following topics:

- **Describe How to Provide End-User Support for Connectivity and Voice Quality Issues:** This section reviews the basic troubleshooting method as it applies to a Unified Communications environment.
- **Describe CUCM Reports and How They Are Generated:** This section reviews the content of the built-in reports for CUCM and how to create them.
- **Describe CUCM CAR Reports and How They Are Generated:** This section reviews CUCM call detail record reports and how they are created.
- **Describe Cisco Unified RTMT:** This section reviews the RTMT and how to use it for system monitoring.
- **Describe the Disaster Recovery System:** This section summarizes the features and uses of the native backup and restore service in CUCM.

CHAPTER 16

CUCM Monitoring, Maintenance, and Troubleshooting

Cisco Unified Communications Manager (CUCM) is a large and complex application and, in most deployments, it is considered "mission critical," which means that when trouble happens, it is important to be able to find out what is wrong and fix it quickly. A solid troubleshooting methodology will help you keep your head when everyone around you is losing theirs.

"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 16-1 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 16-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Describe How to Provide End-User Support for Connectivity and Voice Quality Issues	1–3
Describe CUCM Reports and How They Are Generated	4
Describe CUCM CAR Reports and How They Are Generated	5–8
Describe Cisco Unified RTMT	9
Describe the Disaster Recovery System	10

1. Cisco defines a series of steps in the process of troubleshooting. Which of the following lists those steps in the correct order?

   a. Gather facts.
   Define the problem.
   Consider possibilities.
   Create action plan.
   Implement action plan.
   Observe results.

b. Create action plan.
Gather facts.
Define the problem.
Observe results.
Consider possibilities.
Implement action plan.

c. Consider possibilities.
Gather facts.
Define the problem.
Create action plan.
Implement action plan.
Observe results.

d. Define the problem.
Gather facts.
Consider possibilities.
Create action plan.
Implement action plan.
Observe results.

2. Rob is having problems with his IP phone. It is not working. Rob says he has tried "fiddling with a few things on the phone." Where should you begin troubleshooting?

a. Examine CUCM to see whether the phone is registered.

b. Verify that the DHCP server is active, reachable from Rob's phone, and has addresses available.

c. Verify that the TFTP service is running on the CUCM.

d. Verify that the local settings on Rob's phone are correct.

e. Verify that the switch configuration is correct.

3. Greg is an end user in the Engineering Department. He has done some reading on the Internet and has learned that there is a Unified Reporting tool he can use to run reports. However, he phones you to tell you that he can't run any reports because he is denied access to the web page. What action will allow Greg to run reports?

a. Modify the permissions on the Unified Reporting web pages to allow Greg access.

b. Give Greg a copy of Crystal Reports and the Platform Administration account.

c. Install the RTMT on Greg's PC.

d. Make Greg a member of the standard CCM super users group.

e. Tell Greg he is not allowed to run reports.

4. The CAR Reporting tool allows three types of users to access reports: administrators, managers, and users. What defines a report user as a manager as opposed to just a user?
   a. Their account is referenced in the Manager User ID field of another user's account.
   b. Their account is a member of the standard CAR manager users group.
   c. The Manager check box is selected in the CAR User Configuration page.
   d. Managers log in to a different CAR Reports tool than users do.

5. Aunt Beru wants to find out who on her team makes the longest phone calls. Which CAR report should she run?
   a. Bills > Department
   b. Bills > Individual
   c. Top N > By Duration
   d. Top N > By Charge

6. Greg is a CAR reports user. How can he be given access to the manager-level reports?
   a. Add Greg's UserID to the Manager User ID field in another user's configuration page.
   b. Add Greg to the standard CAR managers access control group.
   c. Add Greg to the standard CCM end users access control group.
   d. Add the string **YES** to the Manager User ID field in Greg's user configuration page.

7. Janice is upset because the custom IP phone service she commissioned is not being adopted by many users. Which CAR report will determine how many phones are subscribed to her custom service?
   a. Cisco IP Phone Services (with the custom service selected)
   b. Top N > Service Subscriptions
   c. Cisco Unified Communications Manager Assistant > Manager Call **Usage**
   d. Top N > By Number of Calls

8. You are the CUCM administrator. A couple months ago, management asked you to implement client matter codes to track employees' personal calls. What report can you run to provide a list of calls made with the CMC assigned to personal calls?
   a. Traffic > Summary
   b. Traffic > SummarybBy Extension
   c. FAC / CMC > Client Matter Code
   d. FAC / CMC > Authorization Level

9. Luke has been a CUCM administrator for two years. He is trying to use his RTMT to look at system summary information for the new CUC server. He complains that the menu is not visible. What should Luke do to make the CUC menu visible?
   a. Under **Edit > Preferences**, check the **CUC** box under System menu.
   b. Install the Linux version of RTMT on his PC.
   c. Download and install the RTMT from the CUC server.
   d. Luke must be made a member of the standard RTMT administrators group.
10. What previously available storage option is no longer available to the disaster recovery system in CUCM v10.x?
   a. Local disk file
   b. FTP
   c. Local tape drive
   d. USB stick
   e. SFTP

Foundation Topics

Describe How to Provide End-User Support for Connectivity and Voice Quality Issues

Troubleshooting a complex application like CUCM can be challenging. The scope of CICD requires us to keep it relatively simple, so the following sections should by no means be considered a comprehensive CUCM troubleshooting manual. In this chapter, you learn how to troubleshoot basic IP phone registration issues and look at the extensive reporting capabilities of the CUCM system, which helps you monitor the health and well-being of the servers in your deployment.

Note that the following section on troubleshooting methodology is duplicated in Chapter 15, "Common CME Management and Troubleshooting Issues." It appears again here because it is important and it makes it easier to refer to as you read this chapter.

Troubleshooting

When troubleshooting, employing a consistent and systematic methodology saves time and helps prevent errors from making the situation worse. The sequence of steps described here is supported by Cisco best practices as one model for effective troubleshooting. Figure 16-1 illustrates the troubleshooting sequence.

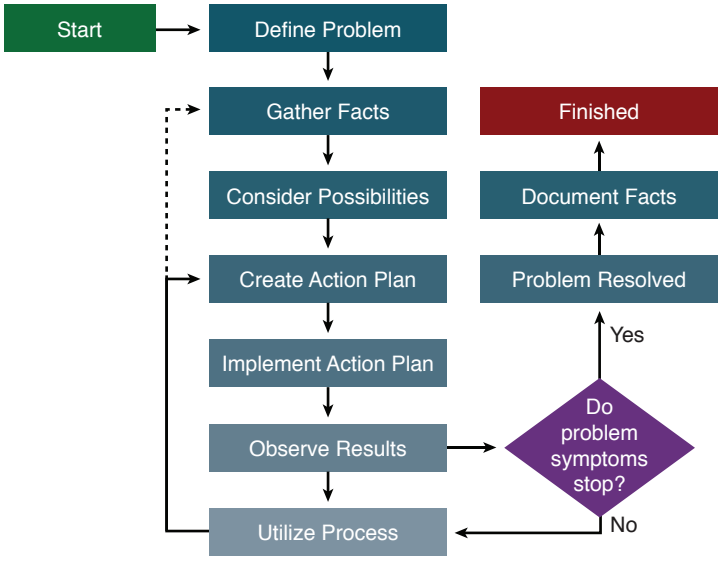


Figure 16-1 *Troubleshooting Methodology*

Here are the steps illustrated in Figure 16-1:

1. **Define the problem:** Analyze the problem and create a clear problem statement. Define the symptoms and probable causes. Compare current conditions to a baseline "normal" condition.
2. **Gather facts:** Collect and consider command outputs and user statements. Eliminate possible causes to reduce the number of potential issues. Ask: When did this problem occur? What changed before the problem started? It is intermittent or constant? Is there a pattern to the intermittence? Are there any error messages? Is anyone else having the problem?
3. **Consider possibilities:** Based on the facts gathered in Step 2, identify a short list of likely causes. This may be a quick, almost intuitive process, or it may require significant research and discussion.
4. **Create action plan:** Beginning with the most likely cause on the list from Step 3, define a plan of action to correct the problem. The plan should modify only one variable at a time, in order that the effect of that one change can be easily evaluated.
5. **Implement action plan:** Execute the commands or make the changes decided in Step 4. Do not improvise: Follow the plan. If new information or ideas come up, you may want to start at Step 3 again. Make sure at each step that the action taken does not make the problem worse; if it does, undo the change. Minimize the impact of changes on production systems, especially limiting the duration of security vulnerabilities, such as temporarily removing access lists to see if they are the problem.
6. **Observe results:** Has the problem been solved?
   - **7a. Unsolved:** If the problem is not solved, undo the change implemented in Step 5 and return to Step 4.
   - **7b. Solved:** If the problem is solved, document the solution, the root cause, and the changes made to the system.
8. You are done.

A list like that (which you need to memorize) needs a good mnemonic. Here's one for you:

> Define, Gather, Consider, Create, Implement, Observe: "Dogs Gobble Cookies, Cats Irritate Owners."

Troubleshooting IP Phone Registration Problems

The IP phone registration process is deceptively complex, and several discrete areas may cause problems—and, of course, if one step fails, subsequent steps fail, too. That being the case, you can use a divide-and-conquer methodology: Quickly check which steps have succeeded, and then start troubleshooting from the first point of failure. IP phone registration problems can be categorized according to the following points of failure:

- Local to the IP phone
- VLAN or switch mismatches
- DHCP problems
- TFTP problems
- CUCM registration problems

Let's examine a scenario in which the phone is not registering. In this scenario, the phones are supposed to use Dynamic Host Control Protocol (DHCP). Each point that follows describes a possible place where problems may be happening. Best practices dictate that we follow these troubleshooting procedures in the order that follows; there will be times when experience or specific knowledge allows us to skip to a later procedure:

- **Local to the IP phone:** The IP phone itself can display its current configuration and settings, which can quickly indicate which part of the sequence has failed. Press the **Settings** button, and then select **Network Configuration** from the displayed list. Scroll down to IP Configuration and verify that the phone has received an IP address (in the correct subnet), subnet mask, default gateway, and the correct TFTP server address. If the entries are absent or incorrect, verify that the phone is configured to use DHCP by pressing **Settings > Network Configuration**, and then scrolling down to DHCP Enabled and verifying that it is set to **Yes**. If all that is correct but the phone is still not receiving an address from DHCP, move on to the next step.
- **VLAN or switch mismatches:** Verify that the switch is correctly configured to support IP phones. The switch should have a voice VLAN defined, and if there is a PC connected to the phone, a separate access VLAN. (See Chapter 3, "Understanding Cisco IP Phones," for the configurations.) Verify that the VLAN numbers are correct. If the switch configuration is correct, move on.
- **DHCP problems:** Verify that the DHCP server is running and that it has not run out of IP addresses. Make sure that the DHCP scopes (subnets or pools) are correct with respect to the IP address range being assigned, the subnet mask, default gateway, and Option 150 (TFTP server IP address). On the IP phone, navigate to **Settings > Network Configuration**. Verify that the DHCP Server entry lists the IP address of the correct DHCP server. Check that an IP address has been assigned, and if so, that it is in the correct range. Verify that the TFTP Server 1 address entry is correct.

Note If the DHCP server is on a remote subnet from the IP phones, the local router blocks the DHCP broadcasts by default. Use the **ip helper-address** *ip_address* command on the local router to allow it to forward DHCP requests to the IP of the DHCP server.

- **TFTP problems:** As it boots, the phone queries the TFTP server (at the address learned via DHCP) for its configuration file. The filename it asks for is called SEP<mac>.cnf.xml. If the phone has been successfully added to the CUCM or Cisco Unified Communication Manager Express (CME) application, the file will exist and will be downloaded to the phone. If the phone has never been added to the application before, the file will not be there. The phone will then ask for the file called XMLDefault.cnf.xml. This default file is always available. If the phone is not getting its config file, verify that the phone has the correct TFTP address in the Network Configuration list. Verify that the TFTP service is running on the server at that IP. You can check on the status of the TFTP process on the phone by pressing Settings > Status Messages; example messages include File Not Found:SEP<mac address>.cnf.xml, TFTP Timeout: SEP<mac address>.cnf.xml, and SEP<mac address>.cnf.xml.
- **CUCM registration problems:** The TFTP download file contains the IP address of the CUCM server with which it is supposed to register. Check **Settings > Device**

Configuration > Unified CM Configuration to verify that the Unified CM IP address listed is correct. There may be a backup and tertiary server IP listed, depending on how the cluster is configured. Verify that the Cisco CallManager Service is running on the servers listed; you may also need to verify that auto-registration is correctly set up (only if you are actually using auto-registration, of course).

If all the previous are verified as correct, there may be a problem with the phone itself; that type of troubleshooting is beyond the scope of CICD.

Deleting Unassigned Directory Numbers Using the Route Plan Report

When using auto-registration, one of the more common issues encountered is that the phones fail to register, displaying "Error DB Config" or a similar message on the IP phone screen. The source of the problem is that the range of directory numbers (DNs) allocated for auto-registration has been used up; auto-registration is working, but there are no more DNs available to assign to the phones. This situation arises because it is normal practice to change the DN of an auto-registered phone (which is assigned sequentially from the range defined for auto-registration) to its "real" production DN. An odd thing happens to the auto-registration-assigned DN: It is not released back to the available range, but instead is marked as "Unassigned" and held in "database limbo." Unassigned auto-registration DNs are not visible unless you go looking for them, so it is not obvious that they are the source of your problem.

The fix is simple: Either add to the range of auto-registration DNs, or use the following steps to "reclaim" them so they can be re-used on newly registering phones:

Step 1. Navigate to **Call Routing > Route Plan Report**.

Step 2. Set the first filter (the far-left field) to **Unassigned DNs**.

Step 3. Click **Find**.

Step 4. Delete all the listed unassigned DNs. You can do this easily by selecting all the listed DNs using the check boxes to their left and then clicking **Delete Selected**.

The DNS are now released back to the auto-registration range as available for assignment.

These steps are also used to "clean up" the database after modifications to your partitions design. Another interesting behavior of the CUCM database is that when a DN is assigned to a different partition, it still exists in the previous one but is flagged as unassigned. These unassigned DNs can create confusion, because they do appear in lists as selectable (for example, when building a line group)—but they do not function because they are not assigned to any device.

Note You may deliberately choose to have the same DN or route pattern available in two different partitions. This may be part of a localized dial plan or a particular solution to what are called "vanity numbers," which means route calls to the same number differently, if they are dialed by different phones. Remember that a DN or route pattern plus its partition assignment is what CUCM considers as the call routing target; that is why we talked about the relevance of the partition order in Chapter 6, "Understanding the CME Dial Plan."

You should be familiar with using the Route Plan Report to delete unassigned DNs as a routine maintenance task.

Describe CUCM Reports and How They Are Generated

CUCM includes numerous reporting tools. This section reviews how to generate and access those reports and how to use them for troubleshooting, maintenance, and system analysis.

The Cisco Unified Reporting tool pulls information from a range of sources, and formats the data into a single simplified output. The report tool alerts the user if the report job will cause performance issues for the server or take an excessive amount of time.

The reports pull data from the Publisher and the Subscribers, including the following sources:

- Real-Time Monitoring Tool (RTMT) counters
- Call detail records (CDRs) and the CDR Administration and Reporting database
- CUCM database
- Disk files (traces and logs)
- Prefs settings
- Command-line interface (CLI)
- Real-Time Information Server (RIS)

The reporting system uses the Cisco Tomcat service and Remote Procedure Calls (RPC) to the other servers via HTTPS. Make sure that the Tomcat service is running and that HTTPS traffic can reach and return from the servers.

Generating Reports

Access the Cisco Unified Reporting tool from the navigation drop-down at the top right of the CUCM Administration interface or directly via the URL https://<ip_address>/cucreports. By default, the only users with the necessary privilege to view the reports are member of the CCM super users group, the only member of which by default is the CUCM application administration account defined at install.

The reports are accessed under the System Reports menu, as shown in Figure 16-2.

Select the desired report from the menu list. The Reporting tool stores one of each previously created report for later access; if the report selected has not been run before, a message is displayed, indicating that the report does not exist and the user should generate a new report. The Generate a New Report link is directly below this message.

If an old copy of the report exists, a message is displayed to that effect and a link to the report is listed. Bear in mind that the old report contains old information; check the time/date stamp on the report to be sure that the report is recent enough to be valid. To re-create the report, click the icon at the top right to run it again.

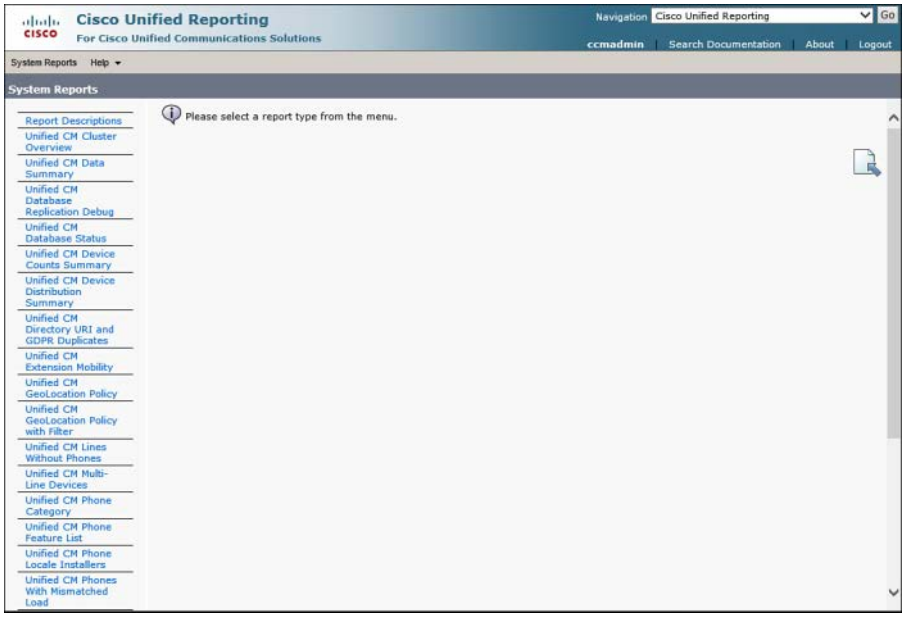


Figure 16-2 *Cisco Unified Reporting: System Reports Menu*

Figure 16-3 shows a sample report (in this case, a Device Counts Summary). The green checkmark at the top indicates that the report ran successfully. The other buttons to the right side of the page allow you to upload an Extensible Markup Language (XML) report that is stored on your local workstation to keep it on the CUCM server, download the report to your local workstation, or run it again.

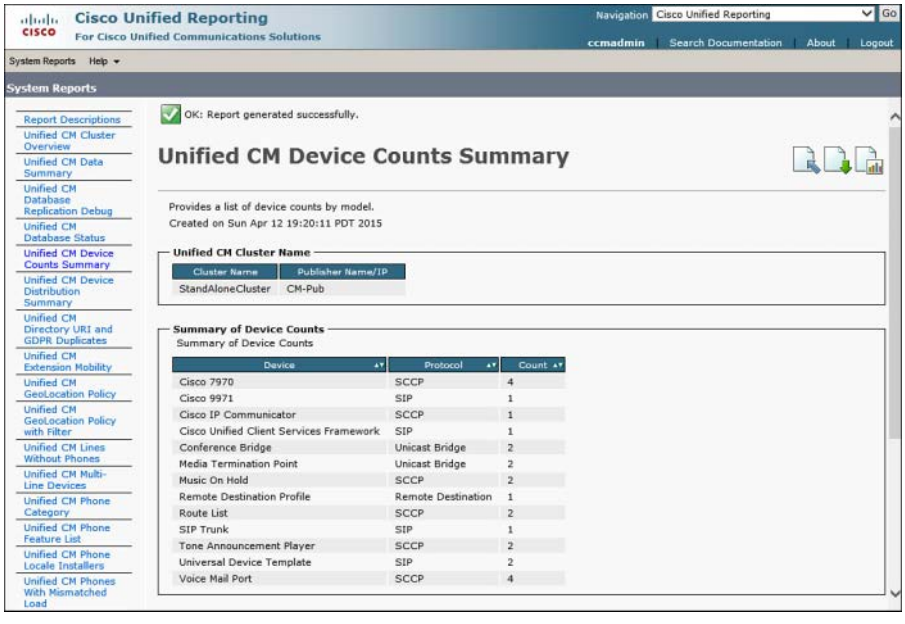


Figure 16-3 *Unified Reporting: Sample Report*

Analyzing Reports

The reports you generate can be used as part of the following tasks:

- **Troubleshooting:** For gathering facts, considering possibilities, and observing results.
- **Maintenance:** Find configuration or load mismatches, or summarize system information.
- **System Analysis:** List phones by type, feature, or several other filters.

Understanding CUCM CDR Analysis and Reporting Tool Reports

In this section, we review the Call Detail Record Analysis and Reporting (CAR) tool—its general parameters, system settings, scheduler options, and database. This section also goes over how to generate these reports about users, the system, and devices.

Every call that CUCM processes can be logged. These logs, called call detail records (CDRs) and call management records (CMRs), contain information about the call and the voice quality metrics for the call. These CDRs are stored as flat files on the subscriber servers and uploaded to the CDR/CAR database on the Publisher at regular intervals. (The interval can be administratively set.) In addition to providing useful information for internal administrative purposes, the CDR database can be used by third-party billing applications to prepare internal or external billing reports.

Administrators can pull reports manually using the web interface at https://<*ip_address*>/car or set up reporting jobs to occur automatically. The option to load CMRs in addition to CDRs is determined administratively; CMRs are not loaded by default. Figure 16-4 shows the CAR Reports tool.

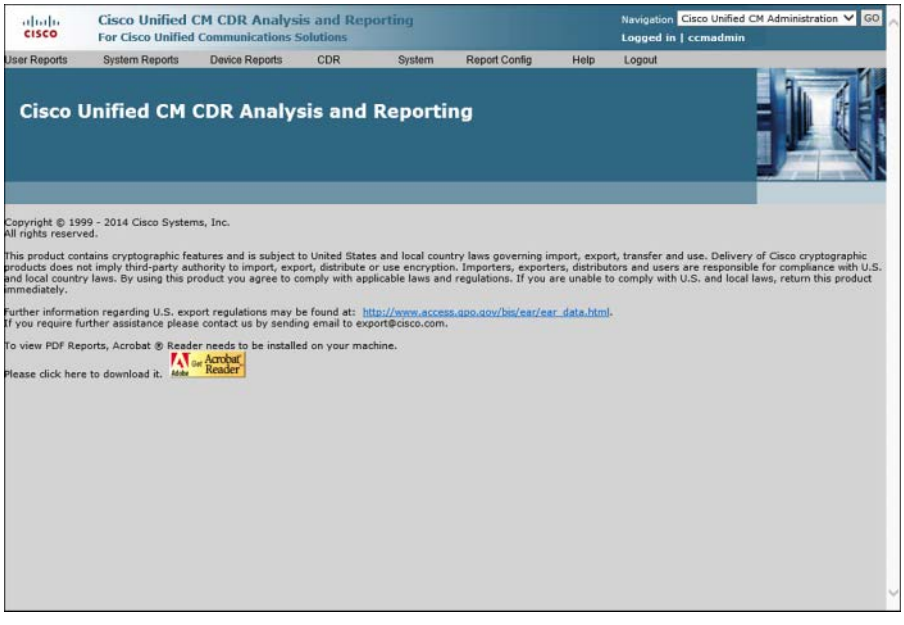


Figure 16-4 *CAR Report Tool*

Activate CAR-Related Services

To use CAR, you must activate the Cisco CAR Web Service:

Step 1. From the Unified Serviceability page, navigate to **Tools > Service Activation.** Select the **Cisco CAR Web Service** and click **Save.**

Step 2. If an external billing server is to be used, you must also activate the **Cisco SOAP-CDROnDemand Service.** (SOAP stands for Simple Object Access Protocol.)

Configure CDR Service Parameters

In the CM Administration interface, navigate to **System > Service Parameters**. Select a server from the first drop-down, and then select the **Cisco CallManager** service. Click the **Advanced** button at the top of the page to display all parameters. Adjust the following as required:

- **CDR Enabled Flag:** This setting determines whether CDRs will be generated. This must be set on all servers. The default is False (CDRs not collected).
- **CDR Log Calls with Zero Duration Flag:** Setting this parameter to True causes CUCM to generate CDRs for calls that never connect or that last less than 1 second. Calls that are unsuccessful (including calls that result in reorder tone or that fail because of a busy trunk) are always logged regardless of this setting. The default setting is False.
- **Call Diagnostics Enabled:** This parameter enables the logging of CMRs. You have the choice to never generate CMRs, to generate them only if CDRs are also being generated, or to generate CMRs whether CDRs are being collected or not. The default value is Disabled.
- **Display FAC in CDR:** This parameter controls whether the forced authorization code used to make a call will be included in the CDR. The default value is False.
- **Show Line Group Member DN in finalCalledPartyNumber CDR Field:** For calls to call hunting systems, this parameter determines whether the hunt pilot number or the DN that picked up the calls is recorded in the CDR. The default is False. (The hunt pilot number is recorded, not the DN.)
- **Add Incoming Number Prefix to CDR:** This parameter controls whether the incoming prefix (several are defined in the service parameters) is added to the calling party number in CDRs. Prefixes added to an inbound call are always recorded in CDRs; this setting controls whether prefixes are added to CDRs if they are added to outbound calls. The default value is False.

CAR Tool Users

The CUCM CAR tool allows three types of users to have access to the tool:

- **Administrators** can use the tool to access all reporting features to build reports for system performance analysis, load balancing verification, and troubleshooting purposes. Any end user or application user can be given administrator access to the CAR tool by making them a member of the standard CAR admin users group.
- **Managers** can generate reports for users, departments, and quality of service (QoS). Managers are defined by the Manager User ID field in CM Administration: If User A's ID is selected in the Manager User ID field on User B's configuration page, User A can run manager reports on User B. Managers can set up automatic reports to be delivered to their configured mail ID.
- **Users** can generate a billing report for their calls. Users can generate reports for a specific date range and can have the system email the report. Users must be members of the standard CCM end users group to access these reports, and the devices they want to generate reports for must be associated with their account.

CDR and CMR Architecture

CDRs are generated by CUCM servers that are processing calls (those that are running the CallManager Service). The CDRs contain information about the called and calling numbers, the time/date stamp for connect and disconnect, and why the call was disconnected. CMRs contain information about latency, jitter, packet loss, and the amount of data sent during the call. Each call may generate several CDRs and CMRs. The call processing nodes collect the CAR data (the collective term for CDRs and CMRs) in a local log and periodically upload them to the CDR repository node using SFTP. The repository node runs the CDR Repository Manager Service, which is responsible for maintaining the CDR and CMR files, managing the disk space used by the CDR data, and sending the files to (up to) three configured locations (typically third-party billing servers).

CAR System Parameters

The CAR system requires some setup to function most effectively. The following tasks need to be completed:

- Configure mail parameters so that the CAR system can send reports and alerts by email.
- Configure the dial plan to match local calling pattern so that CDRs are interpreted correctly. (Four example, 4-digit calls are classified as On Net, and 10-digit calls are local.) The default settings are based on the North American Numbering Plan (NANP).
- Configure the gateways in the CAR tool. Gateways configured in CUCM are automatically added and deleted, but the area codes local to the gateway must be added so that the reports can determine which calls are long distance.

- Set the COMPANY_NAME value (maximum of 64 characters) as desired; this name appears in the header of CAR reports.
- Set up the CAR Scheduler to control which types of records are loaded, at what intervals, and for how long. The aim is to allow sufficient loading time while not impacting the server performance. Loading the CDR and CMR file should not be confused with the actual generation of the CDRs and CMRs; loading refers to the Repository node pulling the raw CDR/CMR data from the call processing nodes into the CDR/CAR database.
- Configure CDR/CAR database purging. Automatic Purge is on by default; you can adjust the High and Low Water Mark values to control when the purging begins and stops, based on the percentage utilization of the available database disk space. Which records to purge is based on the age of the records. Manual purging is also available.
- Configure automatic report generation. Choose which reports should be automatically generated and optionally select whether you would like the reports emailed. The interval for report generation is fixed (daily, weekly, or monthly), but the start time can be customized using the Scheduler interface.

Exporting CDR and CMR Records

CDR and CMR files can be downloaded from the server as a CSV file, typically to be imported into a billing application. The steps are as follows:

Step 1. From the CAR tool, navigate to **CDR > Export CDR/CMR**.

Step 2. Set the **From Date** and **To Date** values.

Step 3. In Select Records, check **CDR Records**, **CMR Records**, or both.

Step 4. Click **Export File**.

Step 5. In the new window, choose either **CDR Dump** or **CMR Dump**, and then click **Save As** to select a file location on the workstation.

Step 6. Selecting the **Delete File** check box causes the CAR tool to delete the downloaded records from the CAR database. This is recommended to prevent the database size from ballooning unnecessarily.

Generating CDR Reports

As mentioned previously, users, managers, and administrators can use the CAR report tool to generate different reports. This section discusses the reports in more detail.

The following reports are available to users, managers, and administrators, as indicated in each description:

- **Bills**
  - **Individual:** Available to users, managers, and administrators. Provides call information for a specified date range in summary or detail format. Report can be viewed or emailed.
  - **Department:** Available to managers and administrators. Provides call and QoS information in summary or detail format, for all users who report to the manager or to selected users.
- **Top N**
  - **By Charge:** Available to managers and administrators. The report lists the top number of users in order of call charges for the specified time period (N is the number of users in the list). Reports can also be configured to report by charges to the destination of the calls, or by all calls, which lists the top N calls that incurred the most charges.
  - **By Duration:** Available to managers and administrators. Reports list users sorted by duration of call during the specified time period. The report can also list top calls in order of duration by destination or all calls by duration.
  - **By Number of Calls:** Available to managers and Administrators. Reports list users by number of calls or extensions by number of calls.
- **Cisco Unified Communications Manager Assistant**
  - **Manager Call Usage:** Available to administrators. Reports list summary or detail information for call completion by managers using Cisco Unified Communications Manager Assistant. Reports can list the calls managers made for themselves, calls that assistants handled for managers, or calls handled by both for managers.
  - **Assistant Call Usage:** Available to administrators. Reports can list the calls assistants made for themselves, calls that assistants handled for managers, or calls handled by assistants for both assistants and managers.
- **Cisco IP Phone Services:** Available to administrators, this report shows selected IP phone services, the number of users subscribed to the services, and the utilization percentage for each.

Report Generation Example

The following steps illustrate how to generate a report using the CAR tool. As an example, we run a report that tells us what users have made the most calls:

Step 1. Navigate to the CAR Reports tool at https://<*ip_address*>/car, as shown previously in Figure 16-4.

Step 2. Select **User Reports > Top N > By Number of Calls**, as shown in Figure 16-5.

Step 3. The next screen allows you to define the parameters for the report, including call types, user types, and date range, as shown in Figure 16-6.

Step 4. Click **View Report** to see the report output, as shown in Figure 16-7.

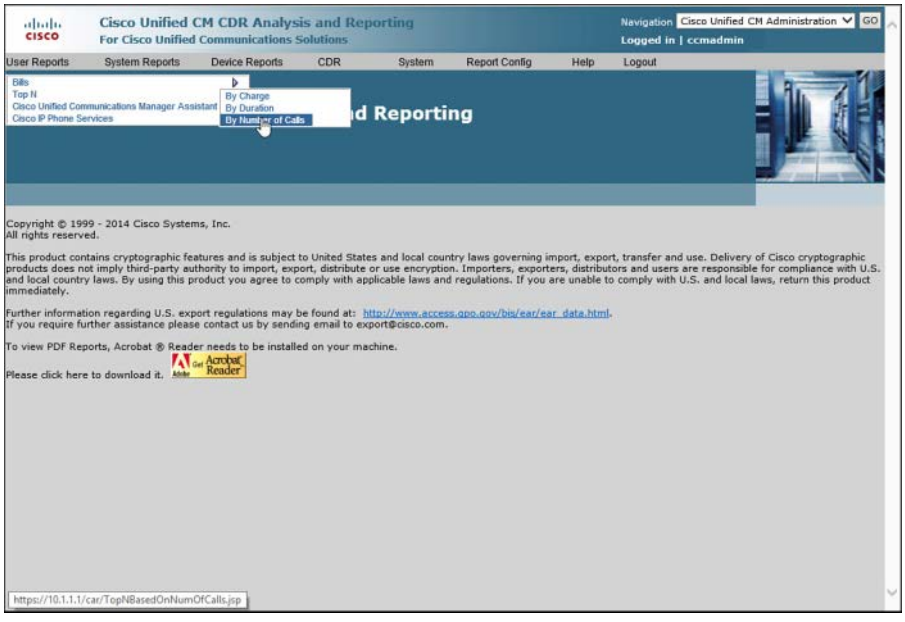


Figure 16-5 *Selecting a User Report: Top N by Number of Calls*

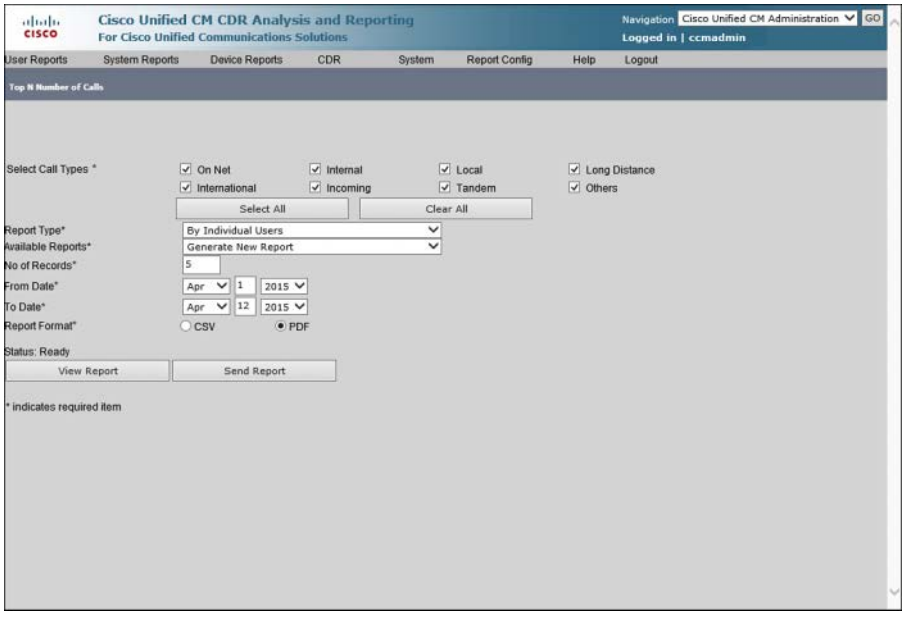


Figure 16-6 *Top N By Number of Calls Parameters Selection*

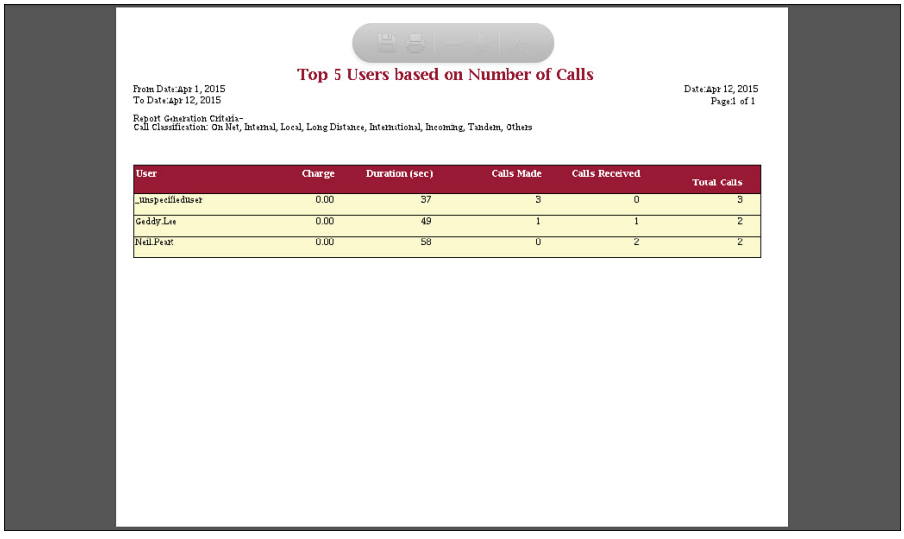


Figure 16-7 *Report Output: Top N by Number of Calls*

Generating System Reports

Key Topic

The CAR tool provides several system reports in addition to the user reports just listed. The following sections summarize the available system reports:

- QoS
  - **Detail:** Available to administrators. Provides detailed QoS statistics for calls handled by CUCM during the specified date range. Useful for system-wide voice-quality monitoring.
  - **Summary:** Available to managers and administrators. Provides pie chart format showing QoS ratings for calls of specified classifications and time frame and includes a summary table for calls per QoS grade.
  - **By Gateway:** Available to managers and administrators. Report lists percentage of calls per selected gateways meeting defined QoS criteria. Report can be generated hourly, daily, or weekly.
  - **By Call Type:** Available to administrators. Lists percentage of calls by selected type that meet chosen QoS criteria. Report can be generated hourly, daily, or weekly.
- Traffic
  - **Summary:** Available to administrators. Displays call volume for selected call types and QoS categories for a specified time frame. Useful for displaying the number of calls made hourly/daily/weekly.
  - **Summary by Phone Number:** Available to administrators. Displays call volume per specified Phone Number and call types during the selected time frame.

- **Forced Authorization Code/Client Matter Code (FAC/CMC)**
  - **Client Matter Code:** Available to administrators. Lists called and calling numbers, call duration, and call classification for specified time period.
  - **Authorization Code Name:** Available to administrators. Lists called and calling numbers, call time stamps, duration, and call classification for specified time period by FAC name (includes authorization level).
  - **Authorization Level:** Available to administrators. Lists called and calling numbers, call time stamps, duration, and call classification for a specified time period by FAC authorization level (includes FAC name).
- **Malicious Call Details:** Available to administrators. Displays details for calls tracked by the Malicious Caller Identification (MCID) service for the specified time period.
- **Precedence Call Summary:** Available to administrators. The report lists (in bar graph format) summary information for calls that were preempted by the selected Multilevel Precedence and Preemption (MLPP) levels for the specified time period.
- **System Overview:** Available to administrators. Provides high-level information about the CUCM network.
- **CDR Error:** Available to administrators. Lists statistics for errors encountered during CDR data transfer.

Generating Device Reports

The CAR tool provides several reports to monitor loading and performance of CUCM-related devices, such as gateways and conference bridges. These device reports include the following:

- **Gateway:** Detail, Summary, and Utilization reports display gateway utilization according to various call and gateway criteria.
- **Route Patterns and Hunt Groups:** Includes the following reports:
  - Route/Line Group Utilization
  - Route Pattern/Hunt Pilot Utilization
  - Hunt Pilot Summary
  - Hunt Pilot Detail
- **Conference Bridge:** Conference Call Detail and Conference Bridge Utilization reports monitor conference resources.
- **Voice Messaging:** The Voice Messaging Utilization report estimates the percent utilization of voice-messaging devices.

Describe Cisco Unified RTMT

The Cisco Unified Real-Time Monitoring Tool (RTMT) enables administrators to collect, view, interpret, and monitor the various counters, trace files, and logs generated by CUCM, Cisco Unity Connection (CUC), and Cisco Unified Presence (CUP).

The RTMT is a client application installed on an administrative workstation. All current versions of Windows, as well as Linux (KDE or Gnome), are supported. The software can be downloaded from the CUCM, CUC, CUP, and Cisco Unified Contact Center Express (CUCCX) servers. The RTMT for each server product is specific to that server product, with the exception that the RTMT version for CUCM and for CUC are interchangeable.

If you want to install multiple instances of RTMT, you must use different installation directories and duplicate and rename the desktop application icon. RTMT uses HTTPS to connect to Unified Communications servers and monitor system performance, device status, device discovery, CTI applications, and voice-messaging ports. The server-side Cisco Alert Manager Collector Service (AMC) allows the RTMT application to collect information real-time. The following services and servlets provide RTMT with information and capabilities:

- **Cisco Communications Manager Servlet:** This service, which supports the Cisco Unified RTMT, starts up automatically after the installation.
- **Cisco RIS Data Collector:** The Real-time Information Server (RIS) maintains real-time information such as performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications to retrieve the information that is stored on the server.
- **Cisco Tomcat Stats Servlet:** The Cisco Tomcat Stats Servlet enables you to monitor the Tomcat perfmon counters by using RTMT or the CLI.
- **Cisco Trace Collection Servlet:** The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces by using the RTMT client.
- **Cisco Trace Collection Service:** The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the RTMT client.
- **Cisco Log Partition Monitoring Tool:** This service, which starts up automatically after the installation, monitors the disk usage of the log partition on a server.
- **Cisco SOAP-Real-Time Service APIs:** The Cisco SOAP-Real-Time Service application programming interfaces (APIs), which start up automatically after the installation, enable you to collect real-time information for devices and CTI applications.
- **Cisco SOAP-Performance Monitoring APIs:** This service, which starts up automatically after the installation, allows you to use performance monitoring counters for various applications through SOAP APIs.
- **Cisco RTMT Reporter Servlet:** This service, which starts up automatically after the installation, allows you to publish reports for RTMT.
- **Cisco Serviceability Reporter:** The Cisco Serviceability Reporter service enables you to publish reports for RTMT.

End users (or application users) must be added to the standard CCM admin users and standard RealtimeAndTraceCollection groups to use RTMT. They can log in to RTMT using their user ID and password. Of course, adding a user to the standard CCM super users group will provide the necessary privileges as well.

The administrative capabilities of RTMT include the following:

- Monitor predefined system health objects
- Generate email alerts for objects that fall below or exceed defined threshold values
- Collect and view trace files from different services
- View syslog messages
- Configure and monitor performance counters

RTMT Interface

The RTMT graphical user interface (GUI) includes the following menus and options (plus several others not listed):

- **File:** Save, restore, and delete RTMT profiles; monitor Java Virtual Machine (JVM) information; access the report archive; access the Unified reporting tool; log off; or exit.
- **Edit:** Set up categories for table format views, set polling rates for performance counters and devices, show/hide Quick Launch Channel, and edit trace settings for RTMT.
- **Window:** Close current (or all) RTMT windows.
- **Application:** Provides links to administration, serviceability, and application-specific interfaces, depending on which application-specific RTMT is in use.

When RTMT is in use, the RTMT menu is divided into submenus:

- **System:** Allows monitoring of platform health, including CPU and memory and disk utilization. Administrators can set up and monitor various performance counters, alerts, and traces and access the Trace & Log Central tool and syslog viewer.
- **Voice/Video:** If RTMT is connected to a CUCM server, administrators can view summary information about the server, search for devices, and monitor services.
- **IM and Presence:** If RTMT is connected to a CUCM server, administrators can view summary information applicable to the CUP application.
- **Unity Connection:** Visible only if RTMT is connected to a CUC server, here administrators can use the Port Monitor Tool and view statistics and summaries applicable to CUC.
- **Analysis Manager:** If the RTMT is connected to a CUCM server, the administrator can display configuration and licensing summaries, and use the Call Path Analysis Tool.

To clarify the preceding section a little bit: When you are using Cisco Unified RTMT with Cisco Unified Communications Manager, the menu has four submenus: System, Voice/Video, Analysis Manager, and IM and Presence. When you are using Cisco Unified RTMT with Cisco Unity Connection, the menu includes only two submenus, System and Unity Connection.

Monitoring CUCM with RTMT

The sections include examples that show some of the ways in which RTMT can monitor a CUCM server.

Voice and Video Summary

The Voice and Video Summary view shows graphs for registered phones, calls in progress, and active MGCP gateway ports and channels, as shown in Figure 16-8.

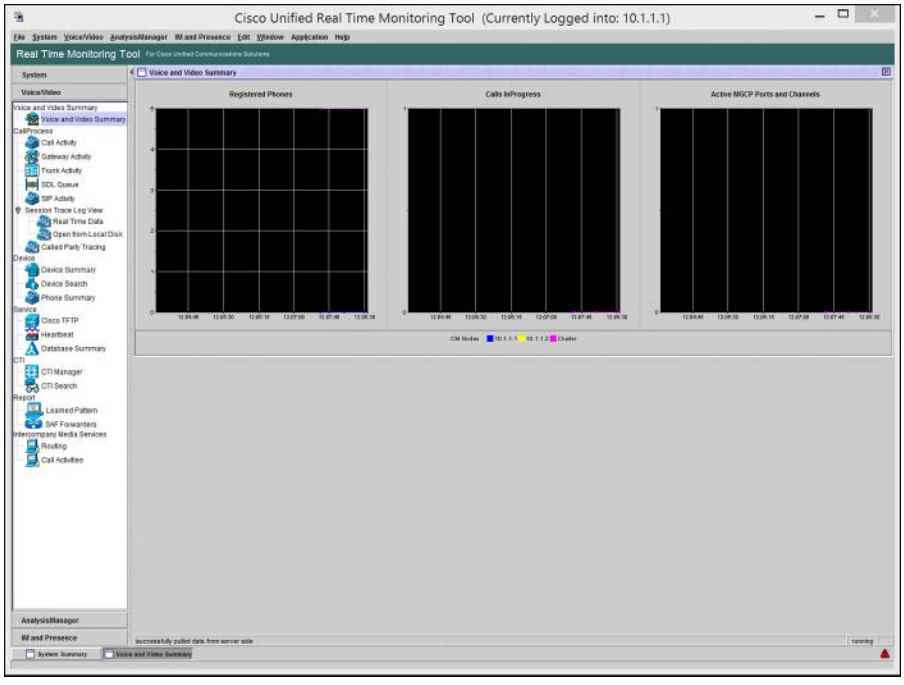


Figure 16-8 *RTMT Voice and Video Summary Screen*

Gateway Activity

The Gateway Activity view displays a summary of calls in progress for a specific type of gateway (MGCP FXS/FXO/T1/PRI or H.323). Information on the number of completed calls per gateway type (per server or per cluster) can also be displayed, as shown in Figure 16-9.

Note This information is listed per gateway type, not per gateway.

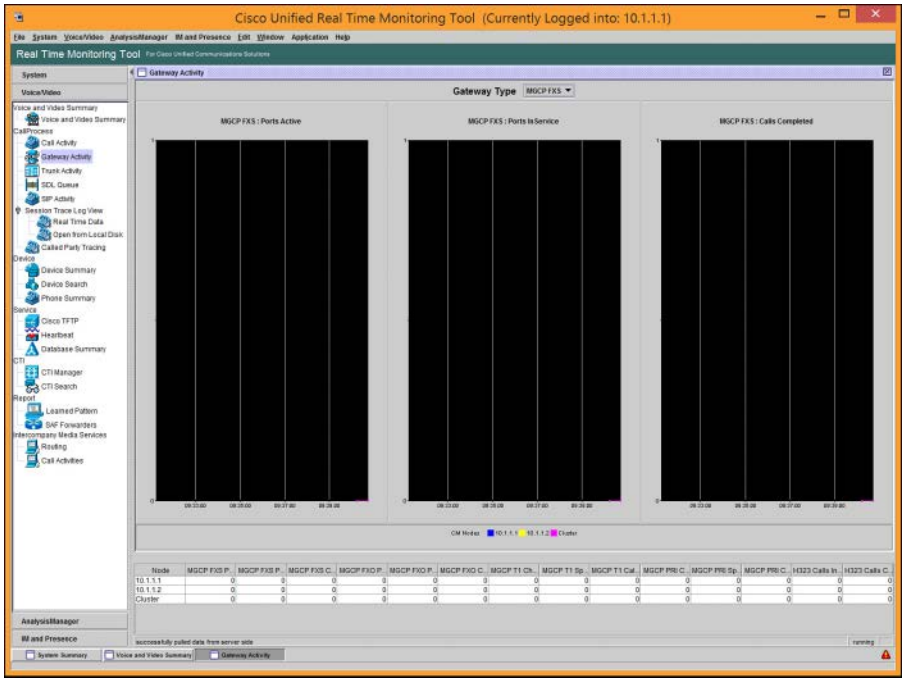


Figure 16-9 *RTMT Gateway Activity Screen*

Device Search

Administrators can search for phones, gateway devices, H.323 devices, CTI devices, voice-messaging devices, media resources, hunt lists, and Session Initiation Protocol (SIP) trunks. For each type of device, the administrator can search by status (registered, unregistered, rejected, any status, and devices that are only configured in the database). In addition, the search can be limited to a specific model of device or (for phones) specific protocol. The search results are presented in table format, one row per device and one column for each criterion selected for display, as illustrated in Figure 16-10.

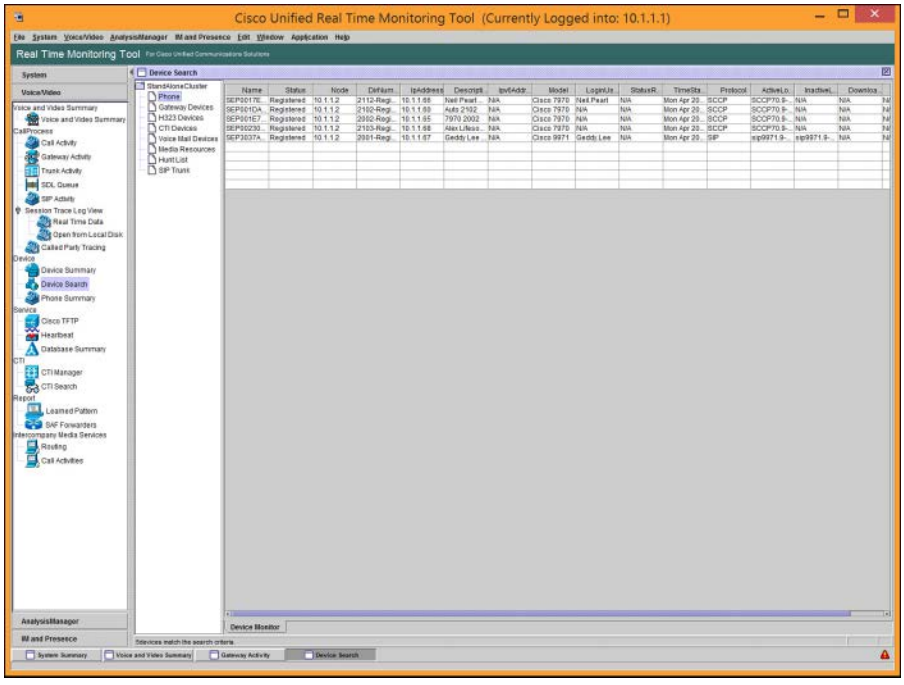


Figure 16-10 *RTMT Device Search (Phones) Screen*

Database Summary

The Database Summary view, as shown in Figure 16-11, shows the replication status, number of replicates created, the number of change notification requests queued in the database and in memory, and the total number of connection clients. For each server in the cluster, it can also display the current replication status.

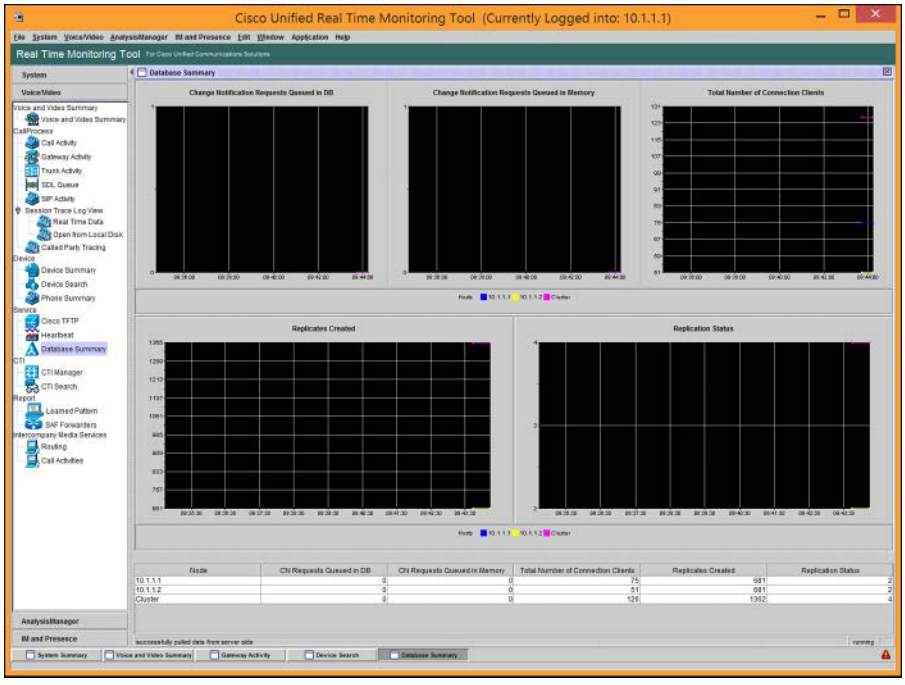


Figure 16-11 *RTMT Database Summary Screen*

Call Activity

The Call Activity view, shown in Figure 16-12, graphs the following:

- Calls completed
- Calls attempted
- Calls in progress
- Logical partition failures total

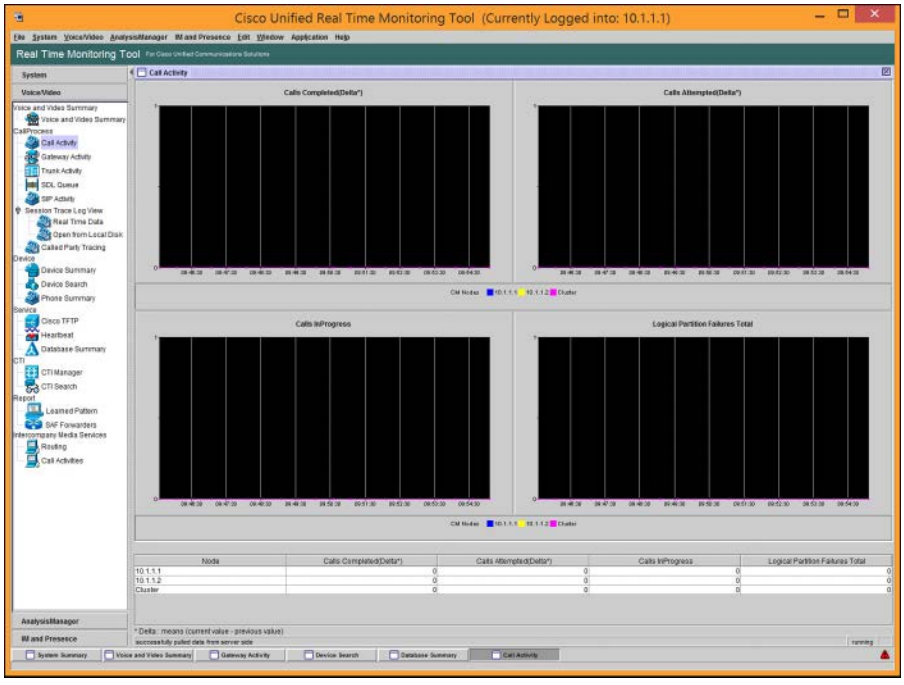


Figure 16-12 *RTMT Call Activity Screen*

You can also create custom views of specific performance counters by using the **System > Performance** screen. From a selected server, using the tree structure you can select up to six graphs to display. (You can also display the data in a chart format.) Figure 16-13 shows a custom Performance view.

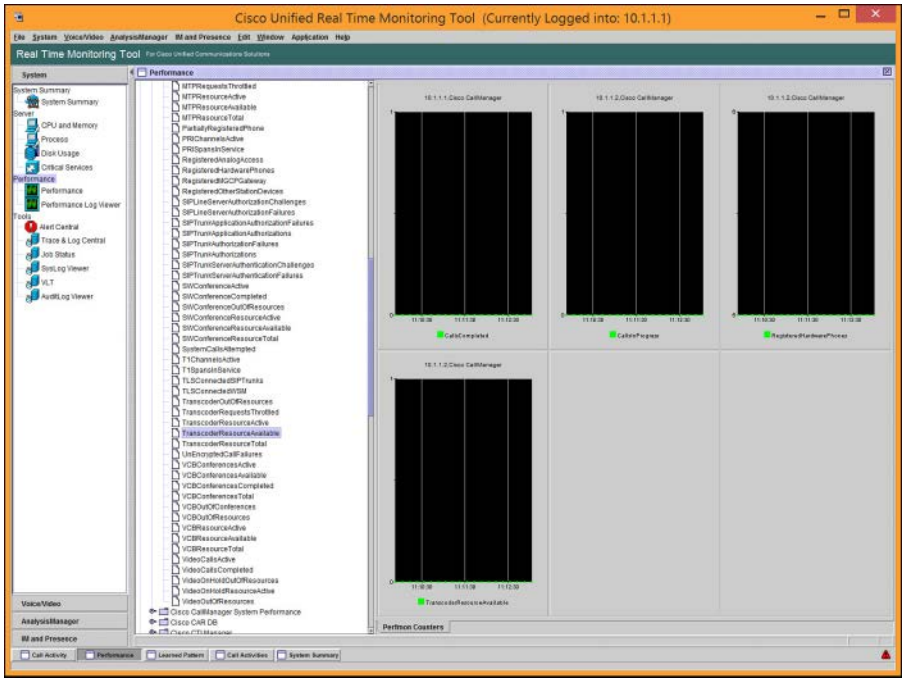


Figure 16-13 *RTMT Call Activity Screen*

Alert Central

The Alert Central view, shown in Figure 16-14, displays both predefined and custom-configured alerts in a chart format. You can right-click any alert and select **Alert Details** to read detailed information about the alert.

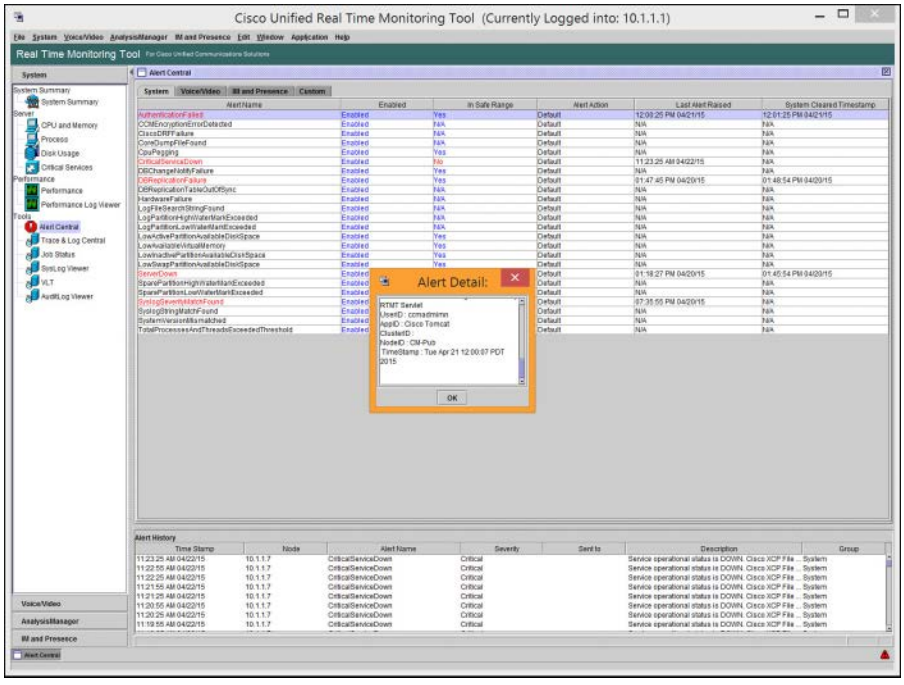


Figure 16-14 *RTMT Alert Central Screen*

Remote Browse

RTMT provides the capability to browse through trace files on the server (or, alternatively, they can be downloaded via FTP/SFTP). Enabling trace file collection puts a performance load on the server and should be done only when troubleshooting, but the information is useful and easily accessed via RTMT using **System > Tools > Trace and Log Central > Remote Browse**. You must then select the services to gather info from and browse through.

Syslog

RTMT provides a simple-to-use syslog viewer. From **System > Tools > Syslog Viewer**, select the node for which you want to see syslog entries, and then choose the appropriate file. (They are date/time named.) Figure 16-15 shows a sample syslog output.

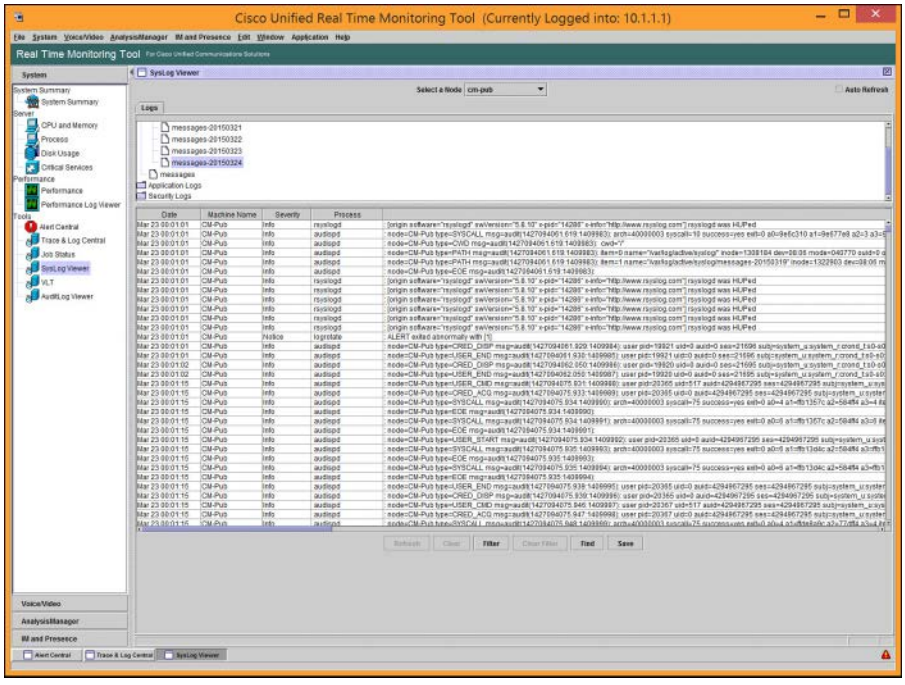


Figure 16-15 *RTMT Alert Central Screen*

Describe the Disaster Recovery System

Key Topic

The disaster recovery system (DRS) enables administrators to perform scheduled backups or manual backups of the CUCM and CDR/CAR databases. It also backs up and restores its own configuration settings, so in the event of a restore, the DRS does not have to be totally reconfigured.

The DRS includes GUI and CLI user interfaces, a backup scheduler, SFTP backup storage (in CUCM 10.x the local tape device option is no longer an option), and a distributed system architecture for backup and restore functions. Backups must be restored to the same version of the application. The DRS cannot be used as an upgrade/downgrade mechanism.

The DRS architecture features a local agent on each server in the cluster (which performs the backup and restore operations) and a master agent on the Publisher. The master agent does the following:

- Stores system-wide component registration information
- Maintains the schedule of backup tasks and sends the tasks to the local agents as scheduled
- Stores backups on a local tape drive or a remote SFTP server
- Interfaces with the administrator via the DRS web page

The DRS web interface is accessed at https://<*ip_address*>/drf or by using the drop-down navigation selection at the top-right of the CUCM administration page. By default, only the Platform Administration account has access to the DRS, but other accounts can be given the necessary privilege.

The DRS is a common feature of all Linux-based Unified Communication applications, but different components are backed up based on the application. Table 16-2 lists the components that can be backed up for CUCM, CUC, and CUP.

Table 16-2 Components Backed Up by DRS

CUCM	CUP	CUC
Platform	Platform	Platform
Cisco License Manager	Cisco License Manager	Cisco License Manager
Trace Collection Tool	Trace Collection Tool	Trace Collection Tool
Syslog	Syslog	Syslog
CUCM DB	CUP DB	CUC DB
TFTP/MoH Files	XCP Data	Mailbox Store
CDR/CAR Data	CUP Data	Greetings

Using the DRS

The DRS is a simple interface. The following sections outline its use.

Set Up a Backup Device

Before any backups can happen, you must create a backup device by following these steps:

Step 1. In the DRS, navigate to **Backup > Backup Device**.

Step 2. Provide a name for the backup device being created.

Step 3. Specify the IP address, SFTP root path, and SFTP account the DRS should use.

Step 4. Click **Save**. (You can create up to 10 backup devices.)

Create a Scheduled Backup

Now that we have a backup device, we can schedule a backup to use it by following these steps:

Step 5. Navigate to **Backup > Scheduler**.

Step 6. Click **Add New**.

Step 7. Provide a name for the schedule.

Step 8. Select the previously defined backup device this job should use.

Step 9. Select the features to back up. Depending on the application, these may be

- **CUCM:** CCM, CDR_CAR
- **CUC:** CONNECTION_DATABASE, CONNECTION_GREETINGS_VOICENAMES, CONNECTION_MESSAGES_UNITYMBXDB1, CUC
- **CUP:** CUPS, CUP

Step 10. Define the schedule for the backup.

Step 11. Enable the scheduled job.

If desired, a manual backup can be started by navigating to **Backup > Manual Backup** and performing the same steps, except that instead of defining a schedule, simply start the backup job.

Whether the backup is scheduled or manual, understand that the process is resource-intensive, and it is recommended that they be run during times of low demand on the server if possible.

The status of the backup jobs can be observed by navigating to **Backup > Current Status**. A list of the components of the backup job and the completion percentage for each component is presented. Components that are complete show a link to the log file.

Perform a Restore

The purpose of having backups is to be able to restore our data when necessary. The following steps describe the basic restore process:

Step 1. Navigate to **Restore > Restore Wizard**.

Step 2. Select the device that holds the backup file from which you want to restore.

Step 3. Select the correct backup file from the list available on that device.

Step 4. Select the features you want to restore. It should be self-evident that if a feature was not backed up, it cannot be restored!

Step 5. If the restore is coming from an SFTP server, you may select the optional **File Integrity Check**, which ensures that the restored data is not corrupted. Doing so takes significant server and network resources and slows down the restore process.

Step 6. Select the servers that should be restored. If the Publisher (first node) is selected for restore, the DRS automatically restores the database on the subscribers (subsequent nodes). However, in either case, all existing data is overwritten by the restore.

Step 7. Monitor the restore progress by navigating to **Restore > Current Status**.

Administrators should be familiar with the content of the *Disaster Recovery System Administration Guide* for their versions of software and should practice restore scenarios in a lab environment.

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 16-3 describes these key topics and identifies the page number on which each is found.

Table 16-3 Key Topics for Chapter 16

Key Topic Element	Description	Page Number
Figure 16-1	Troubleshooting steps	421
Topic	IP phone registration troubleshooting	422
Topic	Generating CDR reports	430
Topic	Generating system reports	433
Topic	Describe Cisco Unified RTMT	434
Topic	Describe the disaster recovery system	444

Definitions of Key Terms

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

troubleshooting, Call Detail Record (CDR), Call Management Record (CMR), Call Detail Record Analysis and Reporting (CAR), Disaster Recovery System (DRS)

This chapter covers the following topics:

- **Generating and Accessing Cisco Unity Connection Reports:** This section reviews how to create and locate CUC reports.
- **Analyzing Cisco Unity Connection Reports:** This section examines the content of CUC reports and how to interpret them.
- **Troubleshooting and Maintenance Operations Using Cisco Unity Connection Reports:** This section provides guidance and examples for using CUC reports for the troubleshooting and maintenance of CUC.

CHAPTER 17

Monitoring Cisco Unity Connection

Cisco Unity Connection (CUC) includes a variety of built-in reports to help administrators track the server's health and performance, as well as the activities of the users. This chapter introduces the use and content of many of these reports.

"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 17-1 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 17-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Generating and Accessing Cisco Unity Connection Reports	1–6
Analyzing Cisco Unity Connection Reports	7–8
Troubleshooting and Maintenance Operations Using Cisco Unity Connection Reports	9–10

1. Cisco Unity Connection provides two built-in reporting interfaces. Name them. (Choose two.)
   - **a.** Cisco Unified Reporting
   - **b.** Cisco Unity Connection Reporting
   - **c.** Cisco Unity Connection Serviceability Reports Tool
   - **d.** Cisco Unified Serviceability Reports Archive
2. Which of the following is not a Cisco Unity Connection Serviceability Reports Tool report?
   - **a.** Server Report
   - **b.** Unused Voice Mail Accounts Report
   - **c.** User Lockout Report
   - **d.** Port Activity Report
   - **e.** Users Report

3. Which of the following are Cisco Unified Serviceability Reports Archive reports? (Choose two.)
   a. Mailbox Store Report
   b. Alert Report
   c. System Configuration Report
   d. Server Report
   e. Message Traffic Report
4. What service must be activated in order to begin the collection of the Cisco Unified Serviceability Reports Archive report data?
   a. Cisco Serviceability Reporter
   b. Cisco UXL Web Service
   c. Cisco Reports Harvester
   d. Cisco Unity Connection Serviceability Harvester
5. How many reports are available in the Cisco Unified Serviceability Reports Archive?
   a. 20
   b. 2
   c. 20 per day
   d. 2 per day of data collection
6. You decide to increase the number of entries that can be held in the audit log. Where can this be done?
   a. It cannot be done.
   b. It is done by saving old log files to a syslog server and removing them from the original log location.
   c. It is done in the Service Parameters configuration page.
   d. In CUC Administration, navigate to **System Settings > Advanced > Reports**.
7. Ermeniglio decides to start using the Serviceability Reports Archive. He starts the correct service, waits until the next day, and opens the Alerts Report. He is confused to discover that the report shows no alerts for the previous day. What could be the issue?
   a. The service sometimes “sticks” and should be restarted.
   b. No alerts were generated by the server.
   c. The Display Alert Threshold setting must be lowered to critical or below.
   d. Ermeniglio must use the RTMT to see alerts.

8. Bob says he wants to see the details of the alerts shown in the Alerts Report in the Serviceability Archive. What should you do?
   a. Open the RTMT for CUC, go to Alert Central, and right-click any alert to see the details.
   b. Open RTMT, go to the Server tab, and look for the alert list.
   c. Select the Include Detail check box when generating the Alerts Report.
   d. Wait 30 seconds to make sure Bob is real, and then download the event log from the CUCM server.

9. The previous CUC administrator recently quit. You have been hired to take her place. You want to get a sense of how well-maintained the CUC server is. How can you find out if any accounts are still active but not in use?
   a. Run the Weekly Diagnostics Report.
   b. Run the Security Report.
   c. Run the Unused Voice Mail Accounts Report.
   d. Run the User Lockout Report.

10. Several days a week, usually between 8:00 a.m. and 9:00 a.m., users complain of MWI problems. Some have new messages, but their lamp is not lit; others complain that their lamp is on, but there are no new messages. You suspect that the server is not making MWI calls. How can you quickly check whether or not this is the case?
    a. Run the Port Simulator utility and send a test message.
    b. Run the Port Status Monitor in the afternoon.
    c. Come in early on Thursday, and try leaving a message for a user to see if the lamp comes on.
    d. Run the Port Activity Report.

Foundation Topics

Generating and Accessing Cisco Unity Connection Reports

There are two main interfaces for generating and viewing reports in CUC: in Cisco Unity Connection Serviceability under Tools > Reports, and in Cisco Unified Serviceability under **Tools > Serviceability Reports Archive**.

Cisco Unity Connection Serviceability Reports

Key Topic

The CUC Serviceability application provides 20 different reports that assist the administrator in monitoring and understanding the status and behavior of the CUC application. Figure 17-1 shows the CUC Serviceability Reports page with all 20 reports listed.

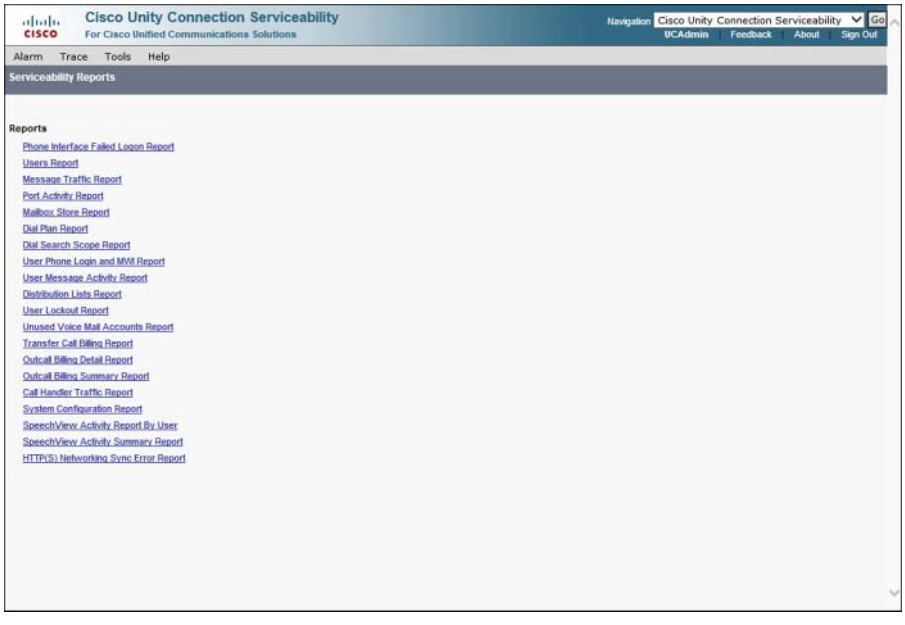


Figure 17-1 *CUC Serviceability Reports Page*

To access these reports, open the CUC Serviceability application and navigate to **Tools > Reports**. The list of reports includes the following:

- Phone Interface Failed Logon Report
- Users Report
- Message Traffic Report
- Port Activity Report
- Mailbox Store Report
- Dial Plan Report

- Dial Search Scope Report
- User Phone Login and MWI Report
- User Message Activity Report
- Distribution Lists Report
- User Lockout Report
- Unused Voice Mail Accounts Report
- Transfer Call Billing Report
- Outcall Billing Report
- Outcall Billing Summary Report
- Call Handler Traffic Report
- System Configuration Report
- SpeechView Activity Report by User
- SpeechView Acitivity Summary Report
- HTTPS Networking Sync Error Report

Let's take the example of running the Users Report. From the CUC Serviceability Reports page, click **Users Report**. The screen shown in Figure 17-2 appears.

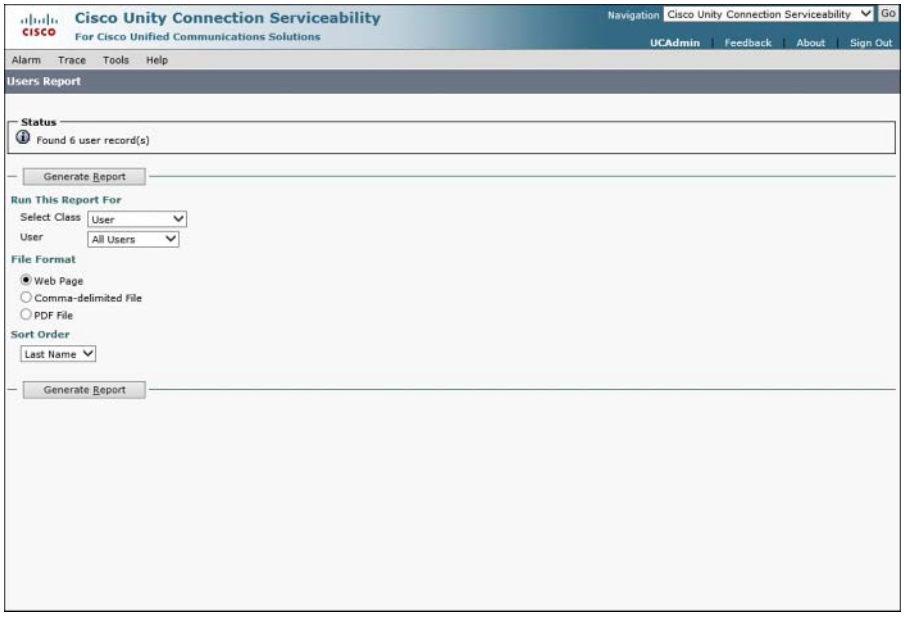


Figure 17-2 *Users Report Configuration Page*

The following selections can be made to customize the report (shown in Figure 17-2):

Run This Report For:

- Select Class:
  - User
  - Distribution List
  - COS
- User:
  - All Users
  - Selected User

File Format:

- Web Page
- Comma-Delimited File
- PDF File

Sort Order:

- Last Name
- First Name
- Extension
- COS

After you customize your selections, click **Generate Report**.

Figure 17-3 shows a sample output of the Users Report.

The Users Report includes the following information, as shown in Figure 17-3:

- Last Name, First Name, and Alias
- Location
- Home Mail Server
- Billing ID, CoS, and Extension
- Account Lockout Status
- Personal Call Transfer Rules Enabled/Disabled Status

The other reports in the CUC Serviceability Reports list are used in a similar way. Each report provides insight into the current status, configuration, and utilization of the CUC server.

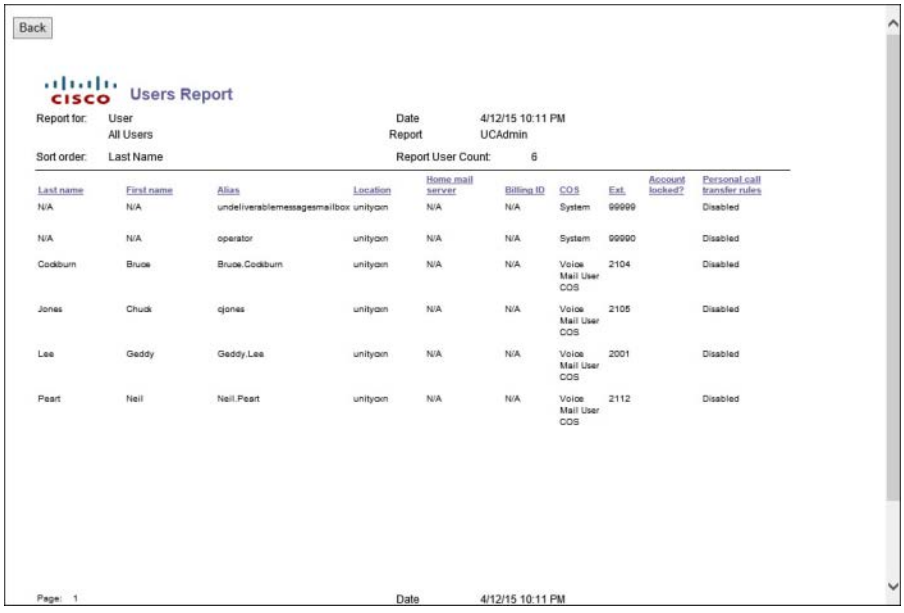


Figure 17-3 *Sample Output: Users Report*

Cisco Unified Serviceability: Serviceability Reports Archive

Key Topic

CUC includes a built-in reporting system to monitor server health and performance. These reports are accessed through the Unified Serviceability web application (not to be confused with the CUC Serviceability application). To access these reports, you must first activate the Cisco Serviceability Reporter service. In Unified Serviceability, navigate to **Tools > Service Activation**. Select the Cisco **Serviceability Reporter service** and click **Save**.

The Serviceability Reporter collects data from log files and populates the Serviceability Reports Archive, which stores report information and makes it available on a daily basis. It is a CPU-intensive service, so consider whether activating it will negatively impact your server health or performance. The type and amount of data collected can be tuned in the CUC Administration interface. Navigate to **System Settings > Advanced > Reports** to modify the following:

- **Enable Audit Log:** Unchecking this box stops the logging of stored procedures. The default setting is Enabled.
- **Maximum Events Allowed in Audit Log:** This setting limits the number of entries in the audit log. When the defined number is exceeded, the oldest entries are overwritten. Values are between 1 and 100,000. The default is 100,000.
- **Enable Security Log:** Unchecking this box stops the recording of stored procedures to the security log. The default setting is Enabled.
- **Maximum Events Allowed in Security Log:** This setting limits the number of entries in the security log. When the defined number is exceeded, the oldest entries are overwritten. Values are between 1 and 100,000. The default is 100,000.
- **Minutes Between Data Collection Cycles:** This value controls how frequently report data is gathered from logs. The default is every 30 minutes.

- **Days to Keep Data in Reports Database:** Determines how many days of historical data should be kept in the reports database. The default is 90 days. Note that even if the report specifies a date range of more than 90 days in the past, the report will still be limited to this setting's value.
- **Reports Database Size (as a Percentage of Capacity) After Which the Reports Harvester Is Disabled:** Sets the maximum percentage of disk space the reports database may take up. When the value is reached, the CUC Report Harvester service is stopped, preventing the database size from growing. The default value is 80 percent.
- **Maximum Records in Report Output:** Limits the number of records presented in the report output. The allowed range is from 5000 to 30,000; the default is 25,000. Some reports impose their own restrictions due to the size of the report (for example, User Message Activity is limited to 25,000 records).
- **Minimum Records Needed to Display Progress Indicator:** This value determines whether running a report will cause a message to pop up before the report is generated, and a progress bar to be shown as it runs. The idea is to provide a warning that the selected report is large and may impact server performance. The allowed range is from 1 to 10,000. The default is 2500.

Figure 17-4 shows the Report Configuration page.

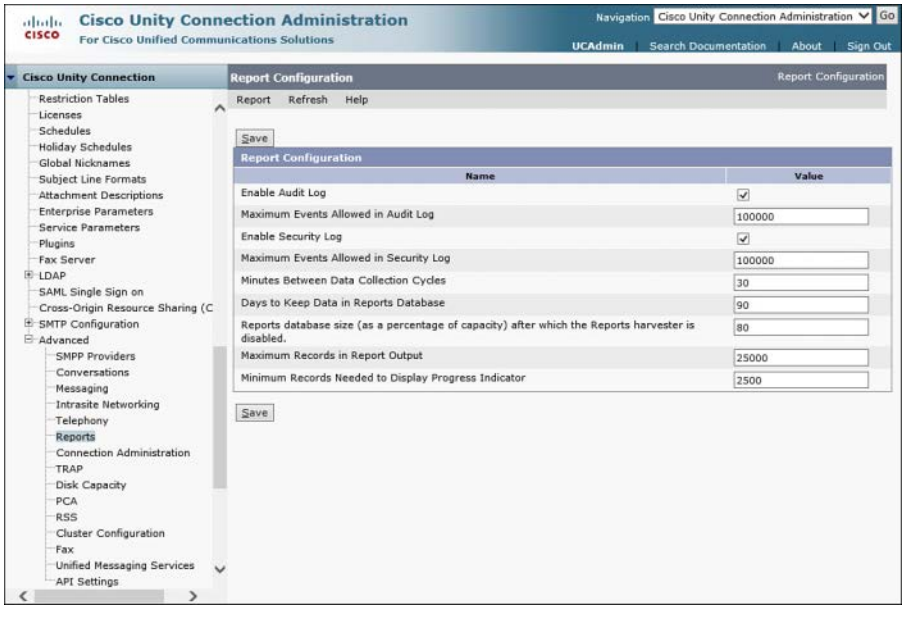


Figure 17-4 *CUC Administration Report Configuration Page*

Analyzing Cisco Unity Connection Reports

Key Topic

In the Cisco Unified Serviceability web application, navigate to **Tools > Serviceability Reports Archive**. Click the month for which you want to view reports, and then click the specific date. Figure 17-5 shows the Serviceability Reports Archive list page.

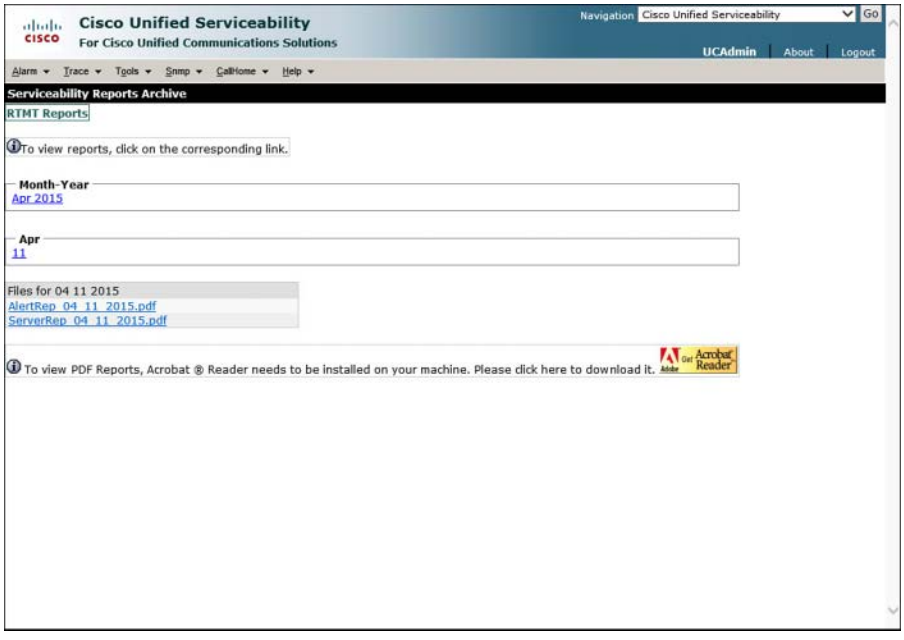


Figure 17-5 *Serviceability Reports Archive List Page*

There are two Serviceability Archive Reports available to view (assuming enough time has elapsed to provide data to collect it).

The Alerts Report displays the following:

- Number of alerts per severity in the cluster
- Number of alerts per server
- Top ten alerts in the cluster

Figure 17-6 shows one of the pages in the Alerts Report.

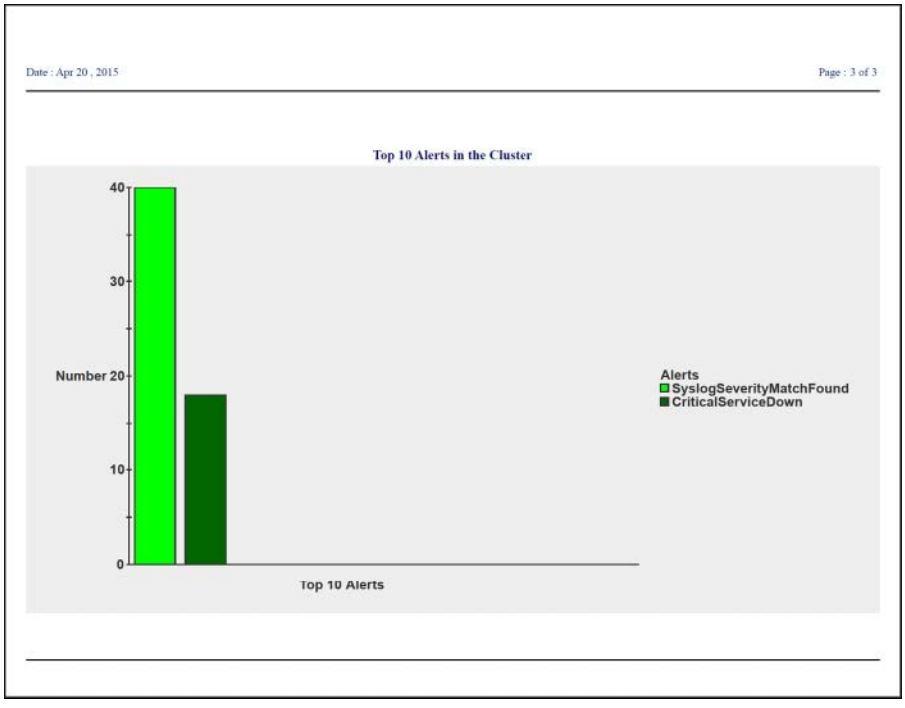


Figure 17-6 *Alerts Report*

Because these reports are just summaries, showing no details of the alerts (only what severity level and to which server they are attributed), it is likely that administrators will want to use the Real-Time Monitoring Tool (RTMT) to look at the server alerts in more detail. By opening Alert Central in RTMT (be sure to use the CUC version of RTMT), administrators can view the list of alerts, right-click any one of them, and select Alert Detail. A window pops up to show the details of the logged alert.

The Server Report provides statistics (in graph format) for the following:

- Percentage CPU per Server
- Percentage Memory Usage per Server
- Percentage Hard Disk Usage of the Common Partition per Server
- Percentage Hard Disk Usage of the Spare Partition per Server

Figure 17-7 shows the Server Report.

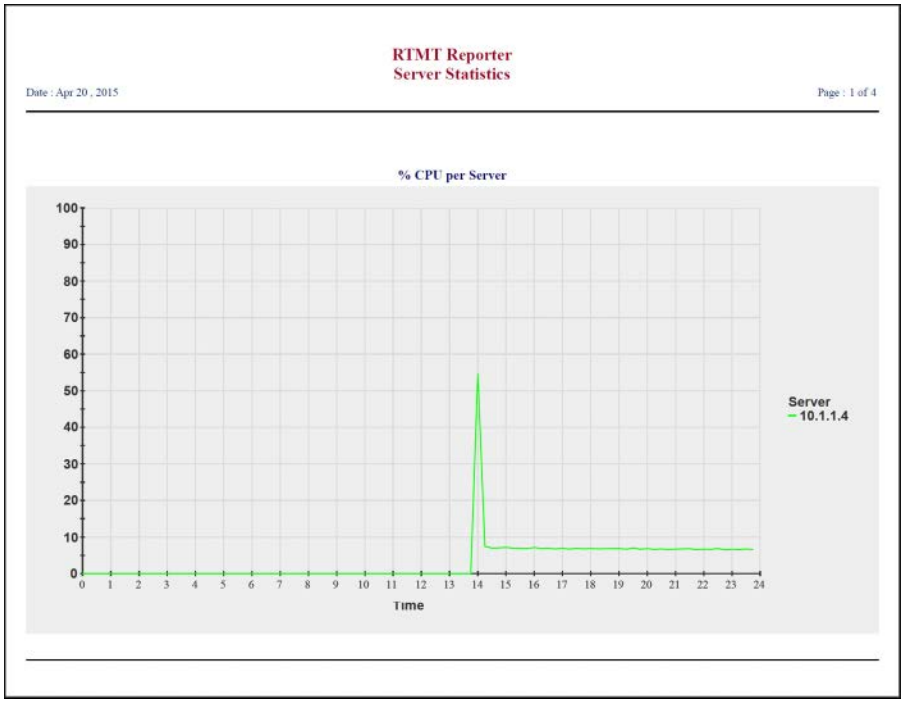


Figure 17-7 *Server Report*

Troubleshooting and Maintenance Operations Using Cisco Unity Connection Reports

Key Topic

The CUC Serviceability Reports provide insight into what is happening on the server. For example:

- An administrator might run the **Phone Interface Failed Logon Report** to see whether there are a significant number of failed logins for a given time period. If there are, the next question is whether these failed attempts to log in are a user issue (which could be resolved by talking with the user) or evidence of an attempt to hack into the user's mailbox. Figure 17-8 shows the Phone Interface Failed Logon Report.

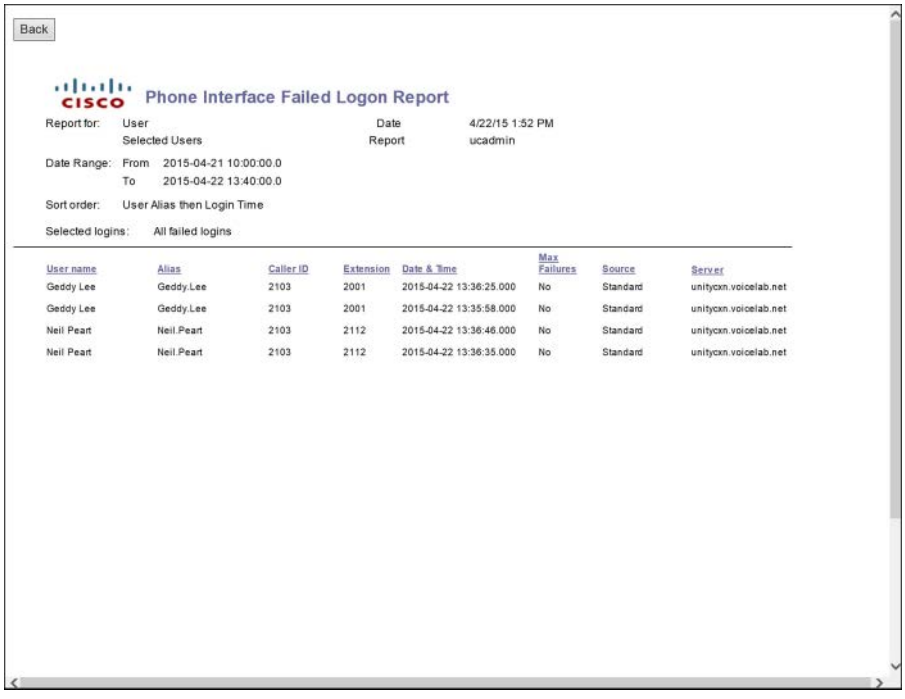


Figure 17-8 *Phone Interface Failed Logon Report*

- The **User Lockout Report** (often run in conjunction with the Failed Login Report) provides a quick list of which accounts are locked out, why, and when they were locked. The administrator can then contact the locked-out users and take any corrective action required; then, in the CUC Administration web application, the administrator can navigate to **Users > Users**, select the affected user, navigate to **Edit > Password Settings**, and click **Unlock Password** to unlock the user's account. Figure 17-9 shows the User Lockout Report.

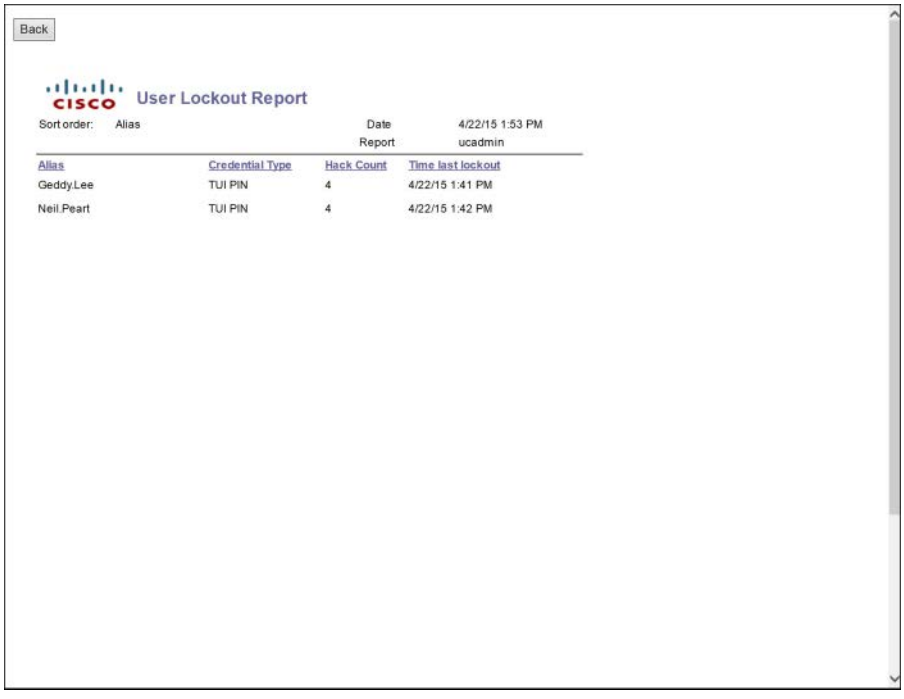


Figure 17-9 *User Lockout Report*

- The **Port Activity Report** shows the following statistics for each voicemail port on the server:
  - Port Name
  - Inbound Calls
  - Outbound MWI
  - Outbound AMIS
  - Outbound Notification
  - Outbound TRAP
  - Port Total

The administrator can determine whether all ports are active and usable and may be able to determine the cause of an MWI problem (perhaps because no ports have been assigned to perform MWI only). Figure 17-10 shows the Port Activity Report.

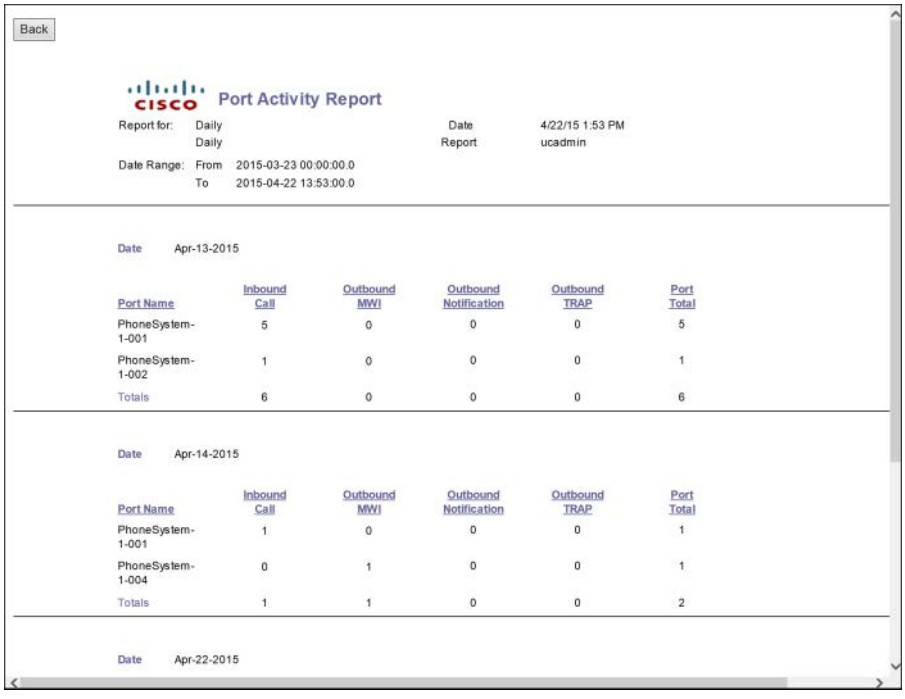


Figure 17-10 *Port Activity Report*

Reports to Support Routine Maintenance

Close monitoring of the mailbox stores helps prevent running out of disk space and spot any other issues before they cause a service interruption. The Mailbox Store Report provides a summary view of the current size, last error condition, and status of the mailbox store. Figure 17-11 shows the Mailbox Store Report.

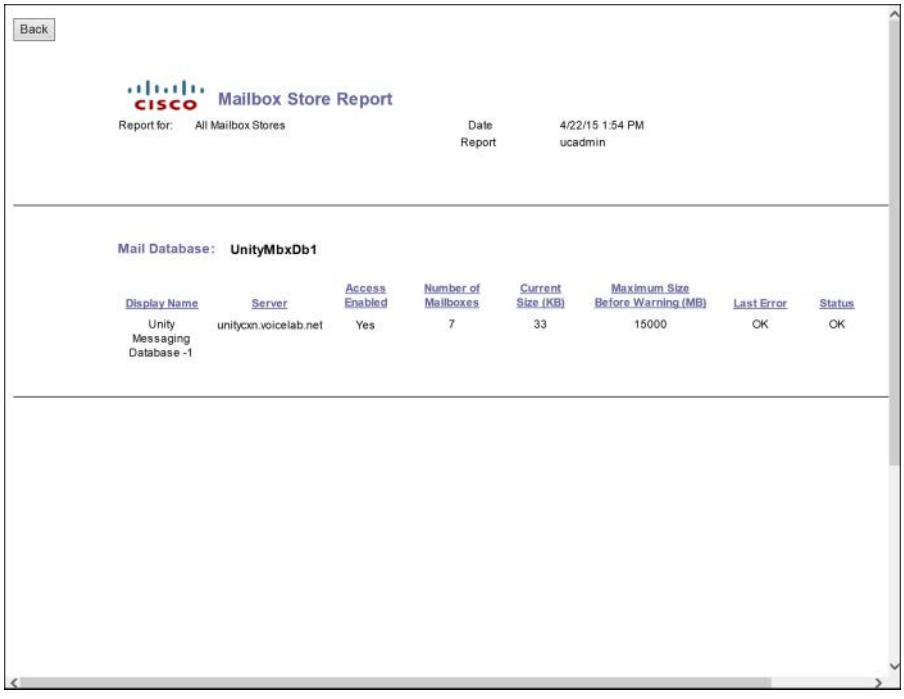


Figure 17-11 *Mailbox Store Report*

In a larger organization, employees sometimes leave the company and the voicemail administrators may not be aware of it. The **Unused Voice Mail Accounts Report** makes it simple to spot accounts that have not been used recently, allowing the administrator to take the appropriate action. Figure 17-12 shows the Unused Voice Mail Accounts Report.

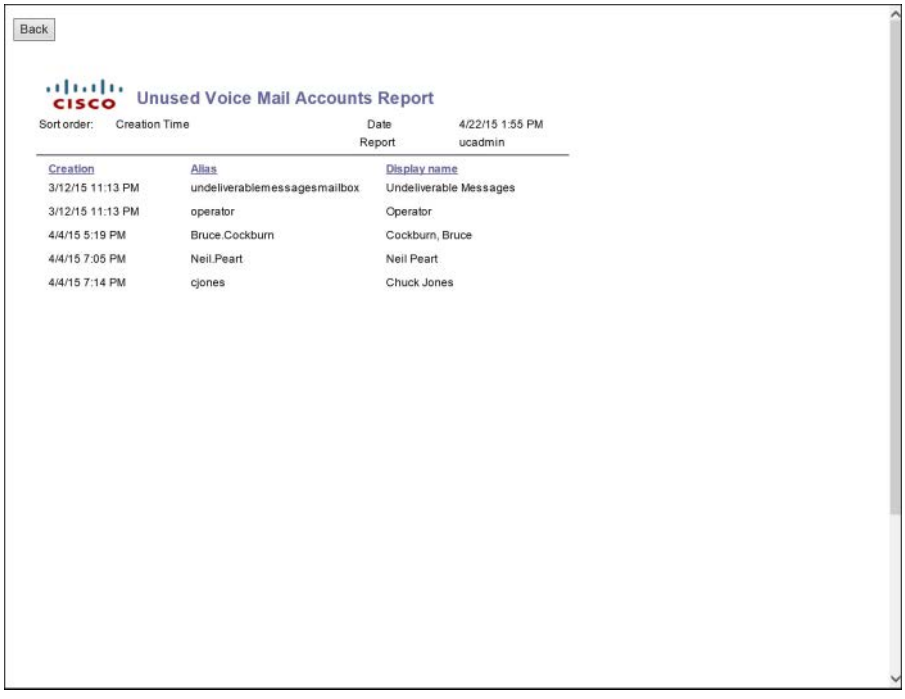


Figure 17-12 *Unused Voice Mail Accounts Report*

It is common to track the number of calls that CUC makes, either for statistical purposes or for actual cost billing purposes. Remember that CUC can place calls at the user's request (assuming their class of service [CoS] allows it), and these calls can incur toll charges. Likewise, if CUC performs Message Notification, it is possible that some of those calls may incur toll charges as well. There are three billing reports available to allow administrators to easily correlate the number and time of these kinds of calls with the user account that caused them to be placed:

- **Transfer Call Billing Report lists:**
  - Name, extension, and billing ID of the user
  - Date/time stamp for the call
  - Called number
  - Transfer result (Connected, Ring No Answer, Busy, or Unknown)
- **Outcall Billing Detail Report** is sorted by day, user extension, and lists:
  - Name, extension, and billing ID of the user
  - Date/time stamp for the call
  - Called number
  - Transfer result (Connected, Ring No Answer, Busy, or Unknown)
  - Duration of the call (in seconds)
- **Outcall Billing Summary Report** is sorted by date, name, extension, and billing ID, and shows the dial-out time in seconds for each hour of the day.

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 17-2 describes these key topics and identifies the page number on which each is found.

Key Topic

Table 17-2 Key Topics for Chapter 17

Key Topic Element	Description	Page Number
Section	Cisco Unity Connection Serviceability reports	452
Section	Cisco Unified Serviceability: Serviceability Reports Archive	455
Section	Analyzing Cisco Unity Connection reports	457
Section	Troubleshooting and maintenance operations using Cisco Unity Connection reports	459

Definitions of Key Terms

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

Cisco Unified Serviceability reports, Cisco Unified Serviceability Archive

The first 17 chapters of this book cover the technologies, protocols, commands, and features required to be prepared to pass the 210-060 CICD (Implementing Cisco Collaboration Devices) exam to become certified as a CCNA Collaboration professional. Although these chapters supply the detailed information, most people need more preparation than just reading alone. This chapter details a set of tools and a study plan to help you complete your preparation for the exam.

This short chapter has two main sections. The first section explains how to install the exam engine and practice exams from the CD that accompanies this book. The second section lists some suggestions for a study plan, now that you have completed all the earlier chapters in this book.

Note Appendixes D, E, and F exist as soft-copy appendixes on the CD included in the back of this book.

CHAPTER 18

Final Preparation

Tools for Final Preparation

This section lists some information about exam preparation tools and how to access the tools.

Exam Engine and Questions on the CD

The CD in the back of the book includes the Pearson Cert Practice Test engine. This software presents you with a set of multiple-choice questions, covering the topics you will likely find on the real exam. The Pearson Cert Practice Test engine lets you study the exam content (using study mode) or take a simulated exam (in practice exam mode).

The CD in the back of the book contains the exam engine. Once installed, you can then activate and download the current CICD exam from Pearson's website. Installation of the exam engine takes place in two steps:

Step 1. Install the exam engine from the CD.

Step 2. Activate and download the CICD practice exam.

Install the Exam Engine

The following are the steps you should perform to install the software:

Step 1. Insert the CD into your computer.

Step 2. The software that automatically runs is the Cisco Press software to access and use all CD-based features, including the exam engine and the CD-only appendixes. From the main menu, click the option to **Install the Exam Engine**.

Step 3. Respond to the prompt windows as you would with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the CD sleeve. This process requires that you establish a Pearson website login. You need this login in order to activate the exam. Therefore, please register when prompted. If you already have a Pearson website login, you do not need to register again; just use your existing login.

Activate and Download the Practice Exam

Once the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

Step 1. Start the Pearson Cert Practice Test (PCPT) software.

Step 2. To activate and download the exam associated with this book, from the **My Products** or **Tools** tab, click the **Activate** button.

Step 3 At the next screen, enter the Activation Key from the paper inside the cardboard CD holder in the back of the book. Once entered, click the **Activate** button.

Step 4. The activation process will download the practice exam. Click **Next**; then click **Finish**.

Once the activation process is completed, the **My Products** tab should list your new exam. If you do not see the exam, make sure you selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam, and click the **Use** button.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab, and select the **Update Products** button. Updating your exams will ensure you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, simply select the **Tools** tab, and click the **Update Application** button. This ensures you are running the latest version of the software engine.

Activating Other Exams

The exam software installation process and the registration process only have to happen once. Then, for each new exam, only a few steps are required. For instance, if you buy another new Cisco Press Official Cert Guide or Pearson IT Certification Cert Guide, remove the activation code from the CD sleeve in the back of that book—you do not even need the CD at this point. From there, all you have to do is start the exam engine (if not still up and running), and perform Steps 2 through 4 from the previous list.

Premium Edition

In addition to the free practice exam provided on the CD-ROM, you can purchase additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition of this title contains an additional two full practice exams as well as an eBook (in both PDF and ePub format). In addition, the Premium Edition title also has remediation for each question to the specific part of the eBook that relates to that question.

Because you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. There is a coupon code in the CD sleeve that contains a one-time use code, as well as instructions for where you can purchase the Premium Edition.

To view the premium edition product page, go to http://www.ciscopress.com/title/9781587144431.

The Cisco Learning Network

Cisco provides a wide variety of CCNA Collaboration preparation tools at a Cisco website called the Cisco Learning Network. Resources found here include sample questions, forums on each Cisco exam, learning video games, and information about each exam.

To reach the Cisco Learning Network, go to learningnetwork.cisco.com, or just search for "Cisco Learning Network." To access some of the features/resources, you need to use the login you created at www.cisco.com. If you do not have such a login, you can register for free. To register, simply go to http://www.cisco.com; click Register at the top of the page; and supply some information.

Memory Tables

Like most Certification Guides from Cisco Press, this book purposefully organizes information into tables and lists for easier study and review. Rereading these tables can be very useful before the exam. However, it is easy to skim over the tables without paying attention to every detail, especially when you remember having seen the table's contents when reading the chapter.

Instead of simply reading the tables in the various chapters, this book's Appendixes D and E give you another review tool. Appendix D, "Memory Tables," lists partially completed versions of many of the tables from the book. You can open Appendix D (a PDF on the CD that comes with this book) and print the appendix. For review, you can attempt to complete the tables. This exercise can help you focus during your review. It also exercises the memory connectors in your brain; plus it makes you think about the information without as much information, which forces a little more contemplation about the facts.

Appendix E, "Memory Tables Answer Key," also a PDF located on the CD, lists the completed tables to check yourself. You can also just refer to the tables as printed in the book.

Chapter-Ending Review Tools

Chapters 1 through 17 each have several features in the "Exam Preparation Tasks" section at the end of the chapter. You may have used some of or all these tools at the end of each chapter. It can also be useful to use these tools again as you make your final preparations for the exam.

Study Plan

With plenty of resources at your disposal, you should approach studying for the CCNA Collaboration exam with a plan. Consider the following ideas as you move from reading this book to preparing for the exam.

Recall the Facts

As with most exams, many facts, concepts, and definitions must be recalled to do well on the test. If you do not work with security technologies and features on a daily basis, you might have trouble remembering everything that might appear on the CCNA Collaboration exam.

You can refresh your memory and practice recalling information by reviewing the activities in the "Exam Preparation Tasks" section at the end of each chapter. These sections will help you study key topics, memorize the definitions of important security terms, and recall the basic command syntax of configuration and verification commands.

Practice Configurations

The CCNA Collaboration exam includes an emphasis on practical knowledge. You need to be familiar with switch features and the order in which configuration steps should be implemented.

This means that hands-on experience is going to take you over the edge to confidently and accurately build or verify configurations (and pass the exam). If at all possible, try to gain access to some Cisco Catalyst switches; Cisco IOS routers running CME; a 7965 and 9971Cisco IP phone; and servers (virtual machines are easiest) running CM, CUC, and CM-IMP. I know that is a tall order, but we cannot avoid the fact that hands-on experience means you need to get your hands on some gear.

If you have access to a lab provided by your company, take advantage of it. You might also have some Cisco equipment in a personal lab at home. Otherwise, there are a number of sources for lab access, including online rack rentals from trusted Cisco Partners and the Cisco Partner E-Learning Connection (PEC), if you work for a partner. Nothing beats hands-on experience.

In addition, you can review the key topics in each chapter and follow the sample configurations in this book. At the least, you will see the command syntax and the sequence in which the configuration commands should be entered.

Using the Exam Engine

The Pearson Cert Practice Test engine on the CD lets you access a database of questions created specifically for this book. The Pearson Cert Practice Test engine can be used either in study mode or practice exam mode, as follows:

- **Study mode:** Study mode is most useful when you want to use the questions for learning and practicing. In study mode, you can select options like randomizing the order of the questions and answers, automatically viewing answers to the questions as you go, testing on specific topics, and many other options.
- **Practice exam mode:** This mode presents questions in a timed environment, providing you with a more exam realistic experience. It also restricts your ability to see your score as you progress through the exam and view answers to questions as you are taking the exam. These timed exams not only allow you to study for the actual 210-060 CICD Exam, they help you simulate the time pressure that can occur on the actual exam.

When doing your final preparation, you can use study mode, practice exam mode, or both. However, after you have seen each question a couple of times, you will likely start to remember the questions, and the usefulness of the exam database may go down. So, consider the following options when using the exam engine:

- Use the question database for review. Use study mode to study the questions by chapter, just as with the other final review steps listed in this chapter. Consider upgrading to the Premium Edition of this book if you want to take additional simulated exams.
- Save the question database, not using it for review during your review of each book part. Save it until the end; so you will not have seen the questions before. Then, use practice exam mode to simulate the exam.

To select the exam engine mode, click the **My Products** tab. Select the exam you wish to use from the list of available exams; then click the **Use** button. The engine should display a window from which you can choose **Study Mode** or **Practice Exam Mode**. When in study mode, you can further choose the book chapters, limiting the questions to those explained in the specified chapters of the book.

Answers Appendix

Chapter 1

1. A
2. B
3. A
4. B, C
5. C
6. D
7. D
8. C, E
9. B
10. C
11. C
12. B, D

Chapter 2

1. A
2. A, B
3. C
4. B
5. D
6. C
7. B
8. D
9. A
10. B
11. B, C

Chapter 3

1. C
2. A, C
3. A, C
4. C
5. A
6. B
7. C
8. D
9. A
10. C
11. A
12. A, B
13. C

Chapter 4

1. A
2. D, E
3. B, C, E
4. A
5. D
6. B
7. C

Chapter 5

1. B, D, E
2. D
3. A
4. B
5. A, B, C, D
6. D
7. A, B, C
8. B
9. A
10. C

Chapter 6

1. A
2. D
3. C
4. E
5. D
6. A, C
7. B
8. C
9. B
10. B
11. C

Chapter 7

1. B
2. A, B, D
3. D
4. D
5. B
6. A, B, C, D
7. D
8. B, D
9. A
10. A

Chapter 8

1. D
2. C, D
3. B
4. B
5. F
6. A, C, E
7. C
8. B, C, F
9. C
10. B

Chapter 9

1. D
2. A
3. B
4. B

5. D
6. C
7. B
8. D
9. A
10. A

Chapter 10

1. B, C
2. B, D
3. A
4. E
5. E
6. A
7. F
8. E, F
9. B, D, E, F
10. D
11. C
12. C

Chapter 11

1. A
2. B
3. A, C, D
4. B
5. D
6. A
7. B, C
8. D
9. A, C, D
10. D

Chapter 12

1. D
2. A, B, C, D, E, F
3. D
4. A
5. C
6. B
7. A
8. B
9. C

Chapter 13

1. D
2. B
3. A, B, C
4. B
5. D
6. D, E
7. A, B, C
8. A
9. C
10. D

Chapter 14

1. C, D
2. A, B, C, D, E
3. E
4. B, D
5. C
6. D, E
7. A, B, C
8. A

Chapter 15

1. B
2. B, C, D
3. B
4. C
5. C
6. B
7. A
8. C
9. B
10. D

Chapter 16

1. D
2. D
3. D
4. A
5. C
6. A
7. A
8. C
9. C
10. C

Chapter 17

1. C, D
2. A
3. B, D
4. A
5. D
6. D
7. B
8. A
9. C
10. D

This page intentionally left blank

APPENDIX B

Exam Updates

Over time, reader feedback allows Cisco Press to gauge which topics give our readers the most problems when taking the exams. To assist readers with those topics, the authors create new material clarifying and expanding on those troublesome exam topics. As mentioned in the Introduction, the additional content about the exam is contained in a PDF document on this book's companion website, at http://www.ciscopress.com/title/9781587144431.

This appendix is intended to provide you with updated information if Cisco makes minor modifications to the exam upon which this book is based. When Cisco releases an entirely new exam, the changes are usually too extensive to provide in a simple update appendix. In those cases, you might need to consult the new edition of the book for the updated content.

This appendix attempts to fill the void that occurs with any print book. In particular, this appendix does the following:

- Mentions technical items that might not have been mentioned elsewhere in the book
- Covers new topics if Cisco adds new content to the exam over time
- Provides a way to get up-to-the-minute current information about content for the exam

Always Get the Latest at the Companion Website

You are reading the version of this appendix that was available when your book was printed. However, given that the main purpose of this appendix is to be a living, changing document, it is important that you look for the latest version online at the book's companion website. To do so

Step 1. Browse to http://www.ciscopress.com/title/9781587144431.

Step 2. Select the **Appendix** option under the More Information box.

Step 3. Download the latest Appendix B document.

Note Note that the downloaded document has a version number. Comparing the version of the print Appendix B (Version 1.0) with the latest online version of this appendix, you should do the following:

- Same version: Ignore the PDF that you downloaded from the companion website.
- Website has a later version: Ignore this Appendix B in your book, and read only the latest version that you downloaded from the companion website.

Technical Content

The current version of this appendix does not contain any additional technical coverage.

APPENDIX C

Managing CME Using the Command Line

As you read this paragraph, you identify yourself as one of two types of people. The first type of person sees the "Managing CME Using the Command Line" title and thinks, "Fantastic! I love working in the command line!" The second type of person sees the same title and thinks, "I would rather drive nails into my eye sockets than deal with the command line." If these two types of people met, they would probably not enjoy each other's company.

Command-line administration still remains the most flexible and supports all Cisco Unified Communications Manager Express (CME) features. However, the graphical user interface (GUI)-based utilities, specifically the Cisco Configuration Professional (CCP), have evolved enough to support simple configuration and troubleshooting for the majority of CME features. In some cases, the configuration performed using CCP is much more efficient than the using command-line administration. With that said, troubleshooting typically lives in the command-line domain, and each upcoming section presents a variety of **show** or **debug** commands that you can use to verify or troubleshoot the operation of your CME router. To access the command-line interface (CLI) of the CME router, use one of three methods:

- **Console port:** This how you initially configure the Cisco router before anyone has assigned a management IP address to the device. You can access the console port using a serial interface on a desktop or laptop PC and a Cisco rollover cable with the appropriate adapters.
- **Telnet access:** Since the 1970s, people have used Telnet to manage a variety of command-line systems. The industry now considers Telnet to be an unsecure protocol because it transmits data in clear text.
- **SSH access:** Secure Shell (SSH) performs the same function as Telnet but secures communication with a heavy dose of encryption. All modern Cisco equipment supports SSH capabilities out of the box, whereas older Cisco equipment might need an IOS upgrade to a security feature set.

Note The foundation IOS commands, such as **enable**, **configure terminal**, and **show**, are covered in the CCENT and CCNA certification guides, which are are not covered here.

To support a majority of the VoIP configuration, Cisco developed a telephony-service configuration mode. You can access this mode from global configuration mode, as shown in Example C-1.

Example C-1 *Accessing Telephony Service Configuration*

```
CME_ROUTER# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CME_ROUTER(config)# telephony-service
CME_ROUTER(config-telephony)# ?
Cisco Unified Communications Manager Express configuration commands.
For detailed documentation see:
http://www.cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_
home.html
  after-hours                   define after-hours patterns, date, etc
  application                   The selected application
  authentication                Config CME authentication server
  Auto                          Define dn range for auto assignment
  auto-reg-ephone               Enable Ephone Auto-Registration
  bulk-speed-dial               Bulk Speed dial config
  call-forward                  Configure parameters for call forwarding
  call-park                     Configure parameters for call park
  caller-id                     Configure caller id parameters
  calling-number                Replace calling number with local for hairpin
  cnf-file                      Ephone CNF file config options
  codec                         Define default codec for CME service
  conference                    Configure conference type for adhoc
  create                        create cnf for ethernet phone
  date-format                   Set date format for IP Phone display
  <output omitted>
```

Although there are commands that move outside of the telephony-service configuration mode (especially the critical dial-peer configurations, which are discussed in Chapter 6, "Understanding the CME Dial Plan"), Cisco keeps the core configurations centralized in one place.

As mentioned, most troubleshooting commands are performed from the CLI. Example C-2 shows one of the most common verification and troubleshooting commands used with CME: **show ephone registered**. This command verifies the active phones registered with CME and the status of their lines.

Example C-2 *show ephone registered Command Output*

```
CME_ROUTER# show ephone registered
ephone-1[0] Mac:0014.A89E.F845 TCP socket:[1] activeLine:0 REGISTERED in SCCP ver 17/9
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:172.30.100.40 36964 7970  keepalive 27761 max_line 8
Button  1: dn 1  number 1005 CH1   IDLE         CH2   IDLE
Preferred Codec: g711ulaw
```

With regard to the CICD exam, most of the basic commands for ephone and ephone-dn creation have been de-emphasized and replaced with knowing how to use CCP. However,

configuring the dial plan and most importantly understanding and troubleshooting the dial plan (including class of restriction [COR]) are still there, so do not skimp on reading Chapter 6, "Understanding the CME Dial Plan."

The output in Example C-3 is direct from the CME router used in building the first part of this book. I have made some annotations to explain what some of the configs do; you should try to understand them all, and you are welcome to borrow the config if you like.

Example C-3 *CICD CME Router Running-Config (Annotated)*

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CICD-CME
!
boot-start-marker
boot-end-marker
!
aqm-register-fnf
!
!
no aaa new-model
!
!
!
!
!



!
ip dhcp excluded-address 10.1.1.1 10.1.1.59
ip dhcp excluded-address 10.1.1.70 10.1.1.254
!
ip dhcp pool CICD-Voice
 network 10.1.1.0 255.255.255.0
 option 150 ip 10.1.1.1
 default-router 10.1.1.253
 lease 2
!
!
!
no ip domain lookup
ip domain name cicd.net
ip cef
no ipv6 cef
!
```

```
multilink bundle-name authenticated
!
!
!
!
!
!
trunk group TrunkGroup1
!
!
crypto pki trustpoint TP-self-signed-1633959155
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1633959155
 revocation-check none
 rsakeypair TP-self-signed-1633959155
!
!
crypto pki certificate chain TP-self-signed-1633959155
 certificate self-signed 01
!
!  ***output omitted***
!
        quit
voice-card 0
!
!
!
voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 no supplementary-service sip handle-replaces
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
 sip
  bind control source-interface GigabitEthernet0/1
  bind media source-interface GigabitEthernet0/1
  session transport tcp
  registrar server expires max 3600 min 120
  no silent-discard untrusted
!
!
voice register global
 mode  cme
 source-address 10.1.1.253 port 5060
!
```

```
! Defines source IP address:port for SIP signaling
!
 max-dn 25
!
! Defines maximum SIP DNs
!
 max-pool 10
!
! Defines maximum SIP phones
!
 load 9971 sip9971.9-2-2SR1-9
 create profile sync 0009464545565545
 camera
 video
!
voice register dn  2
 number 2001
 name Geddy Lee
 label Geddy Lee
 mwi
!
! Creates a SIP DN of 2001 and associates it with user Geddy Lee
!
voice register template  1
 camera
 video
!
voice register pool  2
 id mac 3037.A617.4B92
 type 9971
 number 1 dn 2
 presence call-list
 dtmf-relay rtp-nte
 username Lee.G password cisco
 codec g711ulaw
 no vad
 camera
 video
!
! Creates a SIP phone (type 9971) and associates it with user Geddy Lee
!(Lee.G)
! Associates Button 1 on the phone with SIP DN 2 (2001)
!
!
!
license udi pid 73-11834-11 sn ************
```

```
license boot module c2900 technology-package CollabProSuitek9
hw-module pvdm 0/0
!
!
!
file privilege 0
username ccmadmin privilege 15 password 0 1cisco23
username Peart.N password 0 cisco
!
redundancy
!
!
!
!
!
no ip ftp passive
ip ssh version 2
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.1.250 255.255.255.0
 duplex full
 speed 100
!
interface GigabitEthernet0/1
 ip address 10.1.1.253 255.255.255.0
 duplex full
 speed 100
!
!
ip forward-protocol nd
!
```

```
ip http server
ip http authentication local
ip http secure-server
ip http path flash:
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
!
!
tftp-server flash:IP_Phones/9971/Sip/sip9971.9-2-2SR1-9.loads alias sip9971.9-2-
2SR1-9.loads
!
! Specifies which firmware file 9971 phones will use
!
control-plane
!
!
voice-port 0/2/0
 trunk-group TrunkGroup1
 description CICDport020
 station-id name CICD
 station-id number 6045550020
 caller-id enable
!
voice-port 0/2/1
 trunk-group TrunkGroup1
 description CICDport021
 station-id name CICD
 station-id number 6045550021
!
voice-port 0/2/2
 trunk-group TrunkGroup1
 description CICDport022
 station-id name CICD
 station-id number 6045550022
!
voice-port 0/2/3
 trunk-group TrunkGroup1
 description CICDport023
 station-id name CICD
 station-id number 6045550023
!
! The sections above configure the four available FXO ports and make them
! part of a Trunk Group named TrunkGroup1.
!
voice-port 0/3/0
```

```
!
voice-port 0/3/1
!
voice-port 0/3/2
!
voice-port 0/3/3
 !
 !
 !
 !
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
dial-peer cor custom
 name 911
 name LOCAL
 name LD
!
! Creates the custom COR entries
!
dial-peer cor list 911-CALL
 member 911
!
dial-peer cor list LOCAL-CALL
 member LOCAL
!
dial-peer cor list LD-CALL
 member LD
!
dial-peer cor list 911-ONLY
 member 911
!
dial-peer cor list 911-LOCAL
 member 911
 member LOCAL
!
dial-peer cor list 911-LOCAL-LD
 member 911
 member LOCAL
```

```
 member LD
!
! Creates the custom COR lists for call privilege restrictions
!
dial-peer voice 90 pots
 description Service Dialing
 destination-pattern 9[469]11
!
! Creates a dial peer to match service numbers (411,611,911)
!
dial-peer voice 10 pots
 corlist outgoing 911-CALL
 description 911 Calls
 destination-pattern 911
 no digit-strip
!
! Creates a dial peer to match 911 calls; forwards all digits (911)
!
dial-peer voice 11 pots
 corlist outgoing 911-CALL
 description 9-911 Calls
 destination-pattern 9911
 forward-digits 3
!
! Creates a dial peer to match 9+911 calls; forwards only 911
!
dial-peer voice 91 pots
 corlist outgoing LOCAL-CALL
 description 10-Digit Dialing
 destination-pattern 9[2-9]..[2-9].....
 forward-digits 10
!
! Creates a dial peer to match 9+10-digit PSTN calls;
! forwards last 10 digits only
!
dial-peer voice 92 pots
 corlist outgoing LD-CALL
 description 11-Digit Dialing
 destination-pattern 91[2-9]..[2-9].....
 forward-digits 11
!
! Creates a dial peer to match 9+11-digit PSTN calls;
! forwards last 11 digits only

dial-peer voice 93 pots
 corlist outgoing LD-CALL
```

```
 description International Dialing
 destination-pattern 9011T
 prefix 011
!
! Creates a dial peer to match variable-length PSTN calls;
! Explicitly-dialed digits of 9011 are automatically stripped;
! Prefix of 011 is replaced for PSTN routability.

!
sip-ua
!
!
!
gatekeeper
 shutdown
!
!
telephony-service
 no auto-reg-ephone
 max-ephones 10
 max-dn 25
 ip source-address 10.1.1.253 port 2000
 service phone videoCapability 1
 cnf-file location flash:
 load 7970 SCCP70.9-2-1S.loads
!
! Specifies 7970 SCCP firmware load
!
 max-conferences 8 gain -6
 web admin system name ccmadmin password 1cisco23
!
! Identifies web admin account
!
 dn-webedit
 time-webedit
 transfer-system full-consult
 night-service code *1234
!
 directory entry 1 8262 name Randy Bachman
!
! Manually creates directory entry for Canadian rock legend Randy Bachman
!
 create cnf-files version-stamp 7960 Feb 09 2015 00:21:40
!
!
ephone-dn  1  dual-line
```

```
 number 2112
 label Neil Peart
 description Neil Peart  2112
 name Neil Peart
 hold-alert 30 originator
!
! Creates a SCCP DN of 2112 and associates it with user Neil Peart
!
ephone-dn  2  dual-line
 number 2002
 label Gord Downie
 description Gord Downie 2002
 name Gord Downie
 hold-alert 30 originator
 night-service bell
!
! Creates a SCCP DN of 2002 and associates it with user Gord Downie
!
ephone-dn  3
 number A200208
 description Intercom
 name Gord Downie
 intercom A211208 label "Intercom to Neil"
!
! Creates a SCCP intercom pair of A200208 to A211208 and associates it
! with user Gord Downie (target is Neil Peart's phone)
!
ephone-dn  4
 number 2004
 label Alex Lifeson
 name Alex Lifeson
!
! Creates a SCCP DN of 2004 and associates it with user Alex Lifeson
!
ephone-dn  5
 number A211208
 description Intercom
 name Neil Peart
 intercom A200208 label "Intercom to Gord"
!
! Creates a SCCP intercom pair of A211208 to A200208 and associates it
! with user Neil Peart (target is Gord Downie's phone)
!
!
ephone-dn  6
 number 7001
```

```
 description Main Floor Offices
 name Zone1
 paging ip 239.0.0.1 port 2000
!
! Creates a Paging group named "Zone 1"
!
ephone  1
 device-security-mode none
 mac-address 0017.E00C.C267
 username "Peart.N" password cisco
 type 7970 addon 1 7914
 button  1:1 8:5
!
! Creates a 7970 SCCP phone, associates it with user Neil Peart, puts DN
! 2112 on button 1, an intercom DN on button 8, and adds a 7914 add-on
! module.
!
ephone  2
 device-security-mode none
 mac-address 001E.7A25.50AA
 username "Downie.G"
 paging-dn 6
 type 7970
 button  1:2 8:3
!
Creates a 7970 SCCP phone, associates it with user Gord Downie, puts DN 2002 on button
1, and the other intercom DN on Button 8.
!
ephone  3
 device-security-mode none
 mac-address 1234.5678.90AB
 username "Lifeson.A"
 paging-dn 6
 type CIPC
 button  1:4
!
! Creates the IP Communicator softphone, associates it with user Alex
! Lifeson, and puts DN 2004 on Button 1.
!
ephone  100
 device-security-mode none
!
!
ephone-hunt 1 longest-idle
 pilot 8535937
 list 2002, 2004, 2112
```

```
 no-reg pilot
 fwd-final orig-phone
 description Helpdesk
!
! This is the Hunt system configuration
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login local
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 logging synchronous
 login local
 transport input telnet ssh
line vty 5 14
 exec-timeout 0 0
 logging synchronous
 login local
 transport input telnet ssh
line vty 15
 logging synchronous
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp server 192.168.1.1
!
end
```

GLOSSARY

802.1Q An industry-standard trunking protocol that allows traffic for multiple VLANs to be sent between switches.

802.3af Power over Ethernet (PoE) Industry-standard method of supplying power over an Ethernet cable to attached devices.

802.3at A PoE (Power over Ethernet) standard that supports devices requiring more power (up to 25.5W) such as pan/tilt/zoom IP cameras, door locks, and point-of-sale terminals.

AAR Automated Alternate Routing is an optional configuration that dynamically reroutes calls as PSTN calls when CAC determines there is not enough bandwidth to route the call over the WAN. AAR is transparent to the user; the call is redialed with a full PSTN number without any user interaction.

Access Control Group Associated with one or more roles. Users who are members of a group inherit the privileges of the role(s) associated with the group. Membership in multiple groups may create conflicting privilege assignments; the enterprise parameter Effective Access Privileges for Overlapping User Groups and Roles defines whether the effective privilege is Maximum or Minimum.

administration via telephone (AVT) system Gives an administrator an easy way to record custom prompts and to quickly record and enable the AA alternate greeting via a telephone connection.

Administrative Extensions for XML (AXL) Method by which user accounts in a CUCM database may be replicated and synchronized with the user account database in CUC.

analog signal A method of signaling that uses properties of the transmission medium to convey sound characteristics, such as using electrical properties to convey the characteristics of voice.

application (CUCM) Includes CM Administration, Unified Serviceability, Cisco Extension Mobility, and so on. Each application has resources that roles are permitted or restricted from viewing and/or editing.

auto-assignment A feature that allows the Cisco Unified CME router to distribute ephone-dns to auto-registered IP phones.

auto-attendant A common application of Interactive Voice Response (IVR) that allows callers to use automated menus to navigate to specific areas of your company.

auto-registration A Cisco Unified CME feature that allows Cisco IP phones to register with the CME router without an existing ephone configuration; auto-registration is turned on by default.

automated attendant (AA) Provides a business with the ability to answer and direct incoming phone calls to the appropriate person within the business without requiring human intervention.

Automatic Number Identification (ANI) Describes caller ID information delivered to a voice-processing device. Closely related to Dialed Number Identification Service (DNIS), which identifies dialed number information.

Call Admission Control (CAC) Call Admission Control refers to one of several techniques for monitoring the total remaining bandwidth available for voice traffic over a WAN link. The purpose of CAC is to prevent the transmission of voice traffic in excess of what the link can support without overflowing the QoS voice priority queue and causing voice packets to be dropped by the router, resulting in very poor quality for all concurrent calls. CAC can be implemented using the CUCM Locations configuration within or between clusters, using RSVP, or using Gatekeeper routers.

call coverage A general term for a set of features that provide alternatives to a call being unanswered; specific features include forwarding, pickup, hunt systems, voicemail, and so on.

Call Detail Record (CDR) A log of specific information about a phone call that can be used for billing, analysis, reporting, and troubleshooting.

Call Detail Record Analysis and Reporting (CAR) A built-in reporting system that allows administrators to easily generate reports from the CDR/CMR database.

call forward A general term for a set of configurations that forward a call from the original dialed extension to another, or to a voicemail pilot. Forwarding options can be set for both internal (on-net) calls and external (off-net) calls and for the Call Forward All, No Answer, Busy, No Coverage and Unregistered conditions.

call handler A software element that answers a call, typically plays an informational greeting recording, may offer user input options for navigation, and may allow transfer of the call to other call handlers or user extensions.

Call Management Record (CMR) A log of voice quality statistics about IP phone calls.

call park A Cisco Unified CME feature that allows you to park a call on hold in a virtual "parking spot" until it can be retrieved.

call pickup A Cisco Unified CME feature that allows you to answer another ringing phone in the network.

call routing rules One of the primary mechanisms that CUC uses to analyze and direct calls to the appropriate call handler, conversation, or extension. Two basic types are available: Direct, for calls dialed directly to CUC, and Forwarded, for calls forwarded because of Busy or RNA events.

CFUR Destination number to which calls will be forwarded if the phone is unregistered at CUCM. Commonly used in conjunction with SRST to provide call coverage to the DID or attendant number at the branch durimng a WAN outage.

channel associated signaling (CAS) A method of digital signaling in which signaling information is transmitted using the same bandwidth as the voice.

Cisco Configuration Assistant (CCA) The GUI tool created by Cisco to provision, manage, troubleshoot, and maintain the Smart Business Communications System.

Cisco Discovery Protocol (CDP) Protocol that allows Cisco devices to discover other, directly attached Cisco devices. Switches also use CDP to send voice VLAN information to attached IP phones.

Cisco Emergency Responder Dynamically updates location information for a user based on the current position in the network and feeds that information to the emergency service provider if an emergency call is placed.

Cisco Inline Power Cisco-proprietary, prestandard method of supplying power over an Ethernet cable to attached devices.

Cisco IOS license A license from Cisco that allows a router to run the IOS software; most newly purchased routers come with an IOS license.

Cisco Smart Assist The name commonly associated with the group of wizard-like features integrated into the Cisco Configuration Assistant that simplifies the provisioning and maintenance of the SBCS suite.

Cisco Unified Communications An architecture that seeks to minimize the differences between the way we would like to communicate and the way we have to communicate given time, device, and location constraints.

Cisco Unified Communications 500 (UC500) The small business call processing platform that is able to support up to 48 users.

Cisco Unified Communications Manager The multiserver call processing platform that is able to support up to 30,000 users per cluster.

Cisco Unified Communications Manager Express (CME) The call processing platform that is able to support up to 250 users (depending on router hardware).

Cisco Unified Communications Manager IP Phone Service (CCMCIP) Used to list user-associated devices that can be used for communication.

Cisco Unified Contact Center Express A call center application that is able to support up to 300 agents.

Cisco Unified MeetingPlace Provides a multimedia conference solution that gives you the capability to conference voice, video, and data into a single conference call.

Cisco Unified Mobility Allows users to have a single contact phone number that they can link to multiple devices.

Cisco Unified Presence Provides status and reachability information for the users of the voice network.

Cisco Unified Serviceability Archives reports Two reports per day of collected data: one for Alerts and one for Server statistics (CPU, hard-disk utilization).

Cisco Unified Serviceability reports A set of 19 built-in reports to provide administrators with information about the configuration, utilization, and status of the CUC application.

Cisco Unity The unified messaging platform that is capable of supporting up to 7,500 users per server and redundant server configurations.

Cisco Unity Connection The single-server unified messaging platform that is capable of supporting up to 7,500 users.

Cisco Unity Express The unified messaging platform that is integrated into a Cisco Unified CME router; capable of supporting up to 250 users.

Cisco Unity Express administrator A subscriber that is a member of the administrators group.

Cisco Unity Express Advanced Integration Module (AIM-CUE) An entry-level hardware platform for Cisco Unity Express, providing up to 50 mailboxes, 14 hours of storage, and either four or six ports that can be used for simultaneous voice sessions, depending upon the model of Cisco ISR router it is installed in.

Cisco Unity Express automated-attendant (AA) script A collection of software steps that defines each action to be performed on a received call.

Cisco Unity Express CLI The command-line interface used to configure and administer Cisco Unity Express.

Cisco Unity Express custom scripting The act of modifying the default Cisco Unity Express AA script to match a business need.

Cisco Unity Express Editor A PC software application that is used to create Cisco Unity Express custom scripts.

Cisco Unity Express Enhanced Network Module (NME-CUE) The high-end hardware platform for Cisco Unity Express, providing up to 250 mailboxes, 300 hours of storage, and 24 ports that can be used for simultaneous voice sessions.

Cisco Unity Express greeting/prompt A recorded message played to a caller.

Cisco Unity Express GUI Provides subscribers and administrators with a web interface to use and manage Cisco Unity Express features and functions.

Cisco Unity Express Network Module (NM-CUE) The lower-midlevel hardware platform for Cisco Unity Express, providing up to 100 mailboxes, 100 hours of storage, and eight ports that can be used for simultaneous voice sessions.

Cisco Unity Express Network Module with Enhanced Capability (NM-CUE-EC) The upper-midlevel hardware platform for Cisco Unity Express, providing up to 250 mailboxes, 300 hours of storage, and 16 ports that can be used for simultaneous voice sessions.

Cisco Unity Express password Used to authenticate subscribers via the GUI.

Cisco Unity Express PIN Used to authenticate subscribers via the TUI.

Cisco Unity Express subscriber A user account configured in Cisco Unity Express.

Cisco Unity Express telephony user interface (TUI) Provides subscribers and administrators with a telephone interface to use and manage Cisco Unity Express features and functions.

Class of Restriction (COR) The method used to implement calling restrictions in the CME environment. An inbound COR list assigns privileges, whereas an outgoing COR list restricts calling.

Class of Service (CoS) Group of settings that provides or restricts access to licensed features, advanced features, or user capabilities.

Client Services Framework (CSF) The client-side foundations for CUPC and other CUC-integrated applications, such as Microsoft Outlook.

common channel signaling (CCS) A method of signaling in which information is transmitted using a separate, dedicated signaling channel.

community A group of devices managed by the Cisco Configuration Assistant via its IP address.

compliance As it relates to CUPS, compliance refers to the preservation of IMs on an external PostgreSQL database or compliance server.

Computer Telephone Interface Quick Buffer Encoding (CTIQBE) The protocol used for CUPC desk phone control.

Customer Admin An administrative account built for on-site customer administration. This account has access to most telephony functions, but no router functions.

Date/Time Group 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.

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.)

dial-peer Logical configuration used to define dial plan information on a Cisco router.

Dialed Number Identification Service (DNIS) Describes dialed number information delivered to a voice processing device. Closely related to Automatic Number Identification (ANI), which identifies caller ID information.

Direct Inward Dial (DID) A voice configuration that allows users from the PSTN to dial directly into an individual phone at an organization without passing through a receptionist or automated attendant application.

directed pickup A method used with call pickup to answer a phone directly by dialing the extension number of the ringing phone.

Disaster Recovery System (DRS) The built-in Unified Communications platform backup and restore utility.

dual-tone multifrequency (DTMF) A type of address signaling in which the buttons on a telephone keypad use a pair of high and low electrical frequencies to generate a signal each time a caller presses a digit.

Dynamic Trunking Protocol (DTP) Allows switches to dynamically negotiate trunk links.

E.164 An international numbering plan created by the ITU and adopted for use on the PSTN.

Ear and Mouth (E&M) Analog interface type that acts as a trunk to a PBX system.

ephone A configuration in the CME router that represents a single IP phone (or IP telephony device).

ephone-dn A configuration in the CME router that represents a single directory number (DN).

extended super frame (ESF) A modern T1 signaling method that sends 24 T1 frames at a time.

Extensible Messaging and Presence Protocol (XMPP) Used for instant messaging with CUPS.

Extension Mobility A feature that allows a user to log in to any IP Phone and have their personal extension numbers, speed dials, services, calling privileges, etc. applied to the phone. This feature is ideal in an environment where users move to different work locations within an organization.

feature license A license dictating the number of IP phones a Cisco Unified CME router is able to support.

feature ring Causes an IP phone to ring with three consecutive pulses; configured by using the f button separator.

Foreign Exchange Office (FXO) Analog interface type that connects to a telephone carrier central office (CO) or PBX system; FXO ports receive dial tone from the attached device.

Foreign Exchange Office (FXO) ports Analog interfaces that allow you to connect a VoIP network to legacy telephony networks such as the PSTN or a PBX system.

Foreign Exchange Station (FXS) Analog interface type that connects to a legacy analog device (station); FXS ports provide dial tone to the attached device.

Foreign Exchange Station (FXS) ports Analog interfaces that allow you to connect a legacy analog telephony device to a VoIP network.

G.711 Uncompressed audio codec consuming 64 kbps of bandwidth.

G.722 Uncompressed, moderate complexity codec with much better voice quality than G.711 while still consuming the same 64kbps of bandwidth (typically)

G.726 Compressed audio codec consuming 32 kbps of bandwidth.

G.728 Compressed audio codec consuming 16 kbps of bandwidth.

G.729 Compressed audio codec consuming 8 kbps of bandwidth.

general delivery mailbox (GDM) A mailbox that is shared by a group of subscribers.

glare An instance in which a user picks up a phone and connects unexpectedly to an incoming call.

ground start signaling A method of signaling that relies on grounding wires connecting to a device to signal a new call; typically used in PBX systems to avoid glare.

H.323 Protocol suite created by the ITU-T to allow multimedia communication over network-based environments.

H.450.2 Industry-standard method of transferring calls without hairpinning.

H.450.3 Industry-standard method of forwarding calls without hairpinning.

hairpinning A problem that occurs when a call is transferred or forwarded from one IP phone to another that keeps the audio path established (or hairpinned) through the original IP phone; this tends to cause QoS issues with the call.

hunt group A CME feature; a hunt group allows a call to a specific number to be directed to a defined set of ephone-dns in the desired sequence.

integrated messaging Provides access to voicemail messages via an email client and allows a subscriber to treat voicemail messages similarly to email messages.

integration Configuration of a voicemail system (CUC) to interact with a call agent (CUCM). An integration provides MWI, call forward to personal greeting, and easy message access.

Interactive Voice Response (IVR) An automated system that provides a recorded, automated process to callers accessing your voice network.

intercom A point-to-point one-way audio call. Intercom is set up as a completely independent configuration, almost like a parallel phone system in CUCM.

Internet Low Bitrate Codec (iLBC) Compressed audio codec consuming 15.2 kbps of bandwidth.

Internet telephony service provider (ITSP) Provides VoIP trunk connectivity to the PSTN to provide a cost savings over traditional telephony service providers (TSP).

Inter-Switch Link (ISL) A Cisco-proprietary trunking protocol, which has been replaced by the industry-standard 802.1Q.

IP Phone Messenger (IPPM) An interface to handle IMs on the desk IP Phone.

key system A system that allows a company to run a private, internal voice network; key systems are usually used in smaller companies and provide shared-line extensions to all devices, although many key systems now provide unique extensions to all devices.

LAN expansion port The 10/100BASE-TX port in the UC520 that is automatically configured in the security configuration as the external system interface. This port is used to connect to a DSL or cable router for Internet access.

live record Enables a subscriber to record a live call and have that call delivered into the subscriber's mailbox.

live reply Enables a subscriber to use the received caller identification number (ANI) and place a phone call to that caller during voicemail message playback.

local directory The directory that is built automatically by the CME router as you define caller ID information for the ephone-dns.

local group pickup A method used with call pickup to answer a ringing phone from within the local group of an IP phone.

local loop The PSTN link between the customer premises (such as a home or business) and the telecommunications service provider.

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).

loop start signaling A method of signaling that relies on connecting the tip and ring wires connecting to a device to complete an electrical circuit; typically used in devices connecting to the PSTN.

mailbox caller features Mailbox features that Cisco Unity Express offers to a caller, where the caller may or may not be a subscriber configured on Cisco Unity Express.

mailbox subscriber features Mailbox features that Cisco Unity Express offers to a configured subscriber.

mean opinion score (MOS) A subjective method of determining voice quality; listeners hear a phrase read over a voice network and rate the quality of the audio on a scale of 1 to 5.

Media Convergence Server (MCS) The server hardware platforms that support Cisco Unified Communications Manager software.

Media Gateway Control Protocol (MGCP) Voice signaling protocol created by the IETF; allows voice gateways to be controlled by a centralized call agent in client/server fashion.

message notification Feature used to generate a call, send an email, or send a page to the subscriber when a new message has arrived in their mailbox.

Message Waiting Indicator (MWI) Provides a mechanism to alert a subscriber that a new message has arrived in a mailbox. This is typically achieved by turning on a light on the subscriber's IP phone.

Mobile Connect The ability to have a call for the user's enterprise IP phone number simultaneously ring up to ten remote devices, and switch seamlessly between IP phone and remote device while in the call. Also known as Single Number Reach.

Mobile Voice Access (MVA) The ability for a user to dial in from a remote device to an enterprise MVA access PSTN number, authenticate, and then place an outbound PSTN call that appears to come from their enterprise IP phone.

Monitor Mode/Watch Mode Line configuration that allows you to assign line instances to a Cisco IP phone that cannot be used for incoming or outgoing calls; rather, they can simply be used to check line status.

Native Presence Refers to CUCM's ability to monitor and display the on-/off-hook status of a DN using BLF Speed Dial or Call and Directory Lists.

Network Time Protocol (NTP) Synchronizes the clock of a network device to a more accurate NTP server.

Night Service A CME feature that designates certain phones to ring when an "after-hours" schedule is in effect—typically, when the receptionist or other staff are not available (the feature can also be activated manually).

Nyquist theorem Describes the method of converting analog audio signals into digital format by sampling at twice the highest frequency of the audio.

other group pickup A method used with call pickup to answer a ringing phone from another group number, which must be specified after pressing the GPickUp softkey.

overlay line Allows shared line configurations by assigning multiple line instances to a single physical line button (overlay) on a Cisco IP phone; configured by using the o, c, or x separator.

packetization interval The amount of data (typically audio) placed into each packet. Cisco defaults to a 20 ms packetization interval for all codecs.

partition, CSS (Calling Search Space) In CUCM, a partition is a container for dialable entities, including DNs, route patterns, translation patterns, and so on. A Calling Search Space is a top-down ordered list of partitions. A CSS is assigned to the calling devices (a phone, DN, gateway, and so on). If the target you are trying to dial is in one of the partitions in your current CSS, the call succeeds; if it is not, it fails.

Persistent Chat Group chats that are preserved when a user rejoins a chat room after logging out.

phone button template 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.

phone user license A license belonging to each Cisco IP Phone that allows it to communicate with a Cisco Unified CME router or Cisco Unified Communications Manager server; most newly purchased IP Phones come with a phone user license.

pickup A Call coverage feature which allows a user to pick up a call ringing on another phone.

power failover (PFO) The feature that allows the UC520 to complete calls out to the PSTN from a designated analog phone in the event of a power failure.

private branch exchange (PBX) A system that allows a company to run an internal, private voice network; PBX systems are usually used in larger companies and provide unique extensions to all devices.

private distribution lists A collection of subscribers created by a single subscriber for exclusive use by that subscriber.

Private Line Automatic Ringdown (PLAR) A configuration used to enable "immediate dial" applications, such as a phone that immediately dials an emergency number when a user lifts the handset.

public distribution list A collection of subscribers that is available to all Cisco Unity Express subscribers to use as a distribution list.

pulse-amplitude modulation (PAM) The process of sampling an analog waveform many times to determine numeric electric amplitude values for digital conversion; PAM is typically combined with pulse-code modulation (PCM).

pulse-code modulation (PCM) The process of converting pulse-amplitude modulation (PAM) values into binary number equivalents that voice equipment can transmit over digital circuits.

pulse dialing A type of address signaling in which the rotary-dial wheel of a phone connects and disconnects the local loop circuit as it rotates around to signal specific digits.

Q.931 A signaling protocol used by ISDN CCS implementations.

quantization The process of assigning analog signals a numeric value that can be transported over a digital network.

Real-Time Transport Control Protocol (RTCP) The UDP-based protocol responsible for transporting audio statistics; uses random, odd-numbered UDP ports from 16,384 to 32,767 for communication.

Real-Time Transport Protocol (RTP) The UDP-based protocol responsible for transporting audio packets; uses random, even-numbered UDP ports from 16,384 to 32,767 for communication.

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

resource May be an administrative web page, part of a web page, or a tool or interface within an application.

robbed bit signaling (RBS) An implementation of channel associated signaling (CAS) that steals the eighth bit of every sixth frame of a digital T1 circuit for signaling information.

role (CUCM) Defines a set of privileges to an application's resources. Privileges may be defined as No Access, Read, or Update.

route group A route group is a collection of devices (gateways and /or trunks) that can physically transmit the call. Route groups are linked to route lists.

route list A route list is linked to a route pattern and lists the top-down preferred order of route groups to use for the call-routing operation; a route list may also perform digit manipulation.

route pattern A CUCM configuration that consists of a string of digits and/or wildcards that matches the dialed digits of a phone call and begins the call routing operation. Route patterns are commonly (but not exclusively) used for PSTN dialing.

router-on-a-stick An inter-VLAN routing configuration that allows a single router to move data between VLANs by using a FastEthernet or greater interface broken into subinterfaces connected to a switch trunk port.

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.

service engine The interface that is created on Cisco Unified CME after the Cisco Unity Express hardware platform is installed and recognized by the router. CME will route calls through this interface to the service module for Cisco Unity Express to process.

service module The internal interface of Cisco Unity Express. Cisco Unity Express routes calls through this interface to the service engine for Cisco Unified CME to process.

Session Initiation Protocol (SIP) Voice-signaling protocol created by the IETF as a lightweight alternative to H.323.

shared line Configuring the same DN on two or more phones; a call to the shared DN rings on all the phones, but once picked up, cannot be seized by another station unless Hold is pressed at the first phone, or the Barge feature is invoked.

Signaling System 7 (SS7) The protocol used within the telephony service provider network to provide inter-CO communication and call routing.

Single Number Reach A feature that allows users to have incoming calls ring another, preconfigured number after a defined time limit. Single number reach also allows for mobility, which allows the transfer of an active call to or from the same, preconfigured number.

SIP for Instant Messaging and Presence Leveraging (SIMPLE) Used for IM with third-party systems.

Skinny Client Control Protocol (SCCP) Cisco-proprietary voice-signaling protocol used to control Cisco IP phones.

smartports A CCA macro that aids in the configuration of roles for individual ports.

softkey 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.

Spanning Tree Protocol (STP) A method designed to prevent loops in switched networks due to redundant inter-switch connections.

super frame (SF) An early T1 signaling method that sent 12 T1 frames at a time.

Survivable Remote Site Telephony (SRST) Survivable Remote Site Telephony; a feature that allows a branch office router to take over the phone registration and call control for branch IP phones in the event that WAN failure cuts off contact with the central site CUCM cluster.

switched virtual interface (SVI) A routed interface on a switch.

system admin The CME administrator with full privileges to all telephony and router operations.

telephony-service The IOS configuration mode in which most telephony configurations are executed.

time-division multiplexing (TDM) A method of transmitting multiple channels of voice or data over a single digital connection by sending data in specific time slots.

troubleshooting A sequence of steps by which the possible causes of a problem, and the possible steps to correct it, are determined and executed.

trunk port A port on a Cisco switch specifically configured to transmit multiple VLANs. Trunks are typically used between switch devices and in router-on-a-stick configurations.

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.

virtual LAN (VLAN) A configuration used to break a switch into multiple broadcast domains and IP subnets.

VLAN Trunking Protocol (VTP) A Cisco-proprietary protocol that replicates VLAN database information to all switches participating in the same VTP domain.

voice expansion port The integrated voice/WAN interface card (VWIC) port in all models of the UC520 that allows for PSTN voice expansion. This port does not support WAN connectivity.

Voice Profile for Internet Mail (VPIM) A feature that allows one voicemail system to exchange messages with another voicemail system.

Voice Register DN The CME term for a SIP ephone-dn.

Voice Register Pool The CME term for a SIP ephone.

VoiceView Express An XML application that provides to subscribers GUI access to their voicemail messages via the Services button on an IP phone.

This page intentionally left blank

Index

Symbols

µ-law (mu-law), G.711 codec, 20, 23

A

A-law, G.711 codec, 20, 23

AAR (Automated Alternate Routing), CUC voice messaging, 356

Access Control Groups (CUCM user management), 220-221

access lists (Mobile Connect), 327-328

applying, 334-335

configuring, 333-334

address signaling, 8

administration (CME) via command-line, 479-491

administration interfaces

CM-IMP

CM-IMP Administration, 224-225

CM-IMP Serviceability, 225-226

CUC, 221

CUC Administration, 222-223

CUC Serviceability, 224

CUCM

accessing, 214

Cisco Unified Operating System Administration, 217

Cisco Unified Reporting, 218

Cisco Unified Serviceability Administration, 215-216

CLI, 218-219

CM Administration, 214-215

DRS, 218

End-User interface, 226-227

passwords, 214

security, 214

Self Care Portal, 226-227

Advanced Features menu (CM Administration interface), 215

Advanced menu (CUC Administration), 223

after-hours call blocking, configuring with CME, 191-194

aging policy (messages), CUC voicemail boxes, 357, 374-375

Alarm menu (Cisco Unified Serviceability Administration interface), 216

alerts, monitoring via RTMT, 442-443

Alerts Report (Serviceability Reports Archive), 457-458

allow multiple logins option (EM in CUCM), 290

analog connections, 6

analog waveforms, 7

CME, Cisco IP phone interaction with PTSN, 36

converting to digital, 9, 17-20

difficulties with, 9

glare, 8

ground start signaling, 8
loop start signaling, 8
PSTN, 14
repeaters, 9
analog telephones, PSTN, 12
analog voice ports
CME dial plans
FXO voice ports, 119, 146-147
FXS voice ports, 116-118
FXO voice ports
CME dial plans, 119
designating POTS lines for emergency calls, 146-147
PLAR, 137
FXS voice ports
CME dial plans, 116-118
PLAR, 136
any voice codec (dial peer 0), 142
Application menu
CM Administration interface, 215
CM-IMP Administration, 224
application users (CUCM), 252, 256
attempt forward rule (forward routing), CUC voice messaging integration, 352
attempt sign-in rule (direct routing), CUC voice messaging integration, 351
audio encryption, SRTP, 60
audio telephony, CUCM, 37
Audio Text Administrator role (CUC voice messaging integration), 349
Audit Administrator role (CUC voice messaging integration), 349
authentication
LDAP authentication, 257
configuring, 262
verifying, 263
local authentication, CME configuration with CCP, 88
authentication rules, CUC voice messaging integration, 352
auto-logout option (EM in CUCM), 290
AutoQoS (Quality of Service), 74-81
auto-registration of IP phones in CUCM, 243, 247-252
AXL (Administrative XML), CUC voice messaging, 357, 369-370

B

B8ZS linecoding, 122
backups, DRS, 444
backup device configuration, 445
CUC, 445
CUCM, 445
CUP, 445
restore process, 446
scheduling backups, 445-446
bandwidth, VoIP networks, 69
Barge feature, CUCM telephony, 299, 304-305
barge-in functionality in intercoms, 185
BAT (Bulk Administration Tool)
end users (CUCM), importing, 256
IP phone registration in CUCM, 243, 250-251
Bell Systems Corporation, analog to digital conversions, 17
best effort QoS model, 71
billing reports, 464
Bitrate codec (iLBC), 21-23
BLF (Busy Lamp Fields) and Native Presence (CUCM), 301-303, 315-317

blind transfers (call transfers), 175
blocking calls after-hours, configuring with CME, 191-194
boot processes, troubleshooting IP phones, 404-407
browsing (remote), monitoring via RTMT, 443
Bulk Administration menu
CM Administration interface, 215
CM-IMP Administration, 225

C

cabling, VoIP, 17
CAC (Call Admission Control), PSTN backup using CAC call flows (CUCM), 275-276
calendar resources, CM-IMP integration, 386
call accounting, configuring with CME, 194-199
call actions, CUC voice messaging, 355
call activity, monitoring via RTMT, 440-442
call blocking after-hours, configuring with CME, 191-194
call coverage, CUCM
Barge feature, 299, 304-305
call forward options, 298-299
call hunting, 300-301, 310-313
call park, 301, 308-310
call pickup groups, 300, 305-308
CFA, 298
CFB internal/external, 299
CFNA internal/external, 299
CFNC internal/external, 299
CFUR internal/external, 299
GPickup, 300
Intercom feature, 301, 313-315
Other Group Pickup, 300
privacy, 300
shared lines, 299, 303-304
Whisper intercom feature, 301
caller input, CUC voice messaging, 355
call flows (CUCM)
call routing
destinations in CUCM, 277-278
digit analysis, 280-281
gateways, 280
hunt groups, 281
route groups, 279
route lists, 279
route patterns, 278-279
sources of, 277
trunking, 280
centralized deployment
considerations/limitations, 275
PSTN backup call flows, 274
centralized remote branch call flows, 273-274
class of control
CSS, 282-283
partitions, 282
distributed deployment call flows, 276-277
DNS (with/without), 270-273
PSTN backup using CAC call flows, 275-276
call forwarding
CME and
CLI, 172-173
H.450.3 call forwarding, 173-175
IP phone calls, 172
CUCM and
CFA, 298
CFB internal/external, 299
CFNA internal/external, 299

CFNC internal/external, 299
CFUR internal/external, 299
CUC voice messaging, 350, 356
CallHome menu (Cisco Unified Serviceability Administration interface), 216
call hunting, CUCM telephony, 300-301, 310-313
call legs (voice), 126-127
call lists, Native Presence-enabled lists (CUCM), 316
Call Management menu (CUC Administration), 222
CallManager. *See* CUCM; CME
call parks
CME and, 177-181
CUCM telephony, 278, 301, 308-310
call pickup
CME and, 182-184
CUCM telephony, 300, 305-308
directed pickup, 183
local group pickup, 183
other pickup, 183
call processing, CME, 34
call progress tones, FXS voice ports, 118
call routing
CUC voice messaging integration, 351-352
CUCM
destinations in CUCM, 277-278
digit analysis, 280-281
gateways, 280
hunt groups, 281
route groups, 279
route lists, 279
route patterns, 278-279
sources of, 277
trunking, 280
Call Routing menu (CM Administration interface), 214
call transfers
blind transfers, 175
CME and, 175-177
consult transfers, 175
CAR (Call Detail Record Analysis and Reporting) tool, 427
CDR and, 429
exporting records, 430
generating reports, 430-433
CMR and
exporting records, 430
system requirements, 429-430
exporting records, 430
generating reports
CDR reports, 430-433
device reports, 434
system reports, 433-434
service activation, 428
service parameter configuration, 428
system parameters, 429-430
user types, 429
cards, PBX systems
control cards, 13
line cards, 13
trunk cards, 13
CAS (Channel Associated Signaling), 10-11
catalyst switch PoE (Power over Ethernet), IP phones, 56
CBarge option (Barge feature), 305
CBWFQ (Class-Based Weighted Fair Queuing), 73
CCMCIP (Cisco Unified Communication Manager IP phone) service, 384
CCM (Cisco CallManager). *See* CUCM

CCP (Cisco Configuration Professional)
capabilities of, 105
CCP GUI, CME end user/endpoint implementation, 107-110
CME dial plans, 151-152, 159-161
CME routers
CME integrated GUI, 89
configuring, 88
managing, 89-93
CME voice networks
after-hours call blocking, 194
call forwarding, 175
call parks, 180-181
call pickup, 183-184
call transfers, 177
directories, 170-171
ephone hunt groups, 201-202
intercoms, 185-187
paging, 189-190
shared ephone-dn, configuring, 206-207
Single Number Reach, 199-200
communities, definition of, 91
COR implementation, 159-161
interface management, 105
license management, 105
Night Service, configuring for CME, 203-206
routers, 105
security, 105
shared ephone-dn, configuring for CME, 206-207
Unified Communications, 105-107
utilities, 105
virtual machines, building, 93
CCP Express (Cisco Configuration Professional Express), 90
CCS (Common Channel Signaling), 11-12
CD, Exam Engine
activating exams, 468
installing, 467
Practice Exam mode, 468-471
Study mode, 470-471
CDP (Cisco Discovery Packets)
AutoQoS and, 76
IP phone VLAN configuration, 63
CDR (Call Detail Records)
CAR tool and, 429
exporting records, 430
generating reports, 430-433
CME and, 194-198
CFA (Call Forward All), CUCM, 298
CFB (Call Forward Busy) internal/external, CUCM, 299
CFNA (Call Forward No Answer) internal/external, CUCM, 299
CFNC (Call Forward No Coverage) internal/external, CUCM, 299
CFUR (Call Forward UnRegistered) option
centralized deployment PSTN back call flows, 274
CUCM, 299
chapter-ending review tools (test preparation), 469
chats, CM-IMP
group chat storage, 384
persistent chats, 387
Cisco IP phones
CME interaction
PTSN-connected interfaces, 36
RTP, 35
SCCP, 35
SIP, 35
CUCM interaction, 38-41

Cisco Learning Network, 469
Cisco Unified Communications Manager Instant Messaging and Presence. *See* IMP
Cisco Unified CUCME as Cisco Unified SRST, CCP and CME router configuration, 92-93
Cisco Unified Operating System Administration interface (CUCM), 217
Cisco Unified Reporting interface (CUCM), 218
Cisco Unified Serviceability
Cisco Serviceability Reporter service, 455
Serviceability Reports Archive, 455-456
Alerts Report, 457-458
Server Report, 458-459
Cisco Unified Serviceability Administration interface (CUCM), 215-216
Cisco Unity Connection
CUCM interaction, 43-44
Exchange and, 42
features of, 42
LDAP directory server integration, 42
mailboxes, 42
voicemail, 42
voice messaging, 41
VPIM, 42
classification and marking mechanisms (QoS), 71
class of control (CUCM call flows), 282-283
Class of Service menu (CUC Administration), 222
CLI (Command Line Interface)
CUCM, 218-219
forwarding calls from, 172-173
clocks, setting in Cisco devices, 65-67
clusters and CUCM, 37-39
CM Administration interface (CUCM), 214-215
CM groups (device pools), 240
CM-IMP (Communications Manager IM and Presence), 381
administration interfaces
CM-IMP Administration, 224-225
CM-IMP Serviceability, 225-226
calendar resource integration, 386
CCMCIP service, 384
components of, 384
conferencing resource integration, 386
CUC integration, 385
CUCM Presence Signaling integration, 393-394
group chat storage, 384
Jabber
chats, 387
compliance, 387
CSF, 383, 390
deskphone mode, 381-382, 386
enterprise IM, 382
IM, 387
integration support, 383
persistent chats, 387
QoS, 387-388
softphone mode, 382, 386
troubleshooting, 394-395
user integration in CM-IMP, 394
user integration in CUCM, 389-392
video calls, 383
voice calls, 383
LDAP integration, 385, 391
MeetingPlace integration, 386

Microsoft Exchange 2003/2007 integration, 386
Microsoft Office Communications Server integration, 385
QoS, 387-388
Rich Presence service, 384
user integration in CM-IMP, 394
user integration in CUCM, 391-392
configuring users, 389
CSF devices, 390
directory number associations, 390
WebEx integration, 386
CME (Communication Manager Express)
administration
CCP and CME, 88-93
CME GUI, 89, 101-103
Customer Admin account creation, 103-104
customer administrators, 100
endpoint implementation, 107-110
end user implementation, 107-110
ephone-dn, 103-104
phone users, 100
SCCP, 104-105
SIP, 104-105
system administrators, 100
user creation, 101
after-hours call blocking, 191-194
call accounting, 194-199
call forwarding
CLI, 172-173
H.450.3 call forwarding, 173-175
IP phone calls, 172
call parks, 177-181
call pickup, 182-184
call processing, 34
call transfers, 175-177
CCP
CCP GUI and end user/endpoint implementation, 107-110
CME configuration, 88
CME management, 89-93
CDR, configuring, 194-198
Cisco IP phones, 35-36
CME GUI, 89
Customer Admin account creation, 103-104
enabling, 101-103
user creation, 101
command-line
administration, 479-491
configuring, 34
COR, 153-161
CTI support, 34
Customer Admin accounts, creating, 103-104
customer administrators, 100
device control, 34
dial plans
CCP and COR implementation, 159-161
CCP and dial plan configuration, 151-152, 159-161
COR, 153-161
dial peer configuration, 125-151, 155
router call processing, 137-142
router digit manipulation, 142-151
voice port configuration, 116-125
direct integration with CUE, 34
EM, 207
ephone hunt groups, configuring, 201-203

ephone-dn
shared ephone-dn, configuring with CCP, 206-207
user creation, 103-104
features of, 34
GUI-based configuration, 34
intercoms, configuring, 184-187
ISR G2 platform support, 33-34
local directory service, 34
managing with CCP, 89-93
MoH, configuring, 198-199
Night Service, configuring with CCP, 203-206
paging, configuring, 187-190
phone users, 100
SCCP, 104-105
Single Number Reach, configuring, 199-200
SIP, 104-105
system administrators, 100
troubleshooting
CME servers, 407
dial plans, 407-410
QoS, 410-413
registration issues, 403-407
voice network directories, configuring, 168-171
VoIP trunking, 34

CMR (CallManager) service and CAR tool
exporting records, 430
system requirements, 429-430

codecs
Bitrate (iLBC), 21-23
G.711, 21
μ-law (mu-law), 20, 23
A-law, 20, 23
G.722, 21
G.726 codec, 23
G.728, 21
G.729, 20-21
G.729a, 21
G.729ab codec, 23
G.729a codec, 23
G.729b, 21
G.729b codec, 23
iLBC (Bitrate), 21-23
Internet Low, 21

command-line (CME)
administration, 479-491
configuration, 34

common phone profiles, IP phones and CUCM implementation, 243

communities, definition of, 91

compatibility, VoIP, 17

compliance, CM-IMP, 387

compression
analog to digital conversion, 20
G.729 codec, 20
header compression (link efficiency mechanisms), 73
MOS, 20
payload compression (link efficiency mechanisms), 72

conferencing resources, CM-IMP integration, 386

congestion avoidance mechanisms (QoS), 72

congestion management mechanisms (QoS), 72

connections
analog, 6
converting to digital, 9, 17-20
difficulties with, 9
glare, 8
ground start signaling, 8
loop start signaling, 8

PSTN, 14
repeaters, 9
waveforms, 7
digital
CAS, 10-11
CCS, 11-12
converting analog connections to, 9, 17-20
PSTN, 14
signal degradation, 10
TDM, 10
console ports, CME administration via command-line, 479
consult transfers (call transfers), 175
Contacts menu (CUC Administration), 222
control cards, PBX systems, 13
COR (Class of Restriction), CME, 153-161
CO switches, PSTN, 13
couplers (inline PoE), IP phones, 56-57
credential policies and end users (CUCM), 253
CSF (Client Services Framework), Jabber, 383, 390
CSS (Calling Search Spaces) and CUCM call flow class of control
line device configuration, 283
partition interaction with, 282
CSS (Common Channel Signaling), SS7, 14
CTI (Computer Telephony Integration), CME support, 34
CUBE (Cisco Unified Border Element), CCP and CME router configuration, 92
CUC (Cisco Unity Connection)
administration interfaces, 221
CUC Administration, 222-223
CUC Serviceability, 224
Cisco Serviceability Reporter service (Cisco Unified Serviceability), 455
CM-IMP integration, 385
CUC Serviceability reports
accessing, 452
billing reports, 464
Mailbox Store Report, 462-463
maintenance with, 462-464
Outcall Billing Detail Report, 464
Outcall Billing Summary Report, 464
Phone Interface Failed Logon Report, 459-460
Port Activity Report, 461-462
Transfer Call Billing Report, 464
troubleshooting with, 459-462
Unused Voice Mail Accounts Report, 463-464
User Lockout Report, 460-461
Users report, 453-454
DRS and disaster recovery, 445
Serviceability Reports Archive (Cisco Unified Serviceability), 455-456
Alerts Report, 457-458
Server Report, 458-459
CUCM (Cisco Unified Communications Manager), 33
administration interfaces
accessing, 214
Cisco Unified Operating System Administration, 217
Cisco Unified Reporting, 218
Cisco Unified Serviceability Administration, 215-216
CLI, 218-219
CM Administration, 214-215
DRS Administration, 218
End-User interface, 226-227
passwords, 214

security, 214
Self Care Portal, 226-227
appliance-based operation, 37
application users, 252, 256
audio telephony support, 37
call coverage
Barge feature, 299, 304-305
call forward options, 298-299
call hunting, 300-301, 310-313
call park, 301, 308-310
call pickup groups, 300, 305-308
CFA, 298
CFB internal/external, 299
CFNA internal/external, 299
CFNC internal/external, 299
CFUR internal/external, 299
GPickup, 300
Intercom feature, 301, 313-315
Other Group Pickup, 300
privacy, 300
shared lines, 299, 303-304
Whisper intercom feature, 301
call flows
call routing and digit analysis, 280-281
call routing and gateways, 280
call routing and hunt groups, 281
call routing and trunking, 280
call routing destinations, 277-278
call routing groups, 279
call routing lists, 279
call routing patterns, 278-279
call routing sources, 277
centralized deployment considerations/limitations, 275
centralized deployment PSTN backup call flows, 274
centralized remote branch call flows, 273-274
class of control, 282-283
distributed deployment call flows, 276-277
DNS (with/without), 270-273
PSTN backup using CAC call flows, 275-276
call processing, 41
call routing
destinations in CUCM, 277-278
digit analysis, 280-281
gateways, 280
hunt groups, 281
route groups, 279
route lists, 279
route patterns, 278-279
sources of, 277
trunking, 280
CAR tool, 427
CDR and, 429-433
CMR and, 429-430
device reports, 434
exporting records, 430
service activation, 428
system parameters, 428-430
system reports, 433-434
user types, 429
Cisco IP phones, 38-41
Cisco Unity Connection interaction, 43-44
clusters, 39
CM-IMP
chats, 387
compliance, 387
CUCM Presence Signaling integration, 393-394
deskphone mode, 381-382, 386

IM, 387
Jabber, 381-383, 386-395
persistent chats, 387
QoS, 387, 388
softphone mode, 382, 386
user integration in CM-IMP, 394
user integration via Jabber, 389-392
CUC voice messaging integration, 347-348
importing accounts via AXL, 357, 369-370
importing users from CUCM, 368-370
CUPS and, 273
database replication, 38
dial plans
call routing and digit analysis, 280-281
call routing and gateways, 280
call routing and hunt groups, 281
call routing and trunking, 280
call routing destinations, 277-278
call routing groups, 279
call routing lists, 279
call routing patterns, 278-279
call routing sources, 277
centralized deployment considerations/limitations, 275
centralized deployment PSTN backup call flows, 274
centralized remote branch call flows, 273-274
class of control, 282
class of control and CSS, 282-283
class of control and partitions, 282
distributed deployment call flows, 276-277
DNS (with/without), 270-273
PSTN backup using CAC call flows, 275-276
directory service support/ integration, 38
DRS, 38, 445
EM
enabling, 291-298
logins, 290
end users
account interaction features, 253-254
application users versus, 252
credential policies, 253
device association, 254
importing via BAT, 256
LDAP attribute mapping, 258-259
LDAP authentication, 257, 262-263
LDAP custom filters, 263
LDAP integration, 256-263
LDAP sync, 256-262
manually importing, 255
passwords, 253
PIN, 253
user locales, 254
features of, 37-38
ICCS, 38
Intercluster trunking, 38
IP phones, 234
auto-registration, 243, 247-252
BAT, 243, 250-251
CDP, 235
common phone profiles, 243
configuration requirements, 240-243
device defaults, 242

device pools, 240-242
DHCP, 235-240
DNS, 235
manual configuration, 243-247
NTP, 234, 241
phone button templates, 242
phone security profiles, 243
PoE, 235
registering, 236, 243-252
self-provisioning registration, 243, 252
service activation, 237
SIP phone registration process, 236
softkey templates, 242
TAPS, 243, 251-252
TFTP, 235
LDAP integration
attribute mapping, 258-259
custom filters, 263
LDAP authentication, 257, 262-263
LDAP sync, 256-262
mobility
Mobile Connect, 326-336
MVA, 328, 336-340
unified mobility architecture, 327-328
Native Presence, 301-303
BLF call lists, 317
BLF speed dials, 315-316
custom presence groups, 317-320
presence-enabled call lists, 316
Presence Signaling integration with CM-IMP, 393-394
redundant server clusters, 37
reports
analyzing, 427
CAR tool, 427-434
generating, 425-426
maintenance reports, 427
route plan reports, deleting unassigned DN, 424-425
system analysis reports, 427
RTMT monitoring
alerts, 442-443
call activity, 440-442
database summaries, 439-440
device searches, 438-439
gateway activity, 437-438
remote browsing, 443
syslog, 443-444
voice/video summaries, 437
runtime data, 38
SIP phones, registering, 236
telephony
Barge feature, 299, 304-305
call coverage, 298-315
call forward options, 298-299
call hunting, 300-301, 310-313
call parks, 301, 308-310
call pickup groups, 300, 305-308
CFA, 298
CFB internal/external, 299
CFN internal/external, 299
CFNC internal/external, 299
CFUR internal/external, 299
GPickup, 300
Intercom feature, 301, 313-315
Native Presence, 301-303, 315-320
Other Group Pickup, 300
privacy, 300
shared lines, 299, 303-304
Whisper intercom feature, 301
TFTP servers, 39

troubleshooting, 421-422
analyzing reports, 427
CAR tool, 427-434
DN, 424-425
generating reports, 425-426
IP phone registration, 422-424
maintenance reports, 427
QoS, 413
system analysis reports, 427
user management
Access Control Groups, 220-221
privileges, 219
roles, 219-220
video telephony support, 37
VMware installation, 37
voice gateway control/ communication, 38
CUCME (Cisco Unified Call Manager Express), CCP and CME router configuration, 92
CUC voice messaging integration, 343
Audio Text Administrator role, 349
Audit Administrator role, 349
authentication rules, 352
call handlers, 350
call routing, 351-352
CUC Message Store, 373
memberships, 374
message aging policy, 374-375
quotas, 375-376
CUCM using SCCP, 347-348
dial plans, 353
direct routing rules, 351
DL, 352
enterprise parameters, 350
forward routing rules, 352
Greeting Administrator role, 349
Help Desk Administrator role, 349
LDAP, 350, 357, 370-372
Mailbox Access Delegate Account role, 349
mailboxes
call actions, 355
caller input, 355
greetings, 354
message actions, 355
message settings, 355
transfer rules, 354
multisite deployments, 347
overview of CUC, 346
Remote Administrator role, 349
service parameters, 350
single-site deployments, 346
SIP and CUC integration, 348
System Administrator role, 350
system settings
general configuration, 349
roles, 349-350
Technician role, 350
User Administrator role, 350
user configuration, 355
AAR, 356
account creation options, 356
alternate extensions/names, 366-367
call forward options, 356
extension numbers, 356
manual configuration, 365-366
notification devices, 356
private DL, 356, 367-368
SRST, 356
toll call control, 356
voicemail boxes, 356
user importation
bulk administration import, 372-373

CUCM, 368-370
LDAP, 370-372
user templates
basic elements of, 353-354
basics of, 358
call actions, 355
caller input, 355
configuring, 357-358
greetings, 354
message actions, 355, 361-362
message settings, 355, 360-361
notification devices, 364-365
password settings, 354, 359-360
phone menu, 362-363
playback message settings, 363-364
roles, 354, 360
transfer rules, 354
TUI settings, 355
voicemail boxes
message aging policy, 357, 374-375
message storage, 373-375
quotas, 357, 375-376
CUE (Cisco Unity Express), direct CME integration, 34
CUPS (Cisco Unified Presence Servers)
CUCM and, 273
DRS and disaster recovery, 445
Customer Admin accounts (CME), creating, 103-104
customer administrators (CME), 100

D

databases
replicating, CUCM, 38
summarizing via RTMT, 439-440
date/time
date time groups (device pools), 241
setting in Cisco devices, 65-67
degrading signal, 10
delay in VoIP networks, 69-70
demultiplexing devices, digital voice ports and CME dial plans, 122
deny login option (EM in CUCM), 290
deskphone mode (Jabber), 381-382, 386
device control, CME, 34
device defaults, IP phones and CUCM implementation, 242
Device menu (CM Administration interface), 215
device pools
CM groups, 240
date/time groups, 241
IP phones and CUCM implementation, 240-242
locations, 241
manual IP phone configuration in CUCM, 244
phone NTP references and SIP phones, 241
regions, 241
device reports, generating via CAR tool, 434
device searches via RTMT, 438-439
device security profiles, manual IP phone configuration in CUCM, 244
DHCP (Dynamic Host Configuration Protocol)
IP phones
CUCM implementation, 235
CUCM support, 237-240
registering, 423
troubleshooting, 423

servers
IP phone boot process, 63, 406
router-based DHCP server configuration, 64-65
troubleshooting, 406
Diagnostics menu (CM-IMP Administration), 225
dial peers
CME dial plans, 125-144, 151, 155
dial peer 0, 142
inbound/outbound dial peers, matching, 139-142
PLAR, 136-137
POTS dial peers, 125-131, 142, 151, 155
router call processing, 137-142
router digit manipulation, 142
designating POTS lines for emergency calls, 146-147
directing operator calls to receptionist, 145-146
PSTN failover using prefix command, 143-145
translation profiles, 148-151
voice call legs, 126-127
VoIP dial peers, 125, 131-133, 143-144
wildcards, 133-134
Dial Plan menu (CUC Administration), 222
dial plans
CME dial plan
CCP and COR implementation, 159-161
CCP and dial plan configuration, 151-152, 159-161
COR, 153-161
dial peer configuration, 125-151, 155
router call processing, 137-142
router digit manipulation, 142-151
voice port configuration, 116-125
CUC voice messaging integration, 353
CUCM
call routing, 277-281
centralized deployments, 274-275
centralized remote branch call flows, 273-274
class of control, 282-283
distributed deployment call flows, 276-277
DNS (with/without), 270-273
PSTN backup using CAC call flows, 275-276
PSTN dial plans, 134-135
troubleshooting, 407-410
DiffServ (Differentiated Services) QoS model, 71
digit analysis and CUCM call routing, 280-281
digit manipulation
CME dial plans, 142
emergency calls, designating POTS lines for, 146-147
operator calls, directing to receptionist, 145-146
PSTN failover using prefix command, 143-145
translation profiles, 148-151
digit-stripping rule (POTS dial peers), 131
digital connections
CAS, 10-11
CCS, 11-12
converting analog connections to, 9, 17-20

PSTN, 14
signal degradation, 10
TDM, 10
digital telephones, PSTN, 13
digital voice ports, CME dial plans, 120-125
direct routing rules, CUC voice messaging integration, 351
directed call park, 301, 309-310
directed pickup, 183
directories
LDAP sync directories, configuring, 261, 262
voice network directories, configuring, 168-171
directory handlers, CUC voice messaging integration, 350
directory numbers, user associations in CUCM via Jabber, 390
directory services
CUCM, 38
local directory service, CME, 34
DirSync and LDAP sync, 260
disaster recovery
CUCM, 38
DRS, 444
backup device configuration, 445
CUC, 445
CUCM, 445
CUP, 445
restore process, 446
scheduling backups, 445-446
DRS interface (CUCM), 218
Distribution Lists menu (CUC Administration), 222
DL (Distributed Lists)
CUC voice messaging integration, 352, 356, 367-368
private DL, 356, 367-368
DN (Directory Numbers)
call hunting, 300, 310-313
call parks, 308-309
call pickup groups, 300, 305-308
call routing in CUCM, 277
custom Native Presence groups (CUCM), 317-320
Intercom feature, 313-315
intercom lines, 301
Native Presence (CUCM), 303
troubleshooting, 424-425
unassigned numbers, deleting via Route Plan Reports, 424-425
DNS (Domain Name Systems)
CUCM call flows
centralized remote branch call flows, 273-274
DNS (with/without), 270-273
IP phones, CUCM implementation, 235
downloading practice exams, 468
DRS (Disaster Recovery System) interface (CUCM), 218
DRS (Disaster Recovery Systems), 444
backup device configuration, 445
CUC, 445
CUCM, 38, 445
CUP, 445
restore process, 446
scheduling backups, 445-446
DSP (Digital Signal Processors)
calculating, 22
PVDM, 22-23
VoIP, 10
VoIP and, 21-23

E

E.164 numbering plan, 15
Edison, Thomas, 6
email, VoIP, 17
emergency calls, designating POTS lines for (digit manipulation scenarios), 146-147
EM (Extension Mobility), 207, 290-298
encoding analog to digital conversions, 19-20
encryption (audio), SRTP, 60
end-to-end delay, VoIP networks, 70
End-User interface (CUCM), 226-227
end users (CUCM)
account interaction features, 253-254
application users versus, 252
credential policies, 253
device association, 254
importing via BAT, 256
LDAP integration
attribute mapping, 258-259
custom filters, 263
LDAP authentication, 257, 262-263
LDAP sync, 256-262
manually importing, 255
passwords, 253
PIN, 253
user locales, 254
enterprise IM and Jabber, 382
ephones (Ethernet Phones), 103
ephone hunt groups, configuring with CME, 201-203
ephone-dn
call parks, 177-180
call pickup, 182-183
CME user accounts, 103-104
CME voice network directories, 168
configuring, 117, 125, 129, 156-158
intercoms, configuring, 185
Notepad templates, call forwarding configuration, 173
paging, configuring, 187
shared ephone-dn, configuring with CCP, 206-207
Single Number Reach, configuring, 201
ESF (Extended Super Frame) framing, 122
Ethernet
ephone-dn, CME user accounts, 103-104
ephones, 103
IP phone connections, 54-55
catalyst switch PoE power, 56
inline PoE couplers, 56-57
power bricks, 57
power patch panels, 56-57
PoE
catalyst switch PoE, 56
inline PoE couplers, 56-57
IP phones and CUCM implementation, 235
PoE Plus, 56
power bricks, 57
power patch panels, 56-57
troubleshooting, 405
verifying, 405
SEP, 65
Exam Engine
activating exams, 468
downloading exams, 468
installing, 467
Practice Exam mode, 470-471

Study mode, 470-471
exam preparation
web resources, 477
Exam Preparation Tasks sections (test preparation), 470
Exchange and Cisco Unity Connection, 42
extension numbers, CUC voice messaging, 356
External Services menu (CUC Administration), 223
external video calls, 46

F

facts, recalling (test preparation), 470
Fax-rate voice (dial peer 0), 142
faxes and VoIP, 17
feature services versus network services, 217
filters (LDAP custom)
creating, 263
syncing, 260
final number forwards, ephone hunt groups, 203
fixed delay in VoIP networks, 69
forwarding calls, configuring with CME
CLI, 172-173
H.450.3 call forwarding, 173-175
IP phone calls, 172
forward routing rules, CUC voice messaging integration, 352
framing (ESF), 122
FXO voice ports
CME dial plans, 119
PLAR, 137
POTS lines, designating for emergency calls, 146-147
FXS voice ports
CME dial plans, 116-118
PLAR, 136

G

G.711 codec, 21
μ-law (mu-law), 20, 23
A-law, 20, 23
G.722 codec, 21
G.726 codec, 23
G.728 codec, 21
G.729ab codec, 23
G.729a codec, 21-23
G.729b codec, 21-23
G.729 codec, 20-21
gateways
call routing in CUCM, 277
CUCM call routing, 280
IOS gateway, VXML configuration, 340
monitoring activity via RTMT, 437-438
glare, analog connections, 8
goodbye call handler, CUC voice messaging integration, 350
GPickup (Group Call Pickup), CUCM telephony, 300
Greeting Administrator role (CUC voice messaging integration), 349
greetings (CUC voice messaging), 354
ground start signaling
analog connections, 8
loop starts versus, 117
group chat storage, CM-IMP, 384
GUI (Graphical User Interface)
CCP GUI, CME end user/endpoint implementation, 107-110

CME GUI, 34
Customer Admin account creation, 103-104
enabling, 101-103
user creation, 101
CME integrated GUI, 89

H

H.450.3 call forwarding standard, 173-175
header compression (link efficiency mechanisms), 73
Help Desk Administrator role (CUC voice messaging integration), 349
Help menu
Cisco Unified Serviceability Administration interface, 216
CM Administration interface, 215
CM-IMP Administration, 225
holding calls. *See* call parks
Holiday Schedules menu (CUC Administration), 223
HTTP (HyperText Transfer Protocol), CME configuration with CCP, 88, 91
hunt groups
CUCM call routing, 281
ephone hunt groups, configuring, 201-203
longest idle hunt groups, 201
parallel hunt groups, 201
peer hunt groups, 201
sequential hunt groups, 201
hunt lists, 282, 300, 311
hunt pilots, 300, 312
call routing in CUCM, 278
CUC voice messaging integration, 347-348
CUCM hunt groups (call routing), 282

I

ICCS (Intracluster Communication Signaling) and CUCM, 38
iLBC (Bitrate) codec, 21-23
IM (Instant Messaging)
CM-IMP, 387
enterprise IM and Jabber, 382
IMP (Instant Messaging and Presence)
features of, 44
interdomain federation, 44
Jabber XCP, 44-46
message compliance, 44
secure messaging, 45
importing users into CUC
bulk administration import, 372-373
CUCM, 368-370
LDAP, 370-372
informational signaling, 8
inline PoE couplers, IP phones, 56-57
inline power. *See* catalyst switch PoE
integration, CUE and CME direct integration, 34
Intercluster trunking, CUCM, 38
Intercom feature, CUCM telephony, 301, 313-315
intercoms
barge-in functionality, 185
configuring with CME, 184-187
no-auto-answer functionality, 185
internal desktop calls, 46
Internet Low codec, 21
interview handlers, CUC voice messaging integration, 350
IntServ (Integrated Services) QoS model, 71
IOS gateway, VXML configuration at, 340

IP addresses, CME router configuration with CCP, 88
IP phones
boot process, 63, 404-407
call routing in CUCM, 277
CDP, 63
clock configuration, 65-67
CME interaction, 35-36
CUCM, adding to
auto-registration, 243, 247-252
BAT, 243, 250-251
manual configuration, 243-247
self-provisioning registration, 243, 252
TAPS, 243, 251-252
CUCM call flows
call routing and digit analysis, 280-281
call routing and gateways, 280
call routing and hunt groups, 281
call routing and trunking, 280
call routing destinations, 277-278
call routing groups, 279
call routing lists, 279
call routing patterns, 278-279
call routing sources, 277
centralized deployment considerations/limitations, 275
centralized deployment PSTN backup call flows, 274
centralized remote branch call flows, 273-274
class of control, 282
class of control and CSS, 282-283
class of control and partitions, 282
distributed deployment call flows, 276-277
DNS (with/without), 270-273
PSTN backup using CAC call flows, 275-276
CUCM implementation
CDP, 235
DHCP, 235-240
DNS, 235
IP phone registration process, 236, 243-252
NTP, 234, 241
PoE, 235
SIP phone registration process, 236
TFTP, 235
CUCM interaction, 38-41
CUCM support
common phone profiles, 243
configuration requirements, 240-243
device defaults, 242
device pools, 240-242
DHCP router IOS configuration, 239-240
DHCP server configuration, 237-239
phone button templates, 242
phone security profiles, 243
service activation, 237
softkey templates, 242
dial plans, 407-410
Ethernet connections, 54-55
forwarding calls from, 172
mobility
Mobile Connect configuration, 331
MVA, 328
paging, configuring, 187

port configuration, 54-55
PortFast, 62
powering
catalyst switch PoE, 56
inline PoE couplers, 56-57
power bricks, 57
power patch panels, 56-57
QoS, 68-69
applying, 74
AutoQoS, 74-81
best effort model, 71
classification and marking mechanisms, 71
congestion avoidance mechanisms, 72
congestion management mechanisms, 72
data network requirements, 70-71
DiffServ model, 71
IntServ model, 71
link efficiency mechanisms, 72-73
policing and shaping mechanisms, 72
queuing algorithms, 73
troubleshooting, 410-413
video network requirements, 70
voice network requirements, 70
registering, 67-68, 422-424
router-based DHCP server configuration, 64-65
SIP phones
custom Native Presence groups (CUCM), 319-320
phone NTP references, 241
registering, 236
troubleshooting
boot process, 404-407
dial plans, 407-410
registration, 422-424
VLAN configuration, 57, 61-63
tagging, 59
trunking, 58-59
voice VLAN, 60
IP Precedence 0 (dial peer 0), 142
IP WAN (Internet Protocol Wide Area Networks), CUCM call flows, 273-274
ISR (Integrated Services Routers), CME support, 33-34

J

Jabber, 384
chats, 387
compliance, 387
CSF, 383, 390
deskphone mode, 381-382, 386
IM, 387
integration support, 383
persistent chats, 387
QoS, 387-388
softphone mode, 382, 386
troubleshooting, 394-395
user integration
CM-IMP, 394
CUCM, 389-392
video calls, 383
voice calls, 383
Jabber XCP (Enterprise Instant Messaging), 44-46
jitter and VoIP networks, 69-70

K - L

key systems, 14
Kiwi Syslog Daemon, 196

LDAP (Lightweight Directory Access Protocol)
attribute mapping, 258-259
CM-IMP integration, 385, 391
CUC voice messaging integration, 350, 357, 370-372
CUCM integration
attribute mapping, 258-259
LDAP authentication, 257, 262-263
LDAP custom filters, 263
LDAP sync, 256-262
custom filters, creating, 263
LDAP authentication, 257
configuring, 262
verifying, 263
LDAP servers, Cisco Unity Connection integration, 42
LDAP sync, 256-258
agreements, 259
configuring, 260-262
custom filters, 260
DirSync activation, 260
requirements/behavior, 259
single instances of, 260
verifying, 262
LDAP menu (CUC Administration), 223
LFI (Link Fragmentation and Interleaving), 73
licenses (CCP), managing, 105
Licenses menu (CUC Administration), 222
line cards, PBX systems, 13
linecoding (B8ZS), 122
line groups
call hunting, 300
CUCM hunt groups (call routing), 282
link efficiency mechanisms (QoS)
header compression, 73
LFI, 73
payload compression, 72
LLQ (Low-Latency Queuing), 73
local authentication, CME configuration with CCP, 88
local directory service (CME), 34
locales (user), end users (CUCM), 254
local group pickup, 183
local loops, PSTN, 12
locations (device pools), 241
logins, EM, 290
longest idle hunt groups, 201
loops (local), PSTN, 12
loop start signaling
analog connections, 8
ground starts versus, 117

M

MAC addresses, manual IP phone configuration in CUCM, 244
Mailbox Access Delegate Account role (CUC voice messaging integration), 349
mailboxes. *See also* voicemail boxes
Cisco Unity Connection, 42
CUC voice messaging, 356
call actions, 355
caller input, 355
greetings, 354
message actions, 355
message settings, 355
transfer rules, 354

Mailbox Store Report (CUC Serviceability reports), 462-463
maintenance, CUC Serviceability reports and maintenance operations, 462-464
maintenance reports (CUCM), 427
manually configuring
CUC voice messaging user accounts, 365-366
IP phones in CUCM, 243-247
Media Resources menu (CM Administration interface), 214
MeetingPlace, CM-IMP integration, 386
Meet-Me numbers, call routing in CUCM, 278
memberships, CUC Message Store, 374
memory tables (test preparation), 469
Message Storage menu (CUC Administration), 222
Message Store (CUC), 373
memberships, 374
message aging policy, 374-375
message quotas, 375-376
messaging
CUC voice messaging
aging policies, 357, 374-375
mailboxes, 355
memberships, 374
quotas, 375-376
user templates, 355, 360-362
playback settings, CUC voice messaging user templates, 363-364
voice messaging systems, comparing, 41
VoIP, 17
Messaging menu (CM-IMP Administration), 224
Microsoft Exchange
Cisco Unity Connection and, 42
Microsoft Exchange 2003/2007, CM-IMP integration, 386
Microsoft Office Communications Server, CM-IMP integration, 385
Mobile Connect. *See also* Single Number Reach
access lists, 327-328
applying, 334-335
configuring, 333-334
configuring
access lists, 333-335
IP phones, 331
remote destination profiles, 331-332
ring schedules for each remote destination, 332
service parameters, 335-336
softkey templates, 329-330
user accounts, 329-330
description of, 326
remote destination profiles
adding remote destinations to, 331-332
configuring, 331
configuring ring schedules for each remote destination, 332
time-of-day access, 327-328
time-of-day access, 327-328
unified mobility architecture, 327-328
mobility in CUCM
EM, 290-298
Mobile Connect
access lists, 327-328, 333-335
configuring, 329-332
description of, 326
remote destination profiles, 327-328, 331-332
ring schedules, 332
service parameters, 335-336

time-of-day access, 327-328
unified mobility architecture, 327-328
MVA, 328
activating MVA service, 337
configuring, 336-340
enabling MVA for each user, 338
media resources, 339
service parameters, 337
VXML application, configuring at IOS gateway, 340
MoH (Music on Hold)
configuring with CME, 198-199
EM and CUCM, 290
monitoring via RTMT (Real-Time Monitoring Tool), 434
CUCM monitoring
alerts, 442-443
call activity, 440-442
database summaries, 439-440
device searches, 438-439
gateway activity, 437-438
remote browsing, 443
syslog, 443-444
voice/video summaries, 437
interface of, 436
multiple instances of, installing, 435
MOS (Mean Opinion Scores), compression, 20
mu-law (µ-law), G.711 codec, 20, 23
multi-VLAN access ports, 60-63
MVA (Mobile Voice Access), 328, 336
activating MVA service, 337
enabling MVA for each user, 338
media resources, 339
service parameters, 337
VXML application, configuring at IOS gateway, 340

N

NANP (North American Numbering Plan), 15-16
Native Presence (CUCM), 301-303
BLF call lists, 317
BLF speed dials, 315-316
custom presence groups, 317-320
presence-enabled call lists, 316
Networking menu (CUC Administration), 222
networks
PSTN
analog connections, 14
analog telephones, 12
components of, 12-13
CO switches, 13
digital connections, 14
digital telephones, 13
key systems, 14
local loops, 12
numbering plans, 15-16
PBX systems, 13
private switches, 13
SS7, 14
trunks, 13
troubleshooting
CME servers, 407
DHCP servers, 406
PoE verification, 405
TFTP servers, 406
Voice VLAN assignments, 405
voice network directories, 168-171
VoIP, 17
network services versus feature services, 217
Night Service (CME), configuring with CCP, 203-206

No Access privilege (CUCM roles), 219
No application support (dial peer 0), 142
no-auto-answer functionality in intercoms, 185
No DID support (dial peer 0), 142
No DTMF relay (dial peer 0), 142
no-mute functionality in intercoms, 185
No Resource RSVP (Reservation Protocol) support (dial peer 0), 142
Notepad templates, ephone-dn call forwarding configuration, 173
notification devices, CUC voice messaging, 356, 364-365
NTP (Network Time Protocol)
  clock configuration on Cisco devices, 65-67
  IP phones, CUCM implementation, 234-235, 241
  SIP phones, phone NTP references, 241
numbering plans
  E.164, 15
  NANP, 15-16
  PSTN, 15-16
Nyquist, Dr. Henry, 17-20

O

Off, Barge option (Barge feature), 305
off hook entries, Native Presence (CUCM), 302
on hook entries, Native Presence (CUCM), 302
online resources for exam preparation, 477
OOB (Out-Of-Band) signaling, 12
opening greeting (call handler), CUC voice messaging integration, 350
opening greeting rule (direct routing), CUC voice messaging integration, 351
opening greeting rule (forward routing), CUC voice messaging integration, 352
operator call handler, CUC voice messaging integration, 350
operator calls, directing to receptionist (digit manipulation scenarios), 145-146
originating number forwards, ephone hunt groups, 203
Other Group Pickup, CUCM telephony, 300
other pickup, 183
Outcall Billing Detail Report (CUC Serviceability reports), 464
Outcall Billing Summary Report (CUC Serviceability reports), 464
Owner User ID, manual IP phone configuration in CUCM, 244

P

packet loss, VoIP networks, 69-70
packetization intervals, 411
packets, VoIP and voice to packet conversions, 17-21
paging, configuring with CME, 187-190
parallel hunt groups, 201
partitions (CUCM call flow class of control), 282
passwords
  CME administration, 88
  CUCM administration interface, 214
  CUC voice messaging user templates, 354, 359-360
  end users (CUCM), 253
  LDAP authentication and CUCM, 257, 262-263
payload compression (link efficiency mechanisms), 72

PBX (Private Branch Exchange) systems
CCS, 12
components of, 13
control cards, 13
ground start signaling, 8
line cards, 13
trunk cards, 13
Pearson Cert Practice Test engine. *See* **Exam Engine**
peer hunt groups, 201
performance, VLAN, 58
persistent chats, CM-IMP, 387
phone button templates, IP phones and CUCM implementation, 242-244, 313
Phone Interface Failed Logon Report (CUC Serviceability reports), 459-460
phone menu, CUC voice messaging user templates, 362-363
phone security profiles, IP phones and CUCM implementation, 243
phone users (CME), 100
PIN (Personal Identification Numbers), 253
PLAR (Private Line Automatic Ringdown), dial peers, 136-137
playback message settings, CUC voice messaging user templates, 363-364
PoE (Power over Ethernet)
catalyst switch PoE, 56
CUCM implementation, 235
inline PoE couplers, 56-57
PoE Plus, 56
power bricks, 57
power patch panels, 56-57
troubleshooting, 405
verifying, 405
policing and shaping mechanisms (QoS), 72
Port Activity Report (CUC Serviceability reports), 461-462
port caller ID, FXS voice ports, 118
PortFast and IP phones, 62
ports
console ports, CME administration via command-line, 479
IP phone port configuration, 54-55
voice ports
analog voice ports, 116-119
CME dial plans, 116-125
digital voice ports, 120-125
FXO voice ports, 119, 137, 146-147
FXS voice ports, 116-118, 136
POTS (Plain Old Telephone Service)
dial peers, 125-131, 142, 151, 155
lines, designating for emergency calls (digit manipulation scenarios), 146-147
power bricks, 57
power patch panels, 56-57
Practice configurations (test preparation), 470
Practice exams
activating, 468
downloading, 468
Practice Exam mode (Exam Engine), 470-471
Presence, CM-IMP
calendar resource integration, 386
CCMCIP, 384
chats, 387
compliance, 387
components of, 384
conferencing resource integration, 386
CUC integration, 385

CUCM Presence Signaling integration, 393-394
deskphone mode, 381-382, 386
IM, 387
Jabber, 381-395
LDAP integration, 385, 391
MeetingPlace integration, 386
Microsoft Exchange 2003/2007 integration, 386
Microsoft Office Communications Server integration, 385
persistent chats, 387
QoS, 387-388
Rich Presence service, 384
softphone mode, 382, 386
user integration
CM-IMP, 394
CUCM, 389-392
WebEx integration, 386

Presence menu (CM-IMP Administration), 224

privacy, CUCM telephony, 300

private DL (Distribution Lists), CUC voice messaging integration, 356, 367-368

private switches, PSTN, 13

privileges (CUCM user management), 219

productivity, VoIP, 17

profiles (phone) and CUCM implementation, 243

PSTN (Public Switched Telephone Networks), 10
analog connections, 14
analog telephones, 12
centralized deployment PSTN backup call flows (CUCM), 274
CME and Cisco IP phone interaction, 36
components of, 12-13
CO switches, 13
dial plans, 134-135
digital connections, 14
digital telephones, 13
emergency calls, designating POTS lines for (digit manipulation scenarios), 146-147
failover using prefix command (digit manipulation scenarios), 143-145
key systems, 14
local loops, 12
MVA, 328
numbering plans, 15-16
PBX systems, 13
private switches, 13
PSTN backup using CAC call flows (CUCM), 275-276
SS7, 14
trunks, 13

Publisher role, CUCM and Cisco IP phone interaction, 39-41

PVDM (Packet Voice DSP Modules), 22-23

Q

QoS (Quality of Service)
applying, 74
AutoQoS, 74-81
best effort model, 71
classification and marking mechanisms, 71
CM-IMP, 387-388
congestion avoidance mechanisms, 72
congestion management mechanisms, 72
definition of, 68
DiffServ model, 71

IntServ model, 71
IP phones, 68-69
applying to, 74
AutoQoS, 74-81
best effort QoS model, 71
classification and marking mechanisms, 71
congestion avoidance mechanisms, 72
congestion management mechanisms, 72
data network requirements, 70-71
DiffServ QoS model, 71
IntServ QoS model, 71
link efficiency mechanisms, 72-73
policing and shaping mechanisms, 72
queuing algorithms, 73
video network requirements, 70
voice network requirements, 70
link efficiency mechanisms
header compression, 73
LFI, 73
payload compression, 72
policing and shaping mechanisms, 72
queuing algorithms, 73
troubleshooting, 410-413
VoIP networks, 68-69
applying to, 74
AutoQoS, 74-81
best effort QoS model, 71
classification and marking mechanisms, 71
congestion avoidance mechanisms, 72
congestion management mechanisms, 72
data network requirements, 70-71
DiffServ QoS model, 71
IntServ QoS model, 71
link efficiency mechanisms, 72-73
policing and shaping mechanisms, 72
queuing algorithms, 73
video network requirements, 70
voice network requirements, 70
quanitization, 19-20
queuing algorithms (QoS), 73

R

RBS (Robbed Bit Signaling), 11
Read privilege (CUCM roles), 219
recalling facts (test preparation), 470
receptionist, directing operator calls to (digit manipulation scenarios), 145-146
redundant server clusters and CUCM, 37
regions (device pools), 241
registering
CME, troubleshooting, 403
CME servers, 407
DHCP servers, 406
PoE verification, 405
TFTP servers, 406
Voice VLAN assignments, 405
IP phones, 67-68
auto-registration, 243, 247-252
BAT, 243, 250-251
CUCM implementation process, 236
manual configuration, 243-247

self-provisioning registration, 243, 252
TAPS, 243, 251-252
troubleshooting registration, 422-424
SIP phones, CUCM implementation process, 236
Remote Administrator role (CUC voice messaging integration), 349
remote browsing, monitoring via RTMT, 443
remote destination profiles (Mobile Connect)
adding remote destinations to, 331-332
configuring, 331-332
time-of-day access, 327-328
repeaters, analog connections, 9
reports
Alerts Report (Serviceability Reports Archive), 457-458
billing reports, 464
CAR tool, 427
CDR and, 429-433
CMR and, 429-430
device reports, 434
exporting records, 430
service activation, 428
service parameter configuration, 428
system parameters, 429-430
system reports, 433-434
user types, 429
Cisco Serviceability Reporter service (Cisco Unified Serviceability), 455
Cisco Unified Serviceability
Cisco Serviceability Reporter service, 455
Serviceability Reports Archive, 455-459
CUC
CUC Serviceability reports, 452-454, 459-464
Serviceability Reporter service (Cisco Unified Serviceability), 455
Serviceability Reports Archive (Cisco Unified Serviceability), 455-459
CUCM reports
analyzing, 427
CAR tool, 427-434
generating, 425-426
maintenance reports, 427
system analysis reports, 427
device reports, generating via CAR tool, 434
Mailbox Store Report (CUC Serviceability reports), 462-463
Outcall Billing Detail Report (CUC Serviceability reports), 464
Outcall Billing Summary Report (CUC Serviceability reports), 464
Phone Interface Failed Logon Report (CUC Serviceability reports), 459-460
Port Activity Report (CUC Serviceability reports), 461-462
Route Plan Reports, deleting unassigned DN, 424-425
Server Report (Serviceability Reports Archive), 458-459
Serviceability Reports Archive (Cisco Unified Serviceability), 455-456
Alerts Report, 457-458
Server Report, 458-459
system reports, generating via CAR tool, 433-434
Transfer Call Billing Report (CUC Serviceability reports), 464

Unused Voice Mail Accounts Report (CUC Serviceability reports), 463-464
User Lockout Report (CUC Serviceability reports), 460-461
Users Report (CUC Serviceability reports), 453-454
restoring from backups via DRS, 446
Rich Presence service (CM-IMP), 384
ring schedules, configuring for each remote destination in Mobile Connect, 332
roles
CUC voice messaging, 349-350, 354, 360
CUCM user management, 219-220
route patterns, call routing in CUCM, 278
Route Plan Reports, deleting unassigned DN 424-425
routers
call processing and dial peers, 137-142
CCP, 105
CME routers
CME integrated GUI, 89
configuring with CCP, 88
managing with CCP, 89-93
DHCP configuration in IOS, IP phone and CUCM support, 239-240
digit manipulation, 142
designating POTS lines for emergency calls, 146-147
directing operator calls to receptionist, 145-146
PSTN failover using prefix command, 143-145
translation profiles, 148-151
DSP, 21-23
ISR, CME support, 33-34
voice ports
analog voice ports, 116-119
CME dial plans, 116-125
digital voice ports, 120-125
FXO voice ports, 119, 137, 146-147
FXS voice ports, 116-118, 136
RTCP (Real-Time Transport Control Protocol) and VoIP, 23-24
RTMT (Real-Time Monitoring Tool), 434
CUCM monitoring
alerts, 442-443
call activity, 440-442
database summaries, 439-440
device searches, 438-439
gateway activity, 437-438
remote browsing, 443
syslog, 443-444
voice/video summaries, 437
interface of, 436
multiple instances of, installing, 435
RTP (Real-Time Transport Protocol)
CME and Cisco IP phone interaction, 35
CUCM call flows
centralized remote branch call flows, 274
DNS (with/without), 270-271
VoIP and, 23-24
runtime data, CUCM, 38

S

sampling analog to digital conversions, 19
SCCP (Skinny Client Control Protocol)
CME
administration, 104-105
Cisco IP phone interaction, 35

CUC voice messaging integration, 347-348
CUCM call flows
centralized remote branch call flows, 274
distributed deployment call flows, 277
with DNS (with/without), 270-271
IP phone registration, 67-68
scheduling
backups via DRS, 445-446
ring schedules, configuring for each remote destination in Mobile Connect, 332
searching for devices via RTMT, 438-439
security
audio encryption, SRTP, 60
CCP, 105
CUCM administration interface, 214
device security profiles, manual IP phone configuration in CUCM, 244
phone security profiles, IP phones and CUCM implementation, 243
VLAN, 58
Self Care Portal (CUCM), 226-227
self-provisioning IP phone registration in CUCM, 243, 252
SEP (Selsius Ethernet Phone), 65
sequential hunt groups, 201
Server Report (Serviceability Reports Archive), 458-459
servers
CME servers, 407
CUPS and CUCM, 273
DHCP servers
boot process, 406
IP phone and CUCM support, 237-239
IP phone boot process, 63, 406
router-based configuration, 64-65
LDAP, Cisco Unity Connection integration, 42
TFTP servers
boot process, 406
CUCM and, 39
IP phone boot process, 63, 406
IP phone registration, 68
registering IP phones, 423
troubleshooting IP phones, 423
VCS, 46-47
service activation (IP phones), CUCM support, 237
service parameters, configuring via Mobile Connect, 335-337
shared lines, CUCM telephony, 299, 303-304
signaling
address, 8
CAS, 10-11
CCS, 11-12
CSS, 14
degradation, 10
ground start, analog connections, 8
ICCS and CUCM, 38
informational, 8
loop start, analog connections, 8
OOB, 12
RBS, 11
SS7 and PSTN, 14
supervisory, 8
Single Number Reach, configuring with CME, 199-200. ***See also*** **Mobile Connect**

SIP (Session Initiation Protocol)
CME
administration, 104-105
Cisco IP phone interaction, 35
CUC voice messaging integration, 348
CUCM call flows
centralized remote branch call flows, 274
distributed deployment call flows, 277
DNS (with/without), 270-271
IP phone registration, 67-68
SIP phones
custom Native Presence groups (CUCM), 319-320
phone NTP references, 241
registering (CUCM implementation process), 236
SIP URI, 278
SNMP menu (Cisco Unified Serviceability Administration interface), 216
softkey templates
IP phones and CUCM implementation, 242
Mobile Connect configuration, 329-330
softphones
softphone mode (Jabber), 382, 386
VoIP and, 17
SRST (Survivable Remote Site Telephony)
CCP and CME router configuration, 92
centralized deployment PSTN backup call flows (CUCM), 274
CUC voice messaging, 356
PSTN backup using CAC call flows (CUCM), 276
SRTP (Secure Real-Time Protocol), audio encryption, 60
SS7 (Signaling System 7), PSTN, 14
SSH (Secure Shell), CME
administration via command-line, 479
configuration with CCP, 88
storing
group chats with CM-IMP, 384
messages, CUC voicemail boxes, 373
memberships, 374
message aging policy, 374-375
quotas, 375-376
Study mode (Exam Engine), 470-471
study Plans (test preparation), 469
Subscriber role, CUCM and Cisco IP phone interaction, 39-41
supervisory signaling, 8
switches and PSTN
CO, 13
private, 13
synchronizing LDAP sync, 256-258
agreements, 259
configuring, 260-262
custom filters, 260
DirSync activation, 260
requirements/behavior, 259
single instances of, 260
verifying, 262
syslog, monitoring via RTMT, 443-444
system administrators
CME, 100
System Administrator role (CUC voice messaging integration), 350
system analysis reports (CUCM), 427
system call handlers, CUC voice messaging integration, 350
System menu
CM Administration interface, 214
CM-IMP Administration, 224

system reports, generating via CAR tool, 433-434

System Settings menu (CUC Administration), 222

T

tagging (VLAN), 59

TAPS (Auto Register Phone Tool), IP phone registration in CUCM, 243, 251-252

TDM (Time-Division Multiplexing), 10

Technician role (CUC voice messaging integration), 350

telephones and PSTN

analog, 12

digital, 13

telephony

CUCM

Barge feature, 299, 304-305

call coverage, 298-315

call forward options, 298-299

call hunting, 300-301, 310-313

call park, 301, 308-310

call pickup groups, 300, 305-308

CFA, 298

CFB internal/external, 299

CFNA internal/external, 299

CFNC internal/external, 299

CFUR internal/external, 299

GPickup, 300

Intercom feature, 301, 313-315

Native Presence, 301-303, 315-320

Other Group Pickup, 300

privacy, 300

shared lines, 299, 303-304

Whisper intercom feature, 301

Telephony Integrations menu (CUC Administration), 223

TelePresence calls, 46

Telnet

CME administration via command-line, 479

CME configuration with CCP, 88, 91

templates

Notepad templates, configuring ephone-dn call forwarding, 173

Phone Button templates, 313

phone button templates

IP phones and CUCM implementation, 242

manual IP phone configuration, 244

softkey templates

IP phones and CUCM implementation, 242

Mobile Connect configuration, 329-330

UDT, 248-250

ULT, 248-250

user templates in CUC voice messaging integration

basic elements of, 353-354

basics of, 358

call actions, 355

caller input, 355

configuring, 357-358

greetings, 354

message actions, 355, 361-362

message settings, 355, 360-361

notification devices, 364-365

password settings, 354, 359-360

phone menu, 362-363

playback message settings, 363-364

roles, 354, 360

transfer rules, 354
TUI settings, 355
Templates menu (CUC Administration), 222
test preparation
chapter-ending review tools, 469
Cisco Learning Network, 469
Exam Engine
activating other exams, 468
activating practice exams, 468
downloading practice exams, 468
installing, 467
Practice Exam mode, 470-471
Study mode, 470-471
Exam Preparation Tasks, 470
memory tables, 469
Practice configurations, 470
Premium Edition, 468
recalling facts, 470
study plans, 469
web resources, 477
TFTP (Trivial File Transfer Protocol)
CUCM and, 39
IP phones
boot process, 63, 406
CUCM implementation, 235
registering, 423
troubleshooting, 406, 423
time/date, setting in Cisco devices, 65-67
time-of-day access in Mobile Connect, 327-328
TMS (TelePresence Management Suite), 47
toll call control, CUC voice messaging, 356
tones (call progress), FXS voice ports, 118
Tools menu
Cisco Unified Serviceability Administration interface, 216
CUC Administration, 223
Trace menu (Cisco Unified Serviceability Administration interface), 216
Transfer Call Billing Report (CUC Serviceability reports), 464
transferring calls
blind transfers, 175
configuring with CME, 175-177
consult transfers, 175
transfer rules, CUC voice messaging, 354
translation patterns, call routing in CUCM, 277
translation profiles, digit manipulation scenarios, 148-151
troubleshooting
best practices, 402-403, 421-422
boot processes, IP phones, 404-407
CME
CME servers, 407
dial plans, 407-410
QoS, 410-413
registration issues, 403-407
CUC Serviceability reports and troubleshooting operations, 459-462
CUCM, 421
analyzing reports, 427
CAR tool, 427-434
DN, 424-425
generating reports, 425-426
IP phone registration, 422-424
maintenance reports, 427
QoS, 413
system analysis reports, 427
DHCP servers, IP phone boot process, 406

dial plans, 407-410
disaster recovery via DRS, 444
backup device configuration, 445
CUC, 445
CUCM, 445
CUP, 445
restore process, 446
scheduling backups, 445-446
DN (unassigned), 424-425
IP phones
boot process, 404-407
dial plans, 407-410
QoS, 410-413
registration, 422-424
Jabber, 394-395
methodology of, 402-403, 421-422
monitoring via RTMT, 434
CUCM monitoring, 437-444
installing multiple instances of RTMT, 435
interface operation, 436
networks
CME servers, 407
DHCP servers, 406
PoE verification, 405
TFTP servers, 406
Voice VLAN assignments, 405
PoE, 405
QoS, 410-413
TFTP servers, IP phone boot process, 406
Voice VLAN assignments, 405
trunk cards, PBX systems, 13
trunking
CUCM
call routing, 277, 280
Intercluster trunking, 38
PSTN, 13
VLAN trunking, 58-59
VoIP trunking and CME, 34
TUI settings, CUC voice messaging user templates, 355

U

UDT (Universal Device Templates), 248-250
ULT (Universal Line Templates), 248-250
unified collaboration, 32
Cisco Unity Connection, 41
CUCM interaction, 43-44
Exchange and, 42
features of, 42
LDAP directory server integration, 42
mailboxes, 42
voicemail, 42
voice messaging, 41
VPIM, 42
CME
call processing, 34
Cisco IP phones, 35-36
command-line configuration, 34
CTI support, 34
device control, 34
direct integrating with CUE, 34
features of, 34
GUI-based configuration, 34
ISR G2 platform support, 33-34
local directory service, 34
VoIP trunking, 34
CUCM, 33
appliance-based operation, 37
audio telephony support, 37

call processing, 41
Cisco IP phones, 38-41
Cisco Unity Connection interaction, 43-44
clusters, 39
database replication, 38
directory service support/ integration, 38
DRS, 38
features of, 37-38
ICCS, 38
Intercluster trunking, 38
redundant server clusters, 37
runtime data, 38
TFTP servers, 39
video telephony support, 37
VMware installation, 37
voice gateway control/communication, 38
IMP
features of, 44
interdomain federation, 44
Jabber XCP, 44-46
message compliance, 44
secure messaging, 45
TMS, 47
VCS, 46-47
Unified Communications (CCP), 105-107
unregistered entries, Native Presence (CUCM), 302
Unused Voice Mail Accounts Report (CUC Serviceability reports), 463-464
Update privilege (CUCM roles), 219
User Administrator role (CUC voice messaging integration), 350
user locales, end users (CUCM), 254
User Lockout Report (CUC Serviceability reports), 460-461
user management
CUCM
Access Control Groups, 220-221
privileges, 219
roles, 219-220
User Management menu (CM Administration interface), 215
usernames (CME administration), CME configuration with CCP, 88
Users menu (CUC Administration), 222
Users Report (CUC Serviceability reports), 453-454
user templates, CUC voice messaging integration
basic elements of, 353-354
basics of, 358
call actions, 355
caller input, 355
configuring, 357-358
greetings, 354
message actions, 355, 361-362
message settings, 355, 360-361
notification devices, 364-365
password settings, 354, 359-360
phone menu, 362-363
playback message settings, 363-364
roles, 354, 360
transfer rules, 354
TUI settings, 355

V

VAD (Voice Activity Detection), 21, 142
variable delay, VoIP networks, 69
VCS (Video Communication Server), 46-47

verifying
LDAP sync, 262
PoE, 405
video
video calls
external video calls, 46
internal desktop calls, 46
Jabber, 383
TelePresence calls, 46
TMS, 47
VCS, 46-47
video telephony and CUCM, 37
voice/video summaries (CUCM), monitoring via RTMT, 437
VLAN (Virtual Local Area Networks)
benefits of, 58
IP phones, 57
configuring, 61-63
registering, 423
troubleshooting, 423
VLAN tagging, 59
VLAN trunking, 58-59
voice VLAN, 60
manageability, 58
multi-VLAN access ports, 60-63
performance, 58
security, 58
tagging, 59
topology independence, 58
trunking, 58-59
VLAN-hopping attacks, 63
voice VLAN, 60
VMware installation and CUCM, 37
voice
VoIP and voice to packet conversions, 17-21
voice calls
Jabber, 383
voice call legs, 126-127
voice gateway control and CUCM, 38
voice messaging and CUC integration, 41, 343
Audio Text Administrator role, 349
Audit Administrator role, 349
authentication rules, 352
call handlers, 350
call routing, 351
call routing rule filters, 352
CUC Message Store, 373
memberships, 374
message aging policy, 374-375
quotas, 375-376
CUCM using SCCP, 347-348
dial plans, 353
direct routing rules, 351
DL, 352
enterprise parameters, 350
forward routing rules, 352
Greeting Administrator role, 349
Help Desk Administrator role, 349
LDAP, 350, 357, 370-372
Mailbox Access Delegate Account role, 349
mailboxes
call actions, 355
caller input, 355
greetings, 354
message actions, 355
message settings, 355
transfer rules, 354
multisite deployments, 347
overview of CUC, 346
Remote Administrator role, 349
service parameters, 350
single-site deployments, 346
SIP and CUC integration, 348
System Administrator role, 350

system settings
general configuration, 349
roles, 349-350
Technician role, 350
User Administrator role, 350
user configuration, 355
AAR, 356
account creation options, 356
alternate extensions/names, 366-367
call forward options, 356
extension numbers, 356
manual configuration, 365-366
notification devices, 356
private DL, 356, 367-368
SRST, 356
toll call control, 356
voicemail boxes, 356
user importation
bulk administration import, 372-373
CUCM, 368-370
LDAP, 370-372
user templates
basic elements of, 353-354
basics of, 358
call actions, 355
caller input, 355
configuring, 357-358
greetings, 354
message actions, 355, 361-362
message settings, 355, 360-361
notification devices, 364-365
password settings, 354, 359-360
phone menu, 362-363
playback message settings, 363-364
roles, 354, 360
transfer rules, 354
TUI settings, 355
voicemail boxes
message aging policy, 357, 374-375
message storage, 373-375
quotas, 357, 375-376
voice network directories, configuring, 168-171
voice ports
analog voice ports
CME dial plans, 116-119
FXO voice ports, 119, 137, 146-147
FXS voice ports, 116-118, 136
CME dial plans
analog voice ports, 116-119
digital voice ports, 120-125
FXO voice ports, 119, 146-147
FXS voice ports, 116-118
digital voice ports, 120-125
voice/video summaries (CUCM), monitoring via RTMT, 437
voice VLAN (Virtual Local Area Networks), 60, 405
voice/video summaries (CUCM), monitoring via RTMT, 437
voicemail
call hunting, 300
Cisco Unity Connection, 42
Unused Voice Mail Accounts Report (CUC Serviceability reports), 463-464
voicemail pilots, CUC voice messaging integration, 347-348
voicemail ports, call routing in CUCM, 277
VoIP, 17

voicemail boxes (CUC voice messaging), 356. *See also* mailboxes
message aging policy, 357, 374-375
message storage, 373-375
quotas, 357, 375-376
Voicemail Port Wizard, CUC voice messaging integration, 347-348
VoIP (Voice over IP)
business benefits of, 16-17
cabling, 17
CME, VoIP trunking, 34
compatibility, 17
cost of, 16
dial peers, 125, 131-133, 143-144
DSP, 10, 21-23
email, 17
faxes, 17
messaging, 17
networks, 17
productivity, 17
PVDM, 22-23
RTCP, 23-24
RTP, 23-24
softphones, 17
voicemail, 17
voice to packet conversions, 17-21
VoIP networks
bandwidth, 69
delay, 69-70
end-to-end delay, 70
fixed delay, 69
IP phones
boot process, 63
catalyst switch PoE power, 56
CDP, 63
clock configuration, 65-67
Ethernet connections, 54-55
inline PoE couplers, 56-57
port configuration, 54-55
PortFast, 62
power bricks, 57
power patch panels, 56-57
QoS, 68-81
registering, 67-68
router-based DHCP server configuration, 64-65
VLAN configuration, 57-63
jitter, 69-70
packet loss, 69-70
potential problems with, 69-70
QoS, 68-69
applying, 74
AutoQoS, 74-81
best effort model, 71
classification and marking mechanisms, 71
congestion avoidance mechanisms, 72
congestion management mechanisms, 72
data network requirements, 70-71
DiffServ model, 71
IntServ model, 71
link efficiency mechanisms, 72-73
policing and shaping mechanisms, 72
queuing algorithms, 73
video network requirements, 70
voice network requirements, 70
variable delay, 69
VOMIT (Voice Over Misconfigured Internet Telephones), voice VLAN, 60
VPIM (Voice Profile for Internet Mail) and Cisco Unity Connection, 42

VXML (Voice eXtensible Markup Language)
MVA, 328
MVA VXML, configuring at IOS gateway, 340

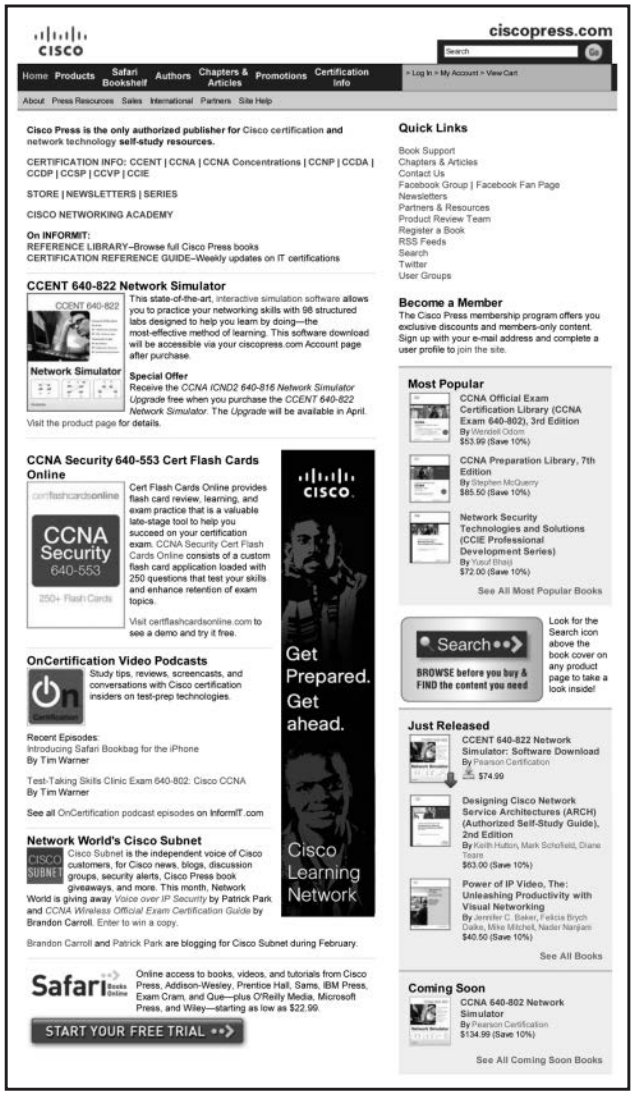
W

waveforms (analog), 7
web resources for exam preparation, 477
WebEx, CM-IMP integration, 386
WFQ (Weighted Fair Queuing), 73
Whisper intercom feature, CUCM telephony, 301
wildcards (dial peer), 133-134
Wireshark, voice VLAN, 60

X - Y - Z

XCP (Extensible Communication Platform). *See* Jabber XCP

ciscopress.com: Your Cisco Certification and Networking Learning Resource



Subscribe to the monthly Cisco Press newsletter to be the first to learn about new releases and special promotions.

Visit **ciscopress.com/newsletters.**

While you are visiting, check out the offerings available at your finger tips.

–Free Podcasts from experts:
- OnNetworking
- OnCertification
- OnSecurity

Podcasts

View them at **ciscopress.com/podcasts**.

–Read the latest author **articles** and **sample chapters** at **ciscopress.com/articles**.

–Bookmark the Certification Reference Guide available through our partner site at **informit.com/certguide**.

Connect with Cisco Press authors and editors via Facebook and Twitter, visit **informit.com/socialconnect**.

APPENDIX D

Memory Tables

Chapter 1

Table 1-4 Memory Table for Chapter 1

Topic	Purpose	Hardware Affiliation
	Measures analog waveform many times per second	Performed by codec in DSP internal to analog-to-digital device (for example, IP phone, gateway)
Quantizing		Performed by DSP
Encoding		Performed by DSP
	Optional, reduces the amount of binary data to represent the encoded sample	Performed by DSP
Channel associated signaling		
Common channel signaling		
RTP	Real-time Transport Protocol	

Chapter 2

Table 2-6 Memory Table for Chapter 2

Product	Capacity (Phones, Users, Mailboxes, and so On)	Platform
CME		
CUCM		
IMP		
CUC		

Chapter 3

Table 3-6 Memory Table for Chapter 3

Feature/Concern	Definition	Purpose
DHCP Option 150		Required for IP phone downloads
	Centralized clock synchronization	Critical for log timestamps, certificates, CDRs, time display
QoS		Critical to maintain acceptable delay and jitter for good voice quality
	End-to-end travel time of a packet	Maximum 150 ms for voice packets
	Delay variation between packets	Maximum 30 ms
	Packet loss in transit	Less than 1%
AutoQoS		Simpler than manual config; manually tunable

Chapter 4

Table 4-3 Memory Table for Chapter 4

Chapter Concept	Activity	Where or What?
Configure CME router to support CCP	Four configurations required to support CCP	
	Basic CME configuration	http://<CME_IP>/ccme.html
	Group of up to 5 devices under CCP management	Initial CCP setup dialog

Chapter 5

Table 5-4 Memory Table: CME User and Endpoint Concepts

Component	CME Element
IP phoneIP phone model and MAC using SCCP	
Extension assigned to a SCCP IP phone	
Extension assigned to IP phone using SIP	
IP phone model and MAC using SIP	
Three of the steps required to access the CME built-in GUI	
Three user access levels in CME	

APPENDIX E

Memory Table Answer Key

Chapter 1

Table 1-4 Memory Table for Chapter 1

Topic	Purpose	Hardware Affiliation
Sampling	Measures analog waveform many times per second	Performed by codec in DSP internal to analog-to-digital device (for example, IP phone, gateway)
Quantizing	Adjusts sample measurement data to closest binary value	Performed by DSP
Encoding	Assigns a binary value to the sample	Performed by DSP
Compression	Optional, reduces the amount of binary data to represent the encoded sample	Performed by DSP
Channel associated signaling	"Robs" some bits from the audio channel to deliver addressing and feature signaling	Associated with T1/E1 circuits
Common channel signaling	Uses a separate, dedicated channel for addressing and feature signaling	Associated with ISDN circuits (BRI, PRI)
RTP	Real-time Transport Protocol	Carries digitized voice payload

Chapter 2

Table 2-6 Memory Table for Chapter 2

Product	Capacity (Phones, Users, Mailboxes, and so On)	Platform
CME	Max 450 phones	Runs on ISR router
CUCM	Max 40,000 phones per cluster	Runs on UCS/VMware appliance platform
IMP	Max 45,000 users with CUCM cluster integration	Runs on UCS/VMware appliance
CUC	Max 20,000 mailboxes	Runs on UCS/VMware appliance

Chapter 3

Table 3-6 Memory Table for Chapter 3

Feature/Concern	Definition	Purpose
DHCP Option 150	TFTP server IP address	Required for IP phone downloads
NTP	Centralized clock synchronization	Critical for log timestamps, certificates, CDRs, time display
QoS	Prioritizes voice traffic at the expense of other traffic	Critical to maintain acceptable delay and jitter for good voice quality
Delay	End-to-end travel time of a packet	Maximum 150 ms for voice packets
Jitter	Delay variation between packets	Maximum 30 ms
Loss	Packet loss in transit	Less than 1%
AutoQoS	Automates QoS consistent best-practices deployment	Simpler than manual config; manually tunable

Chapter 4

Table 4-3 Memory Table for Chapter 4

Chapter Concept	Activity	Where or What?
Configure CME router to support CCP	Four configurations required to support CCP	IP address, level 15 username and password, HTTP/S server enabled, local authentication for Telnet/SSH
Integrated web-based GUI	Basic CME configuration	http://<CME_IP>/ccme.html
CCP Community	Group of up to 5 devices under CCP management	Initial CCP setup dialog

Chapter 5

Table 5-4 Memory Table: CME User and Endpoint Concepts

Component	CME Element
IP phoneIP phone model and MAC using SCCP	ephone
Extension assigned to a SCCP IP phone	ephone-dn
Extension assigned to IP phone using SIP	voice register dn
IP phone model and MAC using SIP	voice register pool
Three of the steps required to access the CME built-in GUI	Download and extract GUI files to flash; set IP HTTP path; define web admin account; enable dn-webedit and time-webedit
Three user access levels in CME	System admin, customer admin, ordinary/ end user

Appendix F

Study Planner

Practice Test	Reading	Task
Labs and Exercises	Video	

Element	Task	Goal Date	First Date Completed	Second Date Completed (Optional)	Notes
Introduction	Read Introduction				
1. Traditional Voice vs. Unified Voice	Read Foundation Topics				
1 .Traditional Voice vs. Unified Voice	Review Key Topics				
1 .Traditional Voice vs. Unified Voice	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 1 in practice test software				
2. Understanding the Components of Cisco Unified Communications	Read Foundation Topics				
2. Understanding the Components of Cisco Unified Communications	Review Key Topics				
2. Understanding the Components of Cisco Unified Communications	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 2 in practice test software				
3. Understanding Cisco IP Phones	Read Foundation Topics				
3. Understanding Cisco IP Phones	Review Key Topics				
3. Understanding Cisco IP Phones	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 3 in practice test software				
4. Getting Familiar with CME Administration	Read Foundation Topics				
4. Getting Familiar with CME Administration	Review Key Topics				
4. Getting Familiar with CME Administration	Define Key Terms				

Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 4 in practice test software				
5. Managing Endpoints and End Users in CME	Read Foundation Topics				
5. Managing Endpoints and End Users in CME	Review Key Topics				
5. Managing Endpoints and End Users in CME	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 5 in practice test software				
6. Understanding the CME Dial-Plan	Read Foundation Topics				
6. Understanding the CME Dial-Plan	Review Key Topics				
6. Understanding the CME Dial-Plan	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 6 in practice test software				
7. Enabling Telephony Features with CME					
7. Enabling Telephony Features with CME	Review Key Topics				
7. Enabling Telephony Features with CME	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 7 in practice test software				
8. Administrator and End-User Interfaces	Read Foundation Topics				
8. Administrator and End-User Interfaces	Review Key Topics				
8. Administrator and End-User Interfaces	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 8 in practice test software				
9. Managing Endpoints and End Users in CUCM	Read Foundation Topics				
9. Managing Endpoints and End Users in CUCM	Review Key Topics				
9. Managing Endpoints and End Users in CUCM	Define Key Terms				

9. Managing Endpoints and End Users in CUCM	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 9 in practice test software				
10. Understanding CUCM Dial-Plan Elements and Interactions	Read Foundation Topics				
10. Understanding CUCM Dial-Plan Elements and Interactions	Review Key Topics				
10. Understanding CUCM Dial-Plan Elements and Interactions	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 10 in practice test software				
11. Enabling Telephony and Mobility Features with CUCM	Read Foundation Topics				
11. Enabling Telephony and Mobility Features with CUCM	Review Key Topics				
11. Enabling Telephony and Mobility Features with CUCM	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 11 in practice test software				
12. Enabling Mobility Features in CUCM	Read Foundation Topics				
12. Enabling Mobility Features in CUCM	Review Key Topics				
12. Enabling Mobility Features in CUCM	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 12 in practice test software				
13. Voice Messaging Integration with Cisco Unity Connection	Read Foundation Topics				
13. Voice Messaging Integration with Cisco Unity Connection	Review Key Topics				
13. Voice Messaging Integration with Cisco Unity Connection	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 13 in practice test software				
14. Enabling CM IM and Presence Support	Read Foundation Topics				
14. Enabling CM IM and Presence Support	Review Key Topics				

14. Enabling CM IM and Presence Support	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 14 in practice test software				
15. Common CME Management and Troubleshooting Issues	Read Foundation Topics				
15. Common CME Management and Troubleshooting Issues	Review Key Topics				
15. Common CME Management and Troubleshooting Issues	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 15 in practice test software				
16. CUCM Monitoring, Maintenance and Troubleshooting	Read Foundation Topics				
16. CUCM Monitoring, Maintenance and Troubleshooting	Review Key Topics				
16. CUCM Monitoring, Maintenance and Troubleshooting	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 16 in practice test software				
17. Monitoring Cisco Unity Connection	Read Foundation Topics				
17. Monitoring Cisco Unity Connection	Review Key Topics				
17. Monitoring Cisco Unity Connection	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 17 in practice test software				
18. Final Preparation	Read Chapter				
18. Final Preparation	Take practice test in study mode for all Book Questions in practice test software				
18. Final Preparation	Review all Key Topics in all chapters				
18. Final Preparation	Complete all memory tables from Appendix D				
18. Final Preparation	Take practice test in practice exam mode using Exam Bank #1 questions for all chapters				
18. Final Preparation	Take practice test in practice exam mode using Exam Bank #2 questions for all chapters				

Where are the Companion Content Files?

Thank you for purchasing this Premium Edition version of:

CCNA Collaboration CICD 210-060 Official Cert Guide

The print version of this title comes with a disc of companion content. As an eBook reader, you have access to these files by following the steps below:

1. Go to **ciscopress.com/account** and log in.
2. Click on the "Access Bonus Content" link in the Registered Products section of your account page for this product, to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps at left, please visit **ciscopress.com/contact** and select the "Site Problems/ Comments" option. Our customer service representatives will assist you.

The Professional and Personal Technology Brands of Pearson

Addison Wesley · Cisco Press · IBM Press · informIT · PEARSON IT Certification · Prentice Hall · que · SAMS · vmware PRESS