



Implementing Cisco Unified Communications Manager, Part 1 (CIPT1)

Foundation Learning Guide Second Edition



**Josh Finke, CCIE® No. 25707
Dennis Hartmann, CCIE® No. 15651**

Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) Foundation Learning Guide

Second Edition

Josh Finke
Dennis Hartmann

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) Foundation Learning Guide

Second Edition

Josh Finke
Dennis Hartmann

Copyright© 2012 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 1 2 3 4 5 6 7 8 9 0

First Printing August 2011

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58720-418-0

ISBN-10: 1-58720-418-5

Warning and Disclaimer

This book is designed to provide information about Cisco Unified Communications administration and to provide test preparation for the CIPT Part 1 version 8 exam (CCNP Voice CIPT1 642-447), which is part of the CCNP Voice certification. Every effort has been made to make this book as complete and 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 authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

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

Corporate and Government Sales

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

For sales outside the United States, please contact: International Sales international@pearsoned.com

Feedback Information

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

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

We greatly appreciate your assistance.

Publisher: Paul Boger

Business Operation Manager, Cisco Press: Anand Sundaram

Associate Publisher: Dave Dushimer

Manager Global Certification: Erik Ullanderson

Executive Editor: Brett Bartow

Senior Development Editor: Christopher Cleveland

Managing Editor: Sandra Schroeder

Copy Editor: John Edwards

Senior Project Editor: Tonya Simpson

Technical Editor: Manny Richardson

Editorial Assistant: Vanessa Evans

Proofreader: Sheri Cain

Book Designer: Gary Adair

Indexer: Tim Wright

Composition: Mark Shirar



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, Quick Study, IronPort, LightStream, Linksys, MediaTone, MeetingPlace, Chime Sound, MGX, Networks, Networking Academy, Network Registrar, PCNow, PIX, PowerPanel, 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 Authors

Josh Finke, CCIE No. 25707, is the practice director for collaboration and networking at Iron Bow Technologies, a Cisco Gold and Master Unified Communications Partner. Josh was previously a lead instructor and director of operations for Internetwork Expert, a leading CCIE training company. Josh has multiple certifications, including the Cisco CCIE Voice, CCNP, CCDP, CCNA, CCDA, and Cisco Meeting Place Specialist. Josh specializes in Cisco UC, routing and switching, and enterprise network design. Josh started working with Cisco networking technologies in 2000 and later became one of the youngest Voice CCIEs in the world. He lives with his wife in Seattle, Washington.

Dennis J. Hartmann, CCIE No. 15651, is a Unified Communications consultant. Dennis is also a lead instructor at Global Knowledge. Dennis was first exposed to CallManager during the CallManager 2.0 time frame when Cisco acquired Selsius. Dennis has various certifications, including the Cisco CCVP, CCSI, CCNP, CCIP, and the Microsoft MCSE. Dennis has worked for various Fortune 500 companies, including AT&T, Sprint, Merrill Lynch, KPMG, and Cabletron Systems. Dennis lives with his wife and children in Hopewell Junction, New York.

About the Technical Reviewer

Manny Richardson, CCIE No. 6056, is a Voice and Routing and Switching CCIE. He is a design and implementation engineer consultant with MARTA and the City of Atlanta in Atlanta, Georgia. He is also an instructor with more than five years of worldwide teaching experience. He has worked in the field of networking for 12 years, with the last three years primarily focused on Cisco Voice.

Dedication

I dedicate this book to the love and support in my life, Alissa.

Acknowledgments

Thank you to my wife, my family, and all of those who have supported and believed in me.

Thank you to Brett Bartow, Chris Cleveland, and the entire Cisco Press team, who are excellent at what they do and made this book possible.

Contents at a Glance

Introduction	xix
Chapter 1	Cisco Unified Communications Manager Architecture 1
Chapter 2	Deployment Models 29
Chapter 3	Cisco Unified Communications Manager Services and Initial Configuration Settings 47
Chapter 4	Managing User Accounts in Cisco Unified Communications Manager 71
Chapter 5	Cisco Unified Communications Manager Endpoints 101
Chapter 6	Cisco Catalyst Switches 123
Chapter 7	Implementing and Hardening IP Phones 141
Chapter 8	Implementing PSTN Gateways in Cisco Unified Communications Manager 185
Chapter 9	Call-Routing Components 221
Chapter 10	Calling Privileges 265
Chapter 11	Digit Manipulation 297
Chapter 12	Call Coverage 327
Chapter 13	Media Resources 351
Chapter 14	Phone Services 387
Chapter 15	Presence-Enabled Speed Dials and Lists 407
Chapter 16	Implementing Cisco Unified Mobility 425
Appendix A	Answers to Review Questions 457
	Index 461

Contents

Introduction	xix
Chapter 1 Cisco Unified Communications Manager Architecture	1
Chapter Objectives	1
CUCM Overview	2
Cisco UC Solution Components	2
Cisco UC Network	4
CUCM Functions	6
CUCM Signaling and Media Paths	7
<i>Example: Basic IP Telephony Call</i>	8
CUCM Hardware, Software, and Clustering	9
CUCM Cluster	10
<i>Cisco 7800 Series Media Convergence Servers</i>	11
<i>CUCM Operating System</i>	12
Cisco UC Database	13
<i>Static Configuration Data</i>	13
<i>User-Facing Features</i>	13
Database Access Control	15
CUCM Licensing	16
<i>License File Request Process</i>	18
<i>Obtaining Additional Licenses</i>	19
<i>Licensing Components</i>	20
<i>Calculating License Units</i>	22
<i>License Unit Reporting</i>	22
Chapter Summary	24
Review Questions	25
Chapter 2 Deployment Models	29
Chapter Objectives	29
CUCM: Single-Site Deployment	30
Multisite WAN with Centralized Call Processing	31
Multisite Deployment with Distributed Call Processing	34
Benefits	36
Best Practices	36
Clustering over the IP WAN	37

CUCM Call-Processing Redundancy	39
Chapter Summary	43
Review Questions	43
Chapter 3 Cisco Unified Communications Manager Services and Initial Configuration Settings	47
Chapter Objectives	47
CUCM Initial Configuration	48
Network Components	48
<i>Network Time Protocol</i>	48
<i>Dynamic Host Configuration Protocol</i>	49
<i>Trivial File Transfer Protocol</i>	49
<i>Domain Name System</i>	49
NTP and DHCP Considerations	50
DHCP	51
DNS	54
Network and Feature Services	57
Network Services	58
Feature Services	58
<i>Service Activation</i>	59
<i>Control Center</i>	60
Global Server Settings	60
<i>Enterprise Parameters</i>	60
<i>Enterprise Phone Configuration</i>	62
<i>Service Parameters</i>	64
Chapter Summary	66
Review Questions	67
Chapter 4 Managing User Accounts in Cisco Unified Communications Manager	71
Chapter Objectives	71
CUCM User Accounts	71
User Account Types	72
User Privileges	73
User Management	76
Managing User Accounts	76
Bulk Administration Tool Overview	82
Bulk Administration Tool Components	83

Bulk Provisioning Service	84
Managing User Accounts Using Cisco Unified Communications Manager BAT	84
Lightweight Directory Access Protocol (LDAP) Overview and Considerations	86
LDAPv3 Integration	86
LDAPv3 Synchronization	87
<i>Synchronization Agreements</i>	88
<i>Synchronization Search Base</i>	90
<i>Synchronization Best Practices</i>	91
<i>LDAPv3 Synchronization Configuration</i>	92
LDAPv3 Authentication	94
<i>LDAPv3 Authentication Configuration</i>	97
Chapter Summary	98
Review Questions	99
Chapter 5 Cisco Unified Communications Manager Endpoints	101
Chapter Objectives	101
CUCM Endpoints	102
Endpoint Features	103
Cisco IP Phone Models	105
<i>Entry-Level Cisco IP Phones</i>	105
<i>Midrange Cisco IP Phones</i>	106
<i>High-End Cisco IP Phones</i>	106
<i>Cisco Unified IP Phone 8900 Series</i>	106
<i>Cisco Unified IP Phone 9900 Series</i>	107
<i>Other Cisco IP Phones</i>	108
Cisco IP Phones: Boot Sequence	111
H.323 Endpoint Support	115
SIP Third-Party IP Phone Support in CUCM	116
SIP Third-Party Authentication	118
Chapter Summary	119
Review Questions	120
Chapter 6 Cisco Catalyst Switches	123
Chapter Objectives	123
Cisco LAN Switches	124
Providing Power to Cisco IP Phones	126

Cisco Original Power over Ethernet Device Detection 127

IEEE 802.3af Device Detection 127

Voice VLAN Support on Cisco IP Phones 129

Single-VLAN Access Port 130

Multi-VLAN Access Port 131

802.1q Trunk Port 132

Native Cisco IOS VLAN Configuration 134

CatOS VLAN Configuration 136

Chapter Summary 138

Review Questions 139

Chapter 7 Implementing and Hardening IP Phones 141

Chapter Objectives 141

Endpoint Configuration Tools and Elements Overview 142

Endpoint Basic Configuration Elements 143

Device Pool 144

Phone Network Time Protocol Reference 146

Date/Time Groups 148

Cisco Unified CM Group 149

Regions 151

Locations 153

Phone Security Profile 155

Device Settings 156

Device Defaults 157

Phone Button Template 157

Softkey Template 158

SIP Profile 161

Common Phone Profiles 162

Phone Configuration Element Relationship 162

Phone Auto-registration 163

Auto-registration Configuration 165

Bulk Administration Tool and Auto-Register Phone Tool 167

Auto-Register Phone Tool 168

TAPS: Phone Insert Process 169

Bulk Administration Tool 169

Bulk Provisioning Service 170

Phone Template 170

<i>Line Template</i>	171
<i>CSV File</i>	172
<i>Phone Validation</i>	174
<i>Inserting IP Phones into the CUCM Database</i>	175
Manual Configuration	176
Endpoint Registration Verification	178
Third-Party SIP Phone Configuration	179
Chapter Summary	182
References	182
Review Questions	183
Chapter 8 Implementing PSTN Gateways in Cisco Unified Communications Manager	185
Chapter Objectives	185
Analog and Digital Gateways	186
Core Gateway Requirements	187
Gateway Communication Overview	188
Gateway Protocol Functions for Cisco Unified Communications Manager Integration	189
MGCP Gateway Implementation	191
Endpoint Identifiers	191
MGCP Gateway Support	193
MGCP Configuration Server	193
Q.931 Backhaul	194
MGCP Gateway Configuration: CUCM	194
MGCP Gateway Configuration: Cisco IOS Configuration	198
MGCP Gateway: Registration Verification	201
Fractional T1/E1 Configuration on an MGCP Gateway	203
Fractional T1/E1 Configuration on Cisco Unified Communications Manager	204
MGCP Gateway Verification	205
MGCP Gateway Considerations	205
H.323 Gateway Implementation	206
Cisco Unified Communications Manager	
H.323 Gateway Configuration	207
Configure Basic Cisco IOS H.323 Functionality	209
<i>Configure CUCM Redundancy on H.323 Gateways: Calls from the H.323 Gateway to the CUCM Cluster</i>	210

<i>Configure CUCM Redundancy on H.323 Gateways: Calls from CUCM to the H.323 Gateway</i>	211
<i>H.323 Gateway Call Survivability</i>	212
SIP Gateway Implementation	212
CUCM SIP Gateway Configuration	213
<i>Add a SIP Trunk</i>	213
<i>Configure SIP Trunk Parameters</i>	214
<i>Configure Basic Cisco IOS SIP Functionality</i>	216
<i>Configure Cisco IOS Call Routing on SIP Gateways</i>	217
<i>SIP Trunking</i>	218
<i>SIP Trunk: MTP Allocation Configuration</i>	218
Chapter Summary	218
References	219
Review Questions	219
Chapter 9 Call-Routing Components	221
Chapter Objectives	221
Dial Plan Components	222
Endpoint Addressing	224
Uniform On-Net Dial Plan Example	227
E.164 Overview	229
Call-Routing Overview	230
Call-Routing Table Entries	232
Route Patterns	233
<i>Route Pattern Examples</i>	236
Digit Analysis	237
Digit Forwarding	244
SCCP Phones: User Input	245
Cisco SIP IP Phones: User Input	246
<i>Type A SIP Phones: No Dial Rules</i>	246
<i>Cisco Type A SIP IP Phones: Dial Rules</i>	246
<i>Cisco Type B SIP Phones: No Dial Rules</i>	247
Special Call-Routing Features	248
Route Filters	248
The ! Wildcard	251
Call Classification	252
Secondary Dial Tone	253

CUCM Path Selection	253
Path Selection Elements	254
Path Selection Configuration	254
<i>Route Group</i>	254
<i>Local Route Group</i>	256
<i>Route List</i>	258
Chapter Summary	261
References	262
Review Questions	262
Chapter 10 Calling Privileges	265
Calling Privileges	265
Partitions and Calling Search Spaces	267
Configuring Partitions and Calling Search Spaces	274
Step 1: Creating Partitions	274
Step 2: Assigning Numbers, Patterns, and Ports to Partitions	275
Steps 3–5: Configuring Calling Search Spaces	276
Time-of-Day Call Routing	277
Step 1: Create Time Periods	280
Step 2: Create a Time Schedule and Associate One or More Time Periods with It	281
Step 3: Assign the Time Schedule to a Partition That Should Be Active Only During the Time Specified in the Time Schedule	282
Client Matter Codes and Forced Authorization Codes	282
Class of Service Approaches	285
Emergency Call Routing and Vanity Numbers	290
Private Line Automatic Ringdown	292
Chapter Summary	294
Review Questions	295
Chapter 11 Digit Manipulation	297
CUCM Digit Manipulation	298
Mechanics of CUCM Digit Manipulation	298
External Phone Number Mask	302
Translation Patterns	303
Transformation Masks	307
CUCM Digit Prefix and Stripping	309
Significant Digits	312

Cisco Unified Communications Manager Global Transformations	312
Calling Party Transformation Pattern Configuration	316
Called Party Transformation Pattern Configuration	317
Transformation Calling Search Space	317
Incoming Number Settings	317
Incoming Calling Party Prefix Example: Globalization of Calling Number	318
Gateway Incoming Calling Party Settings Configuration	319
Device Pool Incoming Calling and Called Party Transformation Calling Search Space	320
Transformation Examples	320
Chapter Summary	323
Review Questions	324

Chapter 12 Call Coverage 327

Call Coverage	328
Call Forwarding	328
Shared Lines	329
Call Pickup	329
Call-Hunting Components and Processes	330
Call-Hunting Options and Distribution Algorithms	334
Call-Hunting Flow	335
Call-Hunting Configuration	337
Task 1: Create the Line Groups, Add Members, and Configure the Distribution Algorithm and Hunt Options	338
Task 2: Create the Hunt List and Add the Line Groups	339
Task 3: Create the Hunt Pilot, Associate the Hunt List with the Hunt Pilot, and Configure Hunt Forward Settings	340
Task 4: Configure Personal Preferences on Phone Lines in the Event That Hunting Ends with No Coverage	341
Call-Forwarding Features	343
Example: Call Forwarding Without Forward No Coverage Settings	343
Example: Forward No Coverage	344
Example: Call Coverage—Forward Hunt No Answer	345
Example: Call Coverage—Forward Hunt Busy	346
Example: Call Coverage—Forward No Coverage External Missing	347
Chapter Summary	348
Review Questions	349

Chapter 13 Media Resources 351

- Media Resources 351
- Media Resource Support 353
 - Audio Conferencing 354
 - MTP 356
 - Annunciator 356
 - MoH 357
- Conferencing 358
 - Cisco Conference Bridge Hardware 359
 - Cisco Conference Bridge Hardware (Cisco Catalyst WS-X6608-T1 and WS-X6608-E1)* 359
 - Cisco IOS Conference Bridge (Cisco NM-HDV and 1700 Series Routers)* 360
 - Cisco Conference Bridge (Cisco WS-SVC-CMM-ACT)* 360
 - Cisco IOS Enhanced Conference Bridge (Cisco NM-HDV2, NM-HD-IV/2V/2VE, 2800 and 2900 Series, and 3800 and 3900 Series Routers)* 360
- Conferencing Media Resource Configuration 362
- MeetMe Conference Configuration 370
- Music on Hold 371
 - MoH Configuration 374
- Annunciator 378
- Media Resource Access Control 379
- Chapter Summary 384
- Review Questions 384

Chapter 14 Phone Services 387

- Cisco IP Phone Services 387
 - Cisco IP Phone Services Subscriptions Overview 388
 - Cisco IP Phone Services Provisioning 389
 - Cisco IP Phone Services Access 391
 - Default Cisco IP Phone Services 391
 - Cisco IP Phone Services Redundancy 393
 - Cisco IOS SLB 393
 - Use of DNS to Provide Cisco IP Phone Services Redundancy 394
- Cisco IP Phone Services Configuration 394
 - Step 1: Verify or Change the Enterprise Parameters Relevant to Cisco IP Phone Services 395

Step 2: Add a New Cisco IP Phone Service	397
Step 3: Configure the Cisco IP Phone Services Parameters of the Added Service	397
Cisco IP Phone Services Subscriptions	402
Subscribe Cisco IP Phone Services: Administrator	402
Subscribe Cisco IP Phone Services: End User	403
Chapter Summary	404
Review Questions	405
Chapter 15 Presence-Enabled Speed Dials and Lists	407
How Presence Works with CUCM	407
Presence Support in CUCM	408
Presence Configuration	410
Step 1: Enable Presence-Enabled Speed Dials	411
Step 2: Configure the BLF Speed Dial	412
Step 3: Allow Presence Subscriptions Through SIP Trunks	412
Presence Access Control	413
Presence Policy Configuration	417
Chapter Summary	420
References	421
Review Questions	421
Chapter 16 Implementing Cisco Unified Mobility	425
Cisco Unified Mobility Overview	425
Mobile Connect and MVA Characteristics	426
Cisco Unified Mobility Features	427
Cisco Unified Mobility Call Flows	427
Mobile Connect Call Flow: Internal Calls Placed from Remote Phone	428
MVA Call Flow	429
Cisco Unified Mobility Implementation Requirements	430
Mobility Configuration Elements	431
Shared Line Between Phone and Remote Destination Profile	432
Relationship of Mobility Configuration Elements	433
Cisco Unified Mobility Considerations	435
MVA Call Flow with MGCP PSTN Gateway Access	435
CSS Handling in Mobile Connect	436
CSS Handling in MVA	436
Cisco Unified Mobility Access List Functions	437

Mobility Phone Number Matching	439
Cisco Unified Mobility Configuration	439
Step 1: Configure Softkey Template	440
Step 2: Configure End User	440
Step 3: Configure IP Phone	441
Step 4: Configure Remote Destination Profile	442
Step 5: Add Remote Destinations to Remote Destination Profile	443
Step 6: Configure Service Parameters	445
Step 7a: Configure Access List	445
Step 7b: Apply Access List to Remote Destination	447
Cisco Unified Mobility: MVA Configuration Procedure	448
Step 1: Activate Cisco Unified Mobile Voice Access Service	448
Step 2: Configure Service Parameters	449
Step 3: Enable MVA per End User	450
Step 4: Configure MVA Media Resource	450
Step 5: Configure MVA on Cisco IOS Gateway	451
Chapter Summary	453
References	454
Review Questions	454

Appendix A Answers to Review Questions 457**Index 461**

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

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

Goals and Methods

The most important goal of this book is to provide you with knowledge and skills in Unified Communications, deploying the Cisco Unified Communications Manager product. Another goal of this book is to help you with the Cisco IP Telephony (CIPT) Part 1 exam, which is part of the Cisco Certified Network Professional Voice (CCNP) certification. The methods used in this book are designed to be helpful in both your job and the CCNP Voice Cisco IP Telephony exam. This book provides questions at the end of each chapter to reinforce the chapter content. Additional test-preparation software from companies such as www.selftestsoftware.com gives you additional test-preparation questions to arm you for exam success.

The organization of this book helps you discover the exam topics that you need to review in more depth, helps you fully understand and remember those details, and helps you test the knowledge you have retained on those topics. This book does not try to help you pass by memorization, but helps you truly learn and understand the topics. The Cisco IP Telephony Part 1 exam is one of the foundation topics in the CCNP Voice certification. The knowledge contained in this book is vitally important for you to consider yourself a truly skilled Unified Communications (UC) engineer. The book helps you pass the Cisco IP Telephony 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
- Providing practice exercises on the topics and the testing process through test questions at the end of each chapter

Who Should Read This Book

This book is designed to be both a general Cisco Unified Communications Manager book and a certification preparation book. This book provides you with the knowledge required to pass the CCNP Voice Cisco IP Telephony exam for CIPT Part 1.

Why should you want to pass the CCNP Voice Cisco IP Telephony exam? The first CIPT test is one of the milestones toward getting the CCNP Voice certification. The CCNP Voice could mean a raise, promotion, new job, challenge, success, or recognition, but ultimately you determine what it means to you. Certifications demonstrate that you are serious about continuing the learning process and professional development. In technology, it

is impossible to stay at the same level when the technology all around you is advancing. Engineers must continually retrain themselves, or they find themselves with out-of-date, commodity-based skill sets.

Strategies for Exam Preparation

The strategy you use for exam preparation might be different than strategies used by others. It will be based on skills, knowledge, experience, and finding the recipe that works best for you. If you have attended the CIPT course, you might take a different approach than someone who learned Cisco Unified Communications Manager on the job. Regardless of the strategy you use or your background, this book is designed to help you get to the point where you can pass the exam. Cisco exams are quite thorough, so don't skip any chapters.

How This Book Is Organized

The book covers the following topics:

- **Chapter 1, “Cisco Unified Communications Manager Architecture,”** discusses the architecture and all the components involved. CUCM hardware requirements, operating system, database, signaling, licensing, and database replication are discussed.
- **Chapter 2, “Deployment Models,”** covers the deployment models in which CUCM can be used. This chapter introduces the technologies required for the different UC models. The advantages and disadvantages of each deployment model are considered.
- **Chapter 3, “Cisco Unified Communications Manager Services and Initial Configuration Settings,”** examines the network configuration, Network Time Protocol (NTP), and DHCP configuration options of CUCM. The chapter also covers frequently adjusted CUCM enterprise and service parameters.
- **Chapter 4, “Managing User Accounts in Cisco Unified Communications Manager,”** examines user account configuration in CUCM administration, the Bulk Administration Tool (BAT), and the Lightweight Directory Access Protocol (LDAP).
- **Chapter 5, “Cisco Unified Communications Manager Endpoints,”** covers the various Cisco Unified IP Phones and the features that they support. Third-party Session Initiation Protocol (SIP) endpoint support is covered, in addition to the Cisco IP Phone boot cycle and registration process.
- **Chapter 6, “Cisco Catalyst Switches,”** covers the power and voice VLAN requirements of the Cisco IP Phone. The Catalyst switch configurations are examined for both Native IOS and CatOS switches. The Cisco and IEEE power specifications are also covered.

- Chapter 7, “**Implementing and Hardening IP Phones**,” covers the methods for endpoint (phone) registration within CUCM, including manual registration and autoregistration, and the tools available for each process.
- Chapter 8, “**Implementing PSTN Gateways in Cisco Unified Communications Manager**,” covers the implementation of the gateways used in conjunction with CUCM. MGCP, H.323, and SIP gateways are each explored.
- Chapter 9, “**Call-Routing Components**,” covers the fundamentals of call routing and a public switched telephone network (PSTN) dial plan. Digit analysis and path selection are achieved through the use of the router pattern, route list, and route group CUCM configuration elements.
- Chapter 10, “**Calling Privileges**,” covers the process of class of service through the use of partitions and calling search spaces. The chapter also covers time-of-day routing through the use of time periods and time schedules.
- Chapter 11, “**Digit Manipulation**,” covers the process of digit manipulation through calling and called party transformation masks, translation patterns, prefixing digits, and digit discard instructions (DDI).
- Chapter 12, “**Call Coverage**,” covers the topic of call-coverage paths through the use of a hunt pilot, hunt list, and line groups. Call-hunting flow is discussed through the various distribution algorithms supported in CUCM.
- Chapter 13, “**Media Resources**,” discusses the media resources supported in and through CUCM. The media resource topics include music on hold (MoH), conference bridges, annunciators, transcoders, and media termination points. Media resource allocation is discussed through the application of CUCM Media Resource Manager (MRM), media resource group list, and media resource groups.
- Chapter 14, “**Phone Services**,” explores the concept of phone services and their use within CUCM, including configuration, subscriptions, and considerations.
- Chapter 15, “**Presence-Enabled Speed Dials and Lists**,” covers presence theory and configuration through the use of presence groups, presence speed dials, and presence calling search spaces.
- Chapter 16, “**Implementing Cisco Unified Mobility**,” covers the concept and configuration of mobility for CUCM end users using constructs such as single-number reach and mobile voice access.
- Appendix A, “**Answers to Review Questions**,” lists the answers to the chapter review questions.

This page intentionally left blank

Chapter 1

Cisco Unified Communications Manager Architecture

A Cisco Unified Communications (UC) deployment relies on Cisco Unified Communications Manager (CUCM) for call processing, device control, call routing, mobility services, phone/system feature administration, and dial plan administration. Understanding the role that CUCM plays in a UC deployment to provide the essential call-routing functions necessary to deploy voicemail, unified messaging, presence, video to the desktop, videoconferencing, TelePresence, and cloud-based services such as those provided by Cisco WebEx Connect is integral to the success of UC.

This chapter introduces and describes the role, architecture, hardware and software requirements, and licensing model of CUCM.

Chapter Objectives

Upon completing this chapter, you will understand the CUCM architecture and be able to meet the following objectives:

- Describe the components of a Cisco Unified Communications solution and each component's functionality.
- Describe the architecture and role of CUCM.
- Describe the hardware requirements for CUCM.
- Describe the characteristics of the CUCM operating system.
- Describe the characteristics of the CUCM database and how it provides redundancy.
- Describe the licensing model of CUCM.
- Describe how to calculate, verify, and add license units to CUCM.

CUCM Overview

Cisco Unified Communications (UC) is an IP-based communications system integrating voice, video, data, and mobility products and applications. It enables more effective, secure communications and can transform the way in which we communicate. UC represents a communications paradigm shift like that of the invention of the telegraph. UC removes the geographic barriers of effective communications through the use of voice, video, and data integration. Business can be conducted with a fluidity that progresses and evolves with you. Information has been at our fingertips for a long time, but UC enables the sharing of this information to create knowledge and value.

Cisco UC is part of an integrated solution that includes network infrastructure, security, mobility, network management products, lifecycle services, flexible deployment, and third-party communication applications.

Cisco UC can impact the bottom line by creating more effective communications without losing the personal nature of a face-to-face conversation. More effective communications lead to reduced time to market and nimble transformation of business processes through collaboration.

Cisco UC Solution Components

The Cisco UC strategy encompasses voice, video, and data traffic traversing a single network infrastructure. Cisco UC equipment is capable of managing all three traffic types and interfacing with all standards-based network protocols.

Cisco UC represent new ways of delivering functionality to enterprise customers. Cisco UC is a coordinated release of an *integrated* set of products that are tested, documented, and supported as a *cohesive system*.

Figure 1-1 illustrates four standard layers of the Cisco UC model with examples of the components within each layer of the model.

The components of the standard layers are as follows:

- **Infrastructure layer:** The infrastructure consists of routers, switches, and voice gateways. The infrastructure layer carries voice, video, and data between all network devices and applications. This layer also provides high availability, management, quality of service (QoS), and network security.
- **Call control layer:** The call control layer provides call processing, device control, and administration of the dial plan and features. Call control can be provided by CUCM, Cisco Unified Communications Manger Express (CUCME), or CUCM Business Edition (CUCMBE). This book focuses on the CUCM product, which is almost identical to CUCMBE. Call processing is independent from the infrastructure layer. CUCM, CUCMBE, or CUCME in San Jose, California, can process call control for a device physically located in another site over a WAN (for example, Chicago).

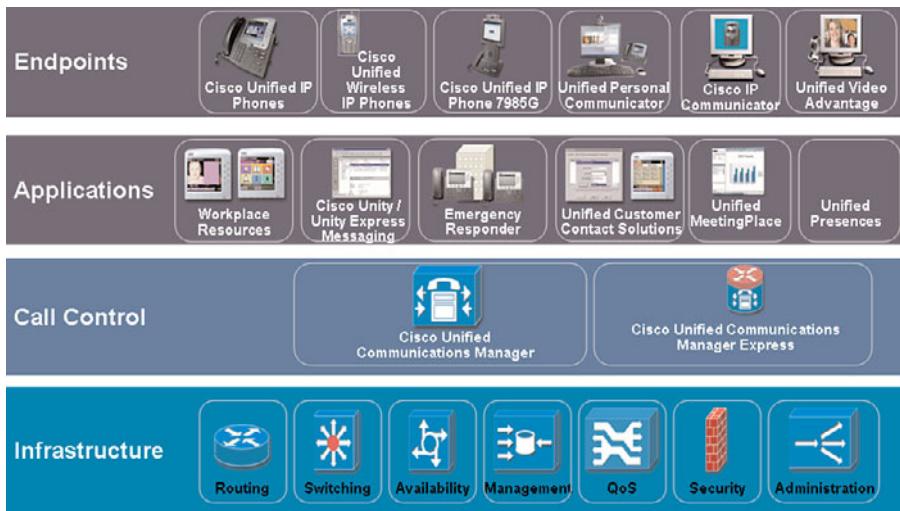


Figure 1-1 Cisco UC Solution Components

- **Applications layer:** Applications are independent from call-control functions and the physical voice ports. Application servers are integrated through IP, which allows the applications to reside anywhere within the network:
 - Voicemail, integrated messaging, and unified messaging applications are provided through Cisco Unity, Cisco Unity Express, or Cisco Unity Connections products.
 - Contact centers of various sizes can be built with Cisco Unified Contact Center (UCC) and Cisco Unified Contact Center Express (UCCX).
 - Cisco Unified MeetingPlace and WebEx are medium- to large-scale conferencing servers that support video integration. The MeetingPlace product integrates lecture-style conferences with scalable collaboration and control tools. Cisco WebEx is positioned to the small- to medium-sized enterprises, with MeetingPlace focused on large enterprise installations.
 - Cisco Emergency Responder (CER) enhances the existing emergency functionality offered by CUCM. Cisco ER provides physical location updates for mobile devices to guarantee that emergency calls to the public safety answering point (PSAP) are properly routed to the PSAP in charge of emergency calls for that site. Cisco ER identifies the caller's physical location to the switch port and maps the call to an emergency line identification number (ELIN) based on a square footage range (as mandated by the National Emergency Number Association [NENA]). An ELIN is an automatic number identification (ANI)/caller identification (CLID) that is registered with the PSAP for the purpose of identifying the physical location of the calling party. The ELIN is associated with an Emergency Response Location (ERL) in the master street address guide (MSAG) located in the PS-ALI (Public Switch - Automatica Location

Identification) database. Deploying this capability helps ensure more effective compliance with legal or regulatory obligations, thereby reducing the life and liability risks related to emergency calls.

- The Cisco Unified Presence (CUP) server collects information regarding the availability, willingness, and communications capabilities of a user and provides this information to watchers of the user as a status indication. The status information is based on the user's device availability (on hook, off hook, or unregistered). The status information is augmented by the user's communication preferences (phone, video, instant messaging, or email) if the user has the ability to publish this information and the watcher's application has the ability to view the information. The Cisco Unified Personal Communicator (CUPC) software client is only supported if there is a CUP server in the cluster.
- Standards-based protocols are used to provide an integration layer between CUCM and other application servers. The protocols leveraged include the following: Telephony Application Programming Interface (TAPI), Java Telephony Application Programming Interface (JTAPI), Simple Object Access Protocol (SOAP), AVVID over the XML Layer (AXL), Q.SIG, H.323, Media Gateway Control Protocol (MGCP), and Session Initiation Protocol (SIP).
- **Endpoints layer:** The endpoints layer brings applications to the user, whether the end device is a Cisco IP Phone, a PC using a software-based phone, or a communications client or video terminal. Cisco UC provides multiprotocol support for Skinny Client Control Protocol (SCCP), H.323, MGCP, and SIP.

Cisco UC Network

The Cisco UC system delivers fully integrated communications, converging voice, video, and data over a single network infrastructure using standards-based protocols. The Cisco UC system delivers capabilities to address current and emerging communications needs in the enterprise environment, as illustrated by the network topology shown in Figure 1-2.

The Cisco UC product suite is designed to optimize functionality, reduce configuration and maintenance requirements, and provide interoperability with a variety of other applications. It provides this capability while maintaining high availability, QoS, and security.

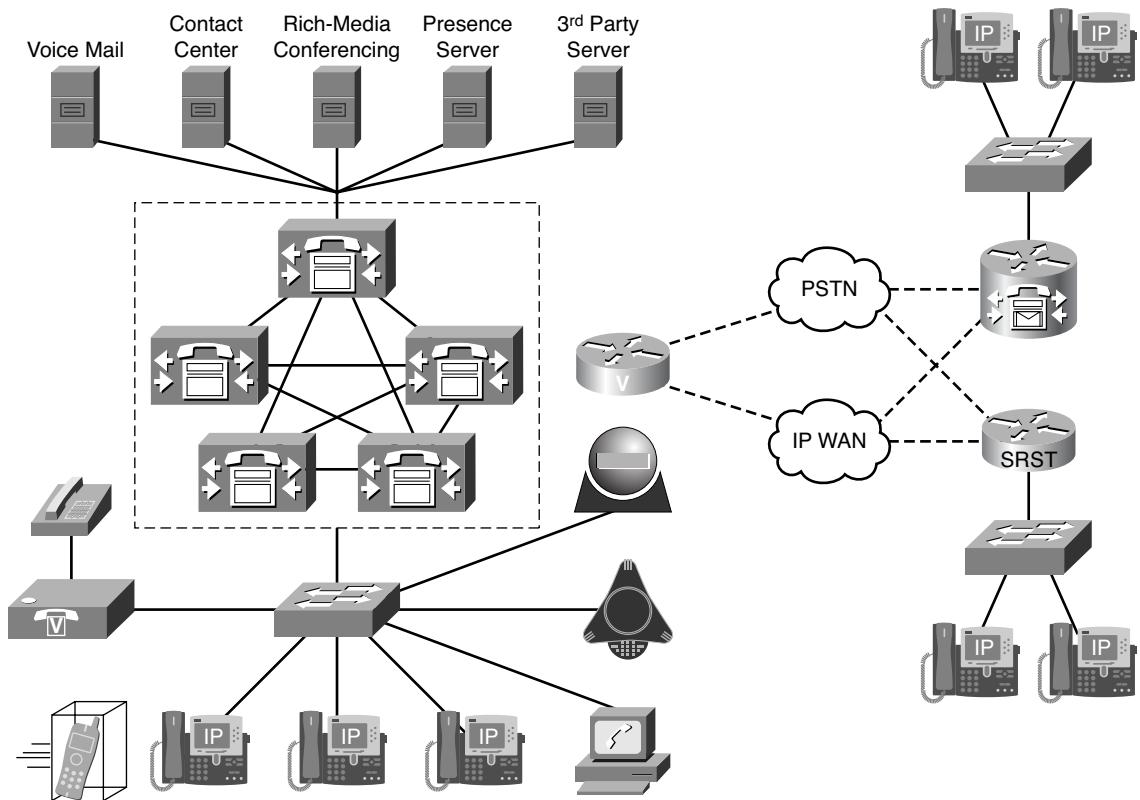


Figure 1-2 Cisco UC Network

The Cisco UC system integrates the following major communications technologies:

- **IP telephony:** IP telephony refers to technology that transmits voice communications over a network using IP instead of time-division multiplexing (TDM) as a transport system. Cisco UC includes a wide array of hardware and software products such as call-processing agents, IP phones, voice-messaging systems, video devices, conferencing, and many other applications.
- **Customer contact center:** Cisco Unified Contact Center products are a combination of strategy and architecture to revolutionize call center environments. Cisco Unified Contact Center promotes efficient and effective customer communications across large networks by enabling organizations to draw from a broader range of resources to service customers. These resources include access to a large pool of agents and multiple channels of communication and customer self-help tools. Unified Contact Center enables powerful applications using database (ODBC) queries, skill-based routing, and queuing based on programming scripts.

- **Video telephony:** The Cisco Unified Video Advantage (CUVA) and Cisco Unified Personal Communicator (CUPC) products enable real-time video communications and collaboration using the same IP network and call-processing capabilities available to Cisco IP Phones. Cisco Unified Video Advantage does not require special end-user training. Video calling with CUVA is as easy as dialing a phone number.
- **Rich-media conferencing:** Cisco Unified MeetingPlace and WebEx create a virtual meeting environment with an integrated set of IP-based tools for voice, video, and web conferencing.
- **Third-party applications:** Cisco works with third-party vendors to provide the broadest selection of innovative third-party IP communications applications and products focused on critical business needs such as messaging, customer care, and workforce optimization.

CUCM Functions

CUCM extends enterprise telephony features and functions to packet telephony network devices. These packet telephony network devices include Cisco IP Phones, media-processing devices, VoIP gateways, and multimedia applications. Additional data, voice, and video services, such as converged messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact with the IP telephony solution through the CUCM application programming interface (API).

CUCM provides these functions:

- **Call processing:** Call processing refers to the complete process of originating, routing, and terminating calls, including any billing and statistical collection processes.
- **Signaling and device control:** CUCM terminates and coordinates all signaling events between call endpoints and directs devices such as phones, gateways, and conference bridges to establish and tear down streaming RTP media connections. Signaling is also referred to as call control and call setup/call teardown.
- **Dial plan administration:** The dial plan is a set of configurable patterns that CUCM uses to perform call routing. CUCM is responsible for digit analysis (DA) of all calls into or out of the CUCM cluster.
- **Phone feature administration:** CUCM extends supplementary services such as hold, transfer, forward, conference, speed dial, redial, and call park to IP phones and gateways.
- **Directory services:** CUCM uses a portion of the Informix Database Server (IDS) Lightweight Directory Access Protocol version 3 (LDAPv3) database to store user information. User authentication can be performed locally or against an external directory service. Directory synchronization allows centralized user management. Directory synchronization allows CUCM to leverage users already configured in a corporate-wide directory service, such as Microsoft Active Directory 2003 and

2008, Microsoft Active Directory Application Mode (ADAM) 2003, Microsoft Lightweight Directory Services 2008, iPlanet Directory Server 5.1, Sun ONE 5.2 and 6.X, and OpenLDAP 2.3.39 and 2.4 directory integrations. The local CUCM database is an LDAP-compliant database (LDAPv3) component in the IBM Informix Database Server (IDS).

- **Backup and restore tools:** CUCM provides a Disaster Recovery System (DRS) to back up and restore the CUCM configuration database. The DRS also backs up call detail records (CDR), call management records (CMR), and the CDR Analysis and Reporting (CAR) database.

Figure 1-3 shows three Cisco IP Phones that have been logically registered with one of the CUCMs in the cluster. Multiple CUCM servers in a cluster share a database that is replicated between the servers. Cisco IP Phones maintain an active TCP port 2000 connection to both their primary and backup CUCM server. Figure 1-3 shows the phone's logical TCP/IP connections to the primary server.

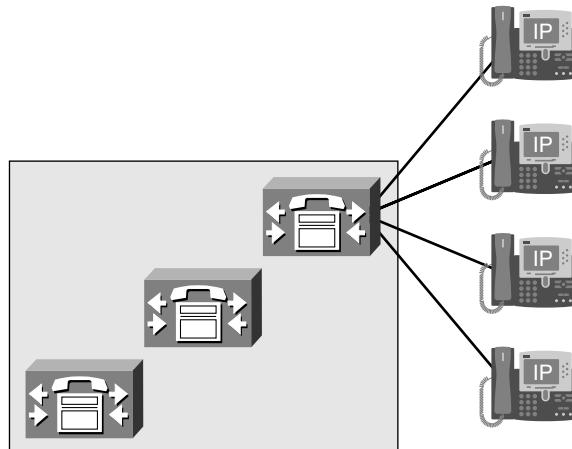


Figure 1-3 CUCM Functions

CUCM Signaling and Media Paths

CUCM uses SIP or SCCP to communicate with Cisco IP Phones for call setup and tear-down tasks. All supplementary services (call hold, park, transfer, conference) are transported as call-signaling events.

When the called party picks up his ringing phone, CUCM completes the call setup phase, resulting in a media exchange that occurs directly between the Cisco IP Phones across the IP network using the Real-Time Transport Protocol (RTP). CUCM is not involved in any call processing after the call has been set up unless a softkey feature is

initiated. The CUCM server could be unplugged from the network during the call and the calls would survive (call survivability/call preservation). The users on the active call would not be aware of the CUCM failure unless they attempted to use a feature on the phone during the call. All supplementary services will fail during the CUCM outage as indicated by the LCD screen message indicated on the IP Phone (CM Down, Features Disabled). CUCM is involved only in call setup, teardown, and the invocation of supplementary service features.

Example: Basic IP Telephony Call

Figure 1-4 illustrates a user at phone A (calling party) placing a call to phone B (called party).

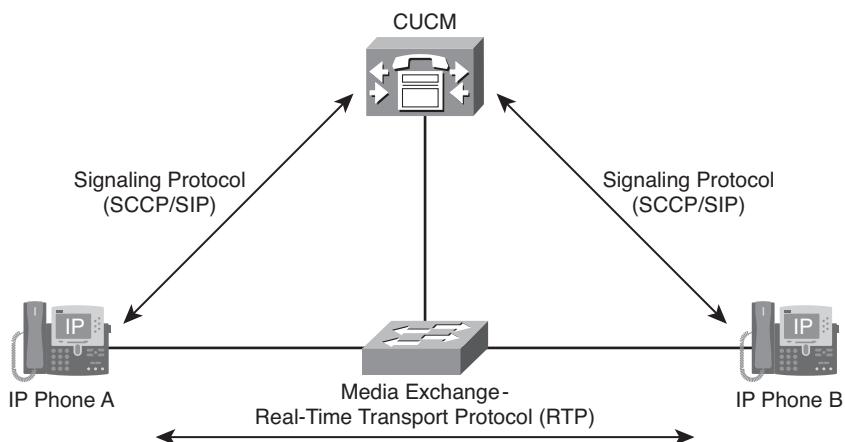


Figure 1-4 CUCM Signaling and Media Paths

As shown in the figure, the following steps occur during a call from phone A to B:

1. The calling party at IP phone A picks up the handset (goes off hook), resulting in an SCCP or SIP message being sent to CUCM, indicating that the device has gone off hook.
2. CUCM responds to this stimulus message with a response message that tells the device to play the dial tone file that is stored in the flash memory of the phone.
3. The calling party at phone A then hears dial tone and begins dialing the phone number of phone B (called party). SCCP phones send their digits to CUCM as they are pressed (digit by digit), whereas SIP phones send their dialed digits digit by digit or in one message (en bloc signaling), depending on the generation of Cisco IP Phone. Type B SIP-based Cisco phones use Keypad Markup Language (KPML) by default. KPML sends digits to CUCM in real time as they are dialed unless SIP dial rules are leveraged. SIP dial rules always send their digits en bloc regardless of whether the Cisco

Phone is a Type A (7940, 7960) or Type B Phone (7970, 79x1, 79x2, 79x5, 7906). Type A Cisco Phones do not support KPML, resulting in enbloc signaling by default.

4. Regardless of how the digits are collected, CUCM performs digit analysis against the dialed digits collected from the calling party.
5. When a match is found in the call-routing database, CUCM routes (steers) the call to the called party based on the call-routing configuration. If CUCM does not find a match, a reorder tone is sent to the calling party.
6. CUCM sends a signaling event to the calling party (phone A) to initiate ringback, so the user at phone A will hear the ringback tone. CUCM also signals the call to the called (destination) phone (ringdown). Additional information is provided to the phones to indicate the calling and called party name and number. (Phone A's LCD will indicate the called party name and number, while phone B's LCD will indicate the calling party name and number).
7. When the user at phone B accepts the call (goes off hook), CUCM sends a signaling message to the devices to coordinate the IPv4 socket (IPv4 address and port number) information that will be used for the duration of the call. The RTP media path is opened directly between the two phones over the network infrastructure, which removes the CUCM reliance during the call.
8. No further communication with CUCM takes place until either phone invokes a supplementary service feature (transfer, conference, hold) or the call is ended.

CUCM Hardware, Software, and Clustering

CUCM Release 8.0 is a complete hardware and software solution that works as a network appliance. A network appliance is a closed system that supports only Cisco-authorized applications and utilities. Goals of the appliance model include simplifying installation, security, and patching of the system. The appliance-based model makes it possible for an administrator to install, implement, and manage a CUCM server without requiring any knowledge of the underlying Linux-based operating system.

The CUCM appliance has these features:

- CUCM servers are preinstalled with all software that is required to operate, maintain, secure, and manage a server or cluster of servers.
- CUCM is also provided as a software-only product, which can be installed on supported Cisco Media Convergence Servers (MCS) or Cisco-approved, third-party server platforms. At press time, CUCM is approved to run on various HP, IBM, and Cisco Unified Computing Servers (UCS).
- System administration is performed through a GUI, CLI, or documented APIs for third-party access.
- CUCM outputs a variety of management parameters through a published interface to provide information to approved management applications, such as NetIQ Vivinet Manager, HP OpenView, and Integrated Research PROGNOSIS.

- The appliance operates with or without keyboard, mouse, and monitor (also known as headed or headless, respectively). Third-party access is allowed through documented APIs only.
- CUCM supports clustering of servers to provide high availability and scalability. Database redundancy is provided by sharing a common database replicated across the CUCM servers. Call-processing redundancy is achieved through the CallManager Group setting, in which multiple servers are assigned to a device for the purposes of providing call-signaling fault tolerance.

A CUCM cluster can have up to 20 servers in it. The cluster consists of one publisher server, which maintains the read/write copy of the CUCM's database. The publisher replicates the database as a read-only database to up to eight subscriber servers in the CUCM cluster. Each cluster has a restriction of four subscriber servers that can perform active call processing. Additional subscriber servers are dedicated standby servers in case the active subscriber server is not available. The additional 11 servers in the cluster are responsible for various services, including TFTP and media resources (conferencing, music on hold, transcoding) and integration with third-party applications through APIs.

CUCM Cluster

Clustering allows the network to scale to several thousands of endpoints, provides redundancy in case of network or server failure, and provides a central point of administration. Figure 1-5 displays a publisher database synchronizing the database to all the other servers in the cluster. The servers running the CCM.exe process are performing call processing, and the other servers are responsible for specialized roles described in later chapters of this book. CUCM clustering allows call signaling to be distributed among multiple servers, increasing the scalability and performance of the product.

Cisco IP Phone configuration settings are stored in the IBM IDS database. The database is the repository for all CUCM configuration information (devices, service parameters, features, device configurations, and dial plan).

The database replicates the configuration information in a hub-and-spoke topology (one publisher, up to eight subscribers). CUCM nodes also use a second communication method to replicate some runtime data (call forwarding, message waiting indicators, hunt login status) using a master-master replication technology referred to as user-facing features (UFF). UFF provides a full-mesh replication topology allowing dynamic registration of active call information that changes much more frequently than the database changes.

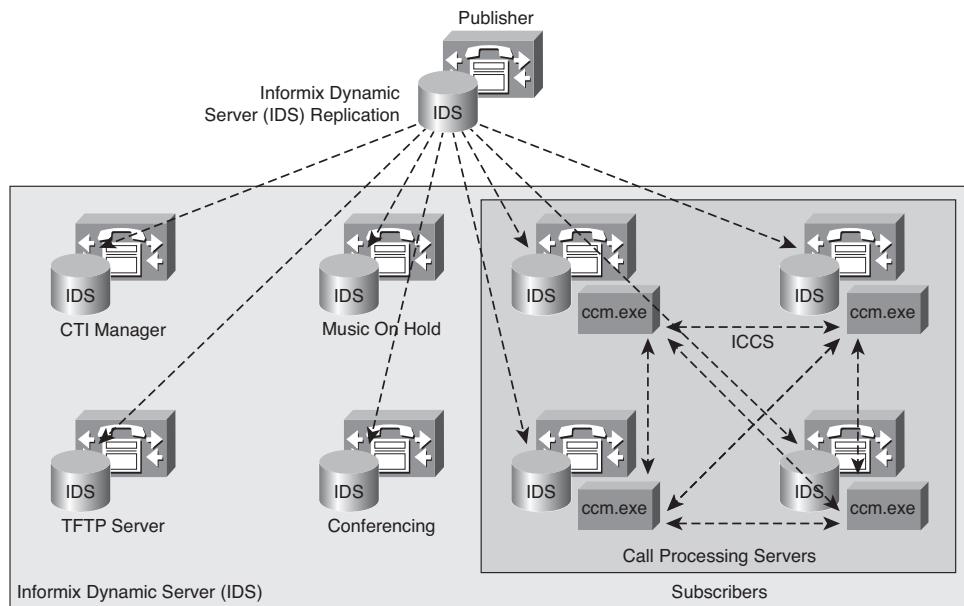


Figure 1-5 CUCM Cluster

Cisco 7800 Series Media Convergence Servers

Although it is possible for CUCM to run on most computers, Cisco only supports CUCM on Cisco-approved hardware that it can support. The minimum hardware requirements for CUCM Release 8.0 are as follows:

- 2-GHz processor
- 2 GB RAM
- 72-GB hard disk

Minimum requirements for CUCM 8 are the same as for CUCM versions 5, 6, and 7. All of these CUCM versions run on the same hardened Linux appliance operating system.

The servers that Cisco sells are manufactured by Cisco (UCS) or IBM. HP servers are supported at the time of this writing, but Cisco no longer resells HP servers. The Cisco 7825 server is a 19- or 23-inch, rack-mountable server that provides a redundant SATA hard drive, but only one power supply. The 7835 server improves reliability and performance by including hot-swappable SCSI hard drives, hardware RAID, and redundant power supplies. The 7845 improves reliability and performance by providing a second CPU and a backup fan assembly.

You can find the most detailed, current Cisco hardware specifications at www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure0900aecd8062a4f9.htm.

Virtualization of CUCM is supported using the VMware vSphere 4 hypervisor beginning with CUCM 8.0. You can find additional information at the following sites:

- **Cisco-approved IBM server solutions:** www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/product_overview09186a0080107d79.html.
- **Cisco-approved HP server solutions:** www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure09186a0080107d79.html.
- **VMware vSphere 4 (ESXi 4.0):** In CUCM versions 7.1(3) and 8.0, Cisco officially supports VMware installations on VMware ESXi 4.0. CUCM can be installed on any other VMware platform for a lab environment (workstation, server, player), but will not be supported for production use.

CUCM Operating System

The operating system that the CUCM application resides on is Red Hat Linux Enterprise. Operating system and application updates are provided by, and digitally signed by, Cisco Systems.

Root access to the file system has been locked down, making it impossible to load any application software on the server other than that authorized and produced by Cisco Systems. Cisco has hardened the underlying Red Hat Linux operating system by disabling all unnecessary accounts and services.

Remote-access support has been integrated into the CUCM Serviceability GUI. Remote access allows Cisco Technical Assistance Center (TAC) engineers to remotely access the CUCM server for a 24-hour time interval with the temporary password generated when remote access is temporary enabled.

The IBM Informix Database Server (IDS) is the database for all Cisco UC applications that use the same hardened Linux operating system. Cisco Unity is the only Cisco UC server that does not support the same hardened Linux appliance model with the IBM IDS. Cisco Unity Connection uses the same model, but Cisco Unity requires Windows 2003 Server with Microsoft Exchange and a Microsoft SQL server database. The IDS database installation and configuration are scripted into the CUCM installation DVDs. No UNIX or IBM IDS database knowledge is required to configure and operate CUCM. More than 90 percent of the product administration takes place in the intuitive CUCM Administration web pages.

Cisco Secure Agent (CSA) is included with the appliance to provide protection against known and unknown attacks. Cisco Secure Agent is a host-based intrusion prevention system (HIPS).

A DHCP server has also been integrated into CUCM to provide IP telephony devices with their IP addressing requirements if required. The DHCP server integrated with

CUCM is in no way meant to replace an enterprise-class DHCP deployment. The CUCM DHCP server component is not recommended for installations of more than 1000 phones.

Cisco UC Database

The data in the CUCM database is divided into two types, which are described in the following sections.

Static Configuration Data

Static configuration data is created as part of the configuration of the CUCM cluster. Read/write access to this data is provided in the publisher server only. Subscriber servers have a local read-only copy of the database that is replicated downstream from the publisher. If the publisher becomes unavailable, the subscriber server's replicated data can be used to process calls locally. Database replication is unidirectional, from the publisher to the subscribers. Only call detail records (CDR) and call management records (CMR) are replicated from the subscriber servers to the publisher. All other configuration information is downloaded from the publisher. CDRs contain call detail fields such as calling party, called party, start time, stop time, call duration, and charge-back (if applicable). The CDRs provided by CUCM are standard for a phone switch/PBX. CMRs provide QoS details regarding the number of packets transmitted and received, maximum jitter, average jitter, mean opinion score (MoS) rating of the call, and so on. CMRs are useful for troubleshooting QoS issues (packet loss, delay, and jitter) that could affect voice quality.

User-Facing Features

The publisher is the only server in the CUCM cluster with a read/write copy of the database, and all configuration changes should be made on the publisher. The publisher then replicates these changes to the read-only subscriber databases. Call-processing redundancy can be provided by subscriber servers, but the single-publisher model represents a single point of failure from the perspective of providing moves, adds, and changes (MAC). The publisher was also the only server in the cluster responsible for call forwarding, extension mobility login, and message-waiting indicator changes in versions of CUCM before CUCM 6.0.

CUCM treats a small portion of the database as dynamic configuration data. Read/write access to dynamic configuration data is provided on all servers, allowing certain information to be modified if the publisher server is unavailable. The dynamic information that can be changed during a publisher outage is referred to as user-facing features (UFF). UFF data is replicated between all servers in the cluster.

Examples of UFFs include the following:

- Call Forward All (CFA)
- Message Waiting Indication (MWI)
- Privacy, Enable/Disable
- Do Not Disturb, Enable/Disable (DND)
- Extension Mobility Login (EM)
- Hunt Group Login Status
- Monitor (future use)
- Device Mobility
- CTI CAPF (Computer Telephony Integration, Certificate Authority Proxy Function) Status

The services listed in Table 1-1 rely on the availability of the publisher server regardless of the version of CUCM used.

Table 1-1 Publisher Server Required Services

Component	Function	When
CCAdmin	Provisions everything	Always
CCUser	Provisions user settings	Always
BAT	Provisions everything initiated by the Bulk Administration Tool	Always
TAPS	Provisions everything initiated by the tool for Auto-Registered Phone Support	Always
AXL	Provisions everything initiated by the AVVID XML Layer service	Always
AXIS-SOAP	Enables and disables services through SOAP	Sometimes
CCM	Inserts phones (auto-registration only)	Administration only
LDAP Sync	Updates end-user information	Always (Local)
License Audit	Updates license tables	Always (Local)

Database Access Control

Database access is secured using the embedded Red Hat Linux, iptables dynamic firewall, and a database security password.

The procedure to allow new subscribers to access the database on the publisher is as follows:

- Step 1.** Add the subscriber to the publisher database using the CUCM Operating System Administration.
- Step 2.** During installation of the subscriber, enter the same database security password that was entered during the installation of the publisher.

After this configuration, the following process occurs to replicate the database from the publisher to the newly added subscriber:

1. The subscriber attempts to establish a connection to the publisher database using the database management channel.
2. The publisher verifies the subscriber's authenticity and adds the subscriber's IP address to its dynamic firewall (iptables).
3. The subscriber is allowed to access the publisher database.
4. The database content is replicated from the publisher to the subscriber.

Figure 1-6 illustrates the iptables firewall allowing subscriber access to the publisher database.

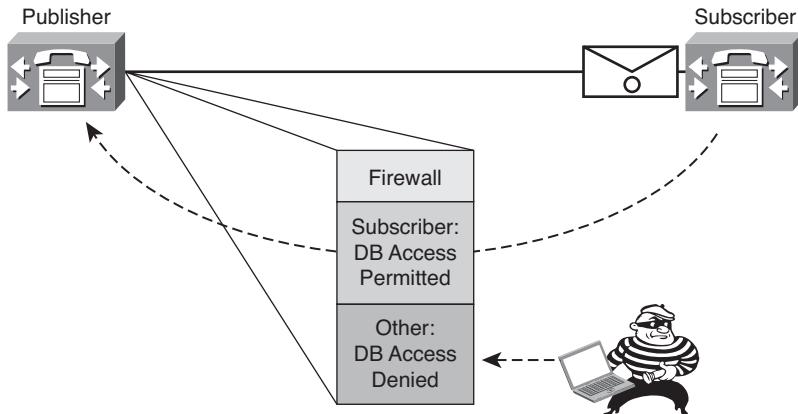


Figure 1-6 Database Access Control

Note CUCM 8.0 TCP and UDP port usage information is available at www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/8_0_1/portlist801.html.

CUCM Licensing

Licensing is implemented in Cisco Unified Communications Manager Administration to track the number of devices that are registered to CUCM, including third-party SIP phones, and to compare that number with the number of device license units (DLU) that have been purchased. License enforcement occurs at the time of phone provisioning and Cisco Unified Communications Manager service activation.

The publisher is the only licensing server. The licensing server is the logical component that keeps track of the licenses purchased and the licenses used. If the publisher fails, new phones cannot register, and no configuration changes will be allowed. Existing phones will continue to operate during a publisher outage.

CUCM tracks the license compliance for devices, applications, and software as follows:

- **Device license units (DLU):**
 - The maximum number of provisioned devices in the CUCM database will be tracked and enforced.
 - Route points and CTI ports are not enforced.
 - The device license units are also called phone licenses.
- **Application licenses:**
 - CUCM software is bound to the MAC address of the publisher.
 - If CUCM is installed on a VMware ESXi server, the license is not tied to the MAC address of the publisher. Instead, a hash of various system settings, such as Time Zone, IP Address, and Certificate Information, is used for the license file.
 - Application licenses are required for every CUCM server. These application licenses are referred to as node licenses.
- **Software licenses:** Software licenses are tied to the major version of the software. Software licenses are required for upgrades from one major version to another. An application license would be required to do a major version upgrade (for example, CUCM 7.1(2) to CUCM 8.0). An application license would not be required for a minor version upgrade (for example, CUCM 8.0 to CUCM 8.5). Licenses are created and distributed in accordance with the Cisco FlexLM process. Cisco product license registration occurs at www.cisco.com/go/license after receiving the Product Authorization Key (PAK).

Note A demo license of 150 DLUs and three call-processing servers is included with the installation of CUCM. The demo license is overwritten when a purchased license is loaded into CUCM.

These two types of product IDs are available:

- **Cisco device license units:** Cisco DLUs are for Cisco devices only.
- **Third-party device license units:** Third-party DLUs can be converted to Cisco units, but not vice versa.

CUCM tracks the number of units required by each device, as shown in Figure 1-7. Each device type requires a fixed number of units. The number of DLUs consumed per device depends on the device type and capabilities of the phone.

Phone License Feature	
Type of Licensed Device	Units Consumed per Device
Analog Phone	0
CTI Port	0
Cisco 12 S	2
Cisco 12 SP	2
Cisco 12 SP+	2
Cisco 30 SP+	2
Cisco 30 VIP	2
Cisco 3951	3
Cisco 7902	1
Cisco 7905	2
Cisco 7906	2
Cisco 7910	2
Cisco 7911	3
Cisco 7912	3
Cisco 7920	4
Cisco 7921	4
Cisco 7931	4
Cisco 7935	3
Cisco 7936	3
Done	

Figure 1-7 Device License Units

The number of units required per device can be viewed from CUCM Administration. DLUs are perpetual and device independent. Figure 1-7 displays the number of DLUs consumed in CUCM 8.0 by some of the phones that Cisco offers.

A new license file will not overwrite an existing license file. The new license file will add DLUs to the number of DLUs in the existing license file. If a 100-DLU license was purchased and uploaded to a server that already included 100 DLUs, the result would be 200 DLUs. CUCM uses additive licensing, while some products' license files replace existing license files. The Cisco FlexLM process is used to obtain licenses. The integrity of the license files is assured by a Cisco manufacturing digital signature.

Example 1-1 shows a sample license file.

Example 1-1 Example License File

```
INCREMENT PHONE_UNIT cisco 8.0 permanent uncounted \
VENDOR_STRING=<Count><Anchor1>1000</Count><OrigMacId><Anchor2>000BCD4EE59D</OrigMacId>
<LicFileVersion>1.0</L icFileVersion> \
HOSTID=000bcd4ee59d NOTICE=<LicFileID>20050826140539162</LicFileID><LicLineID>2
</LicLineID> \
<PAK></PAK>" SIGN="112D 17E4 A755 5EDC F616 0F2B B820 AA9C \
0313 A36F B317 F359 1E08 5E15 E524 1915 66EA BC9F A82B CBC8 \
4CAF 2930 017F D594 3E44 EBA3 04CD 01BF 38BA BF1B"
```

Significant fields are highlighted and described as follows:

- INCREMENT PHONE_UNIT Cisco 8.0 indicates a phone unit license file for Cisco Unified CM 8.0. There is no expiration date for this license, as indicated by the keyword “permanent.”

Note The INCREMENT type for CUCM node licenses is CCM_NODE cisco 8.0 permanent uncounted. The INCREMENT for software licenses is SW_FEATURE cisco 8.0 permanent uncounted.

- This license file includes 1000 license units.
- The MAC address of the license server is 000BCD4EE59D.

License File Request Process

Figure 1-8 displays the license file request process, which includes these steps:

1. The customer places an order for CUCM.
2. The manufacturing database scans the PAK and records it against the sales order.
3. The product (CD or paper claim certificate) is physically delivered to the customer.

4. The customer registers the product at www.cisco.com/go/license or a public web page and provides the MAC address of the publisher device that will become the license server.
5. The license fulfillment infrastructure validates the PAK, and the license key generator creates a license file.
6. The license file is delivered through email to the customer. The email also contains instructions on how to install the license file.
7. The customer installs the license file on the license server (publisher).

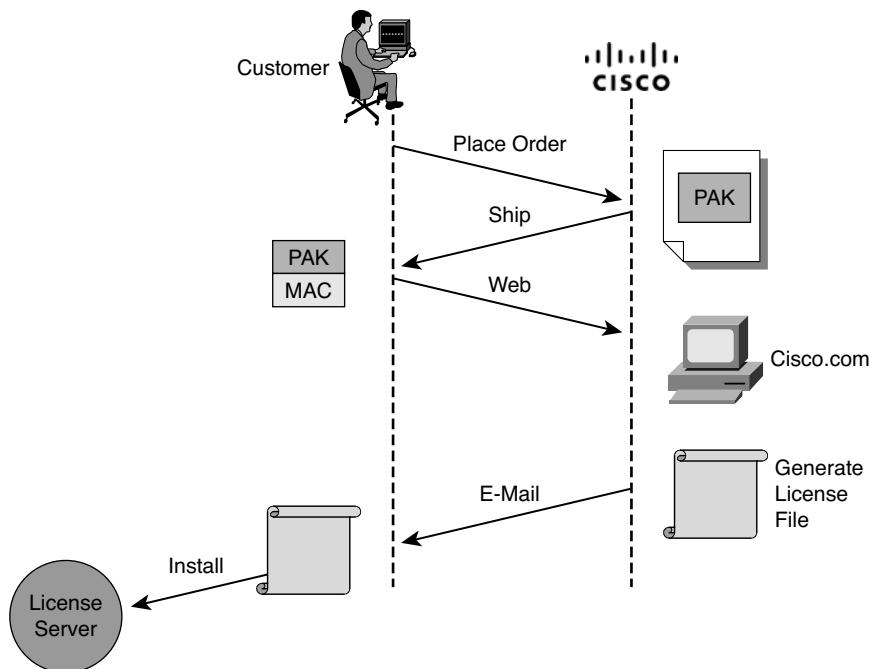


Figure 1-8 License File Request Process

Obtaining Additional Licenses

The process of obtaining additional DLUs and node licenses is as follows:

1. The customer places an order for the additional licenses for a license server (publisher MAC address has to be specified).
2. When the order is received, Cisco.com generates a license file with the additional count and sends it to the customer.
3. The new license file has to be uploaded to the license server and will be cumulative.

Consider this example: A CUCM server has an existing license file that contains 100 DLUs. Another 100 DLUs are purchased. The second license file that is generated will contain only 100 DLUs. When the new license file with 100 DLUs is uploaded to CUCM, the 100 DLUs from the first license file are added to the devices of the second license file, resulting in a total of 200 DLUs.

Licensing Components

The key licensing components of CUCM licensing are the license server and the license manager.

The *license server* service runs on the publisher in the CUCM cluster and is responsible for keeping track of the licenses purchased and consumed. The MAC address of the publisher is required to generate a license file.

The *license manager* acts as a broker between CUCM applications that use licensing information and the license server. The license manager receives requests from the CUCM applications and forwards the requests to the license server. The license manager then responds to the application after the request has been processed by the license server. The license manager acts a licensing proxy server.

An administration subsystem and alarm subsystem complete the functional diagram. Details of these two subsystems are as follows:

- The administration subsystem provides the following capabilities:
 - Keeps information about the license units required for each phone type. The customer can view this information using a GUI.
 - Supports a GUI tool that calculates the required number of phone unit licenses. The customer inputs the number of phones of each phone type that the customer wants to purchase. The output is the total number of licenses that the customer needs for the given configuration.
 - Supports a GUI tool that displays the total license capacity and the number of licenses in use and license file details. The tool can also report the number of available licenses.
- The alarm subsystem generates alarms that are routed to event logs or sent to a management station as Simple Network Management Protocol (SNMP) traps to notify the administrator of the following conditions:
 - **Overdraft:** Occurs when an overdraft condition exists. An overdraft condition occurs when more licenses are used than available but the amount of exceeding licenses is within an acceptable range. (5 percent overdraft is permitted.)
 - **License server down:** Occurs when the license manager cannot reach the license server.

- **Insufficient licenses:** Occurs when the license server detects the fact that there are not sufficient licenses to fulfill the request and raises an alarm to notify the administrator.

Issues with the license file occur when there is a version mismatch between the license file and the CUCM (license file version mismatch alarm), or when the number of licenses in the license file is less than the number of phones provisioned (license file insufficient licenses alarm). Another cause of this condition is an invalid MAC address (for example, after a network interface card [NIC] change).

Figure 1-9 is a functional diagram that steps through the process of a license request, as described here:

1. A request for a certain number of DLU^s is made by the admin subsystem because of an event (for example, phone registration).
2. The License Manager service on a CUCM subscriber forwards the request to the publisher server running the License Server service.
3. The License Server service receives the license request event and allocates the required number of DLU^s required based on the type of device. If not enough license units are available to accommodate the request, a deny message is sent back to the license manager on the subscriber server. If resources are available, the license server grants the request and sends a grant message to the license manager on the subscriber server.
4. The License Manager service on the subscriber server receives the license grant or deny message. If the license request was granted, the subscriber allows the phone to register.
5. If the license request was denied, the subscriber server generates an alarm in the alarm subsystem. The deny message will be available in the CUCM syslog server by default.

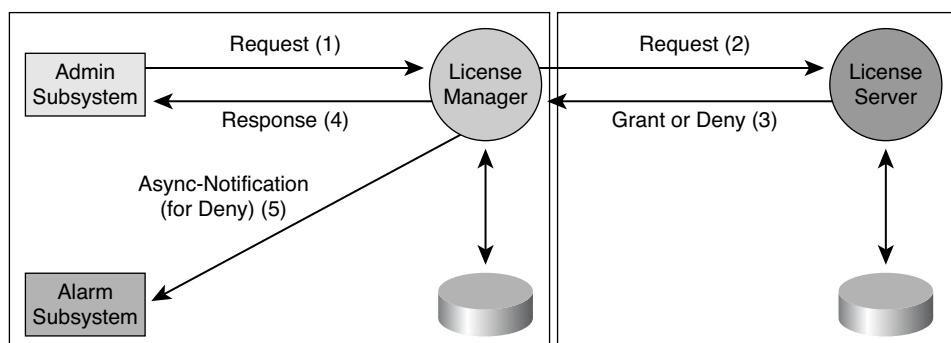


Figure 1-9 Licensing Functional Diagram

Calculating License Units

To calculate the number of phone licenses required, follow these steps:

- Step 1.** Choose System > License > License Unit Calculator. The License Unit Calculator window displays. The number of license units consumed per device and the current number of devices display, as shown in Figure 1-10.

The screenshot shows two tables side-by-side. The top table is titled 'CCM Node License Feature' and lists a single row for 'CCM Node' with values: Type of Licensed Device (CCM Node), Units Consumed per Device (1), Current Number of Devices (1), Number of Units Consumed (1), and Number of Devices (0). Below this table is a summary row: Total CCM Node License Units Used: 1 and Total CCM Node License Units Needed: 0. The bottom table is titled 'Phone License Feature' and lists several rows of phone types with their respective consumption values. All entries in the 'Number of Devices' column are 0.

CCM Node License Feature					
Type of Licensed Device	Units Consumed per Device	Current Number of Devices	Number of Units Consumed	Number of Devices	
CCM Node	1	1	1	0	0
Total CCM Node License Units Used: 1				Total CCM Node License Units Needed: 0	

Phone License Feature					
Type of Licensed Device	Units Consumed per Device	Current Number of Devices	Number of Units Consumed	Number of Devices	
Analog Phone	0	0	0	0	0
CTI Port	0	1	0	0	0
Cisco 12 S	2	0	0	0	0
Cisco 12 SP	2	0	0	0	0
Cisco 12 SP+	2	0	0	0	0
Cisco 30 SP+	2	0	0	0	0
Cisco 30 VIP	2	0	0	0	0

Figure 1-10 License Unit Calculator

- Step 2.** In the Number of Devices column, enter the desired number of devices, corresponding to each node or phone.
- Step 3.** Click Calculate. The total number of CUCM node license units and DLUs required for specified configuration displays.

License Unit Reporting

License unit reports can be run to verify the number of licenses consumed and available for future expansion. Use the following procedure to generate a license unit report:

- Step 1.** Choose System > License > License Unit Report.
- Step 2.** The License Unit Report window displays, as shown in Figure 1-11. This window displays the number of phone licenses and number of node licenses, in these categories:
- Units Authorized
 - Units Used
 - Units Remaining

License files (CCMxxxxx.lic) are uploaded to the publisher (license server). To upload a license file to the publisher server, follow these steps:

- Step 1.** Ensure that the license file is downloaded to a local PC.
- Step 2.** From the PC and using a supported browser, log in to CUCM Administration.

License Unit Report			
License Unit Distribution			
Phone License Feature			
License Server	Units Authorized	Units Used	Units Remaining
cucm	50	13	37
Total Units for Feature	50	13	37
CCM Node License Feature			
License Server	Units Authorized	Units Used	Units Remaining
cucm	1	1	0
Total Units for Feature	1	1	0
Software License Version			
License Server	SW Version		
cucm	6.0		

Figure 1-11 License Unit Report

- Step 3.** Choose System > License > License File Upload, as shown in Figure 1-12. The License File Upload window displays.



Figure 1-12 License File Upload Procedure

- Step 4.** In the window shown in Figure 1-13, click Upload License File.
- Step 5.** Click Browse to choose the license file from the local directory.
- Step 6.** Click Upload.
- Step 7.** After the upload process completes, click the Continue prompt when it appears. The contents of the newly uploaded license file displays.

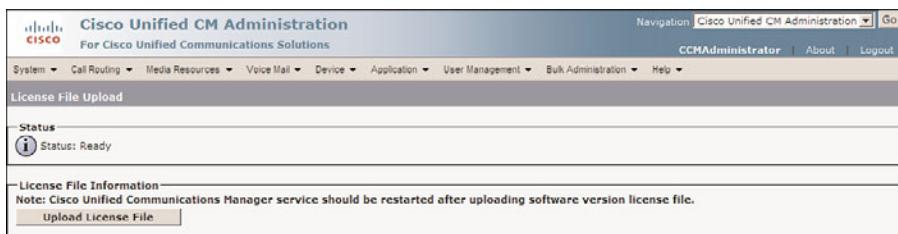


Figure 1-13 License File Upload Procedure (Continued)

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- Cisco Unified Communications (UC) is a community of components designed to enable rapid, efficient communications. UC components include the following:
 - Endpoints
 - Application integration
 - Call control
 - Infrastructure
- Cisco Unified Communications Manager (CUCM) is the call-routing component of the Cisco UC ecosystem, providing call setup and teardown services to both voice and video communications. CUCM provides a centralized command and control topology to configuration management while leveraging the distributed nature of IP communications.
- CUCM is a software solution that is supported on various hardware configurations. Media Convergence Servers (MCS) and Unified Computing Systems (UCS) are Cisco-branded hardware solutions that run on HP or IBM server platforms.
- CUCM versions 5.0 and later use an appliance model, where most administration is performed over a web browser pointed to the web services running on CUCM. The hardened operating system is based on the Red Hat Linux variant. There is no access to the Linux kernel, and this lack of access provides a high level of security to the Cisco UC platform. CUCM versions before 5.0 (4.x and earlier) used a Microsoft Windows-based operating system.
- CUCM versions 5.0 and later leverage the IBM Informix Database Server (IDS) to store all configuration data, including the LDAPv3 user database. Versions before 5.0 used a Microsoft SQL server database for configuration information, while user information was stored in the LDAPv3-compliant DC Directory server.
- CUCM licensing consists of the license server and the license manager. The license server component runs on the publisher server, whereas the license manager runs on every server.

- Three types of licenses are required: devices, applications and software. License files are uploaded using Cisco Unified Communications Manager Administration GUI.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. Which layer of the Cisco Unified Communications components is responsible for delivering a dial tone?
 - a. Endpoints
 - b. Applications
 - c. Call control
 - d. Infrastructure
2. What is the name of the server in a CUCM cluster that maintains a read/write copy of the entire database?
 - a. Member server
 - b. Domain controller
 - c. Subscriber
 - d. Publisher
3. What protocol is responsible for transporting VoIP?
 - a. Skinny Client Control Protocol (SCCP)
 - b. H.323
 - c. Real-Time Transport Protocol (RTP)
 - d. Real-Time Transport Control Protocol (RTCP)
 - e. Media Gateway Control Protocol (MGCP)
 - f. Skinny Gateway Control Protocol (SGCP)
4. How many call-processing agents can be active in a CUCM cluster?
 - a. 20
 - b. 4
 - c. 8
 - d. 9
 - e. 2

5. How many call-processing agents can be in a CUCM cluster?
 - a. 20
 - b. 4
 - c. 8
 - d. 9
 - e. 2
6. How many servers can be in a CUCM cluster?
 - a. 20
 - b. 4
 - c. 8
 - d. 9
 - e. 2
7. Which CUCM server is the license manager component active on?
 - a. Member server
 - b. Domain controller
 - c. Subscriber
 - d. Publisher
 - e. All servers
8. Which CUCM server is the license server component active on?
 - a. Member server
 - b. Domain controller
 - c. Subscriber
 - d. Publisher
 - e. All servers
9. On which server in the CUCM cluster are license files loaded?
 - a. Member server
 - b. Domain controller
 - c. Subscriber
 - d. Publisher
 - e. All servers

10. Which of the following features is *not* a user-facing feature (UFF)?

- a.** Call Forward All (CFA)
- b.** Message Waiting Indication (MWI)
- c.** Attendant Console (Login/Logout)
- d.** Privacy (Enable/Disable)
- e.** Do Not Disturb (Enable/Disable) (DND)
- f.** Extension Mobility (Login/Logout) (EM)
- g.** Hunt Group Login Status

This page intentionally left blank

Chapter 2

Deployment Models

A solid understanding of the redundancy options and the recommended design and deployment practices of Cisco Unified Communications (UC) can provide availability at equal or higher levels to a traditional voice network.

This chapter introduces the Cisco Unified Communications Manager (CUCM) deployment models that provide high availability for call processing. The different redundancy models explored in this chapter can be applied to the different deployment models to provide fault tolerance for CUCM.

Chapter Objectives

Upon completing this chapter, you will understand the CUCM deployment and redundancy options and be able to meet the following objectives:

- Identify the supported CUCM deployment options.
- Describe the characteristics of a CUCM single-site deployment, and identify the reasons for choosing this deployment option.
- Describe the characteristics of a CUCM multisite deployment with centralized call processing, and identify the reasons for choosing this deployment option.
- Describe the characteristics of a CUCM multisite deployment with distributed call processing, and identify the reasons for choosing this deployment option.
- Describe the characteristics of a CUCM multisite deployment with clustering over the WAN, and identify the reasons for choosing this deployment option.
- Explain how call-processing redundancy is provided in a CUCM cluster, and identify the requirements for different redundancy scenarios.

CUCM: Single-Site Deployment

As illustrated in Figure 2-1, the single-site model for CUCM consists of a CUCM cluster located at a single site, or metropolitan-area network (MAN), with no telephony services provided over a WAN. All CUCM servers, applications, and digital signal processor (DSP) resources are located in the same physical location or at multiple physical buildings connected with LAN-based connectivity. LANs are normally defined as having connectivity speeds of 1000 Mbps (1 Gbps) and above.

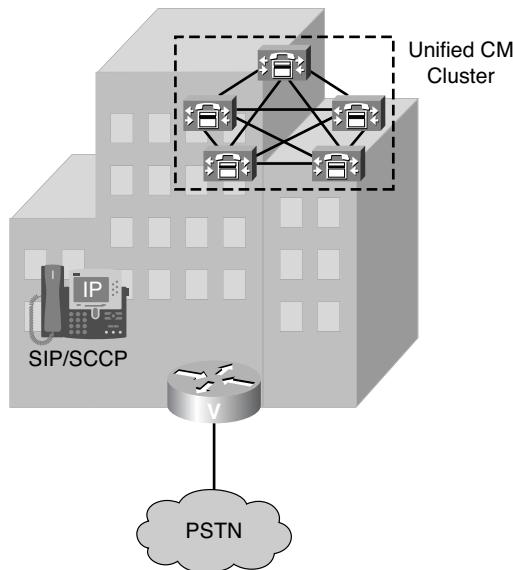


Figure 2-1 Single-Site Model

An enterprise would typically deploy the single-site model over a LAN or MAN, which is responsible for transporting the voice traffic. In this model, calls beyond the LAN or MAN use the public switched telephone network (PSTN). The PSTN is accessible by routing calls to a gateway. Gateways provide time-division multiplexing (TDM) interfaces including T1-CAS, T1-PRI, FXO, FXS, and E&M.

In a single-site deployment model, all CUCM servers, applications, and DSP resources are located in the same physical location.

The single-site model has the following design characteristics:

- 30,000 Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP) endpoints supported per cluster. The actual number of possible phone registrations will vary based on various criteria that Cisco presales or a Cisco partner will provide.
- A maximum of 2100 H.323 devices (gateways, multipoint conference units [MCU], trunks, and clients) or 1100 Media Gateway Control Protocol (MGCP) gateways per CUCM cluster.

Follow these guidelines and best practices when implementing the single-site model:

- Provide a highly available, fault-tolerant infrastructure based on a common infrastructure philosophy. A solid network infrastructure providing QoS is essential to guarantee call quality.
- Know the calling patterns for your enterprise. Use the single-site model if most of the calls from your enterprise are within the same site or to PSTN users outside your enterprise.
- Use high-quality G.711 or G.722 audio codecs for all endpoints. This practice eliminates the consumption of DSP resources for transcoding. Those resources can be allocated to other functions such as conferencing and Media Termination Points (MTP). The G.722 audio codec has higher audio fidelity than G.711, but it is not supported on older, Cisco Type A Phone architectures (for example, 7910, 7905, 7911, 7940, and 7960 model phones).
- Use MGCP gateways for the PSTN if you do not require H.323 functionality. This practice simplifies the dial plan configuration. H.323 might be required to support specific functionality such as support for nonfacility-associated signaling (NFAS) or caller identification (CLID) on FXO analog gateways, or VXML/TCL call applications. CLID is supported on all T1-based MGCP gateways. MGCP does not have the same level of call survivability or reliability as H.323 gateways, but H.323 gateways are out of the scope of this book. The Cisco Press CVOICE book is recommended to learn the proper Cisco IOS configuration required for H.323 and SIP gateways. MGCP gateways are the easiest gateways to provision because they do not require any Cisco IOS knowledge. MGCP gateways are managed and maintained in one centralized location (CUCM database), while H.323 and SIP gateways must each include a Cisco IOS-based dial plan configuration.

Multisite WAN with Centralized Call Processing

The Multisite WAN with Centralized Call Processing model consists of a centralized CUCM cluster that provides services for many sites and uses the IP WAN to transport IP telephony call control (SCCP/SIP/H.323/MGCP) and media (RTP) traffic between sites.

Figure 2-2 illustrates a centralized call-processing deployment, where a CUCM cluster is located at the central site and a QoS-enabled IP WAN connects all the sites. The remote sites rely on the centralized CUCM cluster to handle all call processing, but RTP media paths between phones at each site are connected by the local network infrastructure. Applications (voicemail, interactive voice response (IVR) systems, and so on) are typically centralized to reduce the overall costs of administration and maintenance of technology equipment at branch locations without Information Technology (IT) staff.

The Cisco Unified Survivable Remote Site Telephony (SRST) feature available in Cisco IOS gateways provides call-processing services to remote IP phones during a WAN outage or other type of CUCM unavailability. When connectivity between the IP phones at the remote branch office and CUCM is lost, branch phones will reregister to the local

SRST router. The SRST router processes calls between registered IP phones and can send calls to other sites through the PSTN. SRST has a rich feature set that is very close to the number of features supported by CUCM, but features like Cisco Unified Management Assistant (CUMA) will not work.

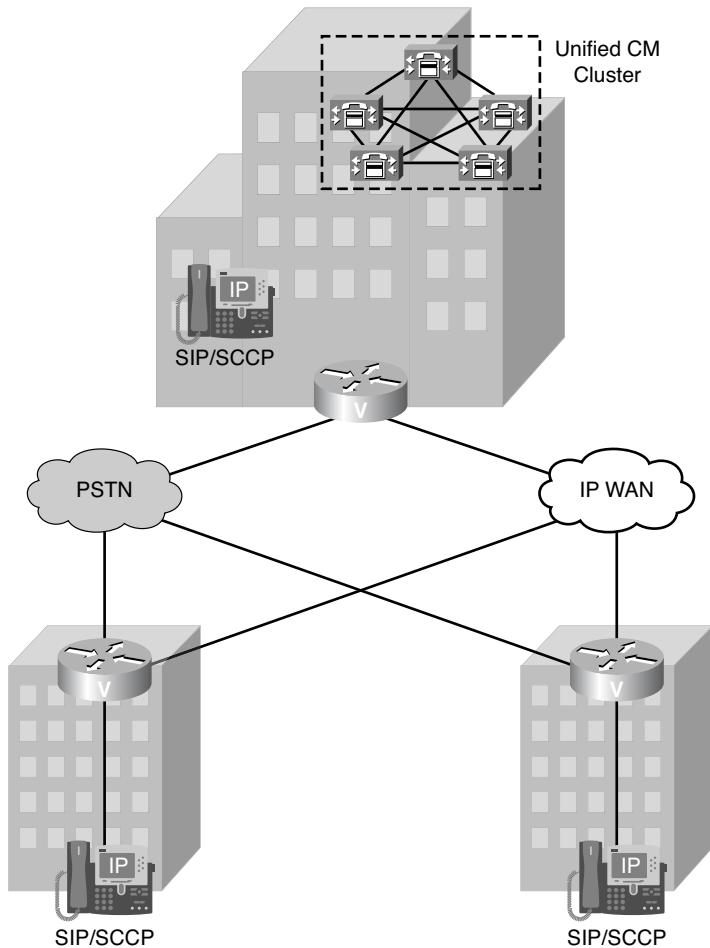


Figure 2-2 Multisite WAN with Centralized Call Processing

Remote sites using MGCP gateways will drop all active PSTN calls as soon as connectivity to CUCM is lost. MGCP gateways rely on connectivity to a call agent (CUCM) to process calls. This gateway limitation can be avoided by using H.323 as a gateway protocol with a Cisco IOS release later than 12.4(9T). Call preservation must be configured on an H.323 gateway to provide this resiliency level.

Deterioration of phone call quality can occur when WAN links are oversubscribed. The quality of service priority queue (PQ) mechanism is implemented to guarantee call

quality over the WAN. If the number of calls routed through the QoS priority queue exceeds the capacity of the priority queue, packet loss will ensue. To limit the number of calls between the sites, use call admission control (CAC) in CUCM locations. IP-based phone systems do not have any bandwidth management mechanisms turned on by default. CAC artificially limits the number of phone calls that can be routed over the WAN by providing a static configuration that is mapped to devices at the particular site. Call admission control is covered in detail in the Cisco Press book *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide*.

Centralized call processing models can take advantage of automated alternate routing (AAR) features. AAR allows CUCM to dynamically reroute a call over the PSTN if the call is denied because of limited bandwidth (call admission control). AAR rerouting normally requires digit manipulation because OnNet intersite dialing is normally performed with an abbreviated dial plan, while the PSTN is going to require more digits based on the provider network and the location of the sites.

When implementing the multisite WAN model with centralized call processing, consider the following guidelines:

- A maximum of 2000 locations per CUCM cluster.
- A maximum of 2100 H.323 devices (gateways, MCUs, trunks, and clients) or 1100 MGCP gateways per CUCM cluster.
- The delay between CUCM and remote locations should be minimized with quality of service (QoS) to reduce voice cut-through delays.
- The Locations mechanism in CUCM is used to provide CAC over the WAN. The locations can support a maximum of 30,000 IP phones per cluster. Resource Reservation Protocol (RSVP) is a topology-aware CAC mechanism that can be used over the WAN. RSVP is a very CPU intensive protocol that I personally do not recommend based on the amount of CPU overhead it incurs.
- CUCM does not limit the number of devices that can be deployed at a remote branch, but best practice mandates deploying a number of phones equal to the capability provided by the branch router running SRST. SRST provides remote branches with a maximum of 1200 Cisco IP Phones during a WAN outage or failover to SRST when using a Cisco 3945 Integrated Services Router. The number of phones and lines (directory numbers) that are supported by each router is based on the size of the Cisco router hardware. The SRST Administration Guide goes over the number of phones and directory numbers supported by each router model.
- Digital signal processor (DSP) resources required for hardware conference bridges, transcoders, and Media Termination Points (MTP) can be centralized or distributed in this model. DSPs will be covered in more detail in Chapter 13, “Media Resources.”
- A minimum of 768-kbps WAN link speeds. Video is *not* recommended on WAN connections that operate at speeds below 768 kbps.

Multisite WAN with centralized call processing can save operational expenditures on PSTN costs. Instead of routing intersite calls as long distance or costly international PSTN calls, CUCM will route these calls over the IP WAN. IP WAN can also be used to bypass toll charges by routing calls through remote-site gateways, closer to the PSTN number dialed. This practice is known as tail-end hop-off (TEHO) or least cost routing (LCR). TEHO is not legal in some countries (for example, Mexico, China, Dubai, and so on). You will need to check with the local provider in each country to determine the legal issues surrounding TEHO.

This deployment model maximizes the utilization of available bandwidth by combining real-time communications (voice and video) with data traffic over the IP WAN.

The Extension Mobility feature allows roaming users to log in to a phone and have their phone configuration downloaded to the phone. The phone configuration includes the user's directory number, class of service, speed dials, and IP phone services. The Extension Mobility feature is covered in detail in *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide*.

When using the Multisite WAN with Centralized Call Processing deployment model, CUCM administration is centralized and easier to administer than a multisite solution with distributed call processing, where there are multiple CUCM databases to manage.

Multisite Deployment with Distributed Call Processing

Figure 2-3 illustrates a multisite WAN deployment with distributed call processing, where each site has its own CUCM cluster. Each site needs a call-routing and trunk configuration to route intersite calls over the IP WAN. Distributed call processing and trunk configurations are covered in detail in *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide*.

CUCM, applications, and DSP resources will be located at each site in this model. The IP WAN carries signaling and media traffic for intersite calls. All call-signaling and media traffic within a site remains local to the site, while intersite call signaling will always traverse the IP WAN. Intersite voice media will normally traverse the IP WAN to save costs, but PSTN gateways can also be leveraged to transport voice media when the H.323 gatekeeper CAC mechanism rejects a call from traversing the IP WAN.

The Multisite WAN with Distributed Call Processing model has the following design characteristics:

- A maximum of 30,000 endpoints per cluster.
- A maximum of 1100 MGCP gateways or 2100 H.323 devices (gateways, MCUs, trunks, and clients) per CUCM cluster.
- A PSTN gateway is used for all external calls.
- DSP resources for conferencing, transcoding, and MTP.

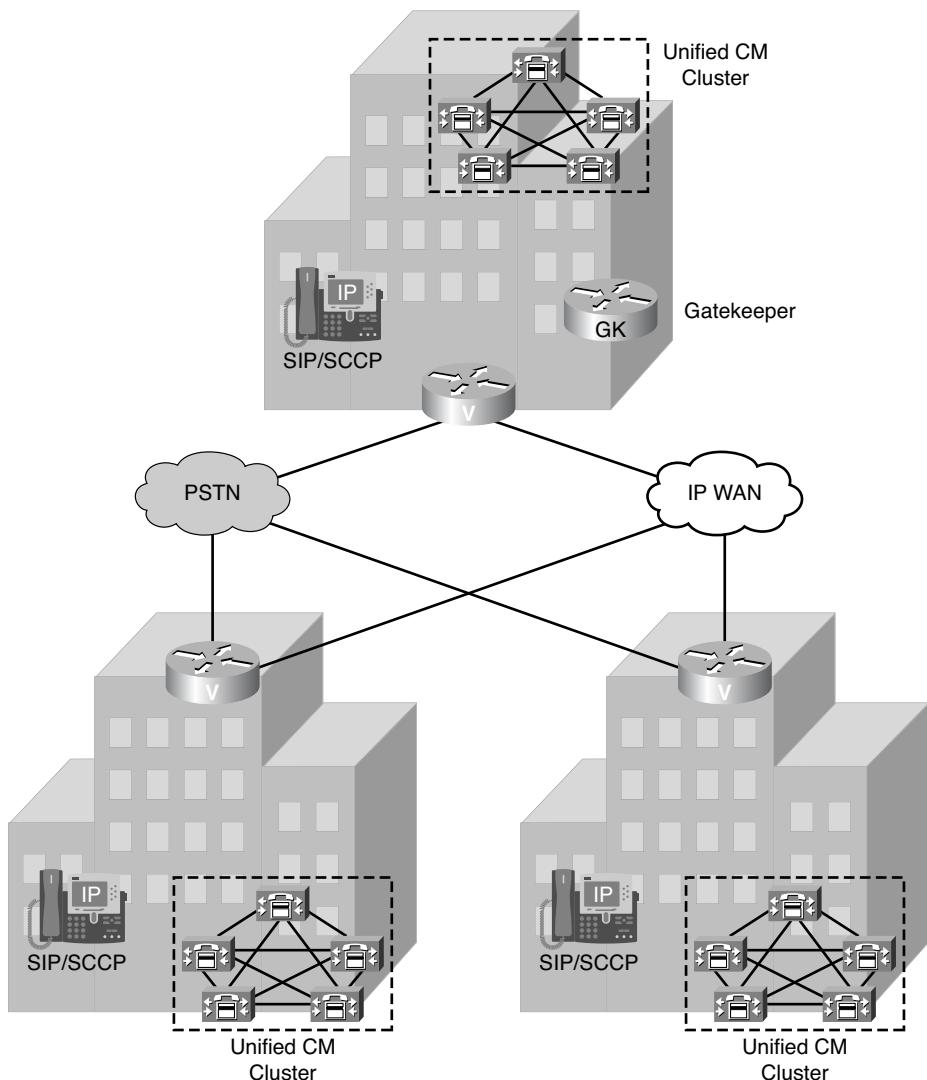


Figure 2-3 Multisite WAN with Distributed Call Processing

- Voicemail, unified messaging, and Cisco Unified Presence components.
- The capability to integrate with legacy PBX and voicemail systems.
- H.323 clients, MCUs, and H.323/H.320 gateways that require a gatekeeper to place calls must register with a Cisco IOS Gatekeeper. Cisco IOS Gatekeepers can also be used to provide intersite call-routing and bandwidth management between CUCM clusters. Multiple Cisco IOS Gatekeepers configured in a gatekeeper clustering configuration can be used to provide redundancy.

- Multipoint conference unit (CUVC 3500 MCU) resources are required in each cluster for multipoint videoconferencing.
- H.323/H.320 video gateways are needed to communicate with H.320 videoconferencing devices on the public ISDN network. All gateways can be located at the regional sites, or they can be distributed to the remote sites of each cluster if local ISDN access is required.
- High-bandwidth audio (G.711 or G.722) should normally be used between devices in the same site where bandwidth usage is of little concern, but compressed audio codecs (G.729 or iLBC) should be used between devices in different sites where WAN bandwidth should be preserved.

Benefits

The Multisite WAN with Distributed Call Processing model provides the following benefits:

- PSTN call cost savings when using the IP WAN for calls between sites.
- Use of the IP WAN to bypass toll charges by routing calls through remote-site gateways, closer to the called party on the PSTN (TEHO).
- Maximum utilization of available bandwidth by allowing voice traffic to share the IP WAN with other types of traffic.
- No loss of functionality during IP WAN failure because there is a call-processing agent at each site.
- 100+ CUCM clusters connected through H.323 gatekeepers providing the intersite dial plan.

Best Practices

A multisite WAN deployment with distributed call processing has many of the same requirements as a single-site or a multisite WAN deployment with centralized call processing. Follow the best practices from these other models in addition to the ones listed here for the Distributed Call Processing model.

Among the key elements of this Multisite WAN model are the H.323 gatekeeper or SIP proxy servers. Both H.323 gatekeepers and SIP proxy servers (CUCM) provide dial plan resolution, while the gatekeeper also provides CAC. CAC can be provided over SIP trunks by mapping a location to the SIP trunk, thereby limiting the number of calls that can be routed over the SIP trunk.

Note Cisco uses the *gateway* terminology to indicate that a call that will be converted to TDM, while *trunk* indicates that a call that will be routed over the TCP/IP network. Traditional phone switches used the word *trunk* to indicate TDM resources.

The following best practices apply to the use of a gatekeeper:

- Use a Cisco IOS Gatekeeper for all intersite dial plan resolution.
- To provide high availability of the gatekeeper, use gatekeeper clustering. Gatekeeper clustering is an extension of the H.323v4 alternate gatekeeper (ALT-GK) functionality. Cisco gatekeeper clustering also includes the Cisco-proprietary Gatekeeper Update Protocol (GUP). GUP is responsible for maintaining CAC and CDR information in the unfortunate event that there was a WAN or gatekeeper failure.
- Use only one type of audio codec on the WAN to simplify the CAC configuration in the H.323 gatekeeper. The H.323 specification does not account for the bandwidth requirements of any packetization overhead. A G.729 audio call using Point-to-Point Protocol (PPP) or Frame Relay requires 26.4 kbps, but CUCM will only request 16 kbps in the RAS (registration, administration, and status) ARQ (admission request) message. H.323 gatekeepers are covered in detail in the Cisco Press CVOICE and GWGK books. Intercluster trunks are covered in more detail in *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide*.

Clustering over the IP WAN

Cisco supports CUCM clustered over the WAN. The publisher server is maintained at one site and the subscriber servers can be distributed among up to eight sites. Characteristics of this call-processing model include the following:

- Applications and CUCM of the same cluster distributed over the IP WAN.
- Media resource and feature sharing.
- Single point of administration.
- IP WAN carries intracluster server communication and signaling.
- Limited number of sites. Up to eight sites for remote failover across the IP WAN (one CUCM server per site).

The cluster design, as illustrated in Figure 2-4, is useful for customers who require high-availability configurations that maintain the same phone feature set functionality when WAN link connectivity is lost. This network design also allows remote offices to support more IP phones than SRST in the event that the connection to the primary CUCM is lost.

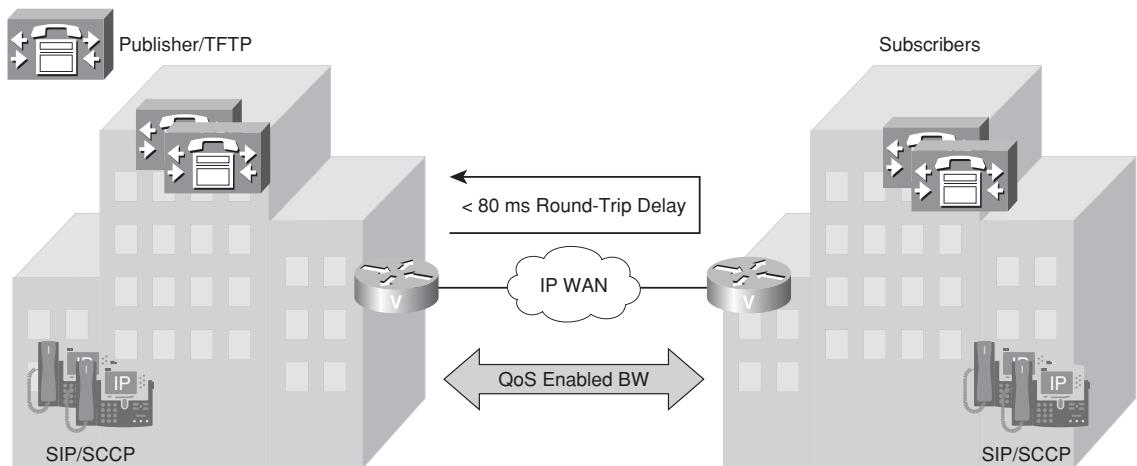


Figure 2-4 Clustering over the IP WAN

The design guidelines for clustering over the IP WAN are as follows:

- Database replication between CUCM servers in a cluster must have a maximum round-trip time (RTT) delay of 80 ms between them. Because of the strict 80-ms database replication requirement, this design should only be used between locations connected through higher-speed WAN links.
- Approximately 1 Mbps of QoS-enabled WAN bandwidth (intracluster runtime) should be dedicated to database replication over the WAN to accommodate this call-processing model. Additional bandwidth of 900 kbps per 10,000 busy-hour call attempts (BHCA) should be provided for higher-volume clusters. BHCA represents the number of call attempts made during the busiest hour of the day, on the busiest day of the year (the worst-case scenario).
- Up to eight sites are supported using the Remote Failover deployment model. Remote failover allows one server per location with a maximum of eight call-processing servers supported in a cluster. In the event of CUCM failure, IP phones register to another server over the WAN. SRST is not required in this deployment model. The remote failover design might require significant additional bandwidth, depending on the number of telephones at each location.

Note In earlier versions of CUCM, subscriber servers in the cluster used the publisher's database for read/write access, and they used their local database for read access only when the publisher's database could not be reached.

Starting with CUCM 6.x, subscriber servers in the cluster read their local database. Database modifications can occur in the local database (for special applications such as

user-facing features). IBM Informix Dynamic Server (IDS) database replication is used to synchronize the databases on the various servers in the cluster. Therefore, when recovering from failure conditions such as the loss of WAN connectivity for an extended period of time, the CUCM databases must be synchronized with any changes that might have been made during the outage. This process happens automatically when database connectivity is restored and can take longer over low-bandwidth links.

In rare scenarios, manual reset or repair of the database replication between servers in the cluster might be required. This reset/repair is performed by using commands such as `utils dbreplication repair all` and `utils dbreplication reset all` at the command-line interface (CLI). Repair or reset of database replication using the CLI on remote subscribers over the WAN causes all CUCM databases in the cluster to be resynchronized, in which case additional bandwidth above 1.544 Mbps might be required. Lower bandwidths can take longer for database replication repair or reset to complete.

Although there are stringent requirements, clustering over the IP WAN design offers these advantages:

- A single point of administration for users at all sites within the cluster
- Feature transparency
- Shared line appearances
- Extension mobility within the cluster
- A unified dial plan

The clustering over IP WAN design is useful for customers who want to combine the resiliency (high-availability) advantages of this model with the benefits provided by a local call-processing agent at each site. Intrisite signaling is kept local, and WAN failures will not result in any loss of functionality. This network design allows remote offices to support more Cisco IP Phones than SRST.

CUCM Call-Processing Redundancy

A CUCM cluster is a group of physical servers working as a single IP PBX system. A cluster can contain up to 20 servers, of which a maximum of eight servers can run the Cisco CallManager service performing call processing in a cluster. Any additional servers above the eight can be used to provide added functionality to support the telephony deployment (for example, TFTP servers, media resources such as conference bridges, music on hold [MOH], MTP, annunciator, and transcoding) and/or support third-party integrations for add-on applications through APIs. Media resources are covered in more detail in Chapter 13, “Media Resources.”

CUCM call-processing redundancy is implemented by grouping servers running the Cisco CallManager service into CM groups. A CM group is a prioritized list of up to three call-processing servers. Figure 2-5 shows this 1:1 redundancy design.

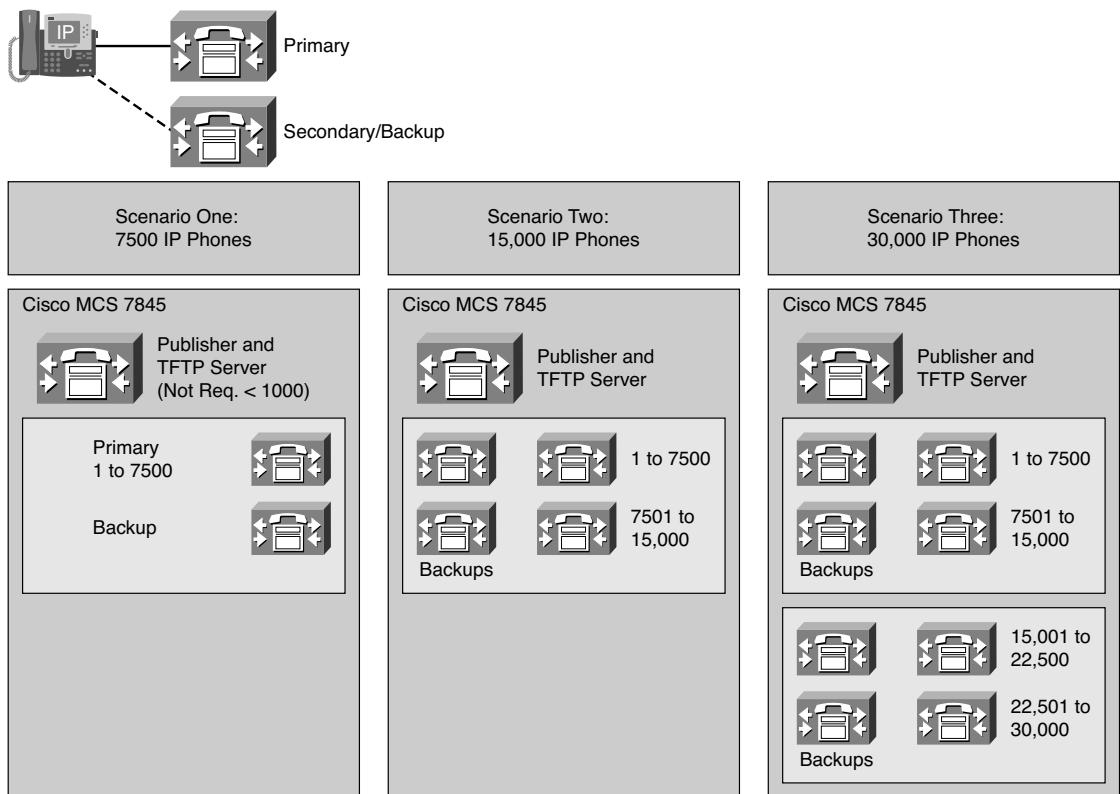


Figure 2-5 1:1 Redundancy Design

The following rules apply for the CM groups:

- Many CM groups can exist in the same cluster.
- Each call-processing server can be assigned to more than one CM group.
- Each device has an assigned CM group that will determine the primary, secondary, and tertiary servers to which it can register.

Cisco IP Phones register with their primary server. When idle, the Cisco IP Phones and CUCM exchange keepalives to ensure that reachability between the devices is maintained. Cisco IP Phones running SCCP establish a TCP session with their primary and secondary servers and exchange TCP keepalives every 30 seconds by default. When the connection to the primary server is lost (no keepalives received for three keepalives), the Cisco IP Phone registers to the secondary server and establishes a TCP connection with the tertiary call-processing server. The Cisco IP Phone continuously tries to reestablish a

connection with the primary server. If the Cisco IP Phone is successful in reaching the primary server when registered to the secondary, the IP Phone waits 120 seconds for the default connection monitor duration timer to expire before reregistering with the primary server. The connection monitor duration alleviates the side effects of an oscillating/flapping WAN link, where the WAN is continuously going up and down. The connection monitor duration is a device pool configuration parameter. (Device pools are discussed in a subsequent chapter.) A 1:1 CUCM call-processing redundancy deployment design guarantees that Cisco IP Phone registrations will never overwhelm the backup servers if there are concurrent primary server failures on different primary servers. The 1:1 design has an increased server count compared to other redundancy design models. This design is not the most cost-effective, but it offers the highest level of fault tolerance.

Each cluster must also provide a TFTP service running on a CUCM server. The TFTP service is responsible for delivering IP phone configurations, firmware (Load ID) upgrades to telephones, and files such as backgrounds and ringtones. The server running the TFTP service might experience significant load in a large cluster. Depending on the number of devices that a server is supporting, you can run the TFTP service on a dedicated server, on the database publisher server, or on any other server in the cluster.

Figure 2-5 illustrates a cluster redundancy model leveraging Cisco 7845 Media Convergence Servers (MCS). Each 7845 server can accommodate up to a maximum of 7500 Cisco IP Phones. Figure 2-5 includes three different scenarios. Scenario one includes three servers, but only two servers would be required if the cluster had fewer than 1250 phones (1000 phones for the 7835 model server). A cluster consisting of 1250 to 7500 phones would require a server dedicated to maintaining the publisher and TFTP functionality.

Scenario one uses two servers for call-processing functionality. One server is the primary call-processing agent, while the other server is the backup call-processing agent. Instead of dedicating a server to a backup-only role, registration-based load sharing can occur between the two servers, and the two servers can back each other up (active/active load sharing). This configuration would need to be manually configured in the CM group that is assigned to the phones. Server A would be the primary for phones 1–3750 and the backup for phones 3751–7500, while server B would be the primary for phones 3751–7500 and the backup for phones 1–3750.

Scenario two leverages everything you covered in scenario one but has doubled the number of call-processing servers and has a dedicated TFTP server. The Cisco CUCM Solution Reference Network Design (SRND) guide recommends one dedicated TFTP server in a cluster of 7500 Cisco IP Phones. Notice that there are two active call-processing servers in the graphic with two dedicated backup servers. Because each CUCM cluster can have up to four active call-processing servers running the CallManager service, a load-sharing configuration like that covered in scenario one can be used to get the full benefit of all four servers.

Scenario three leverages everything discussed in the two prior scenarios, but the number of call-processing servers has again doubled when compared against the last model covered. Load sharing cannot occur in this model because the CUCM is limited to four

active servers. Cisco has a super-clustering model where more than four active servers can be leveraged, but this is a model that involves Cisco Advanced Services design and tuning services. Two TFTP servers must be used in this model because of the number of phones. Best practice is to enable the TFTP service on at least two servers in the CUCM cluster in all the models to provide TFTP redundancy. TFTP server IP addresses allocation is covered in Chapter 3, “Cisco Unified Communications Manager Services and Initial Configuration Settings,” when DHCP Option 150 (TFTP) is covered.

Although the 1:1 redundancy design model provides the highest level of redundancy, it might be excessive. It is unlikely that multiple server failures will occur at the same time, but beware of Murphy’s Law! If it can happen, it will. Because of the low probability of multiple simultaneous server outages and server cost, some environments choose to use a 2:1 redundancy design, as shown in Figure 2-6.

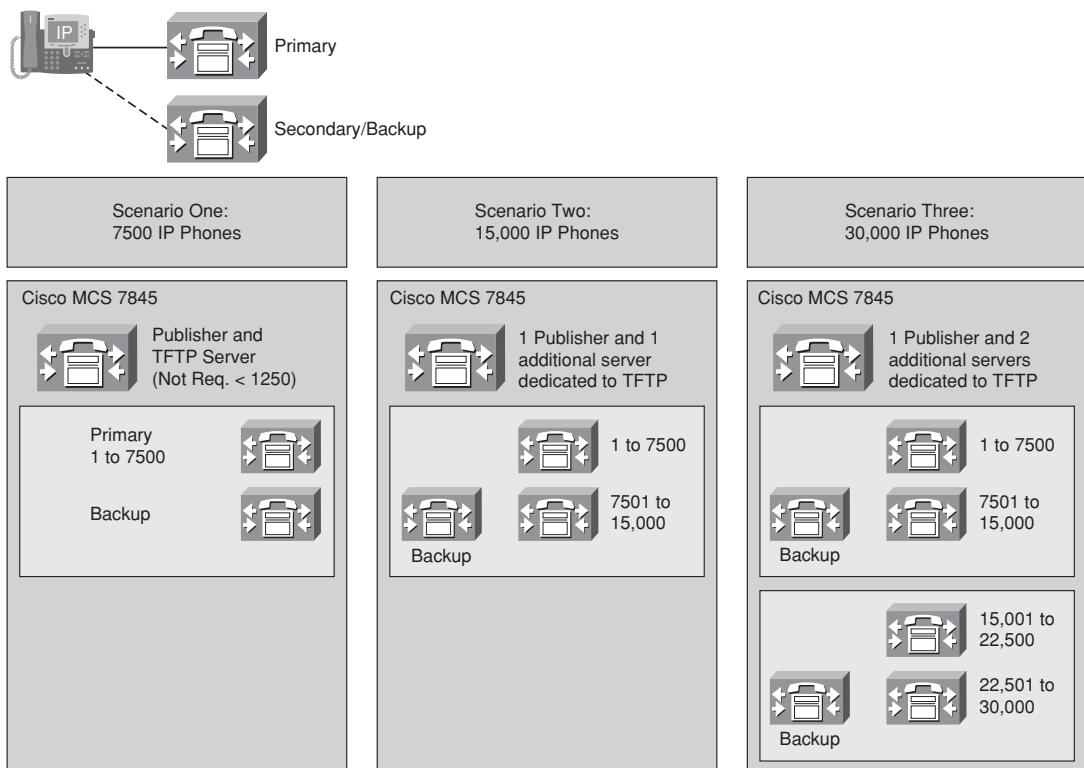


Figure 2-6 2:1 Redundancy Design

Although the 2:1 redundancy design offers some redundancy, there is the risk of overwhelming the backup server if multiple primary servers fail. The 2:1 redundancy model is more popular than the 1:1 model because of its lower costs. Cisco MCS 7845 servers contain a good amount of redundancy features including redundant, hot-swappable power supplies and SCSI hard drives.

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- Supported CUCM deployment models are Single-Site, Multisite with Centralized Call Processing, Multisite with Distributed Call Processing, and Clustering over the IP WAN.
- In the Single-Site deployment model, the CUCM, applications, and DSP resources are at the same physical location; all offsite calls are handled by the PSTN.
- The Multisite with Centralized Call Processing model has a single CUCM cluster. Applications and DSP resources can be centralized or distributed. The IP WAN carries call-control signaling traffic, even for calls within a remote site.
- The Multisite with Distributed Call Processing model has multiple independent sites, each with a CUCM cluster; the IP WAN carries traffic only for intersite calls.
- Clustering over the WAN provides centralized administration, a unified dial plan, feature extension to all offices, and support for more remote phones during failover, but it places strict delay and bandwidth requirements on the WAN.
- Clusters provide redundancy. A 1:1 redundancy design offers the highest availability but requires the most resources and is not as cost-effective as 2:1 redundancy.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. What is the maximum number of phones per CUCM cluster?
 - a. 10,000
 - b. 7500
 - c. 30,000
 - d. 20,000

- 2.** How is call admission control handled in the Centralized Call Processing model?
 - a.** QoS
 - b.** H.323 gateway
 - c.** H.323 gatekeeper
 - d.** CUCM locations
 - e.** CUCM regions
- 3.** What technology is used in the Centralized Call Processing model to reroute a call to a remote destination if there is not enough bandwidth to accommodate the call?
 - a.** Automated alternate routing
 - b.** Call admission control
 - c.** Quality of service
 - d.** Intercluster trunks
- 4.** What technology is used to bypass toll charges by routing calls through remote-site gateways, closer to the PSTN number dialed?
 - a.** Automated alternate routing
 - b.** Tail-end hop-off
 - c.** Extension mobility
 - d.** Call admission control
- 5.** Which call-processing model allows extension mobility between sites?
 - a.** Single-Site model
 - b.** Centralized model
 - c.** Distributed model
 - d.** Clustering over the WAN model
- 6.** Gatekeepers are used within which call-processing model?
 - a.** Single-Site model
 - b.** Centralized model
 - c.** Distributed model
 - d.** Clustering over the WAN model

7. What is the maximum round-trip time requirement between CallManager servers in the Clustering over the WAN model?
 - a. 20 ms
 - b. 150 ms
 - c. 80 ms
 - d. 300 ms
8. What is the minimum amount of bandwidth that must be dedicated to database replication in the Clustering over the WAN model?
 - a. 900 kbps
 - b. 1.544 Mbps
 - c. 80 kbps
 - d. 2.048 Mbps
9. How many servers are required to accommodate 7500 phones using the 7845 server in the 2:1 redundancy model?
 - a. 1
 - b. 2
 - c. 3
 - d. 4

This page intentionally left blank

Chapter 3

Cisco Unified Communications Manager Services and Initial Configuration Settings

Cisco Unified Communications Manager (CUCM) configuration includes basic settings plus specific settings that depend on the features and services used. This chapter describes how basic settings on CUCM are configured to enable the system and prepare CUCM for endpoint deployment.

Chapter Objectives

Upon completing this chapter, you will be able to activate required CUCM services and settings to enable features and remove Domain Name System (DNS) reliance, and you will be able to meet the following objectives:

- Identify elements used for general, initial configuration.
- Identify network configuration options of CUCM.
- Identify the reasons for using Network Time Protocol (NTP) servers and enabling DHCP services in CUCM.
- Describe the reliance on DNS by IP phones when server names are used rather than server IP addresses.
- Describe the difference between network and feature services and explain how they can be managed using the Cisco Unified Serviceability web interface.
- Describe the purpose of enterprise parameters and enterprise phone configuration and explain key parameters.
- Describe the purpose of service parameters and explain key parameters.

CUCM Initial Configuration

After the CUCM installation has been completed, some initial configuration has to be done in the preparation of endpoint provisioning. This initial configuration includes the items listed in Table 3-1.

Table 3-1 Publisher Server Required Services

Configuration Item	Description
Network settings	Basic network settings including Network Time Protocol (NTP), Domain Name System (DNS), and DHCP should be addressed before initial endpoint deployment.
Network and feature services	CUCM servers run network services (automatically activated) and feature services (activated by the administrator). After installation, network services should be checked and desired feature services should be activated.
Enterprise parameters	CUCM has some cluster-wide configuration settings called <i>enterprise parameters</i> . Some enterprise parameters will be modified in most deployments.
Service parameters	CUCM services have configurable parameters that are set on a per-CUCM server. Some service parameter default values will be modified in a standard deployment.

Network Components

CUCM leverages various IP networking protocols and systems, as described in the following sections.

Network Time Protocol

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over IP networks through the use of a hierarchical clock strata organization. A stratum level 1 timing source device is an extremely precise clock source using the rare earth element cesium. Cesium clocks used to be very expensive, but most service providers with large central offices now have local stratum level 1 clocks. Global positioning system (GPS) satellites provide a stratum level 1 clocking source that provides a cost-effective synchronization system.

Stratum level 1 clocks are distributed over networks to provide timing information to a large number of devices. A linear relationship exists between the number of nodes passed and the degradation of the timing quality.

Stratum level 2 timing sources are based on the rare earth element rubidium. Distribution of stratum 2 time information becomes inaccurate more quickly than

stratum 1 information. Stratum level 2 timing is not as accurate as stratum level 1, but the timing is accurate enough to time a large Synchronous Optical Network (SONET) node. SONET nodes are very high-speed networks that are used by service providers to transport time-division multiplexing (TDM) voice calls through networks operating at up to OC-192 speeds (almost 10 Gbps). T1 and T3 voice interfaces are provisioned from SONET nodes, such as the Cisco ONS 15454.

Note More information on SONET, optical networking, and the ONS 15454 is available in *Cisco Self-Study: Building Cisco Metro Optical Networks (METRO)*, by Dave Warren and Dennis Hartmann (Cisco Press, 2003).

CUCM can leverage NTP to obtain accurate time information from a time server. The CUCM publisher server is configured to communicate with one or more NTP servers. The timing that the publisher receives from the timing source is then synchronized to all the subscriber servers. If an external NTP server is not used, the CUCM server can be manually configured with the date and time. However, the system time in most servers is a stratum level 4 timing source and should not be relied on to time a production network.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a protocol that allows IP endpoints to obtain their IP settings dynamically from a server. Cisco IP Phones normally require IP address, subnet mask, default gateway, TFTP server (option 150), and DNS server settings from the DHCP server. CUCM features a DHCP server that was designed to serve Cisco IP Phones only.

Trivial File Transfer Protocol

Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol used by Cisco IP Phones to obtain configuration files and firmware (LOAD ID). A CUCM cluster has to run the TFTP service on at least one server to be able to support Cisco IP Phones. It is recommended to activate the TFTP service on at least two CUCM servers in the cluster for high-availability purposes.

Domain Name System

Domain Name System (DNS) is a name-resolution protocol that allows IP applications to refer to other systems by logical names rather than IP addresses. A CUCM cluster can be configured to use either DNS or IP addresses.

NTP and DHCP Considerations

NTP can be configured during the installation of the CUCM product. NTP can also be configured after the installation procedure using the Cisco Unified Operating System Administration web pages.

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

- Cisco IP Phones display the date and time on the LCD of the phone. The phone's date and time information is obtained from the CUCM subscriber in which the phone registered unless an NTP reference is assigned to the phone. NTP references can be configured in date/time groups in CUCM versions 5.0 and later. The date/time group is assigned to Cisco IP Phone devices by associating the date and time group to the device pool that is assigned to the phone.
- Call details records (CDR) provide time-stamped call-reporting, analysis, and billing information. Call management records (CMR) contain quality of service (QoS) information regarding the quality of phone calls, including the number of packets lost in both the transmit and receive directions, average jitter (delay variation compiled from a sample of the last RTP packets received), and maximum jitter (the maximum amount of delay between two 20-ms (millisecond) samples). CMRs are associated to CDRs by call reference value. Every call processed in the system receives a unique call reference value for billing and troubleshooting purposes.
- Alarms, log files, and trace files include time stamps with millisecond-level accuracy. One second of processing in a CUCM server can have hundreds of lines of trace output. Troubleshooting calls that involve multiple servers frequently require the correlation of alarm, event, and trace information available in the different systems. Correlation of these records is possible only if all devices in the network have the same date and time information.
- CUCM includes features that rely on date and time, including time-of-day call routing, certificate-based security features, and remote support.

Note The Cisco Press book *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide* explains the operation of X.509v3 certificates, certificate trust lists, IPsec, transport layer security, and Secure Skinny Client Control Protocol (SCCPs) in greater detail.

Figure 3-1 displays a master reference clock from which the publisher server is synchronizing time. The publisher server redistributes the timing information to the subscriber servers.

CUCM and all network devices should synchronize their time from a stratum level 1 NTP server. To modify NTP configurations in CUCM, navigate to the OS administration from the Cisco Unified Operating System Administration web pages, as shown in Figure 3-2. NTP servers can be added, deleted, or modified. When the NTP server is first added, the

GUI might display a status indicating, “The NTP service is NOT accessible.” Do not be alarmed by this message. Refresh your web browser with the Refresh icon or the F5 keyboard key and the message should change to “The NTP service is accessible.”

Master Reference Clock

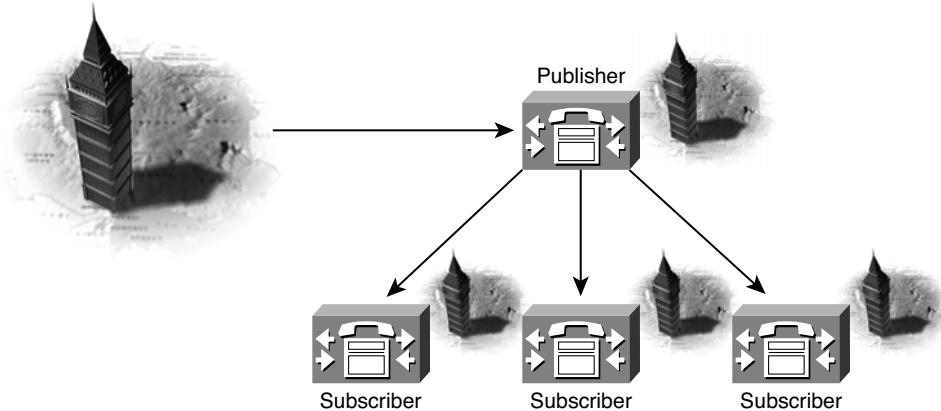


Figure 3-1 Network Time Protocol

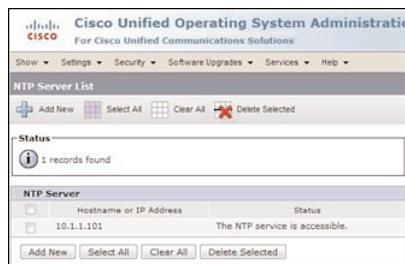


Figure 3-2 Network Time Protocol Configuration

DHCP

The CUCM DHCP server is designed to serve IP phones in small deployments of 1000 devices or less. Cisco provided this feature because some customers were using the Windows 2000 and 2003 Servers in CUCM versions earlier than CallManager 5.0 to provide DHCP services to Cisco IP Phones. Cisco CallManager was rebranded to Cisco Unified Communications Manager (CUCM) as of the 6.0 release. CUCM 5.0 was the first version of the product running the hardened Linux appliance model. CallManager 4.1 and 4.2 ran on Windows 2000 servers, while CallManager 4.3 runs a Windows 2003 server. Cisco Unity still runs on a Microsoft Windows platform at the time of this writing. All other Cisco Unified applications have been migrated to the hardened Linux appliance model with the release of the Cisco UC 8.0 product portfolio.

Most companies are already running enterprise-class DHCP in their server infrastructure. It is a best practice to leverage the existing enterprise-class DHCP server and not use CUCM DHCP services. Smaller deployments and lab environments may require the CUCM DHCP services.

Note Because of the CPU load impact, CUCM DHCP server must not be used in deployments larger than 1000 registered devices. The CPU load of the server can be monitored using the Real-Time Monitoring Tool (RTMT), which is downloadable from the Application menu in CUCM Administration. If high CPU load is experienced, the DHCP service should be provided by other devices (DHCP server, switch, or router). RTMT is covered in *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide*.

Only one DHCP server can be configured per CUCM cluster; no backup configuration is possible. The CUCM DHCP server can be configured with multiple subnets (scopes in Microsoft Windows). DHCP relay must be enabled on remote subnets to allow DHCP broadcast packets to be forwarded across Cisco data network routers to the DHCP server. Routers drop all broadcast packets by default. The Cisco IOS `ip helper-address 10.1.1.1` command would convert all DHCP broadcast packets to a unicast message to a DHCP server at the 10.1.1.1 IP address.

To configure DHCP support on CUCM, follow these steps:

Step 1. Activate the DHCP Monitor Service.

Step 2. Add and configure the DHCP server.

Step 3. Configure the DHCP subnets.

Navigate to the Cisco Unified Serviceability web page. Choose **Tools > Service Activation**. Activate the DHCP Monitor Service by selecting the **DHCP Monitor Service** check box and then clicking the **Save** icon. Figure 3-3 shows a screen capture in which the DHCP Monitor Service has been activated.

Configure the DHCP server by navigating to the CUCM Administration page by choosing **Cisco Unified CM Administration** from the Navigation drop-down menu in the upper-right corner of the page shown in Figure 3-3. Click the **Go** button. Navigate to the following menu item in CUCM Administration: **System > DHCP > DHCP Server**. The Find and List DHCP Servers page displays. Click the **Add New** button. Choose the CUCM server that will be acting as the DHCP server from the Host Server drop-down menu. Configure the **Primary TFTP Server IP Address** field and the **Secondary TFTP Server IP Address** field. It is advisable to have two CUCM servers running the TFTP service for fault-tolerance purposes. Figure 3-4 shows the DHCP Server Configuration page options.

One or more DHCP subnets should now be configured from the CUCM Administration page. Navigate to **System > DHCP > DHCP Subnet**. The Find and List DHCP Subnets page will display. Click the **Add New** button. Choose the DHCP server from the DHCP

Server drop-down menu. All fields on the configuration pages that have an asterisk (*) to the upper right of the configuration option are required fields. Specify the subnet IP address, IP address range, primary router IP address, subnet mask, and TFTP servers. Figure 3-5 displays the DHCP Subnet Configuration page options.

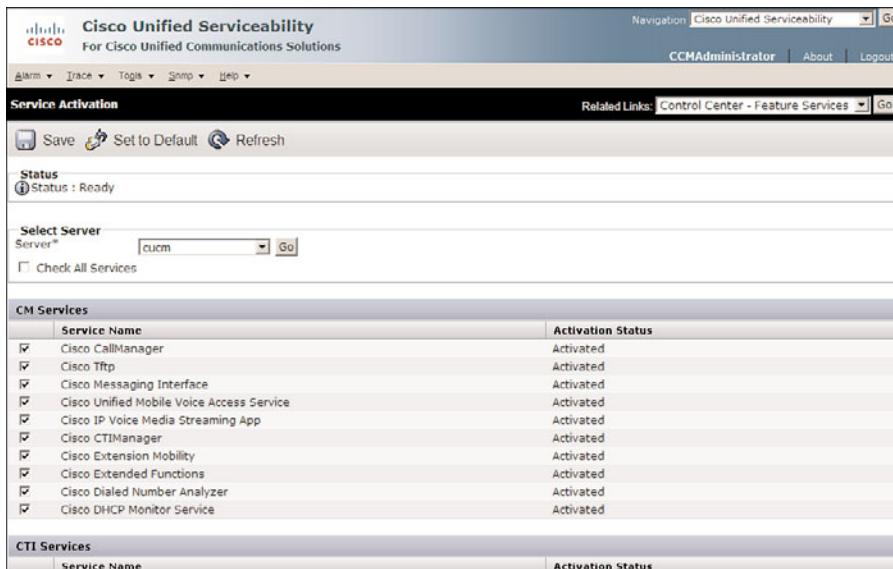


Figure 3-3 Service Activation: DHCP Monitor Service

Host Server*	-- Not Selected --
Primary DNS IP Address	
Secondary DNS IP Address	
Primary TFTP Server IP Address(Option 150)	
Secondary TFTP Server IP Address(Option 150)	
Bootstrap Server IP Address	
Domain Name	
TFTP Server Name(Option 66)	
ARP Cache Timeout(sec)*	0
IP Address Lease Time(sec)*	0
Renewal(T1) Time(sec)*	0
Rebinding(T2) Time(sec)*	0

Figure 3-4 DHCP Server Configuration

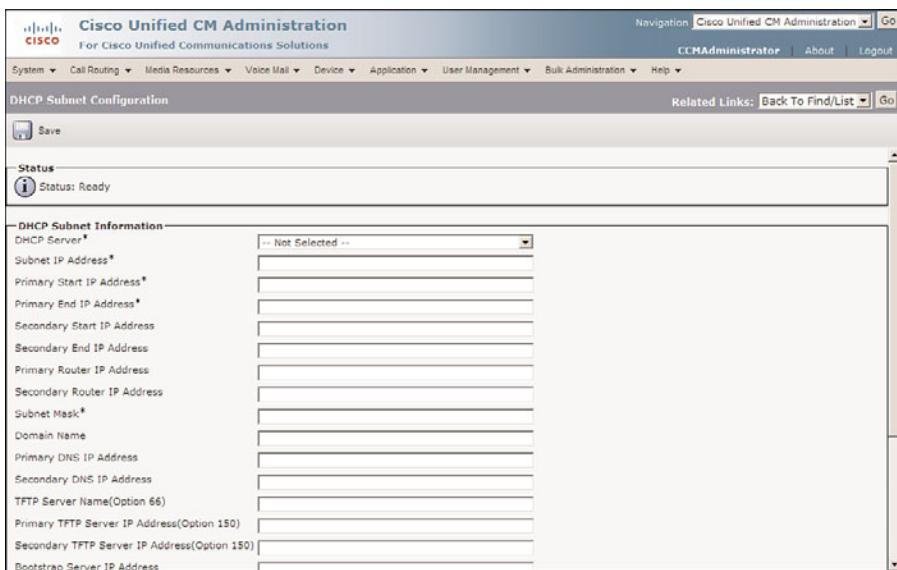


Figure 3-5 *DHCP Subnet Configuration*

DNS

CUCM can use either IP addresses or DNS names to refer to other IP devices in application settings. The use of names requires DNS resolution to dynamically convert names to IP addresses.

Both methods have some advantages:

- **Using IP addresses:** The CUCM system does not depend on a DNS server. This prevents loss of service when the DNS server cannot be reached. Clients, using DNS, query the server with a name lookup request and receive a reply in which the DNS server resolves the host-name record of the query to an IP address. Eliminating the requirement of a DNS server reduces the danger of DNS configuration errors, DNS outages, and any latency (delay) incurred when performing a DNS query. Troubleshooting is simplified when using IP addresses rather than DNS names because there is no need to perform name resolution.
- **Using DNS:** Management is simplified with DNS names because logical names are easier to remember than IP addresses. IP address changes can take place much easier when system-level configuration data is performed based on device names instead of IP addresses. Applications point to a DNS name that does not change. The underlying IP address might change at any time with no consequence to the IP addresses that rely on the server. CUCM server addressing is sent to Cisco IP Phones in the CUCM group configuration setting that is downloaded to the phone when the phone requests its XML (Extensible Markup Language)-based configuration file from the TFTP server.

DNS name resolution is required for the CUCM server name if remote teleworkers will be accessing a CUCM with an RFC 1918 private IP address over a Virtual Private Network (VPN) tunnel. Most companies have at least one remote teleworker with a hardware or software Cisco IP Phone communicating to the CUCM server over a VPN tunnel. DNS is required in this scenario because the IP Phone will send a registration to the private IP address of CUCM that cannot be properly routed over the Internet. Fully qualified domain names (FQDN) (for example, CUCM1.globewisdom.com) can be resolved to a public IP address that is translated to a private IP address at the border of the enterprise network using Network Address Translation (NAT) capabilities. FQDNs follow the following format, which will also be used for Media Gateway Control Protocol (MGCP) gateway authentication purposes: *hostname.domain-name*. The FQDN of CUCM1.globewisdom.com has a host name of CUCM1 and a domain name of globewisdom.com.

RFC 1918 private address space is very popular and includes the following IP address ranges:

Class A: 10.0.0.0

Class B: 172.16.0.0

Class C: 192.168.1.0–192.168.255.0

Table 3-2 summarizes the advantages of using DNS versus IP addressing with CUCM.

Table 3-2 IP Addressing and DNS Comparison

IP Addressing Advantages	DNS Advantages
Does not require a DNS server	Simplifies management because of the use of names rather than numbers
Prevents the IP telephony network from failing if the IP phones lose connectivity to the DNS server	Enables easier IP address changes
Decreases the amount of time required when a device attempts to contact the Unified CM server	Allows server-to-IP phone Network Address Translation (NAT)
Simplifies troubleshooting	

Figure 3-6 illustrates an end-to-end call between two phones in which DNS names are leveraged. The phone must first resolve the DNS name to an IP address in Step 1 before exchanging call-setup signaling events with CUCM in Step 2. CUCM performs digit analysis and routes the call to the destination phone. When the called party at the destination phone goes off hook, CUCM sends a final signaling, coordinating IP address sockets, audio codecs, and sampling rates (20 ms by default) between the two IP phones.

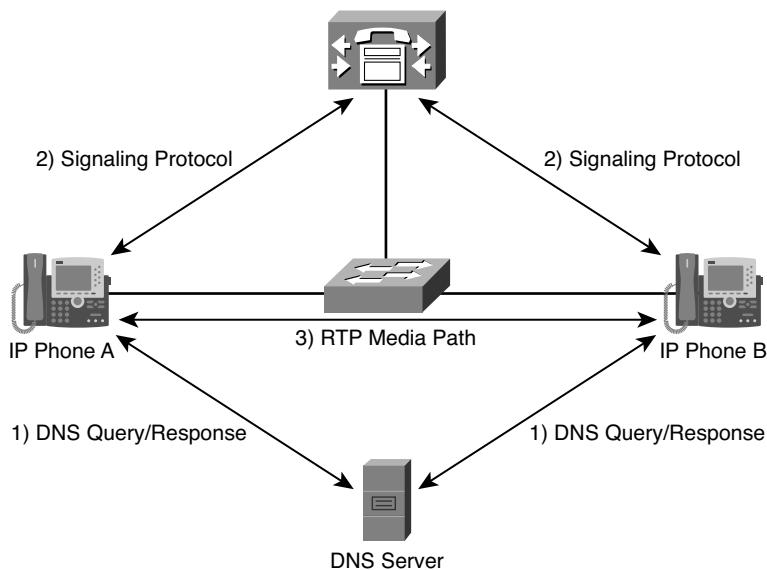


Figure 3-6 Call Flow with DNS

When DNS naming is not used in the CUCM cluster, there is no need to resolve names to an IP address. The signaling between the IP phone and CUCM can be set up directly, and calls can be processed even if the DNS service is not available. CUCM can have higher availability and faster response times by removing any DNS reliance, but DNS might be a requirement to support remote teleworkers. DNS resolution normally occurs with a few milliseconds. Figure 3-7 illustrates call flow without the use of DNS.

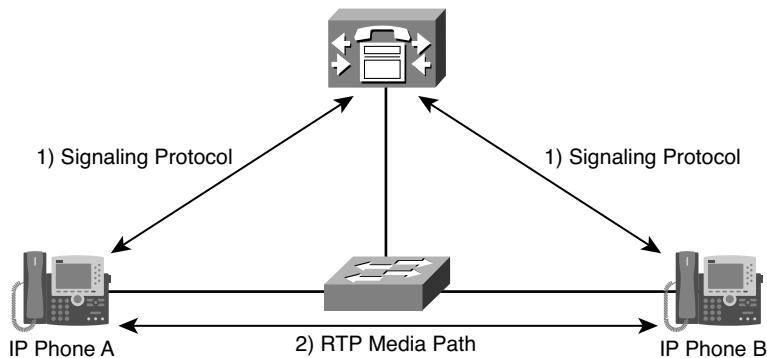


Figure 3-7 Call Flow Without DNS

To change the system name or change the host name used during installation to a different host name, follow these steps:

- Step 1.** In CUCM Administration, choose System > Server.
- Step 2.** Click the Find button and select the first (next) available server from the list of CUCM servers.

Step 3. Change the server name and save the changes, as shown in Figure 3-8.

Note Repeat Steps 2 and 3 for each server in the cluster.

The screenshot shows the 'Server Configuration' page in the Cisco Unified CM Administration interface. At the top, there's a navigation bar with links like System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The current page is 'Server Configuration'. On the left, there's a sidebar with 'Status' (Status: Ready) and 'Server Information' (Database Replication: Publisher, Host Name/IP Address: cucm, MAC Address: blank, Description: blank). At the bottom of the page, there are buttons for 'Save', 'Delete', and 'Add New'. A note at the bottom says '(i) *- indicates required item.'

Figure 3-8 *Server Configuration*

Network and Feature Services

A CUCM cluster can consist of up to 20 servers. Each server can fulfill different tasks, such as running a TFTP or DHCP server, being the database publisher, processing calls (subscribers), and providing media resources.

Depending on the usage of a server, different services have to be activated on the system. There are two types of services on CUCM servers:

- **Network services:** Network services are automatically activated and are required for the operation of the server. Network services cannot be activated or deactivated by the administrator, but they can be stopped, started, or restarted from the Cisco Unified Serviceability web interface. Choose **Tools > Control Center > Network Services**.
- **Feature services:** Feature services can be activated or deactivated on a per-server basis to assign specific tasks or functions (call processing, TFTP, DHCP) to a certain server. Feature services can be activated and deactivated by the administrator from the Cisco Unified Serviceability web interface (**Tools > Service Activation**). Feature services can be started, stopped, or restarted from the Cisco Unified Serviceability web interface (**Tools > Control Center > Feature Services**).

Network Services

Network services are the operating system services that CUCM relies on. Network services are summarized as follows:

- **Performance and monitoring services:** Cisco CallManager Serviceability RTMT, Cisco RTMT Reporter
- **Backup and restore services:** Cisco DRF Master, Cisco DRF Local System Services; Cisco CallManager Serviceability, Cisco CDP, Cisco Trace Collection Service
- **Platform services:** Cisco Database, Cisco Tomcat, SNMP Master Agent
- **DB services:** Cisco Database Layer Monitor
- **Simple Object Access Protocol (SOAP) services:** SOAP Real Time Service APIs and so on
- **CM services:** Cisco CallManager Personal Directory, Cisco Extension Mobility Application, Cisco CallManager Cisco IP Phone Services
- **CDR services:** Cisco CDR Repository Manager, CDR Agent
- **Admin services:** Cisco CallManager Admin

Feature Services

Feature services are the CUCM-related services that run on top of the operating system and database. Feature services are summarized as follows:

- **Database and admin services:** Cisco AXL Web Service, Cisco Bulk Provisioning Service, Cisco TAPS Service
- **Performance and monitoring services:** Cisco Serviceability Reporter, Cisco CallManager SNMP Service
- **CM services:** Cisco CallManager, Cisco TFTP, Cisco CTIManager, Cisco Extension Mobility
- **Computer Telephony Integration (CTI) services:** Cisco CallManager Attendant Console Server, Cisco IP Manager Assistant, Cisco WebDialer Web Service
- **CDR services:** Cisco SOAP, including CDRonDemand Service, Cisco CAR Scheduler, Cisco CAR Web Service
- **Security services:** Cisco CTL Provider, Cisco Certificate Proxy Function
- **Directory services:** Cisco DirSync
- **Voice quality reporter services:** Cisco Extended Functions

Service Activation

To activate or deactivate feature services for a server, follow these steps in the Cisco Unified Serviceability web interface:

- Step 1.** Choose Tools > Service Activation.
- Step 2.** Select the server in which you would like to activate or deactivate a service from the Server drop-down menu.
- Step 3.** Select or deselect the check box for each service you want to modify; click the Save button.
- Step 4.** Use the Control Center to verify that the service has been automatically started (Tools > Control Center > Feature Services).

Figure 3-9 illustrates the Service Activation configuration page in CUCM. The Related Links drop-down menu in the upper-right corner of the page (beneath the Navigation drop-down menu) provides hyperlinks to different menus in the CUCM configuration. Learning how to leverage the related links can increase the speed in which you can provision services in CUCM. It is not typical to turn on every service on every server in the cluster. The Cisco Messaging Interface (CMI) integration service is only required for simplified message desk interface (SMDI) communications to traditional TDM-based voice-mail servers. The CMI service is not required for Cisco Unity, Unity Connection, or Unity Express voicemail/integrated messaging integrations.

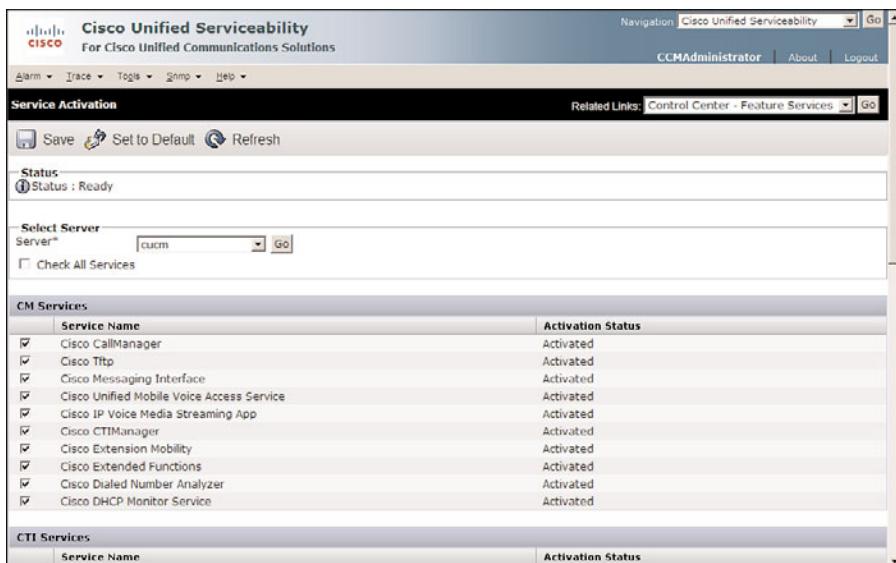


Figure 3-9 Service Activation

Control Center

The Control Center is used to start, stop, or restart services. It is also used to verify the current running status and activation status of services on a per-server basis in the cluster.

Figure 3-10 illustrates the process of viewing a service status and runtime. It also shows the process of selecting the radio button related to a particular service so that the service can be started, stopped, or restarted by clicking the associated buttons at the top of the page. The blue swirly circle icon *only* refreshes the web page; it has no effect on the service status.

The screenshot shows the Cisco Control Center interface. At the top, there are three main sections: "Start, stop, restart, refresh selected service", "Activation status Current status", and "Service start time and up time". Below these are several tables displaying service information:

- Cisco Unified Serviceability** table:

Service Name	Status*	Activation Status	Start Time	Up Time
Cisco AXL Web Service	Started	Activated	Thu Feb 7 09:37:09 2008	0 days 01:32:40
Cisco Bulk Provisioning Service	Started	Activated	Thu Feb 7 09:37:10 2008	0 days 01:32:39
Cisco TAPS Service	Started	Activated	Thu Feb 7 09:37:13 2008	0 days 01:32:36
- Performance and Monitoring Services** table:

Service Name	Status*	Activation Status	Start Time	Up Time
Cisco Serviceability Reporter	Started	Activated	Thu Feb 7 09:35:48 2008	0 days 01:34:01
Cisco CallManager SNMP Service	Started	Activated	Thu Feb 7 09:36:56 2008	0 days 01:32:53
- CM Services** table:

Service Name	Status*	Activation Status	Start Time	Up Time
Cisco CallManager	Started	Activated	Thu Feb 7 09:35:10 2008	0 days 01:34:39
Cisco Itp	Started	Activated	Thu Feb 7 09:35:36 2008	0 days 01:34:13
Cisco Messaging Interface	Not Running	Activated		
Cisco Unified Mobile Voice Access Service	Started	Activated	Thu Feb 7 09:37:15 2008	0 days 01:32:94

A callout box labeled "Select service to start, stop, or restart" points to the first column of the "Database and Admin Services" table.

Figure 3-10 Control Center

Global Server Settings

Two types of settings parameters can be changed in CUCM globally across a server or globally across the entire cluster, as described in the sections that follow.

Enterprise Parameters

Enterprise parameters are used to define cluster-wide system settings. Enterprise parameters apply to all devices and services in the cluster.

Caution Change enterprise parameters only if you are fully aware of the impact of your modifications or if you are instructed to do so by Cisco Technical Assistance Center (TAC).

You can modify many enterprise parameters. Table 3-3 displays some frequently modified enterprise parameters.

Table 3-3 Enterprise Parameters

Parameter	Description	Default Value
Cluster ID	This parameter provides a unique identifier for this cluster.	StandAloneCluster
Enable Dependency Records	Determines whether to display dependency records.	False
CCMUser Parameters	Displays or hides certain user-configurable settings from the CCMUser web page.	Not applicable
Phone URL Parameters	URLs for IP phone authentication, Directory button, Services button, and so on.	Host names rather than IP addresses

Dependency records are a feature of CUCM that enable an administrator to view configuration database records that reference the currently displayed record. Dependency record reports can be run by using the Related Links drop-down menu on most configuration pages throughout CUCM Administration. Dependency record reports search the database and return links to all configuration items that include the configuration item in question. Dependency record reports are useful to run when CUCM will not allow a configuration element to be deleted because it is in use somewhere in the system, but you believe it should no longer be in use in the system. Dependency records could cause a CPU spike in the server. It is not recommended to run dependency record reports during periods with high call volumes.

To modify enterprise parameters, follow these steps in the CUCM Administration web interface:

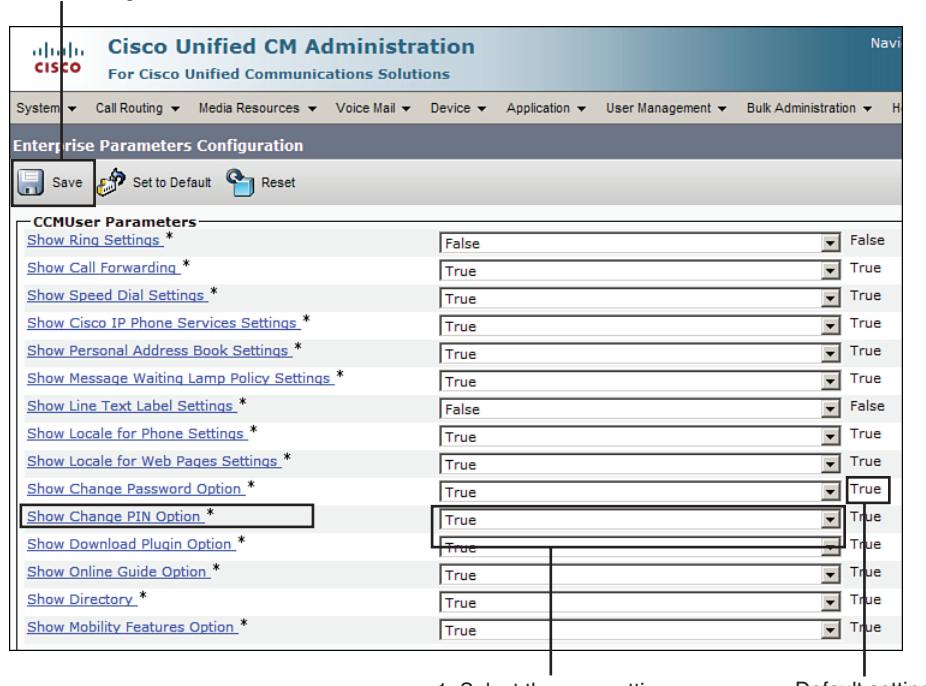
Step 1. Navigate to System > Enterprise Parameters.

Step 2. Change the enterprise parameter values as desired and save the changes.

Note To obtain additional information about specific enterprise parameters, click the ? symbol in the upper-right corner of the screen. The same help system is available by clicking the hyperlink of the enterprise parameter name.

CUCM includes an end-user self-administration web page at the following URL:
`http://CUCM Name or IP Address/CCMUser`. Figure 3-11 is a screen capture of the Enterprise Parameters Configuration page of CUCM; the administrator can use this page to hide configuration options from the end users using this web page. A business might not want end users to be able to change their call-forwarding options of their phone on the CCMUser configuration pages, but the option exists on the page by default. All default settings appear on the right side of the Enterprise Parameters Configuration page.

2. Save the changes



Parameter	Current Value	Default Value
Show Ring Settings *	False	False
Show Call Forwarding *	True	True
Show Speed Dial Settings *	True	True
Show Cisco IP Phone Services Settings *	True	True
Show Personal Address Book Settings *	True	True
Show Message Waiting Lamp Policy Settings *	True	True
Show Line Text Label Settings *	False	False
Show Locale for Phone Settings *	True	True
Show Locale for Web Pages Settings *	True	True
Show Change Password Option *	True	True
Show Change PIN Option *	True	True
Show Download Plugin Option *	True	True
Show Online Guide Option *	True	True
Show Directory *	True	True
Show Mobility Features Option *	True	True

1. Select the new setting

Default setting

Figure 3-11 Enterprise Parameter Configuration

If you removed DNS reliance, all host names within enterprise URL parameters have to be changed to IP addresses. Phone URL parameters change the website that the Cisco IP Phone communicates with when the Settings, Services, or Directory button is pressed on the Cisco IP Phone. The phone URL parameters are part of the enterprise parameters, as shown in Figure 3-12.

Enterprise Phone Configuration

Enterprise phone configuration is used to define parameters that will apply to all phones that support these parameters. These parameters may also exist under the Common Phone Profile configuration and Device Configuration settings. If different parameters

are defined within the two locations, precedence is determined in the following order: Device Configuration, then Common Phone Profile, and finally Enterprise Phone Configuration.

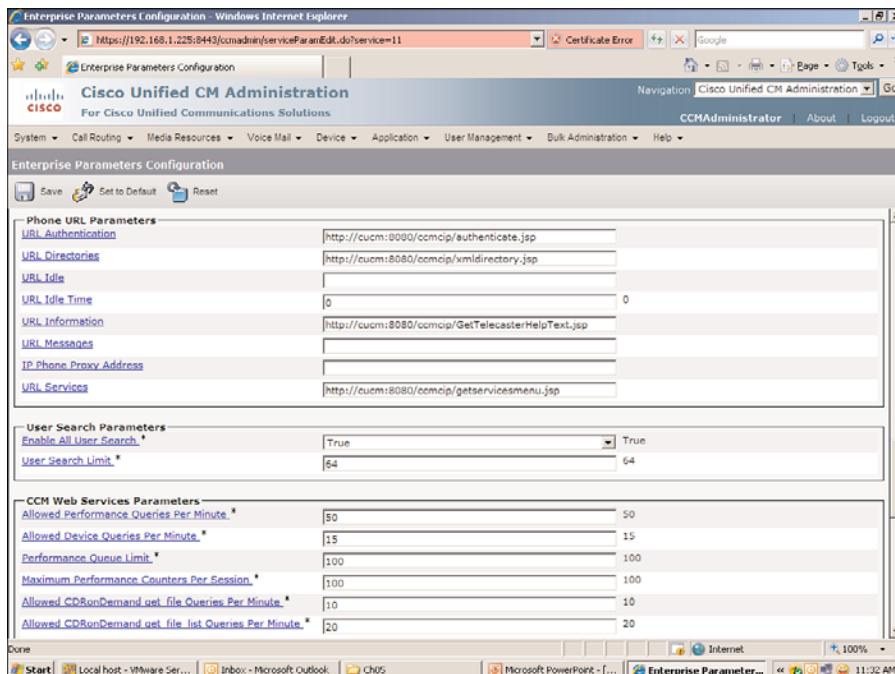


Figure 3-12 Phone URL Parameters

Enterprise Phone Configuration parameters are modified by navigating to **System > Enterprise Phone Configuration**. Figure 3-13 shows the screen for the Enterprise Phone Configuration parameters. Notice the column of check boxes on the far right, which can be used to activate the parameter and override the common settings.

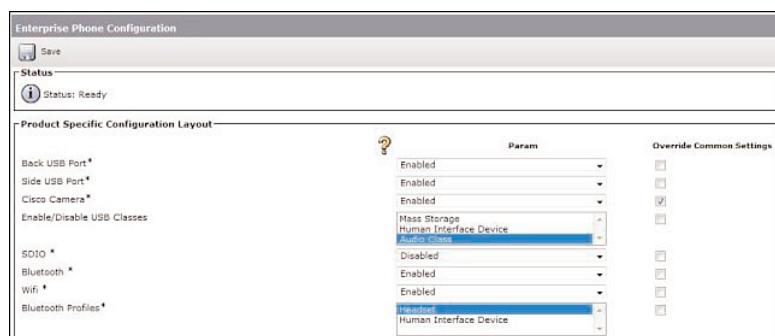


Figure 3-13 Phone URL Parameters

Service Parameters

Service parameters are used to define settings for a specific service (for example, the call-processing CallManager service). They must be configured separately for each server in the cluster. Some are cluster-wide configurations. Some important service parameters for the CallManager service are as follows:

- **T.302 timer:** The T.303 interdigit timeout specifies the interdigit timeout value used to route calls when there are multiple possible matches in the database. Multiple possible matches is a condition that exists when variable-length numbers (international) or overlapping dial plans are being analyzed by CUCM. Reducing the default T.302 value will accelerate the call-routing decision of CUCM when users dial international phone numbers or when there are two overlapping patterns. The default T.302 timer is 15,000 ms (15 seconds). A value of 15 seconds is too long for most environments. Best practice is to reconfigure this timer to a value of 5000 ms (5 seconds). An example of an overlapping dial plan is extension 1500 and extension 15001. CUCM would not know whether it was done receiving digits if the digits of 1500 were received. The user might dial another 1, which would direct the call to a different extension. CUCM would then need to wait for the T.302 timer to expire before routing the call to extension 1500. Most service providers use a 10,000-ms (10-second) T.302 timer value.
- **CDR and CMR:** Call detail records (CDR) are the basis for call reporting, accounting, and billing. Call management records (CMR) document the QoS statistics collected from each individual phone call (lost packets, average jitter, maximum jitter). The CAR (CDR Analysis and Reporting) Cisco Unified Serviceability tool can be used to view CDRs and CMRs.

To see the complete list of service parameters, click the **Advanced** button present on the Service Parameters Configuration page. The Change B-Channel Maintenance Status service parameter is an example of a CallManager service parameter that is not displayed by default. Table 3-4 includes some frequently modified service parameters. Hundreds of service parameters are available to CUCM, many of which you will never encounter. The best way to find one of the parameters listed in Table 3-4 is to use the Find function of your web browser to locate the option on the page.

Table 3-4 Service Parameter Examples

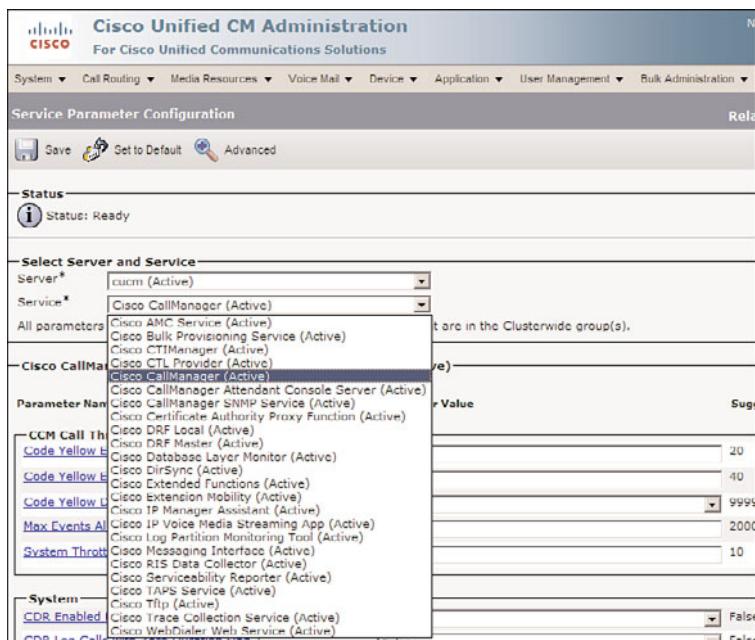
Parameter	Description	Default Value
CDR Enabled Flag	This parameter determines whether CDRs are generated.	False
T.302 Timer	This parameter specifies an interdigit timer for sending the setup acknowledgment message. When this timer expires, CUCM routes the dialed digits.	15 seconds

Table 3-4 Service Parameter Examples

Parameter	Description	Default Value
Automated Alternate Routing Enable	This parameter determines whether to use automated alternate routing when the system does not have enough bandwidth.	False
Change B-Channel Maintenance Status (click the Advanced button first)	This parameter allows CUCM to change individual B-channel maintenance status for Primary Rate Interface (PRI) and channel associated signaling (CAS) interfaces in real time for troubleshooting.	No default

To modify the service parameters, follow these steps in the CUCM Administration web interface. Steps 2 through 4 are illustrated in Figures 3-14 and 3-15.

- Step 1.** Navigate to System > Service Parameters.
- Step 2.** Select the server and the service for which you want to change service parameters.
- Step 3.** Change the service parameter values as desired and save the changes.
- Step 4.** Click Save.

**Figure 3-14 Service Parameters: Server and Service Selection**

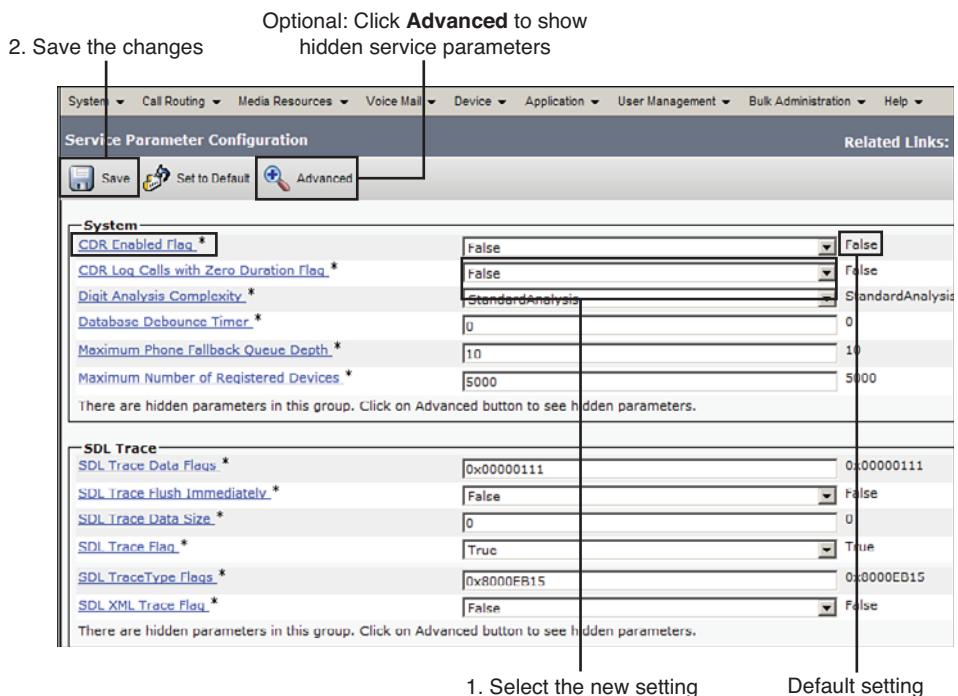


Figure 3-15 Service Parameters: Configuration

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- CUCM initial configuration includes network configuration, activation of feature services, and enterprise and service parameter configuration.
- CUCM network configuration options include NTP configuration, DHCP server configuration, and using DNS versus IP addresses.
- The CUCM DHCP service is designed to serve IP phones.
- To avoid DNS reliance of IP phones, change host names to IP addresses.
- Network services are automatically activated, whereas feature services are activated by the CUCM administrator.
- Enterprise parameters are used to define cluster-wide system settings.
- Service parameters are used to configure parameters of specific services.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

- 1.** How do subscriber servers get their time configuration?
 - a.** Statically
 - b.** Network Time Protocol
 - c.** Synchronized from CUCM publisher
 - d.** Synchronized with the phone
 - e.** Subscriber does not have time information
- 2.** What are the two ways in which Cisco IP Phones get their date and time information?
 - a.** Statically on the phone
 - b.** Messages from the subscriber server
 - c.** Synchronized from the NTP reference
 - d.** Global positioning system satellite
 - e.** Directly from publisher
- 3.** What tool enables you to activate and deactivate a service from CUCM?
 - a.** Cisco Unified Serviceability
 - b.** Control Center
 - c.** Service Activation
 - d.** Add/Remove Programs
 - e.** Microsoft Service Console
- 4.** What information does the DHCP option 150 provide?
 - a.** CUCM publisher IP address
 - b.** CUCM TFTP server IP address
 - c.** DHCP server IP address
 - d.** DNS server IP address
 - e.** XML service server

5. What default signaling protocol is used between CUCM and Cisco IP Phones?
 - a. SIP
 - b. SCCP
 - c. RTP
 - d. RTCP
 - e. H.323
 - f. MGCP
 - g. Ethernet
6. Is the use of a DNS server in an IP telephony environment going to increase or decrease postdial delay?
 - a. Increase
 - b. Decrease
7. What tool enables you to start, stop, and restart CUCM services from CUCM?
 - a. Cisco Unified Serviceability
 - b. Control Center
 - c. Service Activation
 - d. Add/Remove Programs
 - e. Microsoft Service Console
8. Which of the following is used to restart network service in CUCM?
 - a. Cisco Unified Serviceability
 - b. Control Center - Network Services
 - c. Service Activation
 - d. Control Center - Feature Services
 - e. Add/Remove Programs
 - f. Microsoft Service Console
9. In CUCM, where can you change the URLs that phone buttons access?
 - a. Enterprise parameters
 - b. Service parameters
 - c. CUCM Serviceability
 - d. CUCM Administration

10. Where can call details records and call management records be enabled?

- a.** Enterprise parameters
- b.** Service parameters
- c.** CUCM Serviceability
- d.** Cisco Real-Time Monitoring Tool

This page intentionally left blank

Chapter 4

Managing User Accounts in Cisco Unified Communications Manager

Cisco Unified Communications Manager (CUCM) includes several features that are related to user accounts, including end-user features and administrative privileges. CUCM users can be managed using CUCM configuration tools or by integrating CUCM with a supported Lightweight Directory Access Protocol version 3 (LDAPv3) directory. This chapter describes the types of user accounts used by CUCM and discusses how they can be managed.

Chapter Objectives

Upon completing this chapter, you will be able to manage user accounts with CUCM and meet the following objectives:

- Identify the different user accounts in CUCM and explain how they are used.
- Describe how to add and delete users and how to assign privileges to them.
- Identify LDAPv3 synchronization characteristics and name the types of LDAPv3 support provided by CUCM.
- Describe how LDAPv3 can be used for user provisioning and authentication.

CUCM User Accounts

Several CUCM features require user accounts for authentication purposes. These features include an administrative web page, user web pages, and the following applications:

- Cisco Unified Attendant Console
- Cisco Unified Extension Mobility
- Cisco Unified Manager Assistant (CUMA)

Cisco IP Phones can browse corporate and personal directories to find the directory number of a user. CUCM is provisioned with a user's first name, last name, and directory number to provide this directory-browsing functionality. This chapter goes into various directory synchronization capabilities that might not be required by most engineers and administrators, but this information will be required by designer engineers and integrators. It is also a great way to introduce some light Microsoft Active Directory/LDAPv3 information into your technical skillset if you have not worked in this area.

CUCM phone services can be configured to require a user login before providing access to the service. Users can authenticate with their username and password (alphanumeric) or PIN (numeric), depending on the needs of the application. CUCM sends authentication requests to an authentication component called the Identity Management System (IMS) library, which is responsible for authenticating user login credentials against the local user database.

User Account Types

There are two types of user accounts in CUCM:

- **End users:** End users are associated with an individual and have an interactive login. End users do not include any administrative roles by default, but administrative roles can be assigned by associating the end user to a user group with the proper role configuration.
- **Application users:** Application users are associated with applications such as Cisco Unified Attendant Console, Cisco Unified Contact Center Express (UCCX), or Cisco Unified Manager Assistant (CUMA). Application users do not have the ability to log in interactively but are required for authentication between servers.
CCMAdministrator is an example of a default application user that is used when first configuring the CUCM system.

Table 4-1 summarizes the differences between end users and application users.

Table 4-1 User Account Types in CUCM

End Users	Application Users
Associated with an individual	Associated with an application or service (leveraged in UC server integrations: Presence, CER, UCCX, and so on)
Provide interactive logins	Provide noninteractive logins (session-based pass-through authentication)
Provide user feature and system administration authorization	Provide application authorization
Included in phone directory	Not included in phone directory
Can be provisioned and authenticated using an external LDAP directory server	Cannot use LDAP

The attributes associated with end users are separated into three categories, as follows:

- Personal and organizational settings:
 - User ID; first, middle, and last name
 - Manager user ID, department
 - Phone number, mail ID
- Password
- CUCM administration settings:
 - PIN, Session Initiation Protocol (SIP) digest credentials
 - User privileges (user groups and roles)
 - Associated PCs, controlled devices, and directory numbers
 - Application and feature parameters

User Privileges

CUCM allows the assignment of user privileges to application users and end users. Privileges that can be assigned to users include the following:

- Access to administration and user web pages
- Access to specific administrative functions
- Access to application interfaces such as Computer Telephony Integration (CTI) and Simple Object Access Protocol (SOAP)

User privileges are configured using two configuration entities:

- **User groups:** A collection of application users and end users with similar privilege levels
- **Roles:** Resources for an application

Each role refers to exactly one application, and each application has one or more resources. Access privileges are configured per application resource in the role configuration. Roles are assigned to user groups.

Figure 4-1 illustrates the access that four users have to two different applications. The needs of the four users are achieved through the assignment of two user groups.

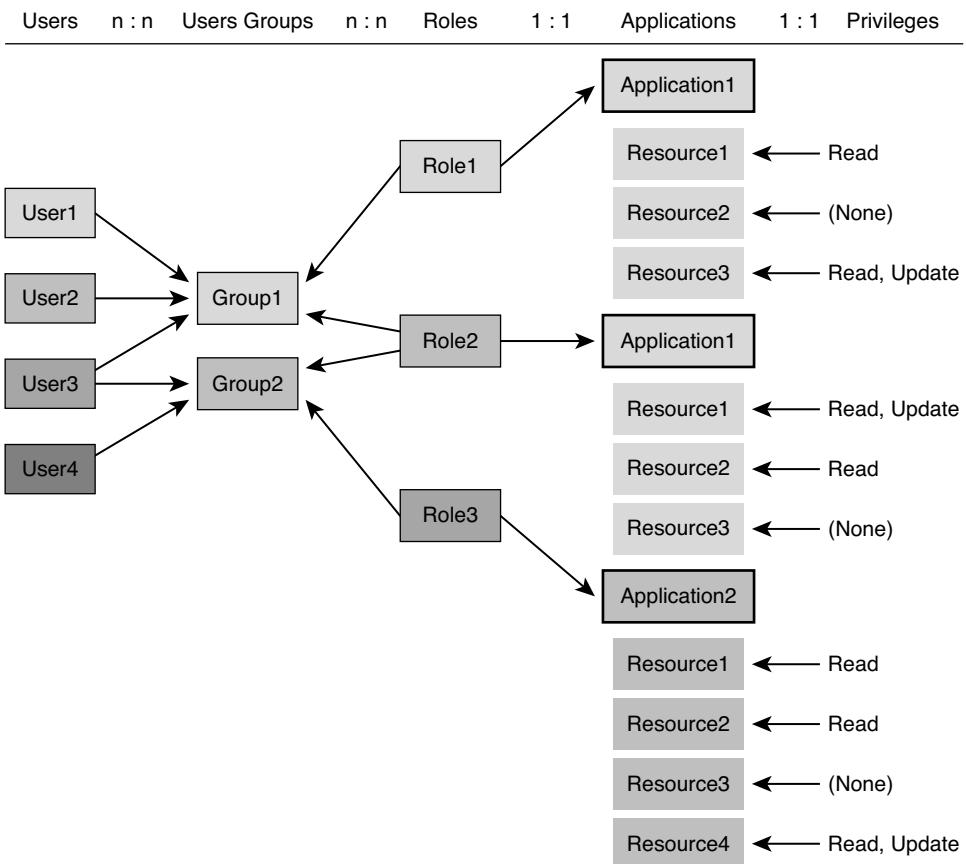


Figure 4-1 User Privilege Component Interaction

User1 and User2 are assigned to Group1, which has two roles assigned to it for Application1. Application1 might be the CUCM Administration or CUCM Serviceability web page. The privilege levels of Role1 and Role2 refer to the same application but provide different levels of access (privileges) to the resource. The result of overlapping privileges can be configured to give the highest or lowest overlapping privilege level. The system default will provide the lowest overlapping privilege level whenever a user has different privilege levels for the same object.

User3 is assigned to user Group1 and Group2. Group1 and Group2 have role assignments of 1, 2, and 3. Role1 and Role2 both control different privilege levels to Application1 and Application2. The most restrictive privileges to each object will prevail whenever there is a privilege level discrepancy between the two different user groups.

User4 is assigned to Group2, which has privilege levels to Application1 and Application2, controlled through Role2 and Role3. User4 does not have overlapping privilege challenges.

The goal of the configuration illustrated in Figure 4-2 is to create administrative groups that have read, write, and update access to the CUCM administration web pages (CCMAdmin), while junior-level administrators get read-only privileges to the CCMAdmin configuration web pages. The following text relates to the example illustrated in Figure 4-2.

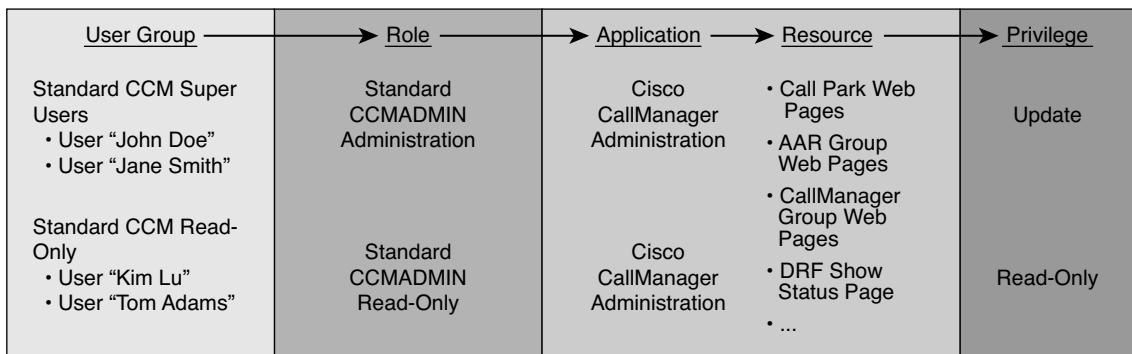


Figure 4-2 Roles and User Groups

CUCM has various administration web pages associated with functions, such as the *Call Park web pages* (used to configure the Call Park feature), the *AAR Group web pages* (used to configure automated alternate routing), the *CallManager group web pages* (for CUCM group configuration), and the *DRF Show Status page* (used to check the status of Disaster Recovery System (DRS) backup or restore jobs).

CUCM has many default roles (24 in CUCM 8.0), called *standard roles*. Some of the standard roles are associated with CUCM Administration (CCMAdmin) applications. By default, there are many predefined roles in CUCM. Two roles are used in Figure 4-2. Standard CCMAdmin Administration has update privileges to all CCMAdmin administration web pages, while the Standard CCMAdmin Read-Only role has CCMAdmin privileges set to read-only access. Standard roles can be copied, renamed, and reconfigured to achieve the access level requirements of the organization deploying CUCM.

CUCM has many default user groups, called *standard user groups*. Two examples of standard user groups are Standard CCM Super Users and Standard CCM Read-Only. User group Standard CCM Super Users is associated with the role Standard CCMAdmin Administration, and user group Standard CCM Read-Only is associated with the role Standard CCMAdmin Read-Only. Although privilege levels are configured in the role configuration, roles are applied to user groups. End users and/or application users are then associated to one or more user groups. The relationship between these configuration elements is illustrated in Figure 4-2.

User Management

User management options in CUCM include the following:

- **CUCM Administration:** Suitable for configuring a small number of users or doing single updates to the configuration of a user. CUCM administration of users is done on a one-by-one basis. This method is not scalable and unsuitable for most medium to large deployments of CUCM.
- **Bulk Administration Tool (BAT):** BAT allows the automation of large insertions, updates, and deletions of configuration information. In this chapter, we look at using BAT for the addition of users. We investigate the use of BAT for the addition of phones in a later chapter. BAT is an excellent tool for initial deployment or large updates to many configuration options, including the user database.
- **LDAPv3 integration:** LDAPv3 integration allows end users to be synchronized from a centralized user database to CUCM's local LDAPv3-compliant database, which is part of the IBM Informix Database Server (IDS). LDAPv3 is useful when there is an existing LDAPv3 database with all the user information. LDAPv3 user synchronization is only used to synchronize end users. Application users are always provisioned locally in the CUCM LDAPv3 IDS. LDAPv3 authentication can be enabled in addition to LDAPv3 synchronization. LDAPv3 authentication passes any password-based login requests through the CUCM server to the LDAPv3 server where user login is authenticated (pass-through authentication). LDAPv3 authentication has the benefit of maintaining one central password database. CUCM does not replicate the passwords that are configured in the central LDAPv3 database.

LDAPv3 synchronization replicates personal and organization user data to the CUCM database. The personal and organizational user data cannot be modified from CUCM administration after LDAPv3 synchronization is enabled. Personal and organizational user data must be modified on the LDAPv3 server by the LDAPv3 administrator, and resynchronization must occur before the changes are reflected in CUCM. Depending on the resynchronization schedule, the resynchronization event might not occur for days or weeks. Manual synchronization can be performed at any time.

Table 4-2 summarizes the differences among the local CUCM database, LDAPv3 synchronization, and LDAPv3 authentication.

Managing User Accounts

CUCM user management is performed from the Cisco Unified Communications Manager Administration User Management menu. The administrator must log in with an account that has user management privileges. Any end-user account that has the user management privilege assigned can modify user accounts. CCMAdministrator is the default administration application user account in CUCM. The CCMAdministrator username can be changed at the time of the CUCM installation.

Table 4-2 End-User Data Location

No LDAPv3 Integration	LDAPv3 Synchronization	LDAPv3 Authentication	
User ID, First Name, Middle Name, Last Name, Manager User ID, Department, Phone Number, Mail ID	Local database	LDAPv3 (replicated to local database)	LDAPv3 (replicated to local database)
Password	Local database	Local database	LDAPv3
PIN, Digest Credentials, Groups, Roles, Associated PCs, Controlled Devices, Extension Mobility Profile, CAPF Presence Group, Mobility	Local database	Local database	Local database

The User Management menu includes options to configure application users, end users, roles, and user groups, as shown in Figure 4-3.

**Figure 4-3** User Management Menu

Figure 4-4 shows an Application User Configuration page. The user ID and password must be configured. Application users are often used as an authentication mechanism between CUCM and other Unified Communications (UC)-related servers, such as Cisco Emergency Responder (CER) or Cisco Unified Contact Center Express (UCCX). When application users are used for UC application server authentication with either of these platforms, the username and password must match on the two servers. The application user in CUCM must also be associated with CTI (Computer Telephony Integration) ports that are used for the communication between the servers. The CTI Manager service in CUCM uses JTAPI (Java Telephony Application Programming Interface) to communicate between the two servers. Navigate to **User Management > Application User** from the CCMAdminstration page to add an application user. Click the **Add New** button.

The screenshot shows the 'Application User Configuration' page. At the top is a 'Save' button. Below it is a section for 'Application User Information' containing fields for 'User ID*', 'Password', 'Confirm Password', 'Digest Credentials', 'Confirm Digest Credentials', and a dropdown for 'Presence Group*' set to 'Standard Presence group'. There are four checkboxes for presence-related options: 'Accept Presence Subscription', 'Accept Out-of-dialog REFER', 'Accept Unsolicited Notification', and 'Accept Replaces Header'. Below this is a 'Device Information' section. It shows a list of 'Available Devices' with items: RP911, RPELIN, SEP012345012345, SEP012345012346, and SEP012345012349. To the right of this list are three buttons: 'Find more Phones', 'Find more Route Points', and 'Find more Pilot Points'. Below the device list is a 'Controlled Devices' section with an empty list box.

Figure 4-4 Application User Configuration

Figure 4-5 shows the bottom of the Application User Configuration page where the application user can be added to user groups. The user group assignment section does not display until you click the Save button on the configuration page. The roles that are assigned to the one or more user groups the user has been associated with are listed in the Roles field in Figure 4-5.

The End User Configuration page is similar to the Application User Configuration page but includes many more configuration parameters. Figure 4-6 displays the End User Configuration page in CUCM. Navigate to **User Management > End User** to add an end user in CUCM Administration. Click the **Add New** button.

Standard roles cannot be deleted or modified. Custom roles, however, can be created from scratch or by copying and then modifying a standard role. Figure 4-7 shows an abbreviated listing of CUCM roles. Navigate to **User Management > Role** to find an existing role configuration. Click the **Find** button to display all existing roles.

Figure 4-8 displays the default Role Configuration page. When configuring a role, an application configuration selection web page is presented. Figure 4-8 displays after the application configuration selection. The application resources displayed on the left side of Figure 4-8 can each be assigned no privileges, read privileges, or update privileges. Role Configuration pages are accessible through **User Management > Role** in CUCM Administration.

Add Application User to User Groups

Application User Configuration	
<input style="float: left; margin-right: 10px;" type="button" value="Save"/> <div style="float: right; margin-top: -20px;">View Details</div>	
Controlled Devices <input style="width: 100%; height: 40px;" type="text"/>	
CAPF Information <div style="display: flex; justify-content: space-between;"> Associated CAPF Profiles <input style="width: 100%; height: 40px;" type="text"/> View Details </div>	
Permissions Information <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> Groups <input style="width: 100%; height: 40px;" type="text"/> Roles <input style="width: 100%; height: 40px;" type="text"/> </div> <div style="flex: 1; text-align: right;"> Add to User Group Remove from User Group </div> </div>	
View Details	

View Roles of Application User

Figure 4-5 Application User Group Configuration

End User Configuration

End User Configuration	
<input style="float: left; margin-right: 10px;" type="button" value="Save"/> <div style="float: right; margin-top: -20px;">View Details</div>	
User Information <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> User ID* <input type="text"/> Password <input type="password"/> Confirm Password <input type="password"/> PIN <input type="password"/> Confirm PIN <input type="password"/> Last name* <input type="text"/> Middle name <input type="text"/> First name <input type="text"/> Telephone Number <input type="text"/> Mail ID <input type="text"/> Manager User ID <input type="text"/> Department <input type="text"/> User Locale <input type="text" value="< None >"/> </div> <div style="flex: 1; text-align: right;"> Associated PC <input type="text"/> Digest Credentials <input type="password"/> Confirm Digest Credentials <input type="password"/> </div> </div>	
Device Associations <input style="width: 100%; height: 40px;" type="text"/>	

Figure 4-6 End User Configuration

Find and List Roles				
<input type="button" value="Add New"/> <input type="button" value="Select All"/> <input type="button" value="Clear All"/> <input type="button" value="Delete Selected"/>				
Status				
31 records found				
Role (1 - 31 of 31)				
Find Role where Name begins with <input type="text"/> <input type="button" value="Find"/> <input type="button" value="Clear Filter"/> <input type="button" value="Print"/> <input type="button" value="Help"/> <input type="button" value="Select item or enter search text"/>				
Name	Application	Description	Copy	
Standard AXL API Access	Cisco Call Manager AXL Database	Access the AXL APIs		
Standard Admin Rep Tool Admin		Administer CAR		
Standard CCM Admin Users		All users with access to CCM web site		
Standard CCM End Users		Access to CCM User Option Pages		
Standard CCM Feature Management	Cisco Call Manager Administration	Standard CCM Feature Management		
Standard CCM Gateway Management	Cisco Call Manager Administration	Standard CCM Gateway Management		
Standard CCM Phone Management	Cisco Call Manager Administration	Standard CCM Phone Management		
Standard CCM Route Plan Management	Cisco Call Manager Administration	Standard CCM Route Plan Management		
Standard CCM Service Management	Cisco Call Manager Administration	Standard CCM Service Management		
Standard CCM System Management	Cisco Call Manager Administration	Standard CCM System Management		
Standard CCM User Management	Cisco Call Manager Administration	Standard CCM User Management		
Standard CCM User Privilege Management	Cisco Call Manager Administration	Standard CCM User Privilege Management		
Standard CCMADMIN Read Only	Cisco Call Manager Administration	Administer all aspects of CCMAdmin system		
Standard CCMUSER Administration	Cisco Call Manager End User	Read access to all CCMAdmin resources		
Standard CTI Allow Call Monitoring	Cisco Computer Telephone Interface (CTI)	Administer all aspects of CCMUser system		
		Allow monitoring of calls		

Figure 4-7 Default Role Configuration

Selected Application

Role Configuration		Related Links:																												
<input type="button" value="Copy"/> <input type="button" value="Add New"/>																														
Role Information <p>Application* Cisco Call Manager Administration</p> <p>Name* <input type="text" value="Standard CCM Route Plan Management"/></p> <p>Description <input type="text" value="Standard CCM Route Plan Management"/></p>																														
Resource Access Information <table border="1"> <thead> <tr> <th>Resource</th> <th>Privilege</th> </tr> </thead> <tbody> <tr> <td>AAR Group web pages</td> <td><input checked="" type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>Access List</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>Add Unity User</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>Announcer web pages</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>Application Dial Rules web pages</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>Application Server</td> <td><input checked="" type="checkbox"/> read <input checked="" type="checkbox"/> update</td> </tr> <tr> <td>Application User CAPF</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>Application User Web Pages</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>BLF Directed Call Park</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>BLF Speeddial</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>Bulk Add/Update Lincs</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>Bulk Add/Update Phones</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> <tr> <td>Bulk CUPS User Page</td> <td><input type="checkbox"/> read <input type="checkbox"/> update</td> </tr> </tbody> </table>			Resource	Privilege	AAR Group web pages	<input checked="" type="checkbox"/> read <input type="checkbox"/> update	Access List	<input type="checkbox"/> read <input type="checkbox"/> update	Add Unity User	<input type="checkbox"/> read <input type="checkbox"/> update	Announcer web pages	<input type="checkbox"/> read <input type="checkbox"/> update	Application Dial Rules web pages	<input type="checkbox"/> read <input type="checkbox"/> update	Application Server	<input checked="" type="checkbox"/> read <input checked="" type="checkbox"/> update	Application User CAPF	<input type="checkbox"/> read <input type="checkbox"/> update	Application User Web Pages	<input type="checkbox"/> read <input type="checkbox"/> update	BLF Directed Call Park	<input type="checkbox"/> read <input type="checkbox"/> update	BLF Speeddial	<input type="checkbox"/> read <input type="checkbox"/> update	Bulk Add/Update Lincs	<input type="checkbox"/> read <input type="checkbox"/> update	Bulk Add/Update Phones	<input type="checkbox"/> read <input type="checkbox"/> update	Bulk CUPS User Page	<input type="checkbox"/> read <input type="checkbox"/> update
Resource	Privilege																													
AAR Group web pages	<input checked="" type="checkbox"/> read <input type="checkbox"/> update																													
Access List	<input type="checkbox"/> read <input type="checkbox"/> update																													
Add Unity User	<input type="checkbox"/> read <input type="checkbox"/> update																													
Announcer web pages	<input type="checkbox"/> read <input type="checkbox"/> update																													
Application Dial Rules web pages	<input type="checkbox"/> read <input type="checkbox"/> update																													
Application Server	<input checked="" type="checkbox"/> read <input checked="" type="checkbox"/> update																													
Application User CAPF	<input type="checkbox"/> read <input type="checkbox"/> update																													
Application User Web Pages	<input type="checkbox"/> read <input type="checkbox"/> update																													
BLF Directed Call Park	<input type="checkbox"/> read <input type="checkbox"/> update																													
BLF Speeddial	<input type="checkbox"/> read <input type="checkbox"/> update																													
Bulk Add/Update Lincs	<input type="checkbox"/> read <input type="checkbox"/> update																													
Bulk Add/Update Phones	<input type="checkbox"/> read <input type="checkbox"/> update																													
Bulk CUPS User Page	<input type="checkbox"/> read <input type="checkbox"/> update																													

Configured Privilege per Application Resource

Figure 4-8 Role Configuration Page

Standard user groups cannot be deleted or modified; however, custom groups can be. Custom user groups can be created from scratch or by copying an existing user group. Figure 4-9 displays an abbreviated list of the default user groups.

Navigate to **User Management > User Group** and click the Find button to display existing user groups. Click the Standard CCM Super Users user group. Figure 4-10 displays the User Group Configuration page in which users can be added to a user group.

Find and List User Groups			
	Name	Roles	Copy
<input type="checkbox"/>	Standard_CCR_Admin_Users		
<input type="checkbox"/>	Standard_CCM_Admin_Users		
<input type="checkbox"/>	Standard_CCM_End_Users		
<input type="checkbox"/>	Standard_CCM_Gateway_Administration		
<input type="checkbox"/>	Standard_CCM_Phone_Administration		
<input type="checkbox"/>	Standard_CCM_Read_Only		
<input type="checkbox"/>	Standard_CCM_Server_Maintenance		
<input type="checkbox"/>	Standard_CCM_Server_Monitoring		
<input type="checkbox"/>	Standard_CCM_Super_Users		
<input type="checkbox"/>	Standard_CTI_Allow_Call_Monitoring		
<input type="checkbox"/>	Standard_CTI_Allow_Call_Park_Monitoring		
<input type="checkbox"/>	Standard_CTI_Allow_Call_Recording		
<input type="checkbox"/>	Standard_CTI_Allow_Calling_Number_Modification		
<input type="checkbox"/>	Standard_CTI_Allow_Control_of_All_Devices		
<input type="checkbox"/>	Standard_CTI_Allow_Reception_of_SRTP_Key_Material		
<input type="checkbox"/>	Standard_CTI_Enabled		
<input type="checkbox"/>	Standard_CTI_Secure_Connection		
<input type="checkbox"/>	Standard_EM_Authentication_Proxy_Rights		
<input type="checkbox"/>	Standard_Packet_Sniffer_Users		
<input type="checkbox"/>	Standard_RealtimeAndTraceCollection		
<input type="checkbox"/>	Standard_TabSync_User		

Figure 4-9 Default User Groups

User Group Configuration		Related Links: Back To Find>List Go
		Copy Add New
Status		
	2 records found	
User Group Information		
Name*	<input type="text" value="Standard_CCM_Super_Users"/>	
User (1 - 2 of 2)		Rows per Page: 50
Find User where <input type="text" value="User ID"/> begins with <input type="text"/> Find Clear Filter		
<input type="checkbox"/> CCMAdministrator	User ID: CCMAdministrator	Full Name: Hart, Permission:
<input type="checkbox"/> dhartmann		Permission:
Add End Users to Group	Add App Users to Group	Select All Clear All Delete Selected

Figure 4-10 User Group Configuration

Figure 4-11 displays the end-user addition to a user group. Click the **Add End Users to Group** button of Figure 4-10 to display the user search page displayed in Figure 4-11. Enter a search string and click **Find**. Choose the user by selecting the check box next to the user, and then click **Add Selected**.

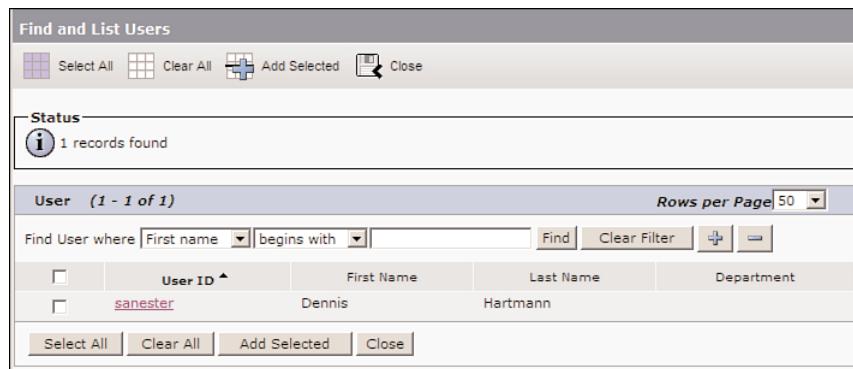


Figure 4-11 User Group Configuration

Assign roles to a user group by selecting the Assign Role to User Group item from the Related Links list box in the upper-right corner of the User Group Configuration page. A new window displays where you can assign or delete roles.

Click the Add Role to Group button. Select the roles that you want to add, as shown in Figure 4-12, and then click the Add Selected button.

Find and List Roles				
<input type="button" value="Add New"/> <input type="button" value="Select All"/> <input type="button" value="Clear All"/> <input type="button" value="Delete Selected"/>				
Find Role where [Name] begins with <input type="text"/> <input type="button" value="Find"/> <input type="button" value="Clear Filter"/>				
Select item or enter search text <input type="text"/>				
Name	Application	Description	Copy	
<input checked="" type="checkbox"/> CCM Read Dial Plan	Cisco Call Manager Administration	Access the AXL APIs	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard AXL API Access	Cisco Call Manager AXL Database	Administer CAR	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard Admin Rep Tool Admin		All users with access to CCM web site	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCM Admin Users		Access to CCM User Option Pages	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCM End Users			<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCM Feature Management	Cisco Call Manager Administration	Standard CCM Feature Management	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCM Gateway Management	Cisco Call Manager Administration	Standard CCM Gateway Management	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCM Phone Management	Cisco Call Manager Administration	Standard CCM Phone Management	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCM Route Plan Management	Cisco Call Manager Administration	Standard CCM Route Plan Management	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCM Service Management	Cisco Call Manager Administration	Standard CCM Service Management	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCM System Management	Cisco Call Manager Administration	Standard CCM System Management	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCM User Management	Cisco Call Manager Administration	Standard CCM User Management	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCM User Privilege Management	Cisco Call Manager Administration	Standard CCM User Privilege Management	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCMADMIN Administration	Cisco Call Manager Administration	Administer all aspects of CCMAdmin system	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCMADMIN Read Only	Cisco Call Manager Administration	Read access to all CCMAdmin resources	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CCMUSER Administration	Cisco Call Manager End User	Administer all aspects of CCMUser system	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CTI Allow Call Monitoring	Cisco Computer Telephone Interface (CTI)	Allow monitoring of calls	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CTI Allow Call Park Monitoring	Cisco Computer Telephone Interface (CTI)	Allow monitoring of call park DNS	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Standard CTI Allow Call Recording	Cisco Computer Telephone Interface (CTI)	Allow recording of calls	<input type="button" value="Copy"/>	<input type="button" value="Delete"/>

Figure 4-12 User Group Role Assignment

Bulk Administration Tool Overview

The Bulk Administration Tool (BAT) is most commonly used when performing configurations that affect multiple users, devices, and other moves, adds, changes, and deletions (MACD). BAT allows management of many devices and records within a short period of time, and eliminates the need for repetitive configuration. A requirement to change the Music on Hold audio source for thousands of lines could be performed with a few

keystrokes. Imagine modifying one parameter across thousands of lines on a one-by-one basis. Cisco Unified Communications Manager BAT does the following:

- Performs bulk transactions to the Cisco Unified Communications Manager database.
- Adds, updates, or deletes phones, users, and features with minimal setup time.
- Exports data (phones, users, gateways, and so on). Exported files can be modified and reimported, simplifying the configuration of comma-separated value (CSV) files.

Note The import and export functions of Cisco Unified Communications Manager BAT can be used to move data records from one CUCM cluster to another. This could be useful when adding a new CUCM cluster to a site that was previously a branch location in a centralized call-processing model. The Disaster Recovery System's (DRS) Restore function includes all server configuration data. Because DRS does not have file-level restore (FLR) functionality, DRS would not be appropriate to move phones across clusters.

- Integrates with the Cisco Unified Communications Manager Administration pages.
- Supports language-based localization.

The Cisco Unified Communications Manager Tool for Auto-Registered Phones Support (TAPS) is also available from the Bulk Administration menu but requires a Cisco Unified Contact Center Express (UCCX) solution to integrate with for script processing. CUCM and UCCX integrate through JTAPI (CTI Manager CUCM Service).

BAT configuration and operation are performed through its own menu within CUCM Administration. This menu allows uploading and downloading files; managing devices, users, and features; and controlling submitted BAT jobs. Earlier versions of CUCM (4.x and prior) had separate administration web pages (similar to CUCM Administration and Cisco Unified Serviceability).

Bulk Administration Tool Components

Cisco Unified Communications Manager BAT templates are used to define general settings that fit a large group of devices that should be added or changed. Comma-separated value (CSV) files are used to define specific settings per device to be bulk configured. Adding, updating, and deleting devices are initiated from the Cisco Unified Communications Manager Administration BAT menu. BAT configuration requests use BAT templates and BAT CSV files. There is a Microsoft Excel template called BAT.xls that can be downloaded from CUCM. BAT.xls greatly simplifies the creation of CSV files used in the BAT operation. Cisco Unified Communications Manager BAT jobs can be executed immediately or scheduled for a later time using the Bulk Provisioning Service (BPS).

Cisco Unified Communications Manager BAT can be used to work with the following types of devices and records:

- Add, update, and delete IP phones, including voice gateway–connected analog phones, CTI ports, and H.323 clients
- Migrate phones from Skinny Client Control Protocol (SCCP) to Session Initiation Protocol (SIP)
- Add, update, and delete users
- Add, update, and delete user device profiles (required for Extension Mobility)
- Add, update, and delete Cisco Unified Communications Manager Assistant (CUMA) and manager associations
- Add or delete various gateways, including Cisco VG200, Catalyst 6624, and Cisco VG224

Note The Cisco Catalyst 6000/6500 WS-X6624 and Cisco VG200 products have reached end of life (EOL).

- Add or delete forced authorization codes (FAC)
- Add or delete client matter codes (CMC)
- Add or delete call pickup groups
- Update or export Cisco Unified Presence (CUP) or Cisco Unified Personal Communicator (CUPC) users
- Export or import user and device configuration information
- Insert, delete, or export remote destinations and remote destination profiles (Cisco Unified Mobile Connect/Single Number Reachability)

Bulk Provisioning Service

Cisco Unified Communications Manager BAT utilizes a dedicated feature service, the Bulk Provisioning Service (BPS), for maintaining and administering submitted Cisco Unified Communications Manager BAT jobs. BPS administers and maintains all jobs that are submitted through BAT. The service is listed under Database Services on the service activation pages, and must be enabled on the publisher for scheduled jobs to execute.

Managing User Accounts Using Cisco Unified Communications Manager BAT

The configuration procedure for BAT includes these steps:

- Step 1.** Configure a Cisco Unified Communications Manager BAT user template. This template is configured with default settings that apply to all users (unless

overwritten in the CSV file). The template might not include any configuration details other than a name. Any configuration information that is applied at the user template level will be applied to every user added with this template. Go to **Bulk Administration > Users > User Template** and enter the name for the template and configure the default user parameters.

- Step 2.** Create the CSV data input file. This file includes the users to be added to the configuration database. For each user, there will be one record containing all settings of the corresponding user. There is a Microsoft Excel BAT.xlt file that can be downloaded from CUCM Administration: **Bulk Administration > Upload/Download Files**. A macro is run in Bat.xlt after clicking the Create Bat Format button after a tabbed page is populated with configuration information such as the number of users to be added. The various tabbed pages include most of the possible BAT configuration options. There are separate tabbed pages for the configuration information of phones, users, users and phones/device association, and so on.
- Step 3.** Upload the CSV data input file after exporting the CSV file from the BAT.xlt file. While it is possible to edit the CSV file manually with the Linux VI or nano text editors, most engineers just don't do that! Use the KISS rule whenever possible! KISS = Keep It Severely Simple or Keep It Simple Stupid. The CSV file we were referring to is actually a .txt file that is formatted as a CSV document. Microsoft Notepad is notorious for inserting hard returns into the document and corrupting the file. It's best to upload the file in CUCM Administration: **Bulk Administration > Upload/Download Files**.
- Step 4.** Configure the Cisco Unified Communications Manager BAT job to add the users. The user template and CSV files are selected from drop-down menus. The BAT job can be executed immediately, but the default radio button selection specifies that the BAT job will be run later. The next step will explain where the jobs can be scheduled: **Bulk Administration > Users > Insert Users**. Select the user template created in Step 1, and then select the CSV file created and uploaded in Step 2. Select whether the job should run immediately or later and click Submit. If you select **Run Later**, you will have to use the Job Scheduler (**Bulk Administration > Find/List Jobs**), which is available under the Bulk Administration menu, to schedule the job.
- Step 5.** Verify the status of the Cisco Unified Communications Manager BAT job by navigating to the following CUCM Administration page: **Bulk Administration > Find/List Jobs**. This is where the status of a job can be checked. BAT jobs that are going to run later are scheduled here as well. BAT jobs are sorted by date and time submission by default. Each BAT job will be displayed with the date and time created, who the job was created by (username), and configuration details (template and CSV file). The details of each job result, including the number of records processed and number of records failed, will be displayed when the job is selected. A log filename will also appear in the job. The log file has further information that can be used to find out why a job failed or why some individual records failed to be inserted into the IDS database.

Lightweight Directory Access Protocol (LDAP) Overview and Considerations

LDAPv3 directories typically store data that does not change often, such as employee information and user privileges on the corporate network. LDAPv3 information is stored in a database that is optimized for a high number of read and search requests and occasional write and update requests.

LDAPv3 Integration

Integration between voice applications and a corporate LDAPv3 directory is a common task for many enterprise IT organizations. Microsoft Active Directory integrations are by far the most popular in the United States, but various LDAPv3 solutions are supported. Various versions of Netscape, Sun One, and Open LDAP LDAPv3 directories are also supported.

LDAPv3 directory services are leveraged to enable user lookups from IP phones. Users can dial a contact directly after looking up the number in the directory. Another common task is to provision users automatically from the corporate directory into the user database of CUCM. This method prevents having to add, remove, or modify core user information manually each time a change occurs in the corporate directory. This could be of considerable concern because Microsoft Active Directory 2003 and 2008 integrations do not support incremental update support. A full synchronization must take place every time a new user is inserted into the Microsoft Active Directory that will need to be placed in the directory services of a Cisco Unified Communications solution.

CallManager 4.x and earlier versions supported incremental update support synchronization, but these earlier versions of the product required schema extensions to the Microsoft Active Directory (AD), and that is a potential nightmare for Microsoft AD administrators who have dealt with a corrupted database before. Windows 2008 R2 server includes a Microsoft Active Directory Best Practices Analyzer (BPA) tool that some readers might find interesting.

Authentication of end users and CUCM administrators using the corporate directory credentials is typically desired. LDAPv3 allows a single sign-on functionality to any applications integrated with the LDAPv3 server. Single Sign On/In used to be referenced by the SSO acronym, but today, SSO is more typically used to describe Non-Stop Forwarding/Stateful Switch Over (NSF/SSO) routing and switching architectures. Single Sign In/On reduces the number of passwords that each user needs to maintain across different applications.

Cisco Unified IP Phones access the LDAPv3 directory when the Directory button on the phone is pressed. The IP phone responds to the Directory button click by sending an HTTP directory lookup request to the Apache web server running on the CUCM Publisher server. The response from CUCM contains Extensible Markup Language (XML)-formatted user information objects that the phone displays to the user. The user can dial the person by pressing the Dial softkey on the phone after selecting the user's name with the phone navigation buttons or touch screen on some models.

Cisco Unified IP Phones perform user lookups against the embedded CUCM database by default, but CUCM supports the following directory integrations as of this writing:

- Microsoft Active Directory (2003 and 2008)
- Microsoft Active Directory Application Mode 2003
- Microsoft Lightweight Directory Services 2008
- iPlanet Directory Server 5.1
- Sun ONE 5.2 and 6.X
- OpenLDAP 2.3.39 and 2.4

CUCM supports two types of LDAPv3 integration. LDAPv3 authentication requires LDAPv3 synchronization to be turned on.

- **LDAPv3 synchronization:** All end users' personal and organizational data is managed in the LDAPv3 directory and synchronized (replicated) to the CUCM IDS database. Directory requests are processed locally on CUCM after synchronization has taken place. Various end user configuration information will no longer be available to change in CUCM Administration.
- **LDAPv3 authentication:** Allows user authentication against an LDAPv3 directory. Passwords are managed in the central LDAPv3 server when LDAPv3 authentication is turned on. The password configuration information will no longer be available through CUCM administration.

Note Application users are not affected by LDAPv3 integration. Application users are always configured and stored in CUCM Administration.

LDAPv3 Synchronization

The Cisco Directory Synchronization (DirSync) process is leveraged to synchronize a number of end-user directory services attributes. The process can be scheduled to run automatically on daily, weekly, and monthly intervals. Directory synchronization can take place immediately with a manual directory synchronization (very useful if you forgot to put one of the senior managers or executives into the system for her first day at work). Users are provisioned on the corporate directory (for example, Microsoft Active Directory) and replicated to the CUCM LDAPv3 database when directory synchronization is activated on the CUCM Serviceability Service Activation page.

LDAPv3 synchronization disallows end-user additions or deletions from CUCM Administration. End users must be added and deleted from the LDAPv3 directory after directory synchronization is enabled. All existing users in the CUCM database must have a matching record in the Microsoft Active Directory system, or they will be marked for deletion and purged from the system after a timer expiry (similar to tombstone timers in Microsoft Active Directory).

End users' personal and organizational data is replicated from the LDAPv3 server to the CUCM publisher. Most replicated user parameters are read-only in CUCM Administration. User passwords and CUCM settings must be configured from CUCM Administration, but all personal and organizational data will be replicated from the LDAPv3 server as read-only (RO) in CUCM.

CUCM user data (associated devices, username, password, PIN, and so on) is stored in the CUCM database. To avoid duplication of effort in the management of user accounts, combine LDAPv3 authentication with LDAPv3 synchronization. CUCM authenticates user credentials against a corporate LDAPv3 directory when using LDAPv3 authentication. End-user passwords are not stored in the CUCM database. All applications requiring passwords will be passed through to the Microsoft Domain Controllers (DC) for password authentication. Applications requiring a PIN (Extension Mobility, Attendant Console logins, and so on) are always authenticated against the CUCM database even if LDAP authentication is configured. User passwords are required to log in to the /ccmuser end-user administration pages.

Synchronization Agreements

LDAPv3 synchronization is performed in one of the following ways:

- Full synchronization is used with Microsoft Active Directory 2003 and 2008. All records are replicated from the LDAPv3 directory to the CUCM database. Full synchronization can cause considerable load on both the Microsoft and Cisco environments in large deployments. Synchronization events should be carefully planned to minimize downtime, network overhead, and high server utilization. It is always best to configure synchronization to occur during periods of low call volume (typically sometime during the night or weekend or both night and weekend when the majority of people are not working—depending on the type of business).
- Incremental synchronization is a method used with all supported directory servers other than Microsoft Active Directory. Only changes are propagated to the CUCM database with the incremental synchronization mechanism. The incremental synchronization method requires fewer resources than the full synchronization method. Microsoft Active Directory synchronizations do not support incremental support. The lack of directory information will not stop a user from being able to use a phone unless there is a requirement for the user to log in to the phone (for example, Extension Mobility). A user would be required for both Cisco Unity and Cisco Unity Connection (with directory synchronization) voicemail/unified messaging deployments. Cisco Unity Connection can synchronize its user database with the CUCM Publisher or directly with Microsoft Active Directory. If Microsoft AD and CUCM are already synchronizing, my preference is to synchronize Unity Connection with CUCM hours or days after the configured Microsoft AD/CUCM synchronization time.

Synchronization agreements are pointers to a domain or subdomain within an LDAPv3 structure. Synchronization agreements have to use the same synchronization method.

One LDAPv3 username attribute (sAMAccountName, uid, mail, or telephoneNumber) has to be mapped to the User ID field of a user in CUCM. This identifier must be unique across all users. If no one knows which AD username attribute is in use, try sAMAccountName. This has worked well for me as I hope it does for you.

Figure 4-13 illustrates the authentication of users against the CUCM database and user lookups from the Cisco IP Phone.

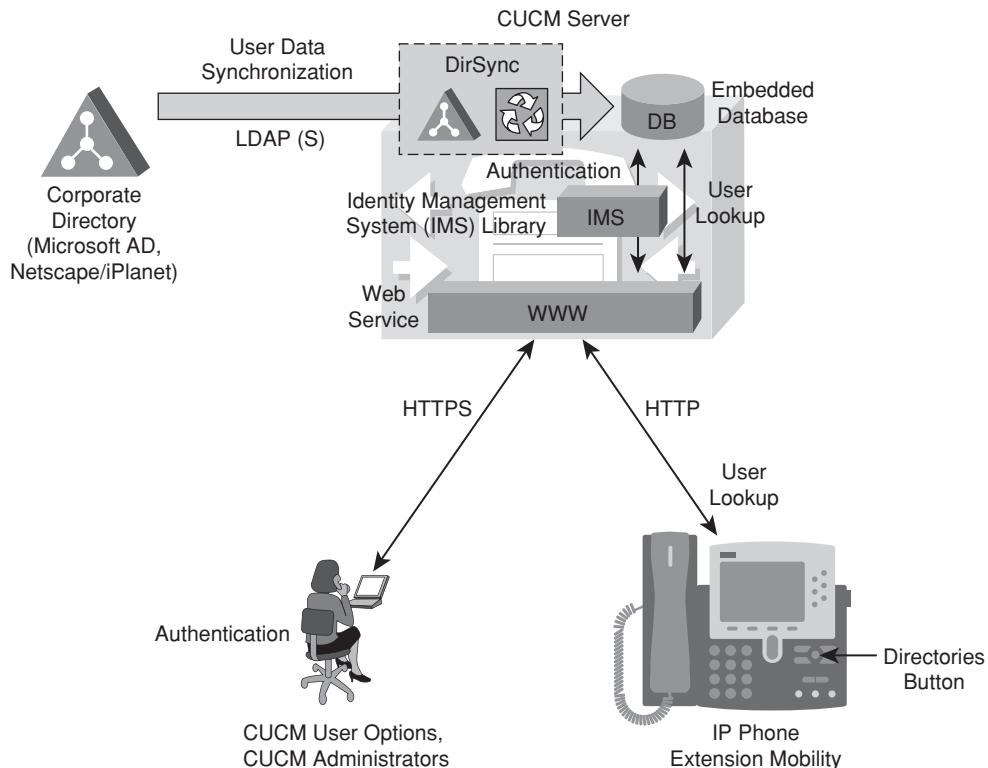


Figure 4-13 *LDAPv3 Synchronization*

The “sn” (last name or surname) attribute in the LDAPv3 server must be populated with data; otherwise, the record will not be imported. The last name is not a required field in small Microsoft Active Directory deployments, and you might find yourself in a scenario where the Microsoft Active Directory must be updated to include the last name in addition to the first name. If the primary attribute used during import of end-user accounts matches any application user in the CUCM database, the user is skipped (should occur rarely if ever).

CUCM database fields provide a choice of directory attributes, but you can choose only a single mapping for each synchronization agreement.

Synchronization Search Base

A synchronization agreement specifies a search base. A search base is an area of the directory that is used for synchronization. The synchronization agreement specifies a position in the directory tree where CUCM begins its search. The search level has access to all levels lower in the tree but not to higher levels in the tree. Users will normally be organized in a structure in the LDAPv3 directory like that shown in Figure 4-14. The existing structure can be used to control the user groups that were imported. A single synchronization agreement can specify the root of the domain, and all users of the domain are synchronized. The search base does not normally point to the domain root unless more than five synchronization agreements are required in the deployment. Organizations that sort their Active Directory domain by site, like that shown in Figure 4-14, would have a five-site limitation.

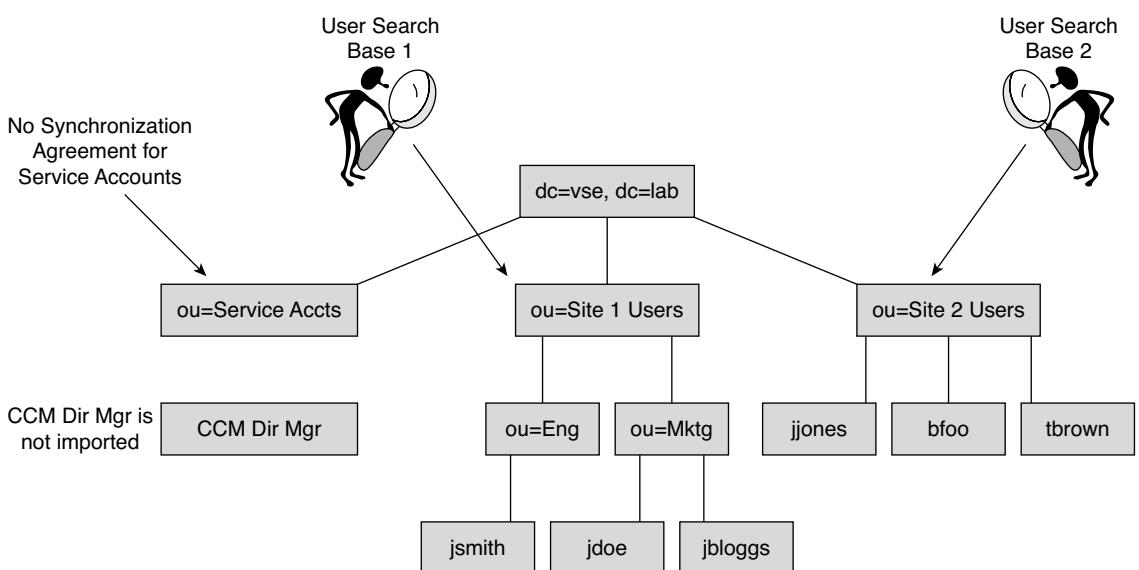


Figure 4-14 User Search Base

In Figure 4-14, two synchronization agreements are represented. One synchronization agreement specifies User Search Base 1 and imports users `jsmith`, `jdoe`, and `jbloggs` from the same root organizational unit (OU) of Site 1 Users. These users are in separate OU containers under the Site 1 Users organizational unit.

Organizational units appear as folders in Microsoft Active Directory Users and Computers (ADUC). Users is the only default OU in Microsoft Active Directory. ADUC is the main point of user administration in Microsoft Active Directory deployments. Microsoft Active Directory is proprietary to Microsoft, but integrations with other vendors are provided in the form of X.500 directory standards-based LDAPv3.

User Search Base 2 in Figure 4-14 represents a second synchronization agreement and imports users jjones, bfoo, and tbrown from the ou Site 2 Users. The CCMDirMgr account is not imported because it does not reside within one of the two specified user search bases. No synchronization agreement has been created to the Service Accts ou because users of the phone system do not want to see systems administration users required for the Information Technology team. Humans are normally only looking for other humans to talk to when they communicate over a telephone.

CUCM performs a bind to the LDAPv3 directory using the LDAPv3 Manager Distinguished Name (DN) in the LDAPv3 directory configuration. The Distinguished Name normally matches the username in the LDAPv3 system. If sanester is the username of someone with domain admin rights, sanester can be used in the user search base. The account used for the LDAPv3 Manager Distinguished Name must be available in the LDAPv3 directory for CUCM to log in. It is recommended that you create a specific account with the permission to at least read only to all user objects within the user search base.

It is possible to control the import of accounts by limiting read permissions of the LDAPv3 Manager Distinguished Name account. For example, if the account is restricted to have read access to ou=Eng but not to ou=Mktg, only the accounts located under the Eng OU will be synchronized.

Synchronization agreements can specify multiple directory servers for redundancy purposes.

Each synchronization agreement is configured with a synchronization start time and a period configured in hours, days, weeks, or months. A synchronization agreement can be configured to run only once.

The synchronization process is as follows:

1. At the beginning of the synchronization process, all existing CUCM end-user accounts are deactivated.
2. If there were any differences in the LDAPv3 server, LDAPv3 user accounts that exist in the CUCM user database are reactivated and their settings are updated.
3. LDAPv3 user accounts that exist in LDAPv3 only are added to the CUCM database and activated.
4. Deactivated accounts are purged from the CUCM database after 24 hours.

Synchronization Best Practices

The account that CUCM uses to read the LDAPv3 directory should be configured in the following way:

- Create a dedicated account used only for synchronization. Set LDAPv3 server permissions for this account to read-only or a higher permissions level for all user objects located below the user search bases specified in the synchronization agreements.

- The password of the account should be set to never expire because this is a service-level account that will not receive a password change notification upon logging in to the system. Password change permission exceptions are normally performed for cross-server authentication purposes.

Synchronization times should be configured during intervals when call activity is lightest. All overhead and management processes in CUCM are scheduled during off-hours to minimize the CPU load overhead incurred as a result. Call-processing impact during business hours is too expensive to the operation of the business to run management tasks during the day. Smaller environments with servers beyond their current requirements should not be too concerned with doing this operation during the day. However, plenty of people have that one story about Bob who did X in the middle of the day on the system—and we all know what happened to Bob.

Different start times should be set to reduce the load on the servers when multiple synchronization agreements are configured. There can be a policy to have one daily backup with a 7-day retention policy, a weekly backup with an 8-week retention policy, and a monthly backup with a 6-month retention policy based on the disaster recovery (DR) plan. This would require three separate synchronization agreements. You would not want to be in the situation where your daily, weekly, and monthly directory synchronizations are all happening at the same time. Setting different synchronization agreement start times makes good sense.

Avoid a single point of failure by configuring at least two LDAPv3 servers, and use IP addresses rather than host names to eliminate Domain Name System (DNS) reliance. Most environments have multiple LDAPv3 servers (Domain Controllers in Microsoft Land).

The connection between the CUCM Publisher server and the directory server can be secured by enabling Secure LDAPv3 (sLDAPv3) on CUCM and the LDAPv3 server. sLDAPv3 enables LDAPv3 end-user attributes to be sent over Secure Socket Layer (SSL) 128-bit level encryption.

LDAPv3 Synchronization Configuration

The LDAPv3 synchronization configuration procedure includes the following steps:

- Step 1.** Add CUCM directory users and assign administrator access rights in the LDAPv3 directory (depends on LDAPv3 directory server).
- Step 2.** Activate the Cisco DirSync service.
- Step 3.** Configure the LDAPv3 system.
- Step 4.** Configure the LDAPv3 directory.

The synchronization is performed by a service in CUCM called Cisco DirSync. DirSync has to be activated on the publisher server because the publisher is the only server in the CUCM cluster with read/write capabilities and information is being inserted into the CUCM IDS database.

The Cisco DirSync service has some service parameters that you can configure from the following CUCM Administration location: **System > Service Parameters**. Choose the Cisco DirSync service from the appropriate server. The service parameters include the maximum number of synchronization agreements, hosts (directory servers), and several timers. This will not be required in most deployments, but might be required in larger environments where LDAP system tuning is very important because of the large nature of the system (scalability).

CUCM Administration: Navigate to **System > LDAPv3 > LDAPv3 System** to configure the LDAPv3 server type (Microsoft Active Directory or other) and the LDAPv3 attribute that should be mapped to the CUCM user ID (many times, this is the sAMAccountName parameter). Select the **Enable Synchronizing from LDAP Server** check box, as shown in Figure 4-15.

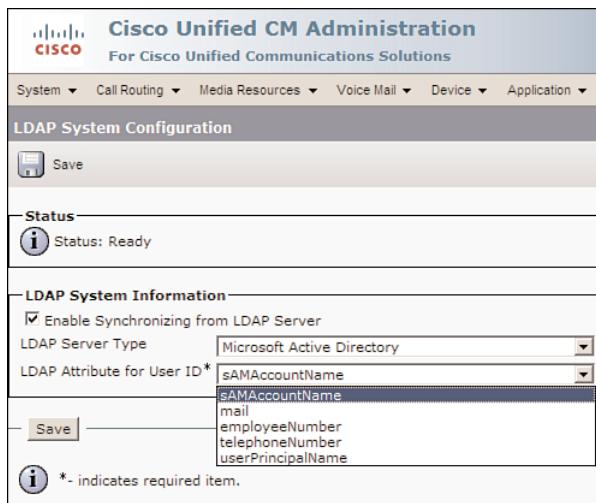


Figure 4-15 *LDAPv3 System Configuration*

The LDAPv3 directory configuration is configured once per synchronization agreement synchronization session. CUCM Administration: Choose **System > LDAPv3 > LDAPv3 Directory** and click **Add New** to add a new synchronization agreement. A warning appears, indicating that all existing end users in the local CUCM user database who are not found in the LDAPv3 directory specified in the synchronization agreement will be deleted. The LDAPv3 directory will overwrite the CUCM user database if the sn (last name) LDAPv3 attribute matches. Figure 4-16 shows the LDAPv3 directory configuration. Depending on the type of LDAPv3 database, various LDAP user fields will be available for selection. These field selections are required whenever the LDAPv3 database has various fields that could be populated with that configuration information (for example, Phone Number can use the “telephoneNumber” or “ipPhone” Active Directory attribute). telephoneNumber is normally populated with the user’s full public switched telephone network (PSTN) 10-digit direct inward dial (DiD) phone number. Phone calls within the CUCM cluster can use abbreviated dialing (for example, 5 digits on net dialing).

Configure search base for
this synchronization agreement

Configure Unified CM directory
user (as configured in LDAP)

LDAP Directory Information LDAP Configuration Name*: White Pine Communications Directory LDAP Manager Distinguished Name*: Directory Manager LDAP Password*: <input type="password"/> Confirm Password*: <input type="password"/> LDAP User Search Base*: ou=EastFishkill, dc=WPHC, dc=Sanester	Related Links: Back to LDAP Directory Find>List Go																				
LDAP Directory Synchronization Schedule Perform Sync Just Once <input type="checkbox"/> Perform a Re-sync Every*: <input type="text"/> DAY Next Re-sync Time (YYYY-MM-DD hh:mm)*: 2008-02-15 00:00																					
User Fields To Be Synchronized <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Cisco Unified Communications Manager User Fields</th> <th>LDAP User Fields</th> <th>Cisco Unified Communications Manager User Fields</th> <th>LDAP User Fields</th> </tr> </thead> <tbody> <tr> <td>User ID</td> <td>sAMAccountName</td> <td>First Name</td> <td>givenName</td> </tr> <tr> <td>Middle Name</td> <td>middleName</td> <td>Last Name</td> <td>sn</td> </tr> <tr> <td>Manager ID</td> <td>manager</td> <td>Department</td> <td>department</td> </tr> <tr> <td>Phone Number</td> <td>telephoneNumber</td> <td>Mail ID</td> <td>mail</td> </tr> </tbody> </table>		Cisco Unified Communications Manager User Fields	LDAP User Fields	Cisco Unified Communications Manager User Fields	LDAP User Fields	User ID	sAMAccountName	First Name	givenName	Middle Name	middleName	Last Name	sn	Manager ID	manager	Department	department	Phone Number	telephoneNumber	Mail ID	mail
Cisco Unified Communications Manager User Fields	LDAP User Fields	Cisco Unified Communications Manager User Fields	LDAP User Fields																		
User ID	sAMAccountName	First Name	givenName																		
Middle Name	middleName	Last Name	sn																		
Manager ID	manager	Department	department																		
Phone Number	telephoneNumber	Mail ID	mail																		
LDAP Server Information Host Name or IP Address for Server*: <input type="text"/> LDAP Port*: 389 <input type="checkbox"/> Use SSL																					

Configure LDAP server(s) Configure synchronization schedule
Configure user field mappings

Figure 4-16 LDAPv3 Directory Configuration

CUCM Administration: Choose **User Management > End User** and check to see whether LDAPv3 synchronization occurred properly. This should be quite easy to do in a lab environment with few or no end users configured, but it will require you to enter users using Microsoft Active Directory Users and Computers (ADUC). Synchronized users in CUCM are marked Active. Inactive users were configured in CUCM, but the last name attribute populated in LDAPv3 did not match (potentially because it's not a required field in Microsoft Active Directory). Inactive users will be deleted after a 24-hour period. Microsoft refers to this 24-hour period as *tombstoning*. Click an active user to view that user's configuration page. Personal and organizational settings cannot be modified, but the password (without LDAP authentication), PIN, digest credentials, and PC association can be changed (CUCM attributes).

LDAPv3 Authentication

When LDAPv3 authentication is enabled, CUCM performs the following tasks:

- End-user passwords are authenticated against the corporate directory.
- End-user passwords are managed in LDAPv3. CUCM Administration will no longer include a password option. Passwords must be changed on the LDAPv3 server.
- End-user passwords are stored only in LDAPv3.

Application users are still authenticated against the local CUCM LDAPv3 database. Application-user passwords are stored only in the local CUCM database, as well as end-user PINs and other CUCM user settings.

In Figure 4-17, LDAPv3 authentication is enabled. End users are authenticated against the LDAPv3 corporate directory, while users of Cisco Unified Communications applications requiring PIN-based logins are authenticated against the local CUCM database. Extension Mobility (EM), Attendant Console (AC), Cisco Agent Desktop (CAD), and Cisco Unified Manager Assistant (CUMA) are examples of applications that require a PIN to be entered from the end user. The PIN is authenticated against the CUCM database, not against the LDAPv3 server. The PIN attribute can be encrypted beginning with the release of CUCM 8.0.

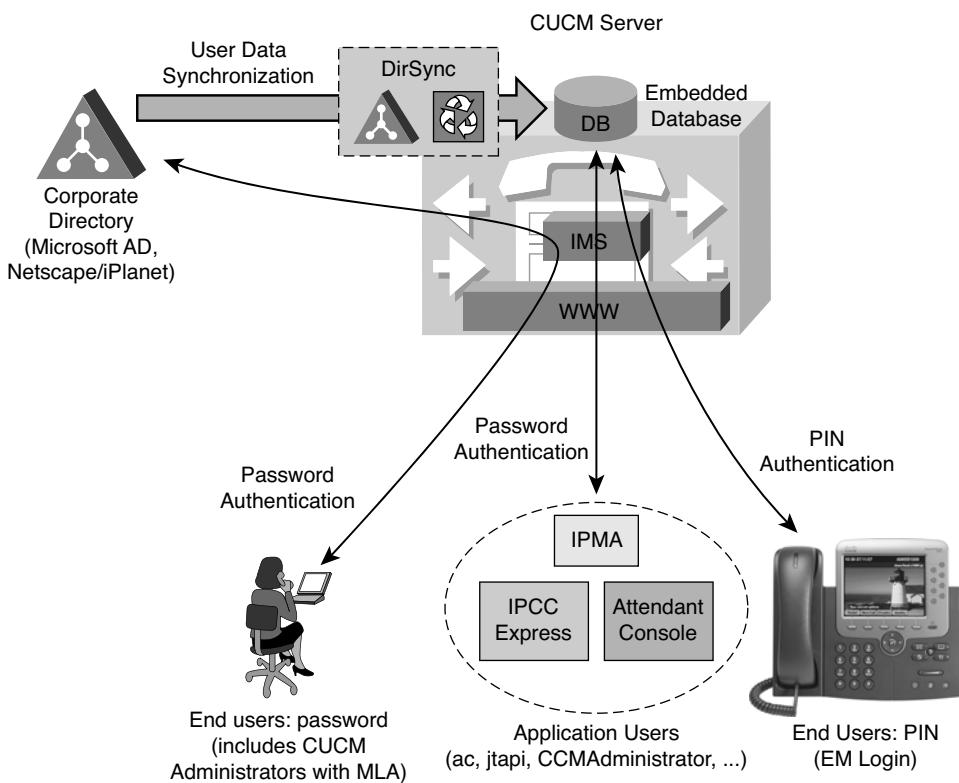


Figure 4-17 LDAPv3 Authentication Overview

It is best practice to configure CUCM to query a Microsoft Active Directory (AD) Global Catalog (GC) server for faster response times. Configure the LDAPv3 server information on the LDAPv3 Authentication page to point to the IP address or host name of a domain controller that has the Global Catalog role enabled, and configure the LDAPv3 port as 3268. This will enable queries against a Microsoft Global Catalog server.

The use of Global Catalog for authentication becomes more efficient if the users belong to multiple Microsoft AD domains. It allows CUCM to authenticate users immediately without having to follow referrals. Point CUCM to a Global Catalog server and set the LDAPv3. Only one user search space can be set in the LDAP authentication, so it is normally a requirement to point the user search base to the root (top) of the domain inverted tree diagram shown in Figure 4-18.

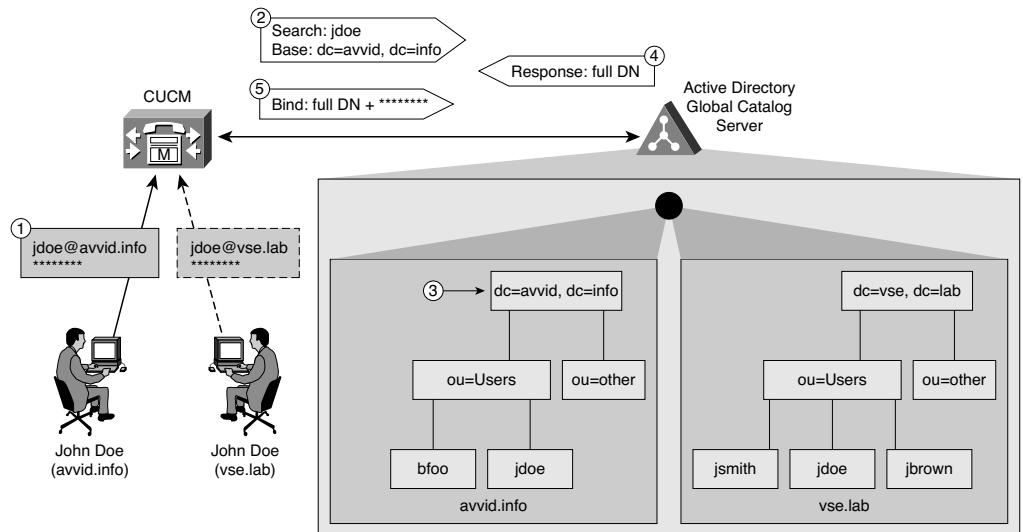


Figure 4-18 LDAPv3 Authentication When Using Microsoft AD with Multiple Domains or Trees

Microsoft AD forests that encompass multiple trees require additional considerations. A single LDAPv3 search base cannot cover multiple namespaces. CUCM must use a different mechanism to authenticate users across discontiguous namespaces.

To support synchronization with an AD forest that has multiple trees, you must use the UserPrincipalName (UPN) attribute as the user ID within CUCM. A user principal name (UPN) is an LDAPv3 attribute that looks like an email address (for example, `jdoe@avvid.info` and `jdoe@vse.lab` in Figure 4-18). The CUCM LDAPv3 authentication configuration page does not allow the LDAPv3 Search Base field when the User ID field uses the UPN. The LDAPv3 configuration page will display the note “LDAPv3 user search base is formed using userid information.”

Figure 4-18 displays a Microsoft AD forest consisting of multiple domains or trees (`avvid.info` and `vse.lab`). The same username can appear in both domains, so CUCM has been configured to use the UPN to uniquely identify users across multiple domains during the authentication process.

The Active Directory Multiple Domain directory search process is as follows:

1. The user authenticates to CUCM through HTTPS with his UPN-based username and password.

2. CUCM performs an LDAPv3 query against a Microsoft AD Global Catalog (GC) server. The username is specified in the UPN (before the @ sign). The LDAPv3 search base is derived from the UPN suffix (after the @ sign—normally a domain suffix). In Figure 4-18, the username is jdoe and the LDAPv3 search base is dc=avvid for one search string and dc=info for the second search string.

Microsoft AD identifies the correct Distinguished Name corresponding to the username in the tree specified by the LDAPv3 query. In this case, “cn=jdoe, ou=Users, dc=avvid, dc=info.”

3. Microsoft Active Directory responds through LDAPv3 to CUCM with the full Distinguished Name for this user.
4. CUCM attempts an LDAPv3 bind with the Distinguished Name provided and the password initially entered by the user. The authentication process then continues as in the standard case.

Support for LDAPv3 authentication with Microsoft AD forests containing multiple trees relies exclusively on the approach just described. Therefore, support is limited to deployments where the UPN suffix of a user corresponds to the root domain of the tree where the user resides. If the UPN suffix is disjointed from the actual namespace of the tree, it is not possible to authenticate CUCM users against the entire Microsoft Active Directory forest.

LDAPv3 Authentication Configuration

The LDAPv3 authentication configuration procedure includes the following steps:

- Step 1.** Add the CUCM directory user and assign administrator access rights in the LDAPv3 directory.
- Step 2.** Configure LDAPv3 authentication. CUCM Administration: Choose **System > LDAPv3 > LDAPv3 Authentication** to configure the CUCM directory user configured in the LDAPv3 directory, the user search base, and the LDAPv3 server(s). Select the **Use LDAP Authentication for End Users** check box, as shown in Figure 4-19. The example would only authenticate users in the EastFishkill organizational unit of the WPHC.sanester domain.

Configure Unified CM directory user (as configured in LDAP)

Cisco Unified CM Administration For Cisco Unified Communications Solutions							
System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administra							
LDAP Authentication							
<input type="button" value="Save"/> Status (i) Status: Ready							
LDAP Authentication for End Users <div style="display: flex; justify-content: space-between;"> <div style="flex-grow: 1;"> <input checked="" type="checkbox"/> Use LDAP Authentication for End Users LDAP Manager Distinguished Name: Directory Manager LDAP Password: ***** Confirm Password: ***** LDAP User Search Base: ou=EastFishkill, dc=WPHC, dc=Sanester </div> <div style="flex-grow: 1;"> LDAP Port*: 389 <input type="checkbox"/> Use SSL </div> </div>							
LDAP Server Information <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;">Host Name or IP Address for Server*</td> <td style="width: 40%; text-align: right;">LDAP Port* <input type="checkbox"/> Use SSL</td> </tr> <tr> <td>192.168.100.240</td> <td style="text-align: right;">389</td> </tr> <tr> <td colspan="2" style="text-align: center; padding-top: 5px;"> <input type="button" value="Add Another Redundant LDAP Server"/> </td> </tr> </table>		Host Name or IP Address for Server*	LDAP Port* <input type="checkbox"/> Use SSL	192.168.100.240	389	<input type="button" value="Add Another Redundant LDAP Server"/>	
Host Name or IP Address for Server*	LDAP Port* <input type="checkbox"/> Use SSL						
192.168.100.240	389						
<input type="button" value="Add Another Redundant LDAP Server"/>							
<input type="button" value="Save"/> (i) * - indicates required item.							

Configure LDAP server(s)

Configure search base
for LDAP authentication**Figure 4-19** LDAPv3 Authentication When Using Microsoft AD

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- CUCM has application users and end users.
- Application and end users can be configured one by one using CUCM Administration.
- Many features, including user administration, can be completed in bulk using the Bulk Administration Tool (BAT).
- LDAPv3 directories are a centralized storage of user information.
- CUCM can integrate with LDAPv3 for user provisioning.
- CUCM can integrate with LDAPv3 for user authentication.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

- 1.** Users are assigned directly to which of the following?
 - a.** User groups
 - b.** Roles
 - c.** Applications
 - d.** Privileges
- 2.** Which of the following contain resources?
 - a.** Users
 - b.** User groups
 - c.** Roles
 - d.** Applications
 - e.** Privileges
- 3.** What type of users are accessible from the Directory button on a Cisco IP Phone?
 - a.** Application users
 - b.** Domain administrators
 - c.** Super users
 - d.** End users
- 4.** What is the name of the technology that CUCM uses for user configuration data by default?
 - a.** SQL Server
 - b.** IDS database
 - c.** LDAPv3
 - d.** Microsoft Active Directory
 - e.** Netscape iPlanet
- 5.** With which system can CUCM synchronize user data?
 - a.** Microsoft Active Directory
 - b.** SQL Server
 - c.** IBM Informix Database Server
 - d.** Microsoft Access database
 - e.** DC Directory Service

- 6.** When synchronizing with Microsoft Active Directory, where does end-user authentication occur?
 - a.** CUCM
 - b.** DC Directory Service
 - c.** Microsoft Active Directory
 - d.** Internet Information Server
 - e.** IBM Informix Database Server
- 7.** When synchronizing with Microsoft Active Directory, where does application-user authentication occur?
 - a.** CUCM
 - b.** DC Directory Service
 - c.** Microsoft Active Directory
 - d.** Internet Information Server
- 8.** What service does Microsoft Active Directory synchronization rely on?
 - a.** LDAPv3
 - b.** IBM Informix Database Server
 - c.** Directory Synchronization
 - d.** CUCM
- 9.** Users cannot be added to the CUCM user database directly when which option is enabled?
 - a.** LDAPv3 Authentication
 - b.** LDAPv3 Synchronization
 - c.** Backup and Restore System
 - d.** LDAPv3 User Search Base

Chapter 5

Cisco Unified Communications Manager Endpoints

An important task of supporting a Cisco Unified Communications (UC) deployment is managing the endpoints. It is important to be able to distinguish between various Cisco UC endpoints that you might encounter during the course of deploying and administering a Cisco Unified Communications Manager (CUCM) network. Understanding the boot and registration communication between a Cisco IP Phone and CUCM can be very valuable for troubleshooting phone registration-related issues.

This chapter describes the various models of Cisco IP Phones and discusses how they work within a Cisco UC solution. The chapter introduces the basic features of Cisco IP Phones, the Cisco IP Phone boot and registration process, and the audio coders-decoders (codecs) that are supported by Cisco IP Phones. The chapter also describes third-party Session Initiation Protocol (SIP) and H.323 endpoints.

Chapter Objectives

Upon completing this chapter, you will be able to describe the general features and unique characteristics of the H.323, Skinny Client Control Protocol (SCCP), and SIP endpoints that interwork with CUCM, and you will be able to meet these objectives:

- Identify the endpoints supported by CUCM.
- Describe the features of Cisco IP Phones.
- Describe the boot sequence of Cisco IP Phones.
- Describe how H.323 endpoints are supported by CUCM.
- Describe how SIP third-party IP phones are supported by CUCM.

CUCM Endpoints

A variety of endpoints, from Cisco and third-party manufacturers, can be used with CUCM. Endpoints include Cisco IP Phones, analog gateways, and video devices. Third-party manufacturer products can be integrated as SIP endpoints, over SIP trunks, or as H.323 terminals, gateways, or gatekeepers. Some H.323 voice and video manufacturers' products can be integrated through a Cisco gatekeeper, while others will be supported natively in CUCM depending on the required feature set support.

CUCM has widespread support for the following protocols to be used for endpoints: SCCP, SIP, and H.323. Figure 5-1 illustrates some of the various protocol options to connect to CUCM. Most Cisco IP Phones support both SCCP and SIP. The Cisco Unified 8900 and 9900 Series IP Phone models exclusively support their entire feature set in the default SIP firmware. Cisco 7900 series Phones ship with SCCP firmware and can be migrated to SIP through the Bulk Administration Tool (BAT), which is covered in Chapter 4, “Managing User Accounts in Cisco Unified Communications Manager.”

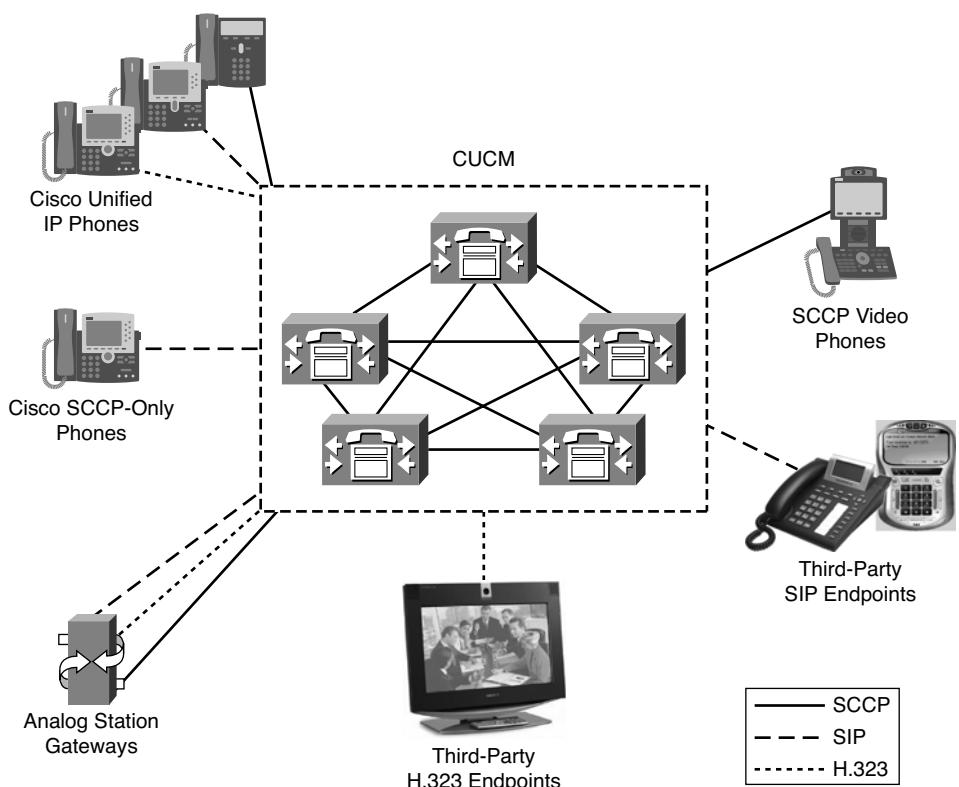


Figure 5-1 CUCM Endpoints

Cisco also offers software-based phones such as the end-of-life (EOL) Cisco IP SoftPhone, Cisco IP Communicator (CIPC), and Cisco Unified Personal Communicator

(CUPC). CIPC looks like a software-based version of the 797x class Cisco IP Phones, with color displays and eight buttons that can be configured with a variety of lines, speed dials, and programmable line key (PLK) features. CIPC has always supported SCCP, and SIP support was added with CIPC 2.1. CUPC requires a Cisco Unified Presence Server (CUPS) to register. The CUPS also performs Computer-Supported Telephony Applications (CSTA) gateway functionality when CUCM is integrated into a Microsoft Office Communication Server (OCS) or Microsoft Lync Unified Communications environment. CUPC is an integrated UC client that operates as a voice, video, and instant messenger (IM) client. CUPC can also be used to promote a voice call into an audio-conference, video call, or videoconference if the network has sufficient components. (Audio-only basic conferencing is covered in Chapter 13, “Media Resources.”) Two-way interactive video calls can be set up natively in CUCM, but videoconferencing between two or more parties requires the purchase of a video-mixing-capable platform like the Cisco Unified Video Conferencing 3500 Series platforms. The Cisco Unified IP Phone 7985 is a high-definition, large-screen desktop videophone, whereas the Cisco Unified IP Phone 792x-based models are wireless LAN (Wi-Fi) phones. The Cisco Unified IP Phone 793x conference stations use licensed Polycom audioconferencing technology. The updated 7937 conference phone supports Power over Ethernet (PoE), while the 7935 and 7936 endpoints required a power brick.

Third-party products are available for most of the supported protocols. Nokia, Windows, and BlackBerry-based mobile phones support the Cisco Unified Mobile Communicator (CUMC) phone client, and there are various phone models available for the Apple iPhone through the App Store. CUMC is a software client that is used on dual-mode mobile phones (cellular and Wi-Fi), allowing cellular PDA phones to register with CUCM over the wireless LAN corporate network. Tandberg and Sony produce various SCCP-enabled video endpoints, and VTGO (IP Blue) offers an SCCP-based software IP phone that emulates standard Cisco 79xx phone lines. Many other third-party endpoints for SIP and H.323 can also be found on the market. X-Lite is an example of a freeware software-based SIP client that can be used in CUCM.

Endpoint Features

The features supported on the Cisco IP Phones vary by the device protocol in which the phone is running. The protocols can be categorized into three groups:

- **SCCP:** SCCP is a Cisco-proprietary protocol and is typically used only by Cisco IP endpoints. Third-party companies such as Sony, Tandberg, and VTGO (IP blue) have licensed SCCP. SCCP offers a rich set of telephony features that are supported on most Cisco handsets.
- **Third-party SIP or H.323:** CUCM supports standards-based SIP and H.323 endpoints. The number of standardized telephony features is limited when compared to the feature richness of SCCP.
- **SIP support for Cisco IP Phones:** Cisco IP Phones using SIP support different features depending on which Cisco IP Phone is used. Cisco SIP Type B phones support

similar features when compared to those supported with SCCP but lack a small portion of the full SCCP-supported feature set. The number of features supported depends significantly on the Cisco IP Phone model being used. Older Type A phones lacked a significant portion of the phone feature set when compared to SCCP because of limited system resources on the first-generation Cisco 7900 Series Phones. The first Cisco 7900 Series Phones were shipping in the year 2000.

Table 5-1 displays the support among various phone types and protocols. Third-party SIP and H.323 endpoints can be used with any other IP telephony devices or systems, including CUCM. Third-party SIP and H.323 endpoints are limited regarding the number of supported telephony features when compared to Cisco SIP or SCCP IP Phones.

Table 5-1 *Endpoint Support*

	Third-Party SIP	Cisco IP Phone SIP	SCCP	Third-Party H.323
Third-party PBX support	Yes	No	No	Yes
Feature support	Small	Medium to large	Large	Large
Supported phones	Third-party	All Cisco phones	All Cisco phones Third-party SCCP phones	Third-party

The Cisco Unified IP Phone Models 7940 and 7960 can be loaded with a special firmware that provides RFC 3261 SIP support for third-party PBX systems. When these models interact with CUCM, both SIP and SCCP implementations provide more features than the phones operating on a third-party SIP proxy server. This option is sometimes used by customers who connect to other IP communication systems (such as Vonage) but want to take advantage of the superior voice quality and look and feel of the Cisco IP Phones. Some Internet telephony service providers (ITSP), offering standard SIP telephony services, provide their customers with preconfigured Cisco Unified IP Phone Models 7940 or 7960 to be used to connect to their SIP proxy servers.

The Cisco Unified IP Phone Models 7905 and 7912 can also be loaded with an H.323 firmware to be used with third-party PBX vendors using H.323. These phones are end of life. Cisco has not created any other phones that accept an H.323-based firmware image.

Cisco IP Phones with SIP support a different number of features depending on whether the phone is a Type A or B model. Type A models include the 7905, 7912, 7940, and 7960. Type A phones support a large number of features but many fewer features than SCCP. The Type A phones also have a different screen appearance when compared to their Type B SCCP counterparts. Type B SIP phones support many more features than Type A SIP phones but have near-feature parity when using SCCP.

Cisco IP Phone Models

Cisco IP Phones range from entry-level phones employing a single directory number, one-way speakerphones, and no display to high-end phones with high-resolution, color, touch-screen displays and Gigabit Ethernet connectivity. Differences in hardware capabilities include the following:

- **Screen:** Different models have screens with different resolution, size, color, and touch-screen capabilities.
- **Codec support:** All Cisco IP Phones support G.711 and G.729 codecs. Most of the Cisco IP Phones support the Cisco wideband audio codec. All Type B phone models support the G.711, G.729, and Internet low-bandwidth codec (iLBC) at 15.2 kbps, and the G.722 wideband audio codec at 64 kbps. The G.722 audio codec requires a high-fidelity handset that ships only with the 79x2 and 79x5 and later phone models. Other Type B phones require a high-fidelity handset upgrade to support the G.722 audio codec. G.722 has a 16-kHz frequency response range, while G.711 has approximately a 4-kHz frequency response range. G.722 is not called high-definition audio, but it has much higher clarity when compared with G.711. Some users experience the audio change as sounding robotic.
- **LAN:** Most Cisco IP Phones have a PC port so that a PC can be connected to the network without requiring its own switch port. Different phone models support different speeds on the PC and switch port of the IP phone.
- **Phone buttons:** The number of IP phone buttons differs per phone model. The 794x series phones have two buttons, while the 796x phones have six buttons and the 797x phones have eight buttons.
- **Speakerphone and headset support:** Most Cisco IP Phones offer speakerphone and headset support.
- **Number of lines:** The number of lines varies per phone model from one to eight. Twenty-eight lines can be added to most of the phones with the 7914 sidecar modules. The 7914 sidecar module has been replaced by the 7915 and 7916 sidecar modules that provide 12 buttons and an A/B button, providing a total of 24 unique, configurable buttons. The 7915 is a black-and-white LCD, while the 7916 is a color LCD.
- **Other features:** Some IP phones provide other special features such as video, Wi-Fi support, or dedicated support for use in conference rooms. The 7936 and 7937 phones support external microphones to provide coverage to large conference rooms.

Entry-Level Cisco IP Phones

The Cisco Unified IP Phone Models 7906 and 7911 fill the communication needs of cubicles, retail, classrooms, or manufacturing. These phones are satisfactory to users conducting low to moderate telephone traffic without the use of advanced features. Four dynamic softkeys guide users through core business features and functions, while a pixel-based display combines intuitive features, calling information, and XML services allowing IP phone service applications.

The Type B entry-level phones mentioned support security features, including encrypted signaling and media. Encrypted voice traffic and security concepts are covered in the Cisco Press book *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide*. All Type B entry-level phones support IEEE 802.3af Power over Ethernet (PoE), Cisco in-line power, or local power through an optional power adapter.

Midrange Cisco IP Phones

Midrange Cisco Unified IP Phones (Models 7940, 7941, 7942, 7960, 7961, and 7962) address the communications needs of those who make frequent use of the phone system. Users providing a majority of their business services through telephone communications normally require a phone with more features than the entry-level phones. They provide a high-quality speakerphone and four dynamic softkeys that guide users through call features and functions. A built-in headset port and an integrated Ethernet switch are standard with these phones. The phones also include audio controls for the full-duplex, high-quality, hands-free speakerphone, handset, and headset.

All Type B phone models have LED-based line keys that allow call states to be represented by different line colors. Type B phones also support the iLBC and G.722 audio codecs.

Note For a detailed list of features per phone model, see the data sheets for the Cisco Unified IP Phone 7900 Series products.

High-End Cisco IP Phones

High-end Cisco Unified IP Phones include the Models 7945, 7965, 7970, 7971, and 7975. These phones include G.722 wideband audio support, backlit color display, and an integrated Gigabit Ethernet chipset. They address the needs of executives and managers with significant phone traffic.

All Cisco IP Phones include a display for easy access to communication information, date and time display, calling party name and number, called party name and number, and presence information. The Cisco IP Phones also accommodate XML applications that take advantage of the display. The phones provide direct access to two to eight telephone lines (or a combination of lines, speed dials, and direct access to telephony features), four or five interactive softkeys that guide you through call features and functions, and an intuitive four-way (plus Select key) navigation cluster. A hands-free speakerphone and handset designed for high-fidelity wideband audio are standard, as is a built-in headset connection. XML and presence are covered in more detail in later chapters.

Cisco Unified IP Phone 8900 Series

The new Cisco Phone lineup, including the 8900 and 9900 Series endpoints, is the next generation of phones and collaboration. Each series offers advanced features, such as high-resolution color displays, Bluetooth, and even wireless capabilities. The Cisco

Unified IP Phone 8900 Series delivers rich multimedia communications and advanced features in an elegant ergonomic design that is both user- and eco-friendly. The Cisco 8900 and 9900 Series phones only support a SIP protocol stack. SCCP is not supported on the Cisco 8900 and 9900 Series IP Phones. CUCM provides signaling conversion between SCCP and SIP endpoints, allowing different generations of Cisco devices to communicate seamlessly. CUCM provides the signaling protocol conversion when setting up communication between two devices running two different signaling protocol stacks. The following signaling protocols are supported in CUCM: SCCP, SIP, H.323, and Media Gateway Control Protocol (MGCP).

Features and benefits include the following:

- Large, backlit, vibrant, high-resolution, fully adjustable color display enhances user experience with easy viewing.
- One standard USB 2.0 port supports USB wired headsets for greater choice and convenience.
- High-definition voice (HD voice) for greater clarity in communications.
- Gigabit Ethernet switch ports support colocation of a multimedia PC for reduced infrastructure costs.
- Tricolor illuminated LED line/feature keys support at-a-glance status for both primary and shared lines.
- XML and MIDlet applications transform business processes and enrich the user experience.
- One Cisco Unified IP Color Key Expansion Module for added scalability of programmable line/feature keys.
- Two color options and handset styles increase flexibility and comfort.
- A display capable of right-to-left language presentation enhances the user experience.
- Rounded ergonomic keys for increased accuracy in interaction.
- Eco-friendly features include
 - Reground and recyclable plastics.
 - Deep-Sleep power option reduces power consumption by up to 90 percent in off-hours compared to the phone in the active state during the workday for energy cost savings.

Cisco Unified IP Phone 9900 Series

Accelerate decision making with the addition of high-performance business video directly from your desk phone. The Cisco Unified IP Phone 9900 Series delivers high-quality, interactive multimedia communications and advanced features in an elegant ergonomic design that is user- and eco-friendly.

Features and benefits include the following:

- Interactive high-performance business video elevates and personalizes communications (requires Cisco Unified Video Camera).
- Large, backlit, vibrant, high-resolution, fully adjustable color displays enrich the user experience for easy viewing.
- Bluetooth 2.0 headsets add freedom at the desk.
- Dual standard USB 2.0 ports support USB wired headsets for greater choice and convenience.
- High-definition voice (HD voice) provides greater clarity in communications.
- Gigabit Ethernet switch ports enable colocation of a multimedia PC for reduced infrastructure costs.
- Tricolor illuminated LED line/feature keys support at-a-glance status for primary and shared lines.
- XML and MIDlet applications add business value.
- Cisco Unified IP Color Key Expansion Module adds scalability with additional programmable line/feature keys.
- Two color options and handset styles increase flexibility and comfort.
- Eco-friendly features include
 - Recyclable plastics.
 - Deep-Sleep power option reduces power consumption up to 90 percent in off-hours compared to the phone in active state during the workday.

Other Cisco IP Phones

Other Cisco Unified IP Phones and endpoints include the following models:

- **Cisco Unified IP Phone 7985:** The 7985 is a personal desktop videophone for the Cisco UC solution. The Cisco Unified IP Phone 7985 offers executives and managers a productivity-enhancing videophone that enables instant, face-to-face communication between physically disparate locations. The 7985 contains a video camera, LCD screen, speaker, keypad, and handset incorporated into one easy-to-use unit.
- **Cisco Unified IP Conference Station 7937:** This conference station combines speakerphone-conferencing technologies with Cisco Unified Communications technologies. The 7937 is an IP-based, hands-free conference station that supports the IEEE 802.3af Power over Ethernet (PoE) standard. The Cisco Unified IP Conference Station 7937 is a Cisco-designed conference room solution that has a much newer look and feel compared to the 7936 Phone based on Polycom technology. The 7935 and 7936 conference phones required the purchase of power bricks because they did not support the IEEE PoE standard.

- **Cisco Unified Wireless IP Phone 792x:** The 792x-class Phones provide a communications solution leveraging the corporate wireless infrastructure. These wireless local-area network (WLAN) phones support a host of calling features and voice-quality enhancements. The 7925G Phone is the latest wireless phone at the time of this writing. The 7925G Phone supports the IEEE 802.3a/b/g WLAN standards.
- **Cisco Unified IP Phone 7931:** The 7931 Phone meets the communication needs of retail, commercial, and manufacturing workers, and anyone with moderate telephone traffic but specific call requirements. Dedicated hold, redial, and transfer keys facilitate call handling in a retail environment. Illuminated mute and speakerphone keys give a clear indication of speaker status. A pixel-based display with a white backlight makes calling information easy to see and delivers a large number of physical buttons that can be used for lines and speed dials.

Cisco IP Phones integrate seamlessly into a Cisco Unified network infrastructure. Cisco IP Phones provide the following network-related features:

- **Cisco Discovery Protocol (CDP) version 2:** Cisco IP Phones send and receive CDP messages, which comprise the communication method used between the IP Phone and the Cisco switch. Cisco Catalyst switches communicate the phone's voice VLAN configuration to the phone over CDP by default. CDP is useful for physical later troubleshooting on the Cisco switches. The switch administrator can tell what Cisco device is plugged into the port. The IEEE 802.1ab Link Layer Discovery Protocol/Multi-Endpoint Discovery (LLDP-MED) standard has standardized a similar, industry-standard network device discovery protocol that is turned on by default in Microsoft Vista and Microsoft Windows 7 operating systems. IEEE 802.1ab support is included in most Cisco Type B phone configurations in CUCM, and most Cisco switches also support IEEE 802.1ab and CDP. CDP is also useful for tracking telephony devices by Cisco Emergency Responder (CER) when 911 is called. CER is an enhanced 911 server that finds mobile users in a dynamic work environment. The CER server is notified by CUCM when there is a new phone registration in the cluster. CER contacts the switches and routers to physically find the device. CDP announcements from the IP phone and IP Communicator make this discovery process viable. The Cisco Unified Video Advantage (CUVA), Cisco Unified Personal Communicator (CUPC), Cisco IP Communicator (CIPC), Cisco Supervisor Desktop (CSD), and Cisco Agent Desktop (CAD) clients also add CDP to the network interface card (NIC) mapping so that CER can easily find the physical location of a device that dialed 911. This information can also be necessary when troubleshooting the network.
- **DHCP:** Cisco IP Phones can have static IP configurations entered at the IP phone or dynamic IP addresses assigned from a DHCP server. Cisco IP Phones default to DHCP dynamic discovery. Manual VLAN configuration must be performed individually on each phone handset. DHCP is appropriate for most environments.
- **MAC address-based device identification:** Cisco IP Phones are identified by the burned-in MAC address of the IP phone. This allows the device to be moved between subnets and simplifies DHCP configuration because no specific IP address is required for an individual phone.

- **TFTP:** Cisco IP Phone configurations are downloaded from the TFTP server component in CUCM. CUCM dynamically generates device-specific configuration files based on the configurations performed in CUCM Administration. Cisco IP Phones obtain the IP address of the TFTP server through a DHCP option (option 150) provided to the phone at the time that the phone requested an IP address from the DHCP server. DHCP clients send a Layer 2 MAC address broadcast at boot time using the “all Fs” destination MAC address (FF-FF-FF-FF-FF-FF). The Layer 2 broadcast is processed by the DHCP server, and the DHCP server allocates an IP address from the DHCP Scope (subnet in CUCM Administration). A phone sends a configuration file request to the DHCP server using the phones’ burned-in MAC address as the name for the configuration file. A phone with a MAC address of 012345012345 will request a configuration file prefixed with SEP (Selsius Ethernet Port) and appended with cnf.xml. The SEP012345012345.cnf.xml filename will be cached in DRAM on the CUCM server(s) running the TFTP service. All configuration files are based on XML.
- **PoE:** Cisco IP Phones do not require a power brick connected to AC power. Cisco IP Phones are normally provided with power over the cabled infrastructure (similar to 48VDC delivery over legacy copper cabling). A Power over Ethernet (PoE)-capable LAN switch is required to provide power to the Cisco phones. Various Cisco Catalyst switches provide PoE in different capacities and using different PoE standards. Old Catalyst switches provided the Cisco 10-watt proprietary power solution only. The Cisco 10-watt power standard was adequate for Type A first-generation Cisco Phones, but most high-end color LCD phones require more than 10 watts of power. Newer Cisco switches provide both IEEE 802.3af (15.4 watts) and the Cisco 10-watt prestandard power. PoE allows power backup in a centralized location. Phone systems are normally protected with uninterruptible power supply (UPS) units to ensure a minimum amount of uptime in the case of a power failure.
- **PC port:** Cisco IP Phones allow PCs to be connected through the IP phone and share the same switch port, as well as share the unshielded twisted-pair (UTP) cabling infrastructure. People typically refer to UTP as Category 5 or Category 6 cabling, but Category 7 is already a standard as of this writing. The voice VLAN feature is configured on the Cisco Catalyst switches and is then downloaded to the Application Specific Integrated Circuit (ASIC) of the Cisco IP Phones. This close tying of the Layer 2 network infrastructure to the telephony solution has allowed Cisco to separate itself from many of its competitors. Voice and data traffic is easily separated by configuring the network layer. The telecom and network team should work together to configure a strategy. After the network infrastructure is programmed with the proper voice VLANS, end users can migrate their Cisco IP Phone connection to another location without the overhead of a change to the phone system configuration. Mobile users can benefit from the device mobility feature that was released in CUCM 6.0. Device mobility will dynamically assign certain device pool configuration data based on the IP subnet of the phone. The IP subnets are related to the geographical location of the phone, which enables the dynamic assignment of certain device pool parameters. Device mobility is covered in detail in *Implementing Cisco Unified*

Communications Manager, Part 2 (CIPT2) Foundation Learning Guide, and device pools are explained in Chapter 7, “Implementing and Hardening IP Phones.”

Cisco IP Phones: Boot Sequence

The Cisco IP Phone has a standard startup process consisting of several steps. The steps are illustrated in Figure 5-2 and outlined in the list that follows.

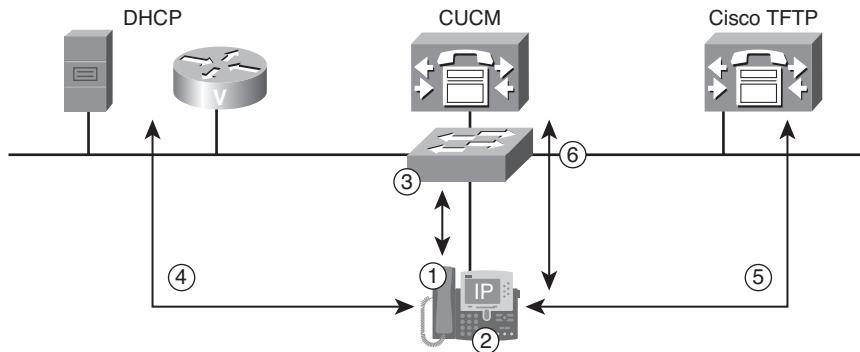


Figure 5-2 Cisco IP Phone: SCCP Boot Process

- Step 1.** PoE: The Cisco IP Phone obtains power from the switch. The switch continuously sends a small voltage on the transmit pins. The voltage sent by the switch is then looped back in hardware from the Cisco IP Phone to the switch’s receiving pins. The switch has now detected an in-line power-requiring device, and the Cisco switch generates the port’s default power allocation. The default power allocation is 10 watts with Cisco-proprietary PoE and 15.4 watts with the IEEE 802.3af in-line power specification. Type B Cisco phones support IEEE 802.3af PoE and Cisco power, but the IEEE specification did not exist when Cisco manufactured the Type A phones. Certain phones and devices have power requirements above 15.4 watts. The IEEE 802.3at standardized PoE of up to 30 watts per port, which should be enough power for future UC, security, wireless, and digital signage technologies (not to mention the ones that we have not yet thought of). Most Cisco IP Phones support IEEE 802.3af and the Cisco original Power over Ethernet (PoE) standard, but most color LCD screen-based phones have power requirements above the original Cisco 10-watt specification. The Cisco Enhanced PoE standard supplies up to 20 watts per port. Twenty watts of power was required for one of the Cisco first-generation 802.11n wireless devices.
- Step 2.** Loading the stored phone image: The Cisco IP Phone has NVRAM memory where the phone’s firmware image (Load ID) is stored. The firmware image is sometimes referred to as the phone’s operating system, the phone’s load, or the phone’s binary image. Most of the images end in .sbin to indicate that

they are digitally signed binary image files. The phone runs a bootstrap loader that loads the phone image from flash memory. Using this binary image, the phone initializes its software and hardware.

Step 3. **Configuring VLAN:** A Cisco Catalyst switch uses CDP to inform the Cisco IP Phone which voice VLAN the phone should use for all Voice over IP (VoIP) traffic. An ASIC in the phone's hardware is used to create Ethernet 802.1q frames before transmitting the Ethernet traffic on the switch port. The ASIC also gives the phone 1p3q1t (one priority queue, three normal queues, and one drop threshold) QoS capabilities and allows the phone to act like a three-port switch. The Cisco IP Phone does not support the weighted random early detection (WRED) congestion-avoidance protocol. The one threshold is set to tail-drop at 100 percent queue utilization. QoS on the Cisco IP Phone is a slightly ridiculous conversation because the 100- or 1000-Mbps port will be oversubscribed by a maximum RTP media stream of under 100 kbps.

Step 4. **Obtaining an IP address:** Cisco IP Phones use DHCP by default to obtain an IP address, subnet mask, default gateway, and TFTP server (option 150). The phone sends out a Layer 2 broadcast to the Ethernet Layer 2 broadcast address of FF-FF-FF-FF-FF-FF. The DHCP server receives this broadcast and returns an IP address lease from the DHCP scope for the Cisco IP Phones, which contains an IP address, default gateway, subnet mask, and TFTP server (option 150). If DHCP is not used in the network, a static network configuration must be assigned to each IP phone locally. If the DHCP server does not respond, the IP phone will make use of the DHCP-obtained information stored in NVRAM. DHCP information will be in NVRAM only if the phone has previously obtained a lease from the DHCP server.

Step 5. **Requesting the configuration file and the profile file:** The TFTP server has configuration files. A configuration file includes parameters for connecting to CUCM and information about which image load a phone should be running.

The IP phone first requests its SEP<*mac-address*>.cnf.xml file from the TFTP server. If the TFTP server does not respond, the IP phone falls back to the last used configuration stored in NVRAM. If the TFTP server responds, but the SEP<*mac-address*>.cnf.xml file is not found on the server, the phone requests the XMLDefault.cnf.xml file. The XMLDefault.cnf.xml file is used to request an autoregistration configuration. Autoregistration is disabled by default. CUCM dynamically generates a directory number and configuration file for the IP phone if autoregistration has been provisioned.

If cryptographic features are enabled in CUCM, the phone then attempts to download a certificate trust list (CTL) in addition to the phone configuration file. CTL files are not implemented in most standard deployments.

Step 6. **Registering:** The configuration file includes a prioritized list of CUCM servers that are configured in CUCM as a CM Group. The Cisco IP Phone attempts to register with the highest-priority CUCM in the CM Group configuration.

The boot sequences for SIP phones are similar to those used for SCCP phones. There are three main differences:

- **SEP<mac>.cnf.xml:** The SIP phones get their entire configuration from the configuration file. The SEP<mac-address>.cnf.xml file is much larger for SIP than for SCCP. The SIP protocol stack is generally larger than the equivalent feature set in the SCCP protocol stack. Because of limited system resources in a Type A phone, a portion of the CUCM SCCP phone feature set could not be enabled in Type A phones converted to SIP. Type B phones offer much closer feature parity between the SCCP and SIP protocol stacks.
- **Dial plan file (optional):** The Cisco SIP phones can download and use local dial plans. Third-party SIP phones can be configured with local dial plans, but they cannot be configured and downloaded from CUCM. Third-party phone configuration takes place on the third-party device. Dial plan files have the ability to increase scalability of the CUCM system and reduce postdial delay for users that are geographically distant from the CUCM subscriber server setting up their phone call. The Cisco IP Phone will evaluate dialed digits locally against the dial plan file when one is in use. This will reduce a lot of the signaling “chattiness” of SCCP that CUCM will not have to process on a real-time basis. Class of service rejections can be performed at the handset level, leaving CUCM’s CPU idle to perform other work. Unfortunately, dial plan files can only be used on SIP-based phones. Dial plan files would be especially effective when the users of the phone system are very geographically far away from the CUCM system (for example, Josh Finke calling from Sydney, Australia, to a Dennis E. Hartmann in Hong Kong, China, using a CUCM system located in San Jose, California).
- **Softkey file:** The SIP phones download their softkey sets in an XML softkey file, while SCCP phones receive these softkey states in the real-time signaling sent using SCCP (TCP port 2000).

Steps 1 through 4 of the Cisco IP Phone boot process using SCCP are identical when using the SIP signaling protocol. Figure 5-2 illustrates a high-level overview of the phone’s boot process, while Figure 5-3 offers a more detailed synopsis of the communication between the Cisco IP Phone with the TFTP server and its primary CUCM server in the CM Group configuration downloaded in the phone’s configuration file.

The following list assumes that the SIP phone has already obtained power, the voice VLAN, and IP addressing information from the DHCP server:

- Step 1.** The SIP phone boots and downloads a certificate trust list (CTL) file from the TFTP server if the CTL provider service is turned on in the publisher server. The CTL provider and Certificate Authority Proxy Function (CAPF) services would need to be turned on in the publisher server to create a public-key infrastructure (PKI) in the CUCM telephony environment. The CTL file contains a set of X.509v3 certificates and is used only when CUCM cluster security has been enabled. Cluster security using digital certificates, Secure Skinny Client Control Protocol (SSCCP), and Secure Real-Time Transport Protocol (SRTP) are not covered further in this book.

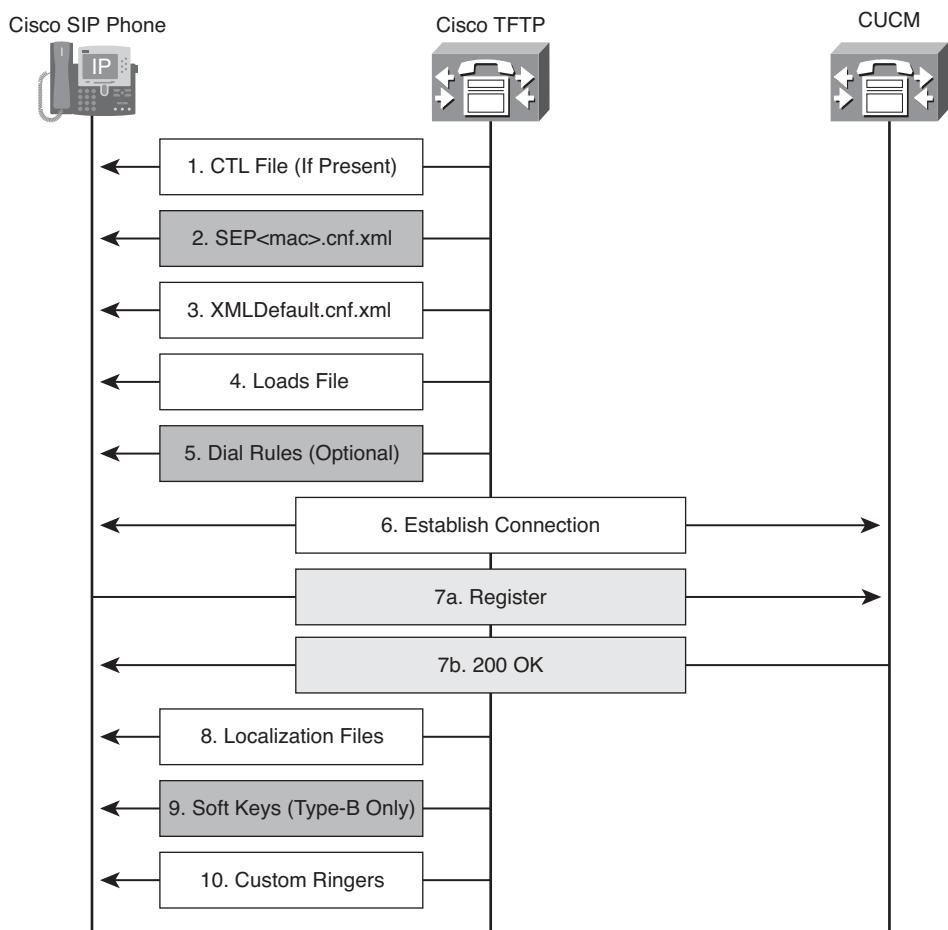


Figure 5-3 Cisco IP Phone: SIP Boot Process

- Step 2.** The SIP phone requests its `SEP<mac-address>.cnf.xml` configuration file from the Cisco TFTP server.
- Step 3.** If the SIP phone has not been provisioned before boot time, the SIP phone downloads the default configuration `XMLDefault.cnf.xml` file from the TFTP server. The default configuration file is used only if autoregistration has been enabled. Autoregistration using SIP requires a file containing a parameter called `auto_registration_name`. If this parameter is blank, the SIP phone will not autoregister. If this parameter is not blank, the SIP phone will attempt to autoregister. Deployments not using autoregistration would have preexisting phone configuration files based on Bulk Administration Tool (BAT) preprovisioning.
- Step 4.** The SIP phone requests a firmware upgrade (Load ID file), if one was specified in the configuration file. This process allows the phone to upgrade the

firmware image automatically when required for a new version of CUCM. Each version of CUCM updates the firmware of the Cisco IP Phones so that they can communicate with CUCM. After the image has been downloaded and authenticated using the Cisco manufacturing self-signed X.509v3 certificate, the SIP phone reboots to load the new image. This process might require many reboots to incrementally upgrade the firmware of the Cisco IP Phone.

- Step 5.** The Cisco IP Phone registers with the highest-priority CUCM server. The default SIP configuration file indicates whether the SIP phone should connect using User Datagram Protocol (UDP) port 5060 (default) or TCP port 5060. The TCP transport layer is supported and configurable on Cisco Type B phones only.

Booting for Type B Cisco IP Phones is slightly different from this procedure, which describes the boot sequence of Type A Cisco IP Phones. Type B Cisco IP Phones first download the SIPdefault.cnf file, which contains the default configuration parameters shared by all SIP phones that use the TFTP server. The Cisco SIP Phone continues requesting the SIP<mac>.cnf file to receive its individual configuration file.

H.323 Endpoint Support

H.323 phones support multiple lines and can be audio, video, or data networking endpoints. H.323 terminals are synonymous with endpoints. The H.323 terminal language is used in the H.323 standard. CUCM supports voice calls from H.323 terminals natively. CUCM can also integrate with H.323 video endpoints using an H.323 gatekeeper.

Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide explains the H.323 video integration in further detail.

H.323 phones do not register with CUCM. H.323 devices are configured by IP address or fully qualified domain name (FQDN). H.323 gateways always show an unknown registration status in CUCM. An unregistered Media Gateway Control Protocol (MGCP) is a bad thing, but unknown H.323 gateways are of no concern. Working H.323 gateways always show up as unknown because there is no shared state information between the H.323 gateway and CUCM. CUCM directs calls to the IP address of the H.323 gateway and accepts calls from the H.323 gateway over the H.225 call-control signaling (TCP port 1720). There is no further integration with either H.323 gateways or gatekeepers. Third-party H.323 devices (terminals, gateways, and gatekeepers) can register with the gatekeeper or integrate directly with CUCM. Be sure to use a logical loopback interface on the gateway router as the IP address of the Cisco router. The Cisco router's H.323 configuration should force the loopback interface to be used as the source interface when communicating to the CUCM server. This can be configured with the **h323-gateway voip bind srcaddr** Cisco IOS interface configuration mode command. Configuration of H.323 devices must be performed on both CUCM and on the phone itself. Dial plan configuration must be configured on each device. Third-party H.323 phones consume two device license units (DLU) in CUCM licensing.

Examples of H.323 terminals include Microsoft NetMeeting and H.323 video devices from Sony, Polycom, and Tandberg. H.323 endpoints often register with H.323 gatekeepers. H.323 gatekeepers contain dial plan elements and allow the devices to perform dynamic e.164 aliasing. Dynamic e.164 aliasing is a process in which the user specifies the phone number that the terminal or gateway device is in charge of. The gatekeeper dynamically loads a dial plan configuration based on the device phone number specified.

H.323 endpoints support a small subset of features compared to Cisco IP Phones using SCCP or SIP. The features that are not supported include, but are not limited to, the following:

- H.323 phones need to be configured by their IP address in CUCM rather than by a MAC address-based device ID. SIP third-party endpoints require digest authentication (DA). Third-party SIP endpoints do not register through their MAC address, but Cisco IP Phones using a SIP protocol stack register with CUCM through the MAC address.
- Phone button templates and softkey templates are not supported in third-party H.323 or SIP devices. Each device's user interface varies by vendor and product.
- Telephony features and applications such as the following:
 - Phone services
 - Cisco Unified Manager Assistant (CUMA)
 - Cisco Unified Video Advantage (CUVA)
 - Call pickup
 - Barge
 - Presence

The high-level configuration steps for H.323 phone implementation are as follows:

- Step 1.** The H.323 phone is added to CUCM with its IP address and directory numbers specified.
- Step 2.** The H.323 phone is configured with the IP address of CUCM.

SIP Third-Party IP Phone Support in CUCM

CUCM supports RFC 3261-compliant, third-party SIP phones. Support for third-party SIP phone features varies greatly from Cisco SIP IP Phone features. Third-party phones have only RFC 3261 SIP version 2 support, whereas Cisco SIP Phones have many Cisco SCCP features that have been rewritten to work in a native SIP protocol stack.

Two different types of third-party SIP phones can be added to CUCM. Third-party SIP phones can be added as basic or advanced phones. Third-party SIP basic phones support one line appearance and consume three DLUs. Advanced third-party SIP phones support up to eight lines and video but consume six DLUs. Basic and advanced third-party SIP phones offer the same industry-standard SIP telephony features.

Third-party SIP phones register with CUCM but do not use a MAC address-based device ID. CUCM uses SIP digest authentication to identify a registering third-party SIP phone.

Both CUCM and third-party SIP phones require a digest authentication password used for digest authentication to work properly. CUCM refers to this as a digest user that is applied to the phone. The end user digest credentials must be configured to match the third-party SIP phone password (configuration parameter language can differ in the third-party device).

SIP standards and drafts supported by CUCM include the following:

- **RFC 3262:** PRACK
- **RFC 3264:** Session Description Protocol (SDP) offer/answer model. SDP is very important to the negotiation of signaling parameters. Early Offer (EO) and Delayed Offer (DO) SIP invite-based signaling is supported, but might require additional configuration. The CUCM Solution Reference Network Design (SRND) guide is a good place to check for additional information.
- **RFC 3311:** UPDATE
- **RFC 3515:** REFER
- **RFC 3842:** MWI package
- **RFC 3891:** Replaces header
- **RFC 3892:** Referred-by mechanism

The following audio and video standards are supported for third-party SIP phones:

- **Audio:**
 - **Audio codecs:** G.711 mu-law, GSM Full-rate, G.723.1, G.711 A-law, G.722, G.728, G.729, iLBC
 - **RFC 2833:** Dual-tone multifrequency (DTMF) Relay (using Named Telephony Events [NTE]/Named Signaling Events [NSE])
- **Video:** Video codecs: H.261, H.263, H.263+, H.263++, H.264

Note For more information about the support of these standards, see the Cisco SIP IP Administrator Guide, Version 8.0 - Compliance with RFC 3261 at www.cisco.com/en/US/products/sw/voicesw/ps2156/products_administration_guide_chapter09186a00807f47e3.html.

Third-party SIP phones support only a few features compared to Cisco IP Phones using SCCP or SIP. The features that are not supported include, but are not limited to, the following:

- MAC address registration
- Phone buttons template

- Softkey templates
- Telephony features and applications such as the following:
 - IP phone services
 - CUCM Assistant
 - Cisco Unified Video Advantage
 - Call pickup
 - Barge
 - Presence

SIP Third-Party Authentication

Digest authentication allows CUCM to act as a server to challenge the identity of a SIP device when it sends a request to CUCM. When digest authentication is enabled for a phone, CUCM challenges all SIP phone requests except keepalive messages. CUCM does not support responding to challenges from SIP phones.

CUCM can challenge SIP devices connecting through a SIP trunk and can respond to challenges received on its SIP trunk interface.

CUCM digest authentication is used to determine the identity of a third-party SIP phone. The phones cannot be authenticated through a MAC address like SCCP devices because third-party SIP phones do not register by MAC address. Digest authentication is the industry standard.

CUCM can ignore the keyed hash that is provided in a digest authentication response and check only whether the provided username exists and is bound to a third-party SIP phone. This is the default behavior. Alternatively, CUCM can be configured to check that the key that was used at the third-party SIP phone to generate the keyed hash matches the locally configured key (called digest credentials) at the end-user configuration in CUCM.

Third-party SIP phones cannot be configured by using the CUCM TFTP server. Instead, they need to be configured using the native phone configuration mechanism, which is usually a web page or a TFTP file. The device and line configuration in the CUCM database must be manually synchronized with the native phone configuration (for example, extension 1002 on the phone and 1002 in CUCM). In addition, if the directory number of a line is changed, it must be changed in both CUCM Administration and in the native phone configuration mechanism.

Third-party SIP phones include their directory number in the registration message. They do not send a MAC address. Third-party SIP phones identify themselves with digest

authentication. The SIP REGISTER message includes a header with a username and the keyed hash, as shown in the following example:

```
Authorization: Digest  
username="3rdpsip",realm="ccmsipline",nonce="GBauADss2qoWr6k9y3hGGVDA  
qnLfoLk5",uri="sip:172.18.197.224",algorithm=MD5,response="126c0643a4  
923359ab59d4f53494552e"
```

CUCM receives the registration message and searches for an endpoint that matches the provided username in the SIP message (3rdpsip in the preceding example). CUCM uses the digest credentials configured for that user to verify the keyed hash (response="126c0643a4923359ab59d4f53494552e" in the preceding example).

Note CUCM must be explicitly configured to verify the keyed hash. By default, CUCM searches only for the end-user name.

CUCM searches for a third-party SIP phone that is associated with the end user and verifies that the configured directory number matches the one provided by the third-party SIP phone in its registration message. If the phone is found and the directory number is the same, the third-party SIP phone registers with CUCM.

To add a third-party SIP phone in CUCM, follow these steps:

- Step 1.** Configure an end user in CUCM, and specify the digest credentials.
- Step 2.** Add the third-party SIP phone in CUCM, and configure its directory number.

Note When you are configuring the third-party SIP phone in CUCM, a dummy MAC address can be specified. The MAC address is not used to identify the device but is required inside the CUCM configuration database.

- Step 3.** Associate the third-party SIP phone with the end user.
- Step 4.** Configure the third-party SIP phone with the IP address of the CUCM, end-user ID, digest credentials, and directory number.

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- CUCM supports SIP, SCCP, and H.323 protocols for endpoints.
- Feature differences exist between SIP, SCCP, and H.323 endpoints and between different IP phone models.

- Cisco IP Phones follow a process during the boot cycle. The Cisco IP Phone learns its voice VLAN ID and IP configuration, and a configuration is downloaded from the TFTP server.
- Third-party H.323 phones are configured on both CUCM and in the phone-configuration interface.
- Third-party SIP phones register by their directory number and a username, provided by digest authentication.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. Choose the Type A phones from the following list. (Choose three.)
 - a. 7905
 - b. 7912
 - c. 7940
 - d. 7941
2. What protocol is used by default on Cisco IP Phones?
 - a. SCCP
 - b. SIP
 - c. H.323
 - d. MGCP
3. Which type of SIP device has the highest number of features?
 - a. Type A
 - b. Type B
 - c. Third-party
 - d. Cisco IP Phone on third-party SIP device
4. Which audio codecs does every Cisco IP Phone support? (Choose two.)
 - a. G.711
 - b. G.729
 - c. G.722
 - d. G.723

5. Which protocol or technology is required to provide the phone with firmware and a configuration file?
 - a. Cisco Discovery Protocol
 - b. TFTP
 - c. FTP
 - d. Power over Ethernet
6. How many watts of power does the IEEE 802.3af power specification deliver?
 - a. 10 watts
 - b. 15.4 watts
 - c. 13.2 watts
 - d. 9.6 watts
7. What protocol or technology is required to provide an IP address, subnet mask, default gateway, and option 150 to a Cisco IP Phone?
 - a. DHCP
 - b. TFTP
 - c. FTP
 - d. Power over Ethernet
8. What protocol or technology is required for power delivery to the Cisco IP Phone?
 - a. Cisco Discovery Protocol
 - b. TFTP
 - c. FTP
 - d. Power over Ethernet
9. Which protocol is used to communicate the Cisco IP Phone VLAN to the IP Phone?
 - a. Cisco Discovery Protocol
 - b. TFTP
 - c. FTP
 - d. Power over Ethernet
10. How are third-party SIP phones authenticated in CUCM?
 - a. MAC address
 - b. Transport layer security
 - c. Digest authentication
 - d. Secure hashing algorithm

This page intentionally left blank

Chapter 6

Cisco Catalyst Switches

Deploying IP telephony requires planning how the IP phones will be powered and how the voice network will be combined with the data network, while ensuring that voice calls maintain high quality.

Cisco Catalyst switches provide three primary features that aid an IP telephony deployment: Power over Ethernet (PoE), voice VLANs, and class of service (CoS). Power over Ethernet (PoE) can save on wiring costs and simplify cable infrastructure management. Multiple VLANs are normally enabled on a single Cisco switch access port, with the phone marking voice VLAN data and the switch port accepting data VLAN information untagged. Dual VLAN access ports simplify configuration when compared to configuring 802.1q trunk links and setting the trunk to only accept traffic from the voice VLAN.

This chapter discusses the three major functions that Cisco Catalyst switches perform in an IP telephony network and describes how to configure a Cisco Catalyst switch to enable these functions.

Chapter Objectives

Upon completing this chapter, you will be able to configure both the Cisco IOS Catalyst and the Cisco CatOS switches to support Cisco IP Phones, third-party IP phones, and software-based phones, and you will be able to meet these objectives:

- Describe the role and features of Cisco LAN switches in a Cisco Unified Communications (UC) solution.
- Describe how power can be provided to IP phones by Cisco LAN switches.
- Configure Cisco LAN switches to provide power to IP phones.
- Describe how voice VLAN support can be provided to IP phones that have a PC attached to their PC port.
- Describe why allowed VLANs on trunk ports should be limited.

- Describe how to configure voice VLANs in Cisco IOS LAN switches.
- Describe how to configure voice VLANs in Cisco CatOS LAN switches.

Cisco LAN Switches

Cisco Catalyst switches can provide three primary features to assist the IP telephony deployment:

- **In-line power/Power over Ethernet (PoE):** In-line power/PoE allows a Cisco Catalyst switch to send power over the Category-X Ethernet cabling infrastructure to a Cisco IP Phone (other PoE devices include wireless devices, digital signage, security devices, and so on) without the need for an external power supply and a nearby AC power outlet. PoE is easy to back up as well because all power is distributed from a central location. IEEE 802.3af-compliant PoE and the Cisco original version were developed by Cisco to accommodate the PoE needs of the marketplace before there was an industry standard. Type A phones support only Cisco PoE, whereas Type B phones support both Cisco PoE and IEEE 802.3af PoE. Most Cisco IP Phones have two physical connections. One is labeled SW and is used to connect to the switch port; the other is labeled PC and is used to connect to the personal computer. The Cisco IP Phone shares its data connection with the phone. The SW interface can receive in-line power; the PC port cannot. This is important if you wanted to temporarily daisy-chain seven phones in a conference room for temporary emergency requirements. Cisco supports up to seven Cisco IP Phones daisy-chained off of one switch port, but only the first phone will receive PoE. The other six phones would require power bricks.
- **Voice VLAN support:** One or more network devices can be connected to the back of the Cisco IP Phone. Voice VLANs place Cisco IP Phone traffic into a voice VLAN that logically separates desktop computer and telephone traffic into two different VLANs (IP subnets). Each VLAN represents a logical broadcast domain (IP subnet).
- **CoS marking:** CoS marking is performed at the Layer 2 frame level (OSI reference model/Osi-Rm). The Layer 2 mechanism that leverages CoS is Layer 2 Ethernet technology. The 802.1q standard includes a 3-bit field referred to as the class of service (CoS), but the 3 bits are further explained in the IEEE 802.1p specification. Prioritizing voice traffic is critical in IP telephony networks. If voice traffic is not given priority, poor voice quality can result when the network devices experience bandwidth congestion or resource contention.

CoS and Differentiated Services Code Point (DSCP) marking is performed natively on the Cisco IP Phone as instructed by Cisco Unified Communications Manager enterprise parameters. Here are the default quality of service (QoS) settings:

- **Signaling (SCCP/SIP):** CoS 3 and DSCP cs3 (class selector 3 or DSCP decimal value 24)
- **Media (RTP):** CoS 5 and DSCP EF (Expedited Forwarding or DSCP 46)

The markings of the Cisco IP Phone will need to be trusted by the Cisco switch that connects the phone to the data network. The three trust states are as follows, but keep in mind that the configured CoS value option is almost never used in production environments because of the requirement to run IEEE 802.1q trunking on an access port and desktop PC:

- **Trusted:** The IP phone sends IEEE 802.1q-tagged frames with IEEE 802.1p prioritizations to indicate the Layer 2 CoS priority value, and the switch port trusts the CoS markings of the IP phone.
- **Untrusted (default):** The switch does not trust the IP phone CoS marking and rewrites the priority value to 0.
- **Configured CoS priority level:** The IP phone changes the 802.1p header with a new CoS priority value if the PC used 802.1p with a different CoS priority level than the new priority value. The IP phone is capable of remarking only Layer 2 CoS. If the PC is not doing 802.1q trunking, the IEEE 802.1p CoS values will never be marked. 802.1q trunking is a prerequisite for IEEE 802.1p CoS values.

The traffic that is sent by the IP phone should normally be trusted, but the default switch port must be explicitly configured to trust either the CoS or DSCP markings of the Cisco IP Phone. The default configuration of untrusted remarks all traffic coming into the switch at a CoS of 0 and DSCP of 0. I prefer to trust on DSCP rather than CoS because the CoS could rewrite the DSCP marking with this pesky thing called the cos-dscp mapping table of the switch. The cos-dscp mapping table is not required when using the mls qos trust dscp configuration. The default cos-dscp mapping table converts the voice media DSCP of 46 (EF) into cs5 (class selector 5 or DSCP 40). Traffic cannot get mapped into the proper WAN service provider class of service unless the proper markings are sent.

Conditional trust boundary is based on the DSCP marking configuration:

```
mls qos trust dscp
mls qos trust device cisco-phone
```

This configuration will trust the DSCP markings, under the condition that a Cisco IP Phone was discovered on the port. Cisco IP Phones are discovered through the Cisco Discovery Protocol (CDP) advertisements. A Cisco IP Phone's firmware version can be seen from the switch with the **show cdp neighbor detail** command. This is useful when you're troubleshooting a remote device that you do not have physical access to. This also assumes that you are aware of the switch port associated with every wallplate that end users are plugged into. The wallplate numbers usually match the patch panels in the switch closet, so this is easy-enough information to ascertain if necessary. The quality of service topics (CoS, DSCP, cos-dscp mapping tables, and so on) are covered in more detail in the book *Quality of Service*, by Wendell Odom (published by Cisco Press).

Providing Power to Cisco IP Phones

Most Cisco IP Phone models can use the following three options for power:

- **PoE:** Power source equipment (PSE) inserts PoE into unshielded twisted-pair (UTP) cabling after a negotiation phase in which the powered device (PD) sends back a signature value to the PSE equipment indicating that the device requires PoE. PoE equipment can be backed up by a rectifier and DC batteries or an uninterruptible power supply (UPS) to guarantee power delivery during a power outage. A UPS or some other type of battery backup is normally required in environments with a backup power generator because it takes a bit of time for the power generator to reach an operational state.
- **Midspan power injection:** Some switches and modular switch blades do not support PoE. A midspan power source can be used instead of an Ethernet switch providing PoE. The midspan power injector is connected between the LAN switch and the powered device and inserts power on the Ethernet cable to the powered device.
- **Wall power:** Wall power requires a DC converter to connect the IP phone to a wall outlet.

Note Cisco IP Phones do not ship with a wall power supply. The wall power supply must be ordered separately from the Cisco IP Phone.

Cisco provides two types of in-line power delivery:

- **Cisco original implementation of PoE:** Cisco was the first to develop PoE. The original Cisco PoE implementation supports the following features:
 - Provides –48 VDC at up to 10 watts (W) per port over pins 1, 2, 3, and 6 of the UTP cable.
 - Supports many Cisco devices (IP phones, wireless access points, and so on).
 - Uses a Cisco-proprietary method of determining whether an attached device requires power. Power is delivered only to devices that require power.
- **802.3af PoE:** Cisco has been driving the evolution of PoE technology toward standardization by working with the IEEE. The IEEE 802.3af standard supports the following features:
 - Specifies –48 VDC at up to 15.4 W per port over data pins 1, 2, 3, and 6 or pins 4, 5, 7, and 8 (all four pairs are used in Gigabit Ethernet, but only pins 1, 2, 3, and 6 are used in 10-Mbps [Ethernet] or 100-Mbps [Fast Ethernet] technologies). Cisco Catalyst switches provide 802.3af PoE using pins 1, 2, 3, and 6.
 - Enables a new range of Ethernet-powered devices (for example, color LCDs, which require significantly more power than their black-and-white counterparts).

- Standardizes a power discovery method to determine whether an attached device requires power. Power is delivered only to devices that have been detected to require it. The IEEE 802.3af standard supports power classification, which allows a powered device to communicate a signature that defines the maximum power requirement. The PSE reads the power signature and budgets the correct amount of power for the powered device (less than the maximum 15.4 watts [class 3]).

A switch without power classification reserves the maximum 15.4 watts of power for every port. This behavior can result in oversubscription of the available power supplies. Oversubscription will cause a condition in which devices requiring power will be denied because all the switch power has been preallocated. Some older 48-port access layer switches would only deliver PoE to the first 24 ports because the power supply did not have enough power to reserve 15.4 watts per port.

IEEE 802.3af power classification defines these five classes:

- 0 (default): 15.4 W reserved
- 1: 4 W
- 2: 7 W
- 3: 15.4 W
- 4: 30 W

All Cisco IEEE 802.3af-compliant switches support power classification.

Cisco Original Power over Ethernet Device Detection

The Cisco original PoE mechanism transmitted a very low-frequency (147-Hz) tone and waited to hear whether the tone (signature) was returned on the receive pins. Cisco IP Phones loop back the 147-Hz tone to the switch port. This process occurs using the same fast link pulse (FLP) process used for autonegotiation of Ethernet port speed and duplex settings (10/100/1000). The switch detects the 147-Hz tone and begins delivering the default power allocation (10 watts by default) to the Cisco IP Phone or other in-line, power-capable endpoint (wireless devices). The Cisco IP Phone then sends a CDP version 2 trigger message with the Power field set to the phone's power requirement (6.3 watts for the 7960 phone).

IEEE 802.3af Device Detection

The PSE detects a powered device (PD) by applying a voltage in the range of -2.8 volts to -10 volts on the transmit pins of the Category 3 cable (hopefully cabling better than Cat 3 will be available to you, but Cat 3 will work fine with 10-Mbps Ethernet power detection). The switch will receive this tone back only if the powered device is IEEE 802.3af compliant. The powered device (Cisco IP Phone) has a 25-k-ohm signature resistor that

allows it to loop back this tone. Compliant PDs must support this resistance method. Figure 6-1 shows the IEEE 802.3af device detection process.

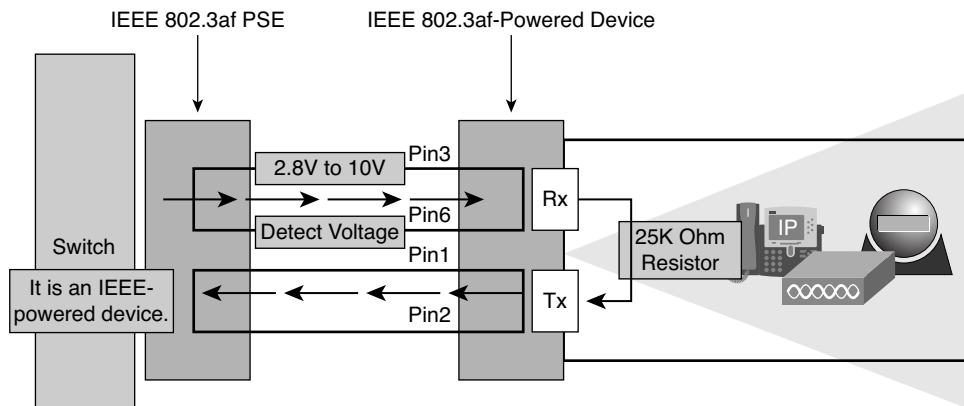


Figure 6-1 IEEE 802.3af Device Detection

The Catalyst Operating System is getting a little long in the tooth at this point. Most readers are probably not using it anymore, but we left this section in for those companies that had an investment in the 8-port Catalyst 6606-T1 gateway modules. Those line cards were \$19,995 list price when they were introduced, and they are only supported in the Catalyst Operating System (CatOS).

As demonstrated in Example 6-1, the **set port inlinepower** command can be used on a switch that is running Cisco CatOS software. The **set port inlinepower** command is not complete without setting one of the power modes: **auto** or **off**. All switch ports are set to **auto** by default, which enables the port to autonegotiate power with the powered device. If the switch port is set to the **off** mode, the switch does not provide power on the port even if an in-line, power-capable device is connected. CatOS feature development was discontinued many years before this book was written.

Example 6-1 CatOS Power Configuration Command

```
CatOS>(enable) set port inlinepower mod/ports ?
auto   Port inline power auto mode
off    Port inline power off mode
```

Use the following interface configuration command on switches that are running native Cisco IOS to change the default in-line power configuration (Catalyst 6500, 4500, 3550, 3750, and 3560 switches):

```
CSCOIOS(config-if)# power inline {auto | never}
```

The PD discovery algorithm is set to **auto** by default. The PD discovery algorithm is disabled if the **power inline** command is configured to **never**.

Note The Cisco Catalyst 6500 Series can run either Cisco CatOS software or native IOS if the switch supervisor engine has a Multilayer Switch Feature Card (MSFC). The Cisco Catalyst 4500 Series has been running native IOS exclusively since the Supervisor 3 module was released.

Use the commands shown in Examples 6-2 and 6-3 to display a view of the power allocated on Cisco Catalyst switches. The switch shows the default allocated power as 10 watts in addition to the in-line power status of every port.

Example 6-2 *CatOS Power Display Command*

```
CatOS>(enable) show port inline power 7
Default Inline Power allocation per port: 10.000 Watts (0.23 Amps @42V)
Total inline power drawn by module 7: 75.60 Watts (1.80 Amps @42V)
Port      InlinePowered      PowerAllocated
          Admin     Oper       Detected      mWatt      mA @42V
-----  -----
7/1        auto      off       no            0           0
7/2        auto      on        yes          6300        150
7/3        auto      on        yes          6300        150
7/4        auto      off       no            0           0
7/5        auto      off       no            0           0
7/6        auto      off       no            0           0
7/7        auto      off       no            0           0
```

Example 6-3 *Native Cisco IOS Power Display Command*

```
Switch# show power inline
Interface      Admin     Oper      Power ( mWatt )      Device
-----  -----
FastEthernet9/1    auto      on       6300                Cisco 6500 IP Phone
FastEthernet9/2    auto      on       6300                Cisco 6500 IP Phone
FastEthernet9/3    auto      off      0                   n/a
```

Voice VLAN Support on Cisco IP Phones

The Cisco IP Phone contains an integrated three-port Fast Ethernet (10/100) or Gigabit Ethernet (10/100/1000) switch, depending on the Cisco IP Phone model. The ports are illustrated in Figure 6-2 and are used as follows:

- Port 0 is an internal interface that carries the Cisco IP Phone traffic.
- Port 1 connects to a PC or other Ethernet device.
- Port 2 connects to the access layer switch. In-line power can be used at port 2.

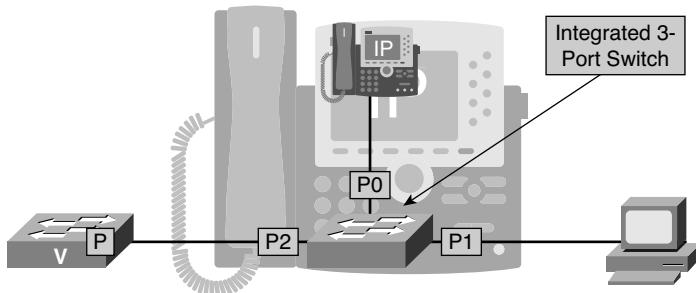


Figure 6-2 Cisco IP Phone Ports

Note Do not use VLAN 1 anywhere in your deployment. If you use VLAN 1 in your network, you might get some confused phones. I have seen a challenge related to the use of VLAN 1, but I can't recall whether the problem occurred with both Type A and Type B phones. If this interests you, test it to see whether it applies to your particular phone. I have noticed plenty of subtle (and sometimes not so subtle) differences in different Cisco IP Phones and firmware combinations. The firmware version is usually directly tied to the Cisco Unified Communications Manager (CUCM) version that is in use, unless you loaded different Load IDs on phones after downloading software. Custom loading might be required during a Cisco Technical Assistance Center (TAC) case, but it is not the norm.

If VLAN 1 is in use, the Cisco IP Phone can broadcast a DHCP Discover Layer 2 broadcast untagged packet before the Cisco IP Phone learns of the voice VLAN. If the DHCP server makes a DHCP offer to the Cisco IP Phone, a Request is sent back and an Acknowledgment is sent back. The Cisco IP Phone will now be in the wrong VLAN/IP subnet. This is a problem because VLAN 1's DHCP Scope (subnet) is probably configured without DHCP option 150 (TFTP server). In addition, there are some security best practices about not using VLAN 1 and changing all the native VLANs on 802.1q trunks.

Single-VLAN Access Port

All Cisco Catalyst switch ports are configured as single-VLAN access ports by default. A single-VLAN access port is typically used for third-party IP phones or IP softphones. It is not recommended to configure Cisco Catalyst switch ports connected to Cisco IP Phones in this way. A single-VLAN access port should be configured with the voice VLAN.

It is not recommended to put both the IP phone and an attached PC into the same VLAN. Separating voice and data services into different VLANs allows IP subnets to be treated separately for QoS and network security applications. The single-VLAN access point concept is illustrated in Figure 6-3.

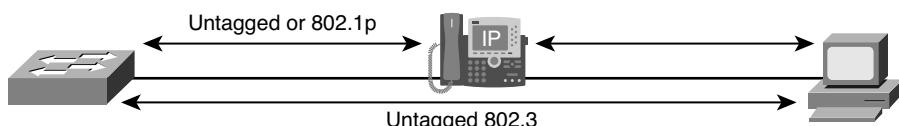


Figure 6-3 Single-VLAN Access Port

A single-VLAN access port

- Is rarely used in production deployments.
- Can be configured as a secure port.
- Works with both Cisco and non-Cisco IP Phones.
- Supports IP phones to leverage 802.1p for CoS, without using VLANs. I've never been in an environment that had this requirement, but I'm sure it's out there.

Non-Cisco switches are typically configured as single-VLAN access ports because they usually do not support the voice VLAN feature. Cisco Catalyst switches connected to third-party IP phones are also configured in this way because of the lack of the voice VLAN feature.

Multi-VLAN Access Port

Multi-VLAN access ports are supported by almost all Cisco Catalyst switches. All data devices connected to the PC port of the phone reside on the access (data) VLAN. A separate voice VLAN is used in the multi-VLAN access port configuration. Catalyst switches running CatOS software refer to the voice VLAN as an auxiliary VLAN, while native IOS uses voice VLAN.

The placement of IP phone RTP media traffic in a separate VLAN than data traffic makes it easier for customers to deploy Cisco IP Phones. IP phones boot in the voice VLAN as instructed by the switch. The switch provides the IP phone with the appropriate voice VLAN configuration through automatically triggered CDP version 2 announcements. The Cisco IP Phone negotiates voice VLAN and power parameters before the Cisco IP Phone can receive an IP address from the DHCP server. Cisco Discovery Protocol is also leveraged in the Cisco Unified Video Advantage (CUVA) video client in the process of associating the CUVA video client to the Cisco IP Phone (Cisco Audio Session Tunnel [CAST]).

Administrators can implement multiple VLANs on the same port by configuring an access port with two VLANS:

- One VLAN configured as an access VLAN
- One VLAN configured as a voice VLAN

An Ethernet frame-tagging mechanism must exist to distinguish among VLANs and provide Layer 2 CoS. IEEE 802.1q is the IEEE standard for tagging frames with a VLAN ID number. The IP phone sends Ethernet frames tagged with 802.1q CoS and VLAN ID values. The PC connected behind the Cisco IP Phone sends native, untagged Ethernet frames that are placed in the proper VLAN (tagged) at the ingress port of the switch. The Application Specific Integrated Circuit (ASIC) hardware sets the 802.1q trunk header. The

802.1q VLAN setting is based on the access VLAN configuration of the switch port. When the switch receives a frame from the network destined for the PC, it removes (strips out) the 802.1q trunk header and forwards a native, untagged Ethernet frame to the PC. The IP phone marks all traffic from the phone into the proper voice VLAN based on the switch configuration.

The following are some advantages in implementing multi-VLAN access ports:

- The voice VLAN ID can be either discovered using CDPv2 or configured on the IP phone. Most deployments use the autonegotiated CDP trust boundary.

Note Some very secure environments cannot use the multi-VLAN access port because CDP is turned off. This is because Cisco IOS advertises information about the switch's software versions, types, and management IP addresses. Hackers could leverage this information to hijack the environment's data unbeknownst to the end users in the system. Certain security levels are required for compliance reasons as well. The Health Insurance Portability and Accountability Act (HIPAA) has requirements that must be met whenever any communication exists between medical personnel. Sarbanes-Oxley compliance is for the finance field, and Payment Card Industry (PCI) compliance is for a business involved in performing credit card transactions of any type. Most of the compliance regulations address encryption of traffic, but voice communications are not required to be encrypted. Voicemail does not need to be recorded and archived, but there are compliance rules that mandate that all email communication is archived for a certain amount of time. This stopped many deployments of Unified Messaging when Cisco Unity shared a Message Store with the Microsoft Exchange server that is used for corporate email. Cisco Unity Connection offers Integrated Messaging with email client accessibility to voicemail without the requirement to archive voicemail for compliance rules. Cisco Unity Connection Information Database Server (IDS) maintains the message store database so that the large voicemail attachments do not have to be archived with email. This solution creates a scalable IP addressing scheme that can easily be accomplished in existing environments by merely adding an additional DHCP scope for each voice VLAN. Most IP subnets have more than 80 percent of their available IP addresses leased, so the single-VLAN access port model is not a very robust solution that can accommodate existing environments. The voice VLAN (IP subnet) allows the introduction of a large number of new devices into the network without modifying the existing IP addressing scheme.

- Dual-VLAN access ports allow the logical separation of data and voice traffic. The voice and data VLAN segregation creates an environment where network security and QoS policy can be configured differently for the two networks.

802.1q Trunk Port

An 802.1q trunk port can be used to connect a Cisco IP Phone to the Layer 2 switch network infrastructure. The multi-VLAN access port is the best practice for connecting a Cisco IP Phone to a Cisco Catalyst switch, but this mechanism was not available in some early Power over Ethernet (PoE)-capable switches. There is a 3524-PWR-XL switch that

supports only 802.1q trunks or single-VLAN access ports. Because almost no one will ever use a single VLAN access port, I find myself using IEEE 802.1q trunk ports in that very rare occasion. IEEE 802.1q trunk ports are a good way to connect Cisco IP Phones to third-party vendor switches. 802.1q trunk ports can also be used when connecting third-party IP phones to Cisco Catalyst switches. Because this is a book on CUCM, I doubt you've read this far with this as a requirement, but any third-party vendor phone is supported in CUCM. Recall from Chapter 5, "Endpoints," that Cisco charges a good deal of licensing for a third-party phone with more than one line (five device license units [DLU]). One-line third-party SIP Phones require only three DLUs.

Frames of the native VLAN on an 802.1q trunk port are transmitted and received as untagged by default. Personal computers send their Ethernet frames untagged, even though most network interface cards (NIC) support IEEE 802.1q trunking (dot-one-queue trunking is used to reference this technology quite often). When a Cisco IP Phone is inserted between the PC and the switch port, the PC frames are transmitted untagged, while the Cisco IP Phone frames are tagged with the voice VLAN.

If the voice VLAN feature is enabled on a trunk port, the port will not allow any other tagged frames on the port. 802.1q trunk ports allow all VLANs by default, unless configured to do otherwise.

With Cisco IP Phone trunk ports, you must consider that Spanning Tree PortFast cannot be enabled on trunk ports of some very old Cisco Catalyst switches. This causes a condition where the IEEE 802.1d Spanning Tree Protocol (STP) must run on the port connected to the Cisco IP Phone. STP can take up to 50 seconds before it allows traffic to be forwarded on the port.

Note Most deployments have migrated to IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), which has the same concept of PortFast but calls the functionality *edge ports*. Cisco decided to continue using the `spanning-tree portfast` command in Cisco IOS, providing edge port functionality. This allowed existing deployments to migrate to RSTP in a more seamless fashion. *Seamless* is supposed to mean without problems, but the longer you're in Information Technology (IT), the more you come to take seamless to mean limited, manageable challenges. Nobody likes getting out of bed at 3 o'clock Monday morning to roll back the configurations to what they were before the migration started Friday night. Cisco is very good at making configuration files portable between different Cisco IOS versions with the same (or similar) feature sets. CUCM still has a Gatekeeper Controlled Intercluster trunk in CUCM version 8.0, even though this intercluster configuration element was replaced by H.225 trunks way back in CallManager version 3.2. H.225 trunks allow trunks to be pointed to H.323 gateways in addition to H.323 gatekeepers. H.225 is a subset of the H.323 protocol suite. H.323 theory is covered in more detail in *Implementing Cisco Unified Communications Voice over IP and QoS (CVOICE) Foundation Learning Guide*.

Native Cisco IOS VLAN Configuration

Example 6-4 shows the configuration of a single-VLAN access port. The switch is configured to transmit and receive CDPv2 frames to enable the Cisco IP Phone to transmit voice traffic in the IEEE 802.1p (Layer 2 CoS or Priority bits) field of the 802.1q trunk header, tagged with VLAN ID 0 (VLAN field). The switch inserts the 802.1p voice traffic into the configured access VLAN of 261. Recall that this configuration is rarely used. I have never seen or heard of it being used. However, it is possible though, and it could appear on your CIPT1 exam if you decide to pursue the Cisco CCNP Voice certification.

Example 6-4 Single-VLAN Access Port Configuration

```
Console(config)# interface FastEthernet0/1
Console(config-if)# switchport mode access
Console(config-if)# switchport voice vlan dot1p
Console(config-if)# switchport access vlan 261
Console(config-if)# spanning-tree portfast
```

Example 6-5 shows a multi-VLAN access port configuration where the voice traffic is sent on VLAN 261 and the data traffic is sent on access VLAN 262. This is what is used in most standard deployments.

Example 6-5 Multi-VLAN Access Port Configuration

```
Console(config)# interface FastEthernet0/1
Console(config-if)# switchport mode access
Console(config-if)# switchport voice vlan 261
Console(config-if)# switchport access vlan 262
Console(config-if)# spanning-tree portfast
```

The **switchport mode access** command configures the switch port to be an access (nontrunking) port. Table 6-1 provides a switch command reference that shows many of the commands that are used in the configuration examples.

Table 6-1 Switch Command Reference

Command	Description
switchport mode access	Configures the switch port to be an access (nontrunking) port.
spanning-tree portfast	Causes a port to enter the Spanning Tree forwarding state immediately, bypassing the listening and learning states. You can use PortFast on switch ports that are connected to a single workstation or server (as opposed to another switch or network device) to allow those devices to connect to the network immediately.
switchport access vlan 100	Configures the interface as a static access port with the access VLAN ID of 100. 4096 VLANs are possible with IEEE 802.1q trunking based on the 12 bits in the header that specify the VLAN. All untagged data traffic coming from the PC connected behind the phone will be marked with this VLAN identifier by the ASIC of the Cisco IP Phone.

-
- switchport voice vlan 99** Configures a voice VLAN ID that the switch will communicate to the Cisco IP Phone through CDPv2 frames that configure the Cisco IP Phone to transmit voice traffic in the proper VLAN without manual configuration of the phone. The switch leaves the traffic in the VLAN unless a Layer 3 switch or router routes the packet to another IP subnet. The Layer 2 header is rewritten at each Layer 3 boundary (router). Switches normally perform Layer 3 routing on Layer 3–enabled Switched Virtual Interfaces (SVI). Here are some optional parameters of the **switchport voice vlan** command that I have never seen used in a deployment:
- Enter the **dot1p** keyword to send CDPv2 packets that configure the Cisco IP Phone to transmit voice traffic in 802.1p frames, tagged with VLAN ID 0 and a Layer 2 CoS value. (The default is 5 for voice traffic and 3 for voice control traffic.) The switch puts the 802.1p voice traffic into the access VLAN.
 - Enter the **untagged** keyword to send CDPv2 packets that configure the Cisco IP Phone to transmit untagged voice traffic. The switch puts the untagged voice traffic into the access VLAN.
 - Enter the **none** keyword to allow the Cisco IP Phone to use its own configuration and transmit untagged voice traffic. The switch puts the untagged voice traffic into the access VLAN.
-

Example 6-6 includes the native Cisco IOS configuration to set up an IEEE 802.1q trunk for the phone. This configuration is common when a Cisco switch infrastructure is used to accommodate third-party phones but rarely used in production environments anymore. Because IEEE 802.1q trunking was the only mechanism supported at one point in ancient history, there are still plenty of boilerplate configurations used by some that configure IEEE 802.1q. I try to avoid this type of configuration when possible, and that turns out to be most of the time. The **native vlan** command is used to set the PC VLAN in this model (similar to the **switchport access vlan** command in the multiport single-access point model). The **switchport trunk allowed vlan** command is a security mechanism that ensures that the port will only accept VLAN information tagged by the Cisco IP Phone in VLAN 261. VLAN 262 is inserted into the Ethernet frame when the untagged frame is received at the port level ASIC.

Example 6-6 802.1q Trunk Port Configuration

```
Console(config)# interface FastEthernet0/1
Console(config-if)# switchport trunk encapsulation dot1q
```

```
Console(config-if)# switchport mode trunk
Console(config-if)# switchport trunk native vlan 262
Console(config-if)# switchport voice vlan 261
Console(config-if)# switchport trunk allowed vlan 261
```

Example 6-7 displays the output from a native Cisco IOS switch trunk verification command. Try using the `show interface trunking` command as well. It displays slightly different runtime information, and I have found it to be useful.

Example 6-7 Trunk Port Verification

```
Class-1-Switch# show interfaces fastethernet 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 262 (VLAN0262)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 261 (VLAN0261)
```

CatOS VLAN Configuration

Example 6-8 shows the configuration of a single-VLAN access port using the CatOS. If you're no longer using the CatOS on your Cisco 6500 Series switch, or if you don't have a Cisco 6500 switch, feel free to skip this section. The commands are similar in nature to native Cisco IOS, but the syntax is different enough to be irritating. CatOS brings my mind back to the days when Cisco first acquired Grand Junction (2900), Kalpana (3000), Granite (4000), and Crescendo (5000/6000). The four different product families were configured differently, but Cisco standardized on native IOS, and the configurations between switch lines are no longer a headache. QoS configurations on the switches could be far more difficult. I highly recommend referencing the QoS switching configuration boilerplates that are part of the QoS Solution Reference Network Design (SRND) guide.

Example 6-8 Single-VLAN Access Port

```
Console>(enable) set port auxiliaryvlan 2/1-3 dot1p
Console>(enable) set vlans 262 2/1-3
Console>(enable) set trunk 2/1-3 off
```

Example 6-9 shows a multi-VLAN access port configuration where the voice traffic is sent to voice VLAN 261 (auxiliary VLAN) and the data is using the access VLAN 262.

Example 6-9 Multi-VLAN Access Port

```
Console>(enable) set port auxiliaryvlan 2/1-3 261
Console>(enable) set vlans 262 3/1-3
Console>(enable) set trunk 2/1-3 off
```

All Ethernet traffic is marked with VLANs on a trunk link using either IEEE 802.1q or the Cisco original Inter-Switch Link (ISL) technology. ISL was a Cisco enhancement to switch infrastructures before there was a standardized method of allowing multiple devices from different subnets to connect to a switch. VLANs were not around in the early 1990s when LAN infrastructures went through a major growth phase. Native VLAN traffic is sent as untagged on the trunk link. The native VLAN is used for the data traffic coming in from the workstation attached to the Cisco IP Phone in the access layer port trunking configurations.

In Example 6-10, VLAN 262 is set as the native VLAN, is untagged, and will be used by the data traffic. VLAN 261 is tagged with 802.1q tagging and will be used by the voice traffic.

In Cisco CatOS, you can change the native VLAN by issuing the **set vlan *vlan-id* *mod/port*** command, where *mod/port* is the trunk port. The **set trunk** command enables you to configure trunk ports and to add VLANs to the allowed VLAN list for existing trunks. The voice VLAN is configured with the **set port auxiliary *vlan*** command.

Example 6-10 IEEE 802.1q Trunk Port

```
Console>(enable) set trunk 2/1-3 on
Console>(enable) clear trunk 2/1-3 1-4096
Console>(enable) set vlan 262 2/1-3
Console>(enable) set port auxiliary vlan 261 2/1-3
Console>(enable) set trunk 261 2/1-3
```

The status of the auxiliary VLAN on a port or module can be verified in two ways:

- The **show port auxiliaryvlan *vlan-id*** command
- The **show port [module/port]** command

The **show port auxiliaryvlan *vlan-id*** command enables you to show the status of that auxiliary VLAN with the module and ports where it is active, as demonstrated in Example 6-11.

Example 6-11 CatOS VLAN Trunking Verification

```
Console> (enable) show port auxiliaryvlan 222
```

AuxiliaryVlan AuxVlanStatus Mod/Ports		
222	active	1/2,2/1-3

The **show port [module/port]** command enables you to show the module, port, and auxiliary VLAN with the status of the port, as demonstrated in Example 6-12.

Example 6-12 CatOS VLAN Verification

```
Console> (enable) show port 2/1
...
Port  AuxiliaryVlan AuxVlan-Status
-----
2/1    222          active
...
```

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- Cisco LAN switches can supply in-line power to IP phones.
- Two types of PoE delivery are supported by Cisco LAN switches.
- PoE delivery methods can be configured on Cisco LAN switches.
- Cisco LAN switches can be configured to support voice traffic in three different ways: single-VLAN access port, multi-VLAN access port, and trunk port.
- Only required VLANs should be allowed on a trunk port.
- Access and trunk ports can be configured to support Cisco IP Phones.
- Voice VLAN configuration can be verified using Cisco CatOS and Cisco IOS commands and tools.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

- 1.** What is the maximum power level generated by the Cisco original power implementation?
 - a.** 6.3 W
 - b.** 10 W
 - c.** 15 W
 - d.** 15.4 W
- 2.** What is the maximum power level generated by the IEEE 802.3af Power over Ethernet specification?
 - a.** 6.3 W
 - b.** 10 W
 - c.** 15 W
 - d.** 15.4 W
- 3.** Which Cisco platform does not support IEEE 802.3af power?
 - a.** 4500
 - b.** 6500
 - c.** 3750
 - d.** EtherSwitch network module
- 4.** On which unshielded twisted-pair cable pins is midspan power injection delivered?
 - a.** 1, 2, 3, 6
 - b.** 1, 2, 4, 5
 - c.** 4, 5, 7, 8
 - d.** 3, 4, 5, 6
- 5.** On which unshielded twisted-pair cable pins is Power over Ethernet delivered?
 - a.** 1, 2, 3, 6
 - b.** 1, 2, 4, 5
 - c.** 4, 5, 7, 8
 - d.** 3, 4, 5, 6

- 6.** Which protocol delivers VLAN information to the Cisco IP Phone?
 - a.** Cisco Discovery Protocol
 - b.** TFTP
 - c.** FTP
 - d.** Power over Ethernet
- 7.** Which port configuration must be used with third-party phones?
 - a.** Single-VLAN access port
 - b.** Multi-VLAN access port
 - c.** Trunk port
- 8.** Which port configuration does not support Spanning Tree PortFast?
 - a.** Single-VLAN access port
 - b.** Multi-VLAN access port
 - c.** Trunk port
- 9.** What mechanism is used to detect a Cisco IP Phone with the Cisco original power implementation?
 - a.** Cisco Discovery Protocol
 - b.** 25-k-ohm resistor in phone
 - c.** Fast link pulse
 - d.** Power always injected
- 10.** What command is used in native IOS to turn off in-line power?
 - a.** power inline off
 - b.** power inline never
 - c.** power inline auto
 - d.** power inline inactive

Chapter 7

Implementing and Hardening IP Phones

Moves, adds, changes, and deletions (MACD) are important functions of the day-to-day activities of a Cisco Unified Communications Manager (CUCM) administrator.

CUCM provides various tools to accomplish the MACD tasks. This chapter describes how to implement Cisco IP Phones and SIP third-party clients in CUCM. This chapter also covers securing the IP phone.

Chapter Objectives

Upon completing this chapter, you will be able to configure Cisco SCCP and SIP phones and third-party SIP phones in CUCM. This chapter also covers the securing of Cisco IP Phones. This chapter targets the following objectives:

- Identify the endpoint configuration elements and tools for adding phones.
- Describe how auto-registration works.
- Describe how to enable auto-registration for automatic insertion of new phones to the CUCM configuration database.
- Describe how the CUCM BAT and CUCM TAPS tools can be used to add IP phones.
- Describe how to use CUCM BAT to add phones to CUCM.
- Describe how to manually add phones to CUCM.
- Describe Cisco IP Phone configuration settings that can be used to harden the IP phone.

Endpoint Configuration Tools and Elements Overview

There are four ways to add IP phones to CUCM:

- Auto-registration
- Bulk Administration Tool (BAT)
- Auto-Register Phone Tool
- Manual configuration

Auto-registration allows Cisco IP Phones to be added to CUCM without the administrator having to first compile a list of MAC address and reserve phones for use for certain parties. Auto-registration automatically populates common phone configuration settings and automatically assigns a phone number (directory number) to the auto-registered phone. Phone configuration changes are made to the Cisco IP Phone using CUCM Administration.

CUCM BAT allows bulk insertion, deletion, or updating of various devices and features, including phones. The BAT functionality referenced here is the same as that covered in Chapter 4, “Managing User Accounts in Cisco Unified Communications Manager.” The configuration requirements of a phone differ slightly from adding users. Investigate all the BAT configuration options by navigating through the tabs on the BAT.xlt template downloaded from CUCM or the Bulk Administration menu in CUCM Administration. Adding Cisco IP Phones using BAT requires the MAC addresses of the IP phones for phone insertion. Dummy MAC addresses can be inserted into the CUCM database by BAT when BAT is used in tandem with the Auto-Register Phone Tool (formerly known as TAPS, or Tool for Auto-Register Phone Support). Engineers typically refer to this functionality by explaining that they “TAPped” in the phone. Engineering has a very metaphysical mystical quality to it, but sometimes it’s only other nerds (a term of endearment) that understand what we’re talking about. Always size up and properly address your target audience. Network engineers can sometimes hide in the wiring closets, but telecom engineers are typically on the front line dealing with end-user communications issues.

The Cisco Unified Communications Manager (CUCM) Auto-Register Phone Tool is a robust, scalable tool, but it requires a separate Cisco Customer Response Solutions (CRS) server. The CRS must be installed, integrated with CUCM, and properly configured with the necessary scripts to perform Auto-Register Phone Tool (TAPS) functionality. MAC addresses must be added to CUCM with dummy MAC addresses, and the correct phone configuration will be applied during the TAPS process when the auto-registered phone’s MAC address updates the dummy MAC addresses added previously in an automated process. Auto-Register Phone Tool can save a lot of time in significantly sized Cisco IP Phone deployments. Most experienced Cisco UC partners run CRS on a virtual machine as a deployment tool at the customer site, even if the customer is not going to be using CRS for its contact center. The CRS product is more often referred to as Unified Contact Center eXpress (UCCX). Cisco rebranded the contact center product line from IPCC (IP Contact Center) to Unified Contact Center around the CUCM 6.0 release.

Manual phone insertion is the easiest mechanism to configure, but it can be tedious and time consuming in a large deployment involving hundreds or thousands of phones. The administrator must compile a list of the MAC addresses of the IP phones and ensure that the phones with those MAC addresses show up on the proper desks and are correctly configured. I find it easiest to scan the MAC address bar code on the back of the phone or on the phone box. Bar-code scanning requires the purchase of a USB-based, bar-code-scanning device, which you should be able to find for less than \$100.

Endpoint Basic Configuration Elements

There are mandatory and optional configuration details that must be set system-wide in preparation for adding Cisco IP Phones. It is advisable to only use default system-wide setting values for these elements if they are applicable to the deployment. Call manager group, region, and location are required configuration parameters that default to values that most people almost never use. The device pool and region are mandatory, but they have default values. Default values that do not work can be copied, renamed, and reconfigured. Name all configuration elements in a way that allows the administrator to clearly define where the element is and what the element's function is. A device pool named NYC-CMG could be used for a CM_group for the New York City office. This chapter covers the following system-level configurations that will be applied to endpoints:

- CUCM Group
- Regions
- Locations
- Date/Time Group
- Regions
- Locations
- Phone NTP Reference
- Presence Group
- Device Pool
- Security Profile
- Softkey Templates
- Phone Button Templates
- SIP Profile (SIP Phones Only)
- Common Phone Profile

Device Pool

Device pools define common characteristics that can be applied to many devices. The device pool structure supports the separation of user and location information. The device pool contains device- and location-related information. This is leveraged by the device mobility feature that will allow many device pool parameters to be dynamically updated based on the physical location of the phone. Device mobility is covered in more detail in Chapter 16, “Implementing Cisco Unified Mobility.”

The Common Device Profile Configuration window is where end-user-related configuration information used to be configured in the device pool, but was moved in CallManager 5.0.

Each device must be associated with a device pool and with a common device configuration, but there are default selections for both. I suggest that you never use the default device pool because, by default, it includes the default CUCM Group. The CUCM Group of default only includes the Publisher server by default. Any Cisco IP Phone assigned to the default device pool would not have any call-processing (CUCM) redundancy and would be registered to the Publisher instead of the Subscriber server.

Note A Cisco best practice is to put all active phone registrations on Subscriber servers. The Publisher maintains the database; all database replication; all moves, adds, changes, and deletions (MACD) in the CUCM cluster; hunt login status (used in call coverage); Extension Mobility logins (covered in Chapter 16); Message Waiting Indicators (MWI - Voicemail LED on Cisco IP Phone); and all call-forwarding changes (for example, call-forward all to cell phone or call-forwarding cancellation when you get back to your desk).

A best practice is to copy the default device pool and then rename the device pool to accommodate your deployment needs. Use good nomenclature when you name your configuration elements and the Description field of the Cisco IP Phones. It is much easier to make updates on a Unified Communications network that was properly designed and labeled in a way that other engineers will understand after you discover you have a windfall and you're an instant millionaire. I'm imagining that engineer “might” not put in his obligatory two-week notice before leaving. Is anyone going to understand what the last engineer left behind? Hopefully every organization requires documentation of its network because, if not, I can get Highpoint Solutions to give you a call for a network inspection/documentation visit. The mantra of this story is documentation and good naming nomenclature goes a long way, even if you decide to leave a company.

Note Some device pool parameters cannot be configured at the Cisco IP Phone configuration page and maybe nowhere else in CUCM Administration for that matter (Region and CUCM Group are two examples). I explore them all, and you'll be a device pool expert in no time.

The following mandatory components must be assigned to a device pool:

- CUCM Group
- Date/Time Group
- Region

The device pool combines individual configuration settings into a single logical construct that can be applied to thousands of devices. Because one CUCM server can handle a theoretical maximum of 7500 phones with a 7845-class server, it is theoretically possible to have 7500 devices associated with a device pool.

The device pool can then be assigned to devices (Cisco IP Phones, gateways, and trunks). To create, modify, or delete a device pool in CUCM Administration, choose **System > Device Pool**. Click **Add New** to display a configuration screen similar to the one shown in Figure 7-1.

Device Pool Settings	
Device Pool Name*	<input type="text"/>
Cisco Unified Communications Manager Group*	<input type="button" value="-- Not Selected --"/>
Calling Search Space for Auto-registration	<input >="" none="" type="button" value="<"/>
Reverted Call Focus Priority	<input type="button" value="Default"/>
Roaming Sensitive Settings	
Date/Time Group*	<input type="button" value="-- Not Selected --"/>
Region*	<input type="button" value="-- Not Selected --"/>
Media Resource Group List	<input >="" none="" type="button" value="<"/>
Location	<input >="" none="" type="button" value="<"/>
Network Locale	<input >="" none="" type="button" value="<"/>
SRST Reference*	<input type="button" value="-- Not Selected --"/>
Connection Monitor Duration***	<input type="text"/>
Physical Location	<input >="" none="" type="button" value="<"/>
Device Mobility Group	<input >="" none="" type="button" value="<"/>
Device Mobility Related Information****	
Device Mobility Calling Search Space	<input >="" none="" type="button" value="<"/>
AAR Calling Search Space	<input >="" none="" type="button" value="<"/>
AAR Group	<input >="" none="" type="button" value="<"/>

Figure 7-1 Device Pool Configuration

There are plenty of configuration elements in the device pool that haven't been covered yet. Don't be intimidated by the list of configuration elements at this time. Although there are many options, the items required for basic operation are simply to setup.

Phone Network Time Protocol Reference

The Phone Network Time Protocol (NTP) reference configuration element is used to provide accurate timing to Cisco IP Phones that are running Session Initiation Protocol (SIP) firmware. All Cisco 7900 Series IP Phones ship with Skinny Client Control Protocol (SCCP) by default, but they can be converted to SIP firmware with the Bulk Administration Tool (BAT). Cisco 8900 and 9900 Series phones ship with SIP firmware by default, and they cannot be converted to SCCP. One or more phone NTP references can be created in CUCM Administration and assigned to a date/time group. If a Cisco SIP phone cannot contact the NTP reference directly, the phone will use the date header in a SIP 200 OK registration response from CUCM. CUCM subscribers receive their timing information from the publisher, which was probably configured with one or more NTP references in the CUCM Operating System Administration pages. SCCP phones always time information within their SCCP signaling from CUCM.

The NTP reference is then assigned to a date/time group, and the date/time group configuration is then assigned to a device pool. The device pool is then assigned to a device (Cisco IP Phone, gateway, trunk) at the respective Device Configuration page.

The date/time group configuration descriptions are as follows:

- **IP Address:** Enter the IP address of the NTP server that the SIP phone should use to get its date and time. The site www.ntp.org is an open-source site used by millions of systems throughout the world. I suggest doing some research at this site and consider pointing your CUCM Publisher server and phone NTP references to it. A public, open-source NTP source might not meet enterprise security guidelines.
- **Description:** Enter a description for the phone NTP reference. CUCM Administration automatically propagates the information in the IP Address field to the Description field, but it can be edited if desired to follow your corporate naming nomenclature.
- **Mode:** From the drop-down list box, choose the networking mode to use for the phone NTP references. There are a lot of values to accommodate different NTP solutions and options:
 - **Directed Broadcast (default mode):** A directed broadcast is also referred to as a Layer 2 subnet broadcast in data networking. Any device providing Layer 3 (IP) routing functionality will discard this IP packet because subnet broadcasts are restricted to their associated broadcast domain. Layer 3 router interfaces and Switched Virtual Interface (SVI) on Cisco switches both represent broadcast domains. Cisco routers and switches have the ability to convert certain types of broadcasts by converting them to unicast (one-to-one conversation) or multicast (one-to-many conversation) traffic on the network. This functionality, called IP Helper, is configured with the following Cisco IOS interface configuration command: Router(config-if)# ip helper-address 192.168.1.1. This command will forward any DHCP broadcasts from remote IP subnets and convert them to a unicast packet to the 192.168.1.1 IP address of the DHCP server.

Cisco IP Phones access date/time information from any NTP server with the directed broadcast option, but a prioritized top-down priority list can be provided so that the Cisco IP Phone attempts to receive its time from those servers first. A phone NTP reference configuration with NTP servers contains server NTP server A listed first (top) and NTP server B listed second (bottom). Server A is the primary and server B is the secondary or backup NTP server. The phone uses a directed broadcast packet delivery method (192.168.1.255 on the 192.168.1.0 /24 subnet) but prioritizes responses from server A and B (in that order). If NTP server A and/or B is not broadcasting time configuration information destined to the exact subnet broadcast address, the phone receives its date and time information from any server configured to announce NTP to the IP subnet broadcast address specified. The phone will fall back to receiving date and time information from the SIP 200 OK response received from CUCM.

- **Unicast:** The phone sends an NTP query packet to the specified individual NTP server. If no NTP servers respond, the phone derives the date/time from the SIP 200 OK received from CUCM.
- **Multicast:** A multicast packet is a one-to-many conversation in data networking. Real-time distance learning applications can create a multicast group for each live class being transmitted over TCP/IP. Multicasts can greatly reduce the amount of data network throughput utilized. Real-time broadcast networks use multicast technology to broadcast different content (television stations) over IP. Each station of Verizon Fios is sent as a multicast stream so that the server does not need to stream out the traffic once for each person watching the television station (unicast). Following this broadcast TV analogy, on-demand content is sent as unicast traffic because the content is sent exclusively to you. Multicast packets are very useful in data networking, but the majority of telephony signaling and media does not use multicast. Music on Hold servers can use multicast, but this topic will be covered in Chapter 13, “Media Resources.”
- **Anycast:** Anycast packets are a broadcast (all-hosts) alternative utilized in IPv6. CUCM introduced IPv6 support in version 7.0 of the product. I don’t know whether anyone cares because of the widespread adoption of IPv4 private addressing and Network Address Translation (NAT)/Port Address Translation (PAT) techniques, but Cisco support will probably ensure that the proper check box is selected when a large company is going through a request for proposal (RFP) process in which a telecom team has architected the RFP questions based on the existing telephone switch manufacturer’s technical abilities. Winning the RFP has nothing to do with the fact that no customers might ever use the feature. I suspect this is why CUCM supports RSVP’s (Resource Reservation Protocol’s) integrated service model approach to quality of service (QoS), but I’m only theorizing. I have heard that RSVP can be beneficial between CUCM and the customer edge (CE) router (RSVP Agent) because RSVP reservations are even stricter than those provided by the QoS priority queue (PQ) mechanisms.

To create or modify a phone NTP reference in CUCM Administration, choose **System > Phone NTP Reference**. Click **Add New** to display the configuration screen shown in

Figure 7-2. Phone NTP references can be added, deleted, or modified from the Phone NTP Reference Configuration page.

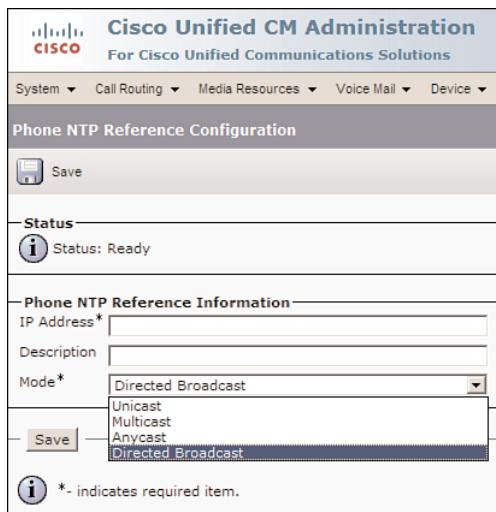


Figure 7-2 Phone NTP Reference

Date/Time Groups

Date/time groups are used to define the time zone that a device (Cisco IP Phone) should use to display the local time. Each device is assigned to a device pool, and each device pool has one assigned date/time group.

Installation of CUCM automatically configures a default date/time group that is called CMLocal. CMLocal synchronizes to the active date and time of the operating system on the Publisher server, which is automatically replicated to all Subscriber servers. CMLocal should be treated in the same way as other defaults. I suggest setting the default CMLocal date/time group to the most widely used time zone in your deployment, but try to not use this date/time group. Copy the default configuration, rename the date/time group, and change the configuration elements. A large, national, centralized call-processing deployment of CUCM would require at least four date/time groups to represent the time zones across the country. Notice that you can also change the way that time is presented to the end users on the LCDs of their Cisco IP Phones by modifying the date format and time format. Most international deployments require a day, month, year (D/M/Y) date format and a 24-hour time format, while U.S. deployments typically use M/D/Y and a 12-hour format.

To modify or delete a date/time group in CUCM Administration, choose **System > Date/Time Group**. Click **Find**. Click **Add New** to add a new date/time group, but I recommend copying, renaming, and reconfiguring an existing date/time group to create a new one. The configuration screen capture can be seen in Figure 7-3.

Date/Time Group Configuration

Status: Add successful
Click on the Reset button to have the changes take effect.

Date/Time Group Information

Date/Time Group: NewYork (used by 0 devices)

Group Name*: NewYork

Time Zone*: Eastern Standard/Daylight Time - (GMT-05:00) Eastern

Separator*: / (slash) (applies to Date Format only)

Date Format*: M/D/Y

Time Format*: 12-hour

Phone NTP References for this Date/Time Group

Selected Phone NTP References**

Add Phone NTP References | Remove Phone NTP References

Save | Delete | Copy | Reset | Add New

Figure 7-3 Date/Time Group Configuration

Cisco Unified CM Group

A CUCM group specifies a prioritized list of up to three CUCMs.

The first CUCM in the list (top) serves as the primary CUCM for that group, the next member of the list (from the top) serves as the secondary CUCM, and the third server in the list is the last in the list (bottom).

If the primary CUCM in the CUCM group is not available, the device tries to register with the second CUCM server listed in the CUCM group. The Cisco IP Phone always maintains an active TCP port 2000 (SCCP) connection open to the current active CUCM and current backup CUCM servers. Keepalives are sent every 30 seconds to the current active and current backup CUCM servers to guarantee reachability.

CUCM groups provide these important features for the CUCM system:

- **Redundancy:** Up to three CUCM servers can be defined in each CUCM group. The Cisco IP Phone has five CUCM references, but only three of them can be populated by the CUCM group configuration element. Triple call-processing redundancy is more than enough for even the most highly available networks.
- **Call-processing load sharing:** The administrator can control active device registrations by configuring multiple CUCM groups using staggered primary servers for each group. This distributes the control of devices and call-processing load. Let's look at an example where there are two CUCM subscriber servers (A and B). CUCM Group 1 would prioritize server A over B, and CUCM Group 2 would prioritize server B over

A. The CUCM groups must be configured, and the device pool will need to be associated to Cisco IP Phones.

A single CUCM server can be assigned to multiple CUCM groups to achieve better load distribution and redundancy. Different CUCM groups are configured in different device pools that collect phone configuration settings. Each CUCM group will require at least one device pool to be created. The number of device pools in the configuration will be dictated by the various configuration elements in the device pool.

To modify or delete a group in CUCM, use the CUCM Administration web page and choose **System > Cisco Unified CM Group**. Click **Find**. Click **Add New** to create a new CUCM group, but I recommend the following procedure again:

- Step 1.** Click **Find**. Click an existing CUCM group that is close to the configuration required for this CUCM group. The only change might be the name of the group and the server selection prioritization order.
- Step 2.** Click **Copy**.
- Step 3.** Rename the CUCM group with a name that describes the usage of the group.
- Step 4.** Reconfigure the CUCM group with the required prioritized list of CUCM servers.
- Step 5.** Click **Save**.
- Step 6.** Click **Reset** (or **Apply** or **Restart**).

Note Do not make any change in CUCM Administration without clicking the Save button. There is no application state information shared between the web browser and the web server. All configuration changes will be immediately discarded unless the Save button is selected. Clicking the Save button might result in a pop-up window explaining that you must reset or apply changes for your changes to be applied. The Apply Config button was new to CUCM 7.1, and I honestly do not know the difference between Apply Config and Reset or Restart because the discrepancies among the three are not well documented. I have been working with CallManager a lot since version 4.0. Depending on the version of CUCM and the phone model you're using, many phone configuration changes are normally made without clicking any buttons. The Save button commits a new configuration file to the TFTP service, and a new configuration file is pushed out to the phone. Some configuration changes only require you to click Apply Config, while others only require Restart, but Reset performs a cold boot of the phone and works nearly all the time. If you're running the same version of CUCM for a long time with the same-model phones, you'll need to figure out what configuration changes require a reset. The Reset button will not drop active phone calls. The Reset button will reset the Cisco IP Phone after it is back on-hook (handset in cradle or Speakerphone button off in the case of a hands-free call). Reset will drop every active call on a gateway device, so you might want to refrain from resetting gateways in the middle of the day. Resetting a gateway from CUCM resets the H.323 or Media Gateway Control Protocol (MGCP) gateway functionality in the gateway device

and CUCM; it will not result in the reloading of a router. Best practice is to remotely access (telnet/SSH) the gateway router and use the **show voice port summary** command. All Foreign Exchange Office (FXO) ports and T1/E1 time slots (64-kbps B channel in ISDN Primary Rate Interface (PRI) and Basic Rate Interface (BRI) interfaces) will have an IN STATUS and OUT STATUS field of on-hook or idle (depending on the type of time-division multiplexing [TDM] port on the gateway).

Figure 7-4 illustrates the CUCM Group Configuration options.

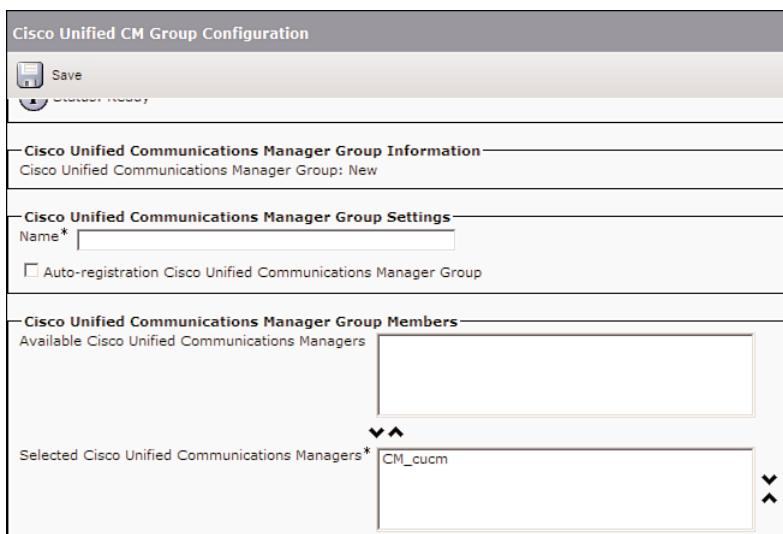


Figure 7-4 CUCM Group

Note Notice the up and down arrows that are used to select Available CUCM Managers and move them to or from the Selected CUCM Managers list. Because the Selected CUCM Managers list can include up to three servers, there is an up and down arrow to the right of the list, where individual servers can be selected and then moved up or down the order in the prioritization list.

Regions

Regions are used to specify the audio and video codecs utilized between two devices on a call-by-call basis that is used per call within and between regions. The configured audio codec determines the type of audio compression used per audio call.

The video call bandwidth comprises the sum of the audio and video bandwidth of the video call.

To modify or delete a region in CUCM, use the CUCM Administration and navigate to **System > Region**. Click **Find**. Click **Add New** to create a region. The configuration screen will appear similar to the one shown in Figure 7-5. In Figure 7-5, GK-NYC devices will use the G.722 codec when placing calls to any other device in the same region. Devices in the same region are normally connected through a LAN at Fast Ethernet (100-Mbps) or higher speeds. To change the association of one region to the other, select the destination region in the **Modify Relationship to Other Regions** screen area, select the **Audio Codec** drop-down menu, and select the video call bandwidth allowable from three video-enabled phones (9900 Series phone, Cisco Unified Video Advantage [CUVA], or Cisco Unified Personal Communicator [CUPC] at the time of this writing).

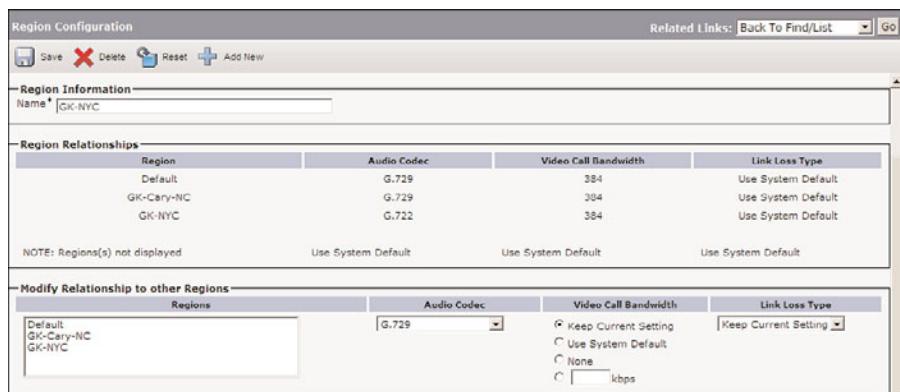


Figure 7-5 Regions

The Region Configuration screen has an additional **Link Loss Type** parameter that can be used to dynamically negotiate the maximum bandwidth between regions. Low Loss indicates a higher-quality, high-bandwidth audio codec like G.722 or G.711, while Lossy indicates a low-bandwidth, higher-complexity audio codec like iLBC (Internet Low Bandwidth Codec) or G.729. The link loss type dynamically negotiates to the highest-quality lossy or low-loss audio codec type that can be used based on maximum bandwidth requirements.

General audio codec references are as follows:

- G.722 64-kbps is preferred over G.722.1.
- G.722 at all bit rates (64, 56, and 48 kbps) is preferred over G.711.
- On low-loss links, G.722 is preferred over Internet Speech Audio Codec (iSAC).
- On lossy links, iSAC is preferred over G.722.

Note At the time of this writing, only the Cisco E20 Video Phone supports the G.722.1 audio codec. The Cisco 8961, 9951, and 9971 IP Phone models support iSAC, while the Cisco 7900 Series phone models do not.

The G.722 and iLBC codecs can generally be enabled and disabled through a CUCM CallManager service parameter (G.722 Codec Enabled/iLBC Codec Enabled option). If G.722 is enabled (the default setting), its usage can be further controlled on a per-device basis through the phone configuration page (choose **Product Specific Configuration Layout > Advertise G.722 Codec**).

The Advertise G.722 Codec parameter indicates whether Cisco IP Phones will advertise the G.722 audio codec capability to CUCM. Codec negotiation involves two steps:

- Step 1.** The Cisco IP Phone advertises the supported audio and video codecs to CUCM.
- Step 2.** CUCM chooses the highest-quality commonly supported audio codec between the calling and called party for that particular phone call. Any phone with a region configuration of Use System Default CUCM checks the Advertise G.722 Codec enterprise parameter before selecting an audio codec (enabled by default).

Note CUCM supports a maximum of 2000 regions. Each region is normally a geographical site. Exceptions to this rule occur over metropolitan-area networks (MAN) and high-speed WANs, where sites are connected through LAN speeds (normally over 100-Mbps WAN bandwidth, but every environment is different). Some large hospitals in the NY/NJ/CT area use 10 Gigabit Ethernet (10GE) as a WAN technology to connect buildings.

Locations

Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables the administrator to limit the number of audio and video calls that can traverse the WAN. WAN bandwidth is limited by the amount of bandwidth that is available for audio and video calls as configured in the priority queue (PQ) of the QoS configuration. It's important to know that voice and video communications that exceed the priority queue will be implicitly policed only when there is congestion on the link. If there is no congestion on the link, RTP media traffic (voice and video) can consume the entire link speed. As soon as there's any congestion on the output interface, all traffic in the priority queue will be limited to the configured bandwidth (implicitly policed) by Cisco IOS on the router. QoS and CAC configurations should match in the number of phone calls to be accommodated.

Note If CAC is not used to limit the audio and video bandwidth on IP WAN links, an unlimited number of calls can be active on that a link at the same time. This situation can cause the quality of all new and active audio and video calls to degrade as the link becomes oversubscribed. Compressed audio and video codecs generally will accommodate a lower amount of packet loss than uncompressed audio calls. This is especially true with G.729, which has a packet loss requirement of less than 1 percent because the compression algorithm is predictive in nature. One lost packet could have an effect on future packets, causing a voice quality degradation avalanche effect.

In a centralized call-processing system, a single CUCM cluster provides call processing for all locations on the IP telephony network. The CUCM cluster usually resides at the main location, but Cisco IP Phones and gateways to the public switched telephone network (PSTN) are distributed among two or more buildings. IP WAN links connect the remote locations to the main location.

CUCM has no concept of bandwidth limitations by default. A CAC mechanism must be used for CUCM to limit the number of calls that can be routed over WAN links. If CAC configuration is not addressed, you might be inviting a condition where 100 G.711 phone calls could be routed over a T1 data link that has QoS provisioned to accommodate seven phone calls. The failure to properly configure CAC could be a Career Limiting Event (CLE) if the CEO's phone calls over the WAN have high packet loss, delay, and jitter (delay variation). Devices can be assigned to different locations at the Cisco IP Phone Configuration of Device Pool configuration pages. Rejected calls can be rerouted over the PSTN gateways at the site using automated alternate routing (AAR) technology. AAR is turned off by default, so the calling party will receive a No Bandwidth error message on the LCD of the Cisco IP Phone. If the call is rerouted with AAR technology, the calling party would see a No Bandwidth, Re-Routing LCD message on his Cisco IP Phone.

To modify or delete a location in CUCM, use the CUCM Administration web page and choose **System > Location**. Click **Find**. Click **Add New** to display a configuration screen similar to the one displayed in Figure 7-6. Choose the location and configure the amount of audio and video bandwidth available to/from that particular location. These configurations should align to the PQ bandwidth that the data network team has provisioned across the IP WAN links. The RSVP Setting drop-down menu is explained in the Cisco Press book *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide*. RSVP is the only topology-aware QoS mechanism with built-in call admission control (CAC), but it's still too CPU intensive for me to recommend. Service providers are not going to react to any RSVP signaling passed to provider edge (PE) routers. Service providers pass the RSVP signaling state (PATH are RESV messages) through their network as customer data plane traffic. The service provider does not get involved in the negotiation of RSVP control plane traffic.

H.323 gatekeepers are a required component in distributed call-processing environments that include two or more CUCM clusters. An H.225 trunk is configured in CUCM Administration to direct all intercluster call signaling to the H.323 gatekeeper, where

CAC is applied through the “zone bandwidth” configuration commands in the H.323 gatekeeper’s gatekeeper configuration mode.

The screenshot shows the 'Location Configuration' page in the Cisco CUCM web interface. The page includes sections for Status (Status: Ready), Location Information (Name: GK-Cary-NC), Audio Calls Information (Audio Bandwidth: Unlimited, 0 kbps), Video Calls Information (Video Bandwidth: 384 kbps), and Modify Setting(s) to Other Locations (Location: Hub_None, RSVP Setting: Use System Default). A 'Save' button is at the bottom.

Location Configuration		Related Links:				
<input type="button" value="Save"/>						
Status (i) Status: Ready						
Location Information Name <input type="text" value="GK-Cary-NC"/>						
Audio Calls Information Audio Bandwidth <input checked="" type="radio"/> Unlimited <input type="radio"/> <input type="text" value="0"/> kbps <small>If the audio quality is poor or choppy, lower the bandwidth setting. For ISDN, use multiples of 56 kbps or 64 kbps.</small>						
Video Calls Information Video Bandwidth <input checked="" type="radio"/> None <input type="radio"/> Unlimited <input type="radio"/> <input type="text" value="384"/> kbps						
Modify Setting(s) to Other Locations <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 50%;">Location</th> <th style="width: 50%;">RSVP Setting</th> </tr> </thead> <tbody> <tr> <td>Hub_None</td> <td style="text-align: center;"><input type="button" value="Use System Default"/></td> </tr> </tbody> </table>			Location	RSVP Setting	Hub_None	<input type="button" value="Use System Default"/>
Location	RSVP Setting					
Hub_None	<input type="button" value="Use System Default"/>					
<input type="button" value="Save"/>						

Figure 7-6 Locations

Note H.323 gatekeeper configuration is covered in the Cisco Press book *Implementing Cisco Unified Communications Voice over IP and QoS (CVOICE) Foundation Learning Guide*.

Phone Security Profile

The Phone Security Profile Configuration window includes security-related settings such as device security mode, Certificate Authority Proxy Function (CAPF) settings, digest authentication settings (SIP phones only), and encrypted configuration file settings. A security profile must be applied to all phones that are configured in CUCM Administration, and the security profiles do not have a default value. Administrators can make use of existing security profiles that have security disabled when encryption is not required between CUCM and the devices in the network (Cisco IP Phones, gateways, and trunks).

To modify or delete a security profile in CUCM, use the CUCM Administration web page and choose **System > Security Profile > Phone Security Profile**. There are three default Phone Security Profile configurations per signaling option (SCCP/SIP) per device type. The default options available are nonsecure, authenticated, and encrypted. Figure 7-7 illustrates the default Cisco 7960 SCCP Non-Secure Phone Security Profile.

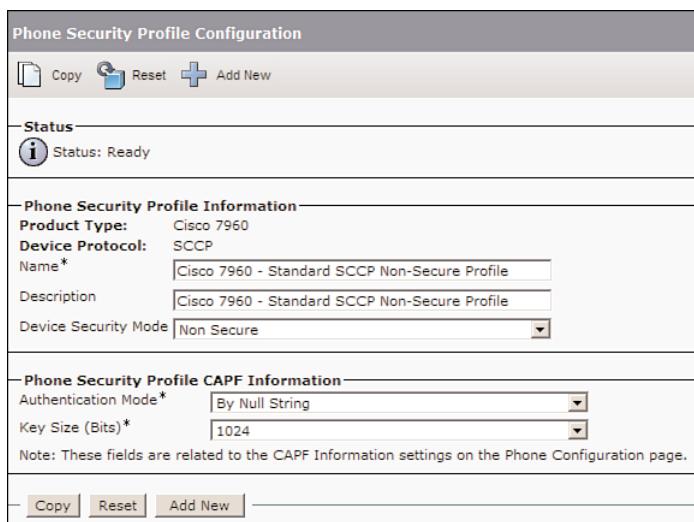


Figure 7-7 Phone Security Profile

Device Settings

Device settings are a submenu under the Device menu that includes default settings, profiles, templates, and common device configuration. Figure 7-8 displays the options that are available from the Device Settings submenu. The following sections investigate some commonly modified items in this area.

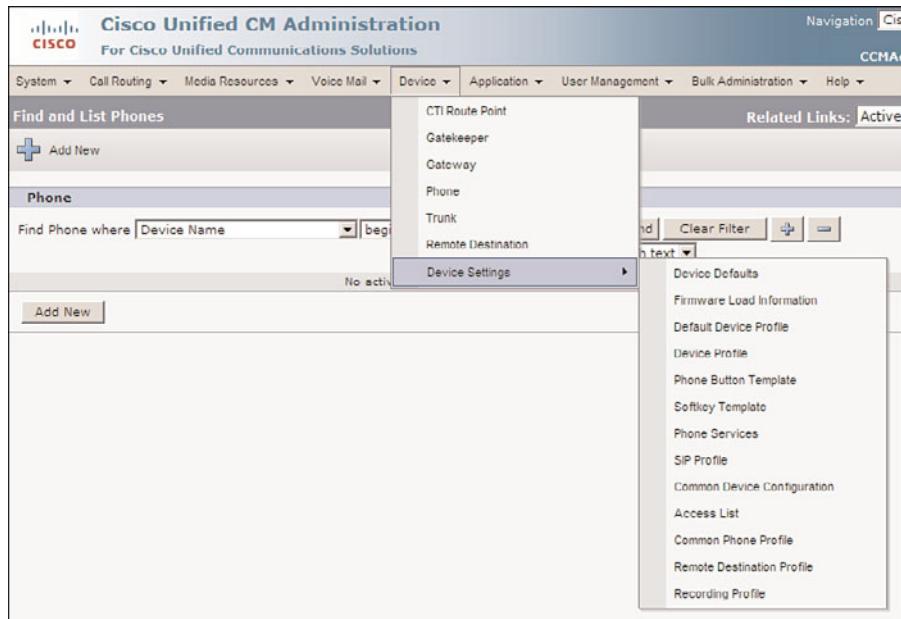


Figure 7-8 Device Settings

Device Defaults

Use device defaults to set new Load ID (phone operating system binary image/firmware) default characteristics for the types of devices used with the CUCM. The device defaults apply to all registered devices of that type within a CUCM cluster. A different phone load name (Load ID) can be specified on the Device Configuration page, next to the device listed that would override the device default ID. It normally holds true that any configuration item configured at the phone level will override any device pool or device defaults inherited has registered. The following device defaults can be set for each device type to which they apply:

- **Device load:** The firmware version that is used with a particular type of hardware device.
- **Device pool:** Allows the administrator to choose to change the firmware for a particular device type in a particular device pool.
- **Phone button template:** Indicates the phone button template that is used by each type of device. The phone button template configures the number of directory numbers, speed dials, service URLs, and programmable line keys (PLK) available to a phone.

Within CUCM Administration, choose **Device > Device Settings > Device Defaults**. Modify the firmware settings that you want to modify and click **Save**. This procedure is normally done if there is a mission-critical feature that's not working properly on many phones. The Cisco Technical Assistance Center (TAC) might have helped you out with the challenge and provided new firmware to load on the servers. Figure 7-9 displays the options available on the Device Defaults Configuration page.

Phone Button Template

Creating and using phone button templates provide a fast way to assign a common button configuration to a large number of Cisco Unified IP Phones.

CUCM includes one default phone button template per protocol (SCCP/SIP) per phone model type. When adding phones, a phone button template is a required configuration parameter, but every phone model has a default phone button template. For example, the Cisco 796x-class phone has two directory numbers (lines) and four speed dials (SD) by default.

All phones must have at least one line (directory number/DN) assigned to the respective phone button template. The remaining physical buttons on the phone can be used for additional lines (DNs), speed dials, privacy buttons, service URLs, or programmable line keys (PLK). PLK was a new feature in CUCM 6.0 that does not work with Cisco Type A phones because of architectural restrictions of the Type A phones. PLKs enable supplementary service phone features such as call hold, park, transfer, and conference to be applied to physical buttons on the phone instead of using softkey buttons underneath the LCD, which includes the call state-specific feature available. I rarely use PLKs because softkey buttons are so easy to use and work with, but it's nice to have plenty of options.

Device Defaults Configuration				
 Save				
Device Defaults Information				
Device Type	Protocol	Load Information	Device Pool	Phone Template
7914 14-Button Line Expansion Module SCCP	SCCP	S00105000300	Default	NONE
Analog Access	Protocol Not Specified	NONE	Default	NONE
Analog Access WS-X6624	Protocol Not Specified	A002H024	Default	NONE
Analog Phone	SCCP	NONE	Default	Standard Analog
Cisco 12 S	SCCP		Default	Standard 12 S
Cisco 12 SP	SCCP		Default	Standard 12 SP
Cisco 12 SP+	SCCP		Default	Standard 12 SP+
Cisco 30 SP+	SCCP		Default	Standard 30 SP+
Cisco 30 VIP	SCCP		Default	Standard 30 VIP
Cisco 3951	SIP	SIP3951.8-0-0-27	Default	Standard 3951 SIP
Cisco 7902	SCCP	CP7902080002SCCP06	Default	Standard 7902
Cisco 7905	SIP	CP7905080001SIP0604	Default	Standard 7905 SIP
Cisco 7905	SCCP	CP7905080002SCCP06	Default	Standard 7905 SCCP
Cisco 7906	SCCP	SCCP11.8-3-0-45S	Default	Standard 7906
Cisco 7906	SIP	SIP11.8-3-0-45S	Default	Standard 7906 SIP
Cisco 7910	SCCP	P00405000700	Default	Standard 7910
Cisco 7911	SCCP	SCCP11.8-3-0-45S	Default	Standard 7911
Cisco 7911	SIP	SIP11.8-3-0-45S	Default	Standard 7911 SIP

Figure 7-9 Device Defaults Configuration

Before adding any IP phones to the system, create phone button templates with all the required combinations of lines and speed dials that you envision using.

To modify or delete a phone button template in CUCM, use the CUCM Administration web page and navigate to **Device > Device Settings > Phone Button Template**. Click **Find** and choose an existing phone button template to display a configuration screen similar to the one shown in Figure 7-10. Notice all the options that can be applied to the physical button in Figure 7-10.

Softkey Template

Softkey templates allow the administrator to manage softkey availability and arrangement/order on Cisco IP Phones. There are many softkey features that are not enabled by default.

Applications that support softkeys can have one or more softkey templates associated with them based on the functionality required. CUCM includes some default softkey templates, including the Standard Feature and the Standard User softkey templates. Every Cisco IP Phone is assigned the Standard User softkey template by default. The default softkey templates are similar to the default roles and user groups in the respect that the defaults in CUCM cannot be changed. A softkey template can be copied, renamed, and reconfigured, but the default softkey templates cannot be modified.

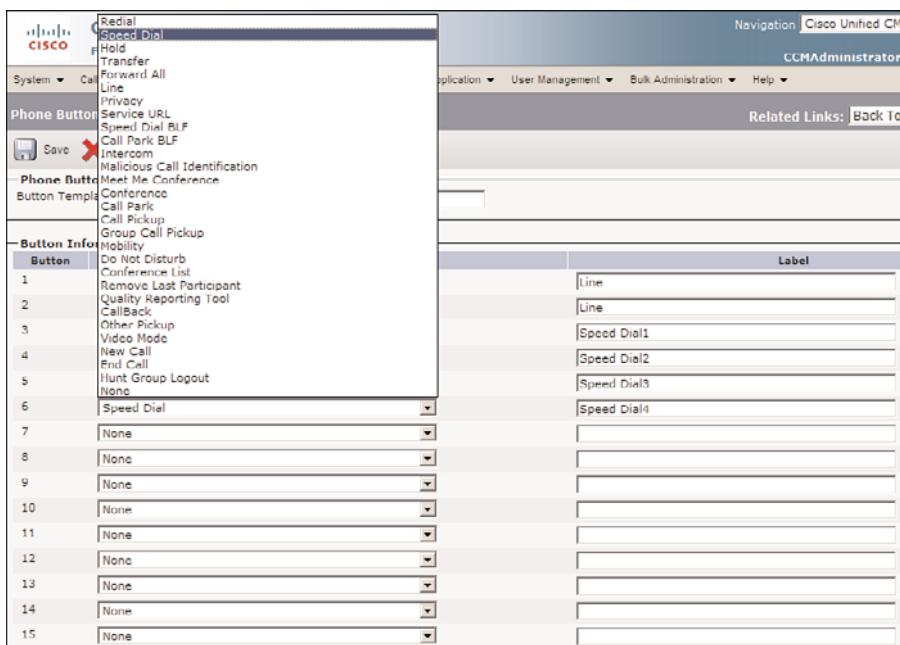


Figure 7-10 Phone Button Template

Choose Device > Device Settings > Softkey Templates to access the Softkey Template Configuration window in CUCM Administration. Click **Find** and choose an existing softkey template. Click the **Copy** button and rename the softkey template. Click **Save**. The resulting page presentation is a bit confusing. Find the Configure Softkey Layout option on the Related Links drop-down menu in the upper-right portion of the screen underneath the Navigation drop-down menu. Click the Go button next to Configure Softkey Layout.

Select a call state to modify the softkey templates for and move the softkeys from the Unselected Softkeys to the Selected Softkeys portion of the screen by selecting the softkey and clicking the left and right arrow buttons. Different softkeys can be enabled/disabled or have their phone display order changed (on a per-call state basis). Call states relate to the operation of the phone at the time in which the end user is looking at the available features illuminated on the LCD of the IP phone above the hardware softkey select buttons. Cisco 797x Series phones have an LCD with touch sensitivity, allowing menu selections to be made by touch. The different call states indicate the operation of the phone. The call state names are somewhat self-explanatory, so I will not spend any time on them, but I encourage you to play with your Cisco IP Phone to see the different softkeys that are displayed.

Note You will receive an error message if you try to enable more than 16 softkeys in any particular call state. You can set 16 softkey functions per call state, but there's a lot of

different call states to play with. Most end users attempt to use softkey features from the Connected (active call) call state. I'm not sure whether 16 was a limitation of the Cisco phone model or the system. I've never felt compelled to research the 16 softkey limitation because it's not much of a limitation. Setting more than a certain number of softkey features can get my end users confused.

The last softkey on the Cisco IP Phone will always be More if there are more than three or four options in that particular call state. The Cisco 794x and 796x phones have four softkey buttons, while the 797x Cisco IP Phones have five softkey buttons as well as a Sleep/Resume button.

Some users might never click the More key to see what's hidden behind door number 2, but this is why end-user training on the new system will be so important. How many of your end users are going to click the More softkey four or five times to use the last of 16 softkey features without knowing that what they're looking for is hiding there?

Softkey position order arrangement is performed by clicking the up and down arrows on the right side (position). Figure 7-11 displays the configuration of a softkey template.

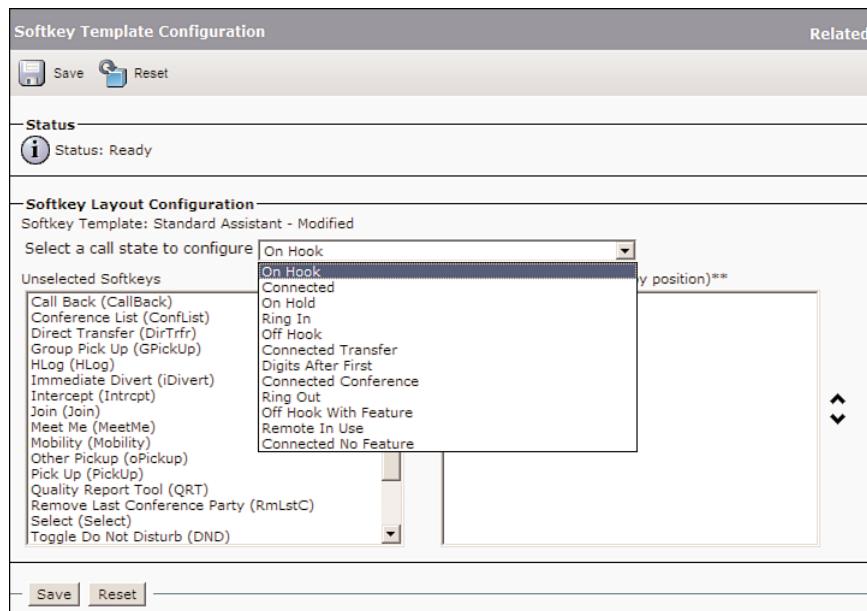


Figure 7-11 Softkey Template

SIP Profile

A SIP profile comprises the set of SIP attributes that are associated with SIP trunks or SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup Uniform Resource Identifier (URI), and so on. The profiles contain some standard entries that cannot be deleted or changed.

SIP profiles are useful for third-party SIP integration. SIP profiles allow the administrator to modify the SIP call-signaling timeouts and retries. There are many options in Internet Engineering Task Force (IETF) standards that different vendors apply differently.

Note A SIP URI consists of a call destination configured with a user@host format, such as xten3@CompB.cisco.com or 20850173285060.

SIP-based phones and SIP trunks have a required SIP profile selection. A default SIP profile (standard SIP profile) can be assigned to SIP phones and trunks. If a third-party integration does not work properly, you will probably need to delve into the details of all the various SIP signaling timers in the SIP profile. The standard SIP profile cannot be deleted or modified. To create a new SIP profile, copy the default SIP profile, change the name of the profile, edit the profile, and save it. SIP profiles are configured from CUCM Administration. Choose **Device > Device Settings > SIP Profile**. Figure 7-12 shows a portion of the SIP Profile Configuration page.

The screenshot displays the 'SIP Profile Configuration' interface. At the top, there are buttons for Copy, Reset, and Add New. The main area is divided into two sections: 'SIP Profile Information' and 'Parameters used in Phone'.

SIP Profile Information:

- Name*: Standard SIP Profile
- Description: Default SIP Profile
- Default MTP Telephony Event Payload Type*: 101
- Redirect by Application
- Disable Early Media on 180

Parameters used in Phone:

Timer Invite Expires (seconds)*	180
Timer Register Delta (seconds)*	5
Timer Register Expires (seconds)*	3600
Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Start Media Port*	16384
Stop Media Port*	32766

Figure 7-12 SIP Profile

Common Phone Profiles

Common phone profiles include phone configuration parameters such as the phone password (for supported Cisco IP Phones), Do Not Disturb (DND), and personalization settings (end-user access to background images and ringers). Common phone profiles are assigned to Cisco IP Phones at the Phone Configuration Administration page. The default Cisco IP Phone unlock password is **#, but the common phone profile provides the ability to change this default password, which locks the end user out of Cisco IP Phone configuration changes (for example, deleting the phone's configuration file requires the phone to be unlocked). Cisco IP Phones can also be rebooted with the **### keypad sequence, but the Cisco IP Phone must be in the Settings menu to unlock or reboot the phone.

Common phone profiles can be accessed by navigating to **Device > Device Settings > Common Phone Profile** in CUCM Administration. There is a default standard common phone profile that can be used as is or as a template for the creation of subsequent common phone profiles. Figure 7-13 shows the Common Phone Profile Configuration administration page.

Common Phone Profile Configuration									
	Save		Delete		Copy		Reset		Add New
Status									
Status: Ready									
Common Phone Profile Information									
Name*	Standard Common Phone Profile								
Description	Standard Common Phone Profile								
Local Phone Unlock Password									
DND Option *	Ringer Off								
DND Incoming Call Alert*	Beep Only								
Phone Personalization*	Default								
<input checked="" type="checkbox"/> Enable End User Access to Phone Background Image Setting									
<input type="button" value="Save"/> <input type="button" value="Delete"/> <input type="button" value="Copy"/> <input type="button" value="Reset"/> <input type="button" value="Add New"/>									

Figure 7-13 Common Phone Profile

Phone Configuration Element Relationship

Figure 7-14 illustrates the relationship of various CUCM configuration elements and their assignment to the Cisco IP Phone. The NTP reference in Figure 7-14 is assigned to the date/time group, and the date/time group is applied to the device pool. The device pool is assigned to the Cisco IP Phone, allowing the IP phone to inherit settings configured at the device pool level.

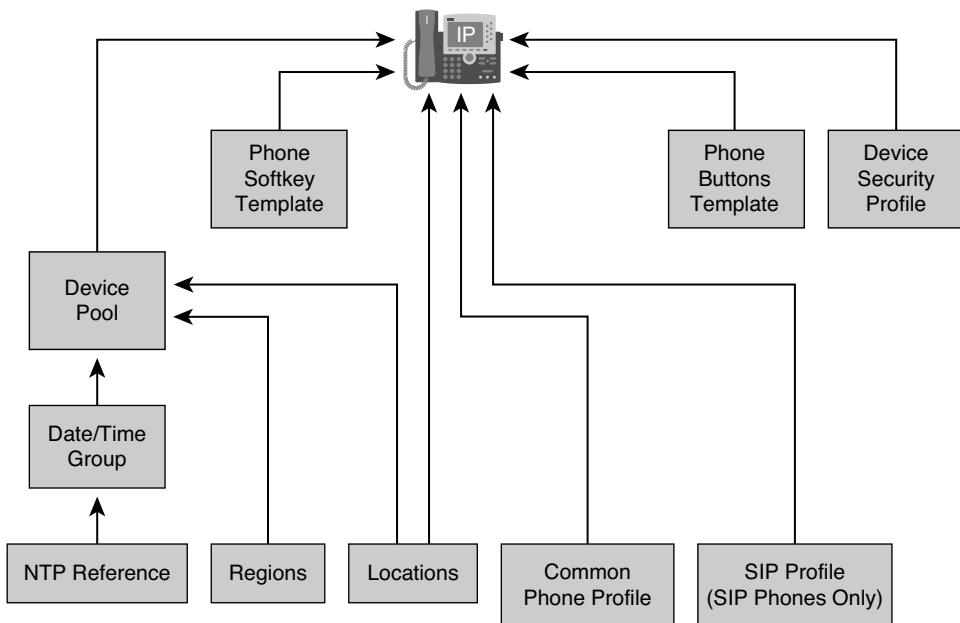


Figure 7-14 Phone Configuration Element Relationship

There are some CUCM configuration parameters that can be applied at both the device pool and the phone configuration page. You might run across the case where you have a configuration discrepancy at the device pool and phone configuration window. Figure 7-14 illustrates that the Locations configuration parameter can be set at both the device pool and phone configuration level. If the device pool was set for Location A and the phone's configuration page was set for Location B, the phone would be placed in Location B. Configuration discrepancies should be avoided at all costs, but they're somewhat inevitable in our world of information technology. The device (phone, gateway, trunk) configuration will be prioritized over any inheritance if there is a configuration discrepancy (mismatch).

Phone Auto-registration

Auto-registration allows CUCM to issue directory numbers to new Cisco IP Phones. This auto-registration process is similar to the way in which a DHCP server automatically distributes IP addresses to devices, so no manual configuration of the TCP/IP stack is required.

Auto-registration eases only one small part of overall CUCM configuration when adding a high number of IP phones. The MAC addresses of the phones are automatically added to the CUCM configuration database. The extensions normally have to be modified on a per-phone basis.

Most CUCM implementations are replacing existing solutions, where end users already have assigned phones with assigned extension numbers that are mapped to a PSTN Direct Inward Dialing (DiD) plan that is printed on the end users' business cards. In other words, there is normally a requirement to have the same phone number assigned to the user's replacement phone. This requirement doesn't make auto-registration useless, but it makes auto-registration less useful as a deployment tool.

If a large number of phone settings need to be changed, CUCM BAT can be used to automate the phone configuration changes.

Note For large deployments, the CUCM Tool for Auto-Registered Phone Support (TAPS) can be used, which allows specific extensions to be assigned to individual phones based on user input.

Auto-registration occurs as part of the IP phone startup process, at the point where the IP phone tries to download its configuration file from the TFTP server. Assuming that the IP phone has a MAC address of 0015C5AABBDD, the following will happen:

1. The Cisco IP Phone attempts to download its configuration from the TFTP server using its burned-in Ethernet MAC address. The TFTP server will not have a configuration file for the phone because it has not been configured (SEP0015C5AABBDD.cnf.xml). Each preconfigured phone in CUCM will have a unique XML configuration file in the CUCM TFTP server. The TFTP server returns a "Read Error" to the IP phone TFTP request. The "Read Error" will display a "Registration Rejected" message on the LCD of the Cisco IP Phone.
2. The Cisco IP Phone then queries the TFTP server for the XmlDefault.cnf.xml file. CUCM automatically creates a phone device record in the configuration database and assigns a directory number (DN) to the first line of the device based on the auto-registration DN range. A unique configuration file (SEP0015C5AABBDD.cnf.xml) is automatically created and added to the TFTP server.
3. The Cisco IP Phone requests a firmware update from the TFTP server if the load (firmware) information defined in the configuration file from CUCM references a newer firmware version than the one the phone is currently running.
4. The Cisco IP Phone registers to the CUCM server configured for auto-registration.

The auto-registration poses a security risk to the UC network. Auto-registration allows anyone with physical access to the plug in an RJ-45 head into a network jack to start making phone calls. Auto-registration is turned off by default. The security risks of auto-registration can be minimized by applying partitions to all route patterns in the CUCM system and configuring the system to assign a Calling Search Space, which exclude these partitions, to all auto-registering phones. This topic is covered in more detail in Chapter 10, "Calling Privileges."

A range of directory numbers must be configured in CUCM to perform auto-registration. CUCM assigns the next available DN out of the configured range. One DN is assigned

per IP phone. The administrator has no way of controlling which DN will be allocated on a per-device basis without the use of the Auto-Register Phone Tool (previously the Tool for Auto-Registered Phone Support [TAPS]).

The default signaling protocol is SCCP for auto-registered IP phones. The default auto-register signaling protocol can be set to SIP in the CUCM Administration Enterprise parameter. Cisco IP Phone endpoints that support only one protocol will still be able to auto-register, even if the auto-registration protocol is set to the other protocol.

Auto-registration Configuration

There are three steps involved in configuring for auto-registration. The fourth step is optional, although nearly always required unless TAPS will be used as well:

- Step 1.** Verify that the desired auto-registration default protocol is selected.
- Step 2.** Ensure that auto-registration is enabled on one CUCM group.
- Step 3.** Configure one or more CUCM subscriber servers in the cluster to use auto-registration.
- Step 4.** (Optional) Reconfigure the automatically added phones to configure the individual settings of each phone. This can be done using CUCM BAT for groups of phones that share a common setting (for example, the Site identifier in the Description field of the phone configuration).

The default auto-registration protocol can be changed in CUCM Administration. Choose **System > Enterprise Parameters** in SCCP. If the auto registration phone protocol is changed, the CallManager service must be restarted for that particular server (Cisco Unified Serviceability: Choose **Tools > Control Center - Feature Services**). Figure 7-15 displays the autoregistration phone protocol enterprise parameter.

Auto registration can be enabled on only one CUCM group. Selecting the Enable Auto-Registration check box on one CUCM group automatically disables the check box on the group that previously had auto-registration enabled (if applicable). In CUCM Administration, choose **System > Cisco Unified CM Group** and select the group that should provide the auto-registration service. Select the Enable Auto-Registration check box. Figure 7-16 displays a Cisco Unified CM Group Configuration page enabled for auto-registration.

Complete these steps to enable auto registration on a CUCM server in the cluster that is running the CallManager service (subscriber server):

- Step 1.** In CUCM Administration, choose **System > CUCM**.
- Step 2.** Click **Find**. Click the server that should be configured for auto-registration.
- Step 3.** Enter a starting directory number and an ending directory number to configure the directory number range. The Auto-registration Disabled on this Cisco Unified Communication Manager check box is selected by default, but will

automatically become deselected after a directory number range has been configured. Verify that this check box is not selected.

Auto-Registration Phone Protocol

Enterprise Parameters Configuration		
<input type="button" value="Save"/> <input type="button" value="Set to Default"/> <input type="button" value="Reset"/>		
Enterprise Parameters Configuration		
Parameter Name	Parameter Value	Suggested Value
Synchronization Between Auto Device Profile and Phone Configuration *	True	True
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120	120
Auto Registration Phone Protocol *	SCCP	SCCP
BLF For Call Lists *	SCCP	Disabled
Advertise G.722 Codec *	SIP	Enabled
Phone Personalization *	0	0
CCMAdmin Parameters		
Max List Box Items *	250	250
Max Lookup Items *	1000	1000
Enable Dependency Records *	False	False

Figure 7-15 Auto-Registration Phone Protocol

Enable auto-registration

Cisco Unified CM Group Configuration

Cisco Unified CM Group Configuration	
<input type="button" value="Save"/>	
Status	
Status: Ready	
Cisco Unified Communications Manager Group Information	
Cisco Unified Communications Manager Group: New	
Cisco Unified Communications Manager Group Settings	
Name *	NYC_CCMG
<input checked="" type="checkbox"/> Auto-registration Cisco Unified Communications Manager Group	
Cisco Unified Communications Manager Group Members	
Available Cisco Unified Communications Managers	
<div style="border: 1px solid #ccc; padding: 5px; height: 100px; margin-bottom: 10px;"></div>	
Selected Cisco Unified Communications Managers *	
<div style="border: 1px solid #ccc; padding: 5px; height: 100px; margin-bottom: 10px;"> <div style="border: 1px solid #ccc; padding: 2px; width: 100%; height: 100%;">CM_cucm</div> </div>	
<input type="button" value="Save"/>	

Figure 7-16 Auto-Registration: CUCM Group Configuration

Step 4. Click Save.

Figure 7-17 displays the Cisco Unified CM Configuration page.

The screenshot shows the 'Cisco Unified CM Configuration' page. At the top right, there is a text input field labeled 'Enter DN range for auto-registration'. Below it, the 'Cisco Unified Communications Manager Information' section shows 'Cisco Unified Communications Manager: CM_cucm (used by 12 devices)'. The 'Server Information' section includes fields for 'CTI ID' (1), 'Cisco Unified Communications Manager Server*' (cucm), 'Cisco Unified Communications Manager Name*' (CM_cucm), and 'Description' (cucm). The 'Auto-registration Information' section contains fields for 'Starting Directory Number*' (1000), 'Ending Directory Number*' (1000), 'Partition' (< None >), and 'External Phone Number Mask'. A checkbox at the bottom left of this section is checked, with the label 'Enable auto-registration' pointing to its right. The checkbox text is 'Auto-registration Disabled on this Cisco Unified Communications Manager'.

Figure 7-17 Cisco Unified CM Configuration

Bulk Administration Tool and Auto-Register Phone Tool

CUCM BAT enables you to bulk-update, -add, or -delete records.

CUCM BAT requires the MAC addresses of the Cisco IP Phones as well as directory number configuration. BAT is capable of configuring most phone parameters, but a small subset of the phone and directory number patterns is normally configured in the customization of the comma-separated value that is normally exported from the Microsoft Excel BAT.xlt file.

Note The MAC address is printed on a sticker in the middle of the back of the phone. The sticker includes the text-based MAC address and a bar code that can be scanned. The same sticker can be found on the outside of the box. This allows bar-code scanners to be used instead of manually typing MAC addresses into the BAT.xlt application.

The CUCM Auto-Register Phone Tool requires Cisco CRS server scripts that are installed onto a Cisco CRS server. The CRS server is the main component of Cisco Unified Contact Center eXpress (UCCX).

The CUCM Auto-Register Phone Tool allows phones to be added to CUCM with their required configurations and dummy MAC addresses. CUCM BAT and auto-registration are vital components of the Auto-Register Phone Tool. BAT creates the unique configuration of each Cisco IP Phone, while auto registration allows the phones to be deployed without coordinating individual hardware phones to individual office or cubicle locations. The real MAC addresses of the user's phone will be updated as part of the auto registration phone tool process.

The Auto-Register Phone Tool is an interactive voice response (IVR) application running on the Cisco CRS.

Auto-Register Phone Tool

The Auto-Register Phone Tool has the following requirements:

- The Bulk Provisioning and CUCM Auto-Register Phone Tool must be activated on the Publisher server in the CUCM cluster and be running. These services can be enabled from Cisco Unified Serviceability by choosing **Tools > Control Center - Feature Services**.
- All the necessary CRS files can be downloaded from CUCM Administration by choosing **Application > Download Plug-In**.
- Installation prerequisites for the Cisco Unified Communications Manager Auto-Register Phone Tool are as follows:
 - CUCM publisher is running with the required services and integrated with Cisco CRS (Java Telephony Application Programming Interface [JTAPI] is used).
 - Cisco CRS is running with the required services and integrated with CUCM.
 - The CRS server is running the required scripts associated to the proper JTAPI triggers.

Note Details for the installation, configuration, and integration of the Cisco CRS server are not part of this book. These concepts are covered in the Cisco course UCXXD. An AXL (AVVID XML Layer) Administrator account needs to be configured for Cisco CRS so that it can access and update the CUCM database.

TAPS: Phone Insert Process

Figure 7-18 illustrates the TAPS insertion process described here:

1. Use CUCM BAT to configure Cisco IP Phones with dummy MAC addresses.
2. A Cisco IP Phone is plugged in to the network. The phone auto-registers with CUCM, which creates a new device record with a directory number from the auto-registration range.
3. Someone must dial the CUCM Auto-Register Phone Tool CRS application. The CRS script will be associated with a Computer Telephony Integration (CTI) route point in CUCM.
4. CUCM routes the call to CUCM Auto-Register Phone Tool application on Cisco CRS.
5. Cisco CRS prompts the user to enter the appropriate directory number. The number is then looked up in the phone configuration records that were previously added using CUCM BAT using a dummy MAC address.
6. Cisco CRS updates the dummy MAC address of the phone with the real MAC address of the Cisco IP Phone in CUCM.
7. The Cisco IP Phone configuration file is pushed from the TFTP server to the Cisco IP Phone.

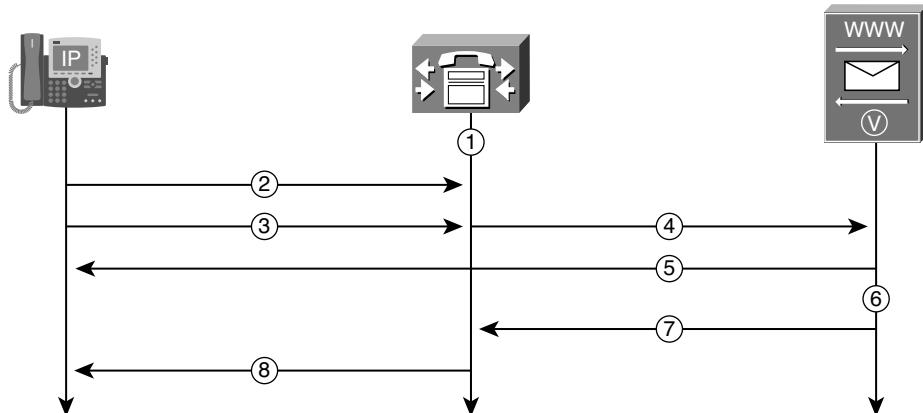


Figure 7-18 Auto-Register Phone Tool: Phone Insertion Process

Bulk Administration Tool

The procedure for adding the Cisco IP Phones using BAT is as follows:

- Step 1.** Verify that the Bulk Provisioning Service has been activated.
- Step 2.** Configure the CUCM BAT template.
- Step 3.** Create a comma-separated values (CSV) data input file (normally exported from BAT.xls).

- Step 4.** Upload the CSV data input file to the CUCM server.
- Step 5.** Validate the data input file.
- Step 6.** Insert the devices into the CUCM database.
- Step 7.** Verify the phone configuration.

Bulk Provisioning Service

You can verify the Bulk Provisioning Service (BPS) status from the Cisco Unified Serviceability pages available at <https://<ip-address>/ccmService>. Alternatively, the serviceability pages can be loaded by choosing Cisco Unified Serviceability from the Navigation drop-down menu in the upper-right portion of most CUCM Administration web pages. Click the Go button (or press Tab+Enter if you're a keyboard-shortcut person like I am).

In Cisco Unified Serviceability, choose **Tools > Control Center - Feature Services** to verify that the Cisco BPS is running. If the service is not activated, choose **Tools > Service Activation** and activate the service. If the service is not running, start the service by selecting the radio button next to the service and clicking the green Start button.

Phone Template

A phone template is required to add a Cisco IP Phone with BAT. The phone template contains common parameters that will normally not differ for any of the phones added with that particular template. The phone template must include the mandatory name field, but that's about all. Phone templates have an abbreviated set of configuration options when compared to those available in the BAT.xlt file used to export the CSV file, which is actually exported as a .txt file. Don't get confused by this. The file that is exported is CSV formatted, but it's actually a regular .txt file that you should never open in a text editor. Text editors can corrupt the file by adding certain line feeds or carriage returns. Individual phone configuration parameters are entered in the CSV data file, while the phone template is meant to be very high level.

Follow these steps to create a phone template:

- Step 1.** In CUCM Administration, choose **Bulk Administration > Phones > Phone Template**. The Find and List Phone Templates window displays.
- Step 2.** Click the **Add New** button. The Add a New Phone Template window is displayed.
- Step 3.** In the Phone Type drop-down list, choose the phone model (one template will be required per phone model) for which the template is to be created. Click the **Next** button.
- Step 4.** Choose the device protocol from the Select the Device Protocol drop-down list. Click **Next**. The Phone Template Configuration window displays, with fields and default entries for the chosen device type.
- Step 5.** In the Template Name field, enter a name for the template. The name can contain up to 50 alphanumeric characters (for example, Sales_7960).

Step 6. Enter the phone settings that will be identical among all phones added with this template. Best practice is to only configure the required fields marked with an asterisk. The phone and line template configuration options are best left to be configured with the CSV file. The Phone Template Configuration page is displayed in Figure 7-19.

Step 7. Click Save.

The screenshot shows the 'Phone Template Configuration' page with the following details:

- Configure device parameters** header at the top right.
- Enter the phone template name** field containing '7961 - SG'.
- Phone Type** section: Product Type: Cisco 7961, Device Protocol: SCCP.
- Device Information** section:
 - Template Name***: 7961 - SG
 - Description**: (empty)
 - Device Pool***: -- Not Selected -- (dropdown menu)
 - Common Device Configuration**: (empty dropdown menu)
 - Phone Button Template***: -- Not Selected -- (dropdown menu)
 - Softkey Template**: < None > (dropdown menu)
 - Common Phone Profile***: Standard Common Phone Profile (dropdown menu)
 - Calling Search Space**: < None > (dropdown menu)
 - AAR Calling Search Space**: < None > (dropdown menu)
 - Media Resource Group List**: < None > (dropdown menu)
 - User Hold MOH Audio Source**: < None > (dropdown menu)
 - Network Hold MOH Audio Source**: < None > (dropdown menu)
 - Location***: Hub_None (dropdown menu)
 - AAR Group**: < None > (dropdown menu)
 - User Locale**: < None > (dropdown menu)
 - Network Locale**: < None > (dropdown menu)

Figure 7-19 Phone Template Configuration

Line Template

Click the Line [1] Add a new DN link in the upper-left corner of the phone configuration window. This information is underlined to indicate that it is a hyperlink to another configuration page. The Line Template Configuration window, shown in Figure 7-19, will be displayed after you click the hyperlink.

The following steps outline the Line Template process:

- Step 1.** Enter the line template name. Click Save. A variety of line (directory number) configuration information can be configured here, but this information is also available in the CSV file created with BAT.xls.
- Step 2.** CUCM BAT adds the line template to the phone template configuration.

Step 3. Repeat the procedure to add more line templates if the phone button template used in the phone template is using more than one directory number. There are many interrelated parameters when it comes to using BAT.

Note The maximum number of lines that display for a CUCM BAT template depends on the model and phone button template that the administrator chose when the administrator created the CUCM BAT phone template.

Enter the line template name	Configure line parameters																										
Line Template Configuration <div style="display: flex; justify-content: space-between;"> Save Related Lines </div> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> Directory Number Information <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Line Template Name*</td> <td>Standard 7961 - Line 1</td> </tr> <tr> <td>Route Partition</td> <td style="text-align: center;"><input type="button" value="< None >"/></td> </tr> <tr> <td>Description</td> <td style="height: 40px;"></td> </tr> <tr> <td>Alerting Name</td> <td style="height: 40px;"></td> </tr> <tr> <td>ASCII Alerting Name</td> <td style="height: 40px;"></td> </tr> <tr> <td><input checked="" type="checkbox"/> Active</td> <td></td> </tr> </table> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Directory Number Settings <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Voice Mail Profile</td> <td style="text-align: center;"><input type="button" value="< None >"/></td> <td rowspan="6" style="vertical-align: middle; font-size: small;">Choose <None> to use system default</td> </tr> <tr> <td>Calling Search Space</td> <td style="text-align: center;"><input type="button" value="< None >"/></td> </tr> <tr> <td>Presence Group*</td> <td style="text-align: center;"><input type="button" value="Standard Presence group"/></td> </tr> <tr> <td>User Hold MOH Audio Source</td> <td style="text-align: center;"><input type="button" value="< None >"/></td> </tr> <tr> <td>Network Hold MOH Audio Source</td> <td style="text-align: center;"><input type="button" value="< None >"/></td> </tr> <tr> <td>Auto Answer*</td> <td style="text-align: center;"><input type="button" value="Auto Answer Off"/></td> </tr> </table> </div>		Line Template Name*	Standard 7961 - Line 1	Route Partition	<input type="button" value="< None >"/>	Description		Alerting Name		ASCII Alerting Name		<input checked="" type="checkbox"/> Active		Voice Mail Profile	<input type="button" value="< None >"/>	Choose <None> to use system default	Calling Search Space	<input type="button" value="< None >"/>	Presence Group*	<input type="button" value="Standard Presence group"/>	User Hold MOH Audio Source	<input type="button" value="< None >"/>	Network Hold MOH Audio Source	<input type="button" value="< None >"/>	Auto Answer*	<input type="button" value="Auto Answer Off"/>	
Line Template Name*	Standard 7961 - Line 1																										
Route Partition	<input type="button" value="< None >"/>																										
Description																											
Alerting Name																											
ASCII Alerting Name																											
<input checked="" type="checkbox"/> Active																											
Voice Mail Profile	<input type="button" value="< None >"/>	Choose <None> to use system default																									
Calling Search Space	<input type="button" value="< None >"/>																										
Presence Group*	<input type="button" value="Standard Presence group"/>																										
User Hold MOH Audio Source	<input type="button" value="< None >"/>																										
Network Hold MOH Audio Source	<input type="button" value="< None >"/>																										
Auto Answer*	<input type="button" value="Auto Answer Off"/>																										

Figure 7-20 Line Template Configuration

CSV File

A CSV file is used to configure the device and directory number configuration parameters of the Cisco IP Phone. Although it is theoretically possible to create your own CSV files with a text editor, Cisco provides a Microsoft Excel spreadsheet on CUCM (BAT.xls) to assist in the creation of the CSV file.

Download the BAT.xls file from CUCM Administration by choosing **Bulk Administration** > **Upload/Download Files**. Click **Find**. A BAT.xls file should be displayed in the list of available files. Select the check box next to BAT.xls, and click the **Download Selected** button. Open the file in Microsoft Excel.

A little bit of Microsoft Excel knowledge goes a long way when working with the BAT.xls file used to generate the CSV file. You will first need to change the macro security settings in Microsoft Excel to enable macros, or the BAT.xls file will not work. The existing macro security setting should be restored after the creation of the CSV file.

Click the **Create File** button and choose the Cisco IP Phone configuration parameters that you will be setting from the Device fields, Line fields, and Intercom fields. BAT can

be run with one or more fields provided. Click the **>>** button to move the field into the Selected Fields portion of the page. Click **Create**.

At this point, a macro is run in Microsoft Excel, and you will see new column heading options that match the fields you had previously selected. Choose the number of phone lines and speed dials that you will be creating. You will need to scroll all the way to right side of your screen to see these options (underneath the Export to BAT Format button).

Configure the fields that were created previously. The number of directory numbers must match the number of line templates that were configured in the phone template. The system will not accept the configuration of a varying number of lines in the same BAT operation.

Click **Export to BAT Format**. Change the default file-saving location to a place where you will be able to easily identify the file (perhaps the desktop).

Follow these steps to upload the CSV file containing the device data to the CUCM server:

- Step 1.** Choose **Bulk Administration > Upload/Download Files**. The Find and List Files window displays.
- Step 2.** Click **Add New**. The File Upload Configuration window displays. See Figure 7-21.

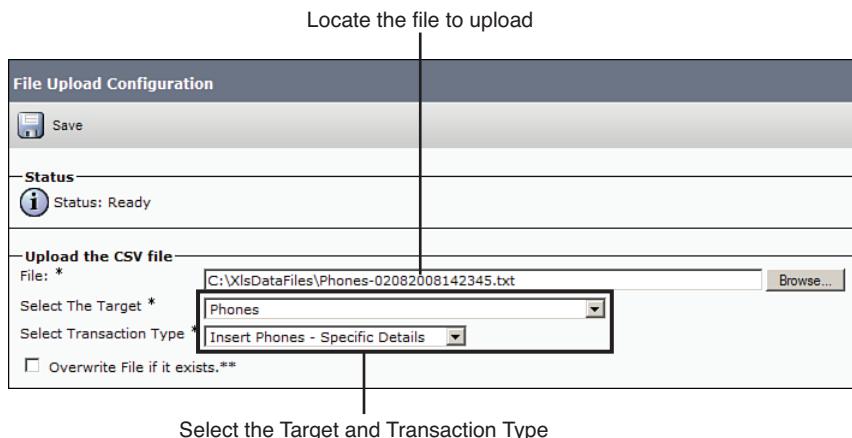


Figure 7-21 CSV File Upload

- Step 3.** Click **Browse** and locate the file.
- Step 4.** From the Select the Target drop-down list, choose **Phones**.
- Step 5.** Notice that there are two options available in the Select Transaction Type drop-down list (Insert Phones - All Details and Insert Phones - Specific Details). Make sure that you select **Insert Phones - All Details** (unless you specified *every* parameter in BAT.xlt). BAT.xlt is normally used to configure a CSV file that might have as few as six or seven configuration parameters, so it is quite common to choose **Insert Phones - Specific Details**. If you choose the wrong option, the BAT process will fail or have failed records.

- Step 6.** If the file is to overwrite an existing file with the same name, do not select the **Overwrite File If It Exists** check box unless you know that a file with that existing name already exists in CUCM and it should be updated by the file you are uploading at this time.
- Step 7.** Click **Save** and wait for updated status information; the status should be **Successful**.

Phone Validation

After uploading the CSV file, it is common to run a validation routine to check that the CSV data file and CUCM BAT phone template have populated all required fields. The validation also checks for existing MAC addresses in the database.

To validate the CSV data file phone records, follow these steps:

- Step 1.** In CUCM Administration, choose **Bulk Administration > Phones > Validate Phones**. The Validate Phones Configuration window appears, as shown in Figure 7-22.

Select the file to validate	Select the template to be used
Validate Phones Configuration	
<input type="button" value="Submit"/>	
Status Status: Ready	
Validate Phones	
<input checked="" type="radio"/> Validate Phones Specific Details	
File Name * <input type="button" value="..."/>	Phones-02082008142345.txt <input type="button" value="View File"/>
Phone Template Name * <input type="button" value="..."/>	
<input type="radio"/> Validate Phones All Details	
File Name * <input type="button" value="..."/>	<input type="button" value="View File"/>
<input type="button" value="Submit"/>	
Start Validation	Validate all details

Figure 7-22 Phone Validation

- Step 2.** Select the **Validate Phones Specific Details** radio button because you will commonly only be configuring certain configuration options. I've never configured them all, and I don't know why you would need to, but the option exists.
- Step 3.** In the File Name drop-down menu, choose the CSV data file by the name that you had previously uploaded to CUCM.
- Step 4.** Choose the CUCM BAT phone template that was created in tandem with the CSV file.

Step 5. Click Submit to begin the validation.

Step 6. The job is submitted and processed immediately.

Check for the status of the validation. Only proceed to the next step if the validation was successful. If the validation was not successful, there are probably mismatches in the phone template, line template, and CSV details (for example, a CSV file configured one line for a phone, but the phone template used for this particular BAT operation is using two line templates). The number of line templates and configured directory numbers in the CSV file must match.

Inserting IP Phones into the CUCM Database

To bulk insert phones, follow these steps:

Step 1. In CUCM Administration, choose Bulk Administration > Phones > Insert Phones. The Insert Phones Configuration window displays (shown in Figure 7-23).

Select the file and template

Insert Phones Configuration	
<input type="button" value="Submit"/>	
Status Status: Ready	
Insert Phones	
<input checked="" type="radio"/> Insert Phones Specific Details	
File Name * <input type="text" value="Phones-02082008142345.txt"/>	(View File) (View Sample File)
Phone Template Name * <input type="text" value="7961 - SG"/>	(View File) (View Sample File)
<input type="checkbox"/> Create Dummy MAC Address (For CTI Port, Create Dummy Device Name)	
<input type="radio"/> Insert Phones All Details	
File Name <input type="text" value="-- Not Selected --"/>	(View File) (View Sample File)
<input type="checkbox"/> Override the existing configuration	
Job Information	
Job Description <input type="text" value="Insert Phones - Specific Details"/>	<input type="radio"/> Run Immediately <input checked="" type="radio"/> Run Later (To schedule and activate this job, use Job Scheduler page.)
<input type="button" value="Submit"/>	

Start the insertion Select immediately

Figure 7-23 Inserting IP Phones

Step 2. Click the Insert Phones Specific Details radio button to insert phone records that use a customized file format.

- Step 3.** In the File Name drop-down list, choose the CSV data file that was previously used in the validation phase.
- Step 4.** Selecting the Override the Existing Configuration check box overwrites the existing phone settings with the information that is contained in the file to be inserted. Use it at your own discretion. In the Phone Template Name drop-down list, choose the BAT phone template that was created previously for this particular BAT transaction. If you are using the Auto-Register Phone Tool (TAPS), select the Create Dummy MAC Address check box.
- Step 5.** In the Job Information area, enter a job description that can later be used as an audit log.
- Step 6.** Click the Run Immediately radio button to insert the phone records immediately, or click Run Later to schedule the job to be processed at a later date and time.
- Step 7.** Click Submit to submit the job for inserting the phone records.

Check for the status of the job. You can check the status of all jobs from CUCM Administration. Choose Bulk Administration > Job Scheduler. Select your job after finding it in the list of previously run BAT jobs. The job details will include the job result status, number of records processed, number of records failed, total number of records, and a link with the log filename.

Manual Configuration

Manually adding new Cisco IP Phones to CUCM can be tedious work when there are many phones to be added. Manual phone configurations will need to be performed to make individual changes, and a good part of our lives is spent utilizing this process as CUCM administrators. I look at creating a phone using only CUCM Administration.

To manually add a Cisco IP Phone to CUCM Administration, choose Device > Phone. Click the Add New button, and then select the phone type. Select the device protocol that should be used with the Cisco IP Phone (SCCP or SIP). This field will default to SCCP. Most of us click the Next button for Cisco 7900 Series phones, but the future seems to be in SIP. Someone probably wrote the same thing about ATM technology at some point in history, and it seems like ATM technology is going the way of the dinosaur.

Each phone in CUCM is uniquely identified by a device ID built from the phone's MAC address. The MAC address of a Cisco IP Phone is printed on a label at the back of the IP phone and can be viewed at the phone by pressing the Settings button and navigating into the Network Configuration.

The following mandatory Cisco IP Phone configuration parameters must be set (see Figure 7-24):

- MAC Address
- Device Pool
- Phone Button Template
- Device Security Profile
- SIP Profile (SIP phone only)

Phone Configuration

Status
(i) Status: Ready

Phone Type
 Product Type: Cisco 7975
 Device Protocol: SCCP

Device Information

<input checked="" type="checkbox"/> Device is trusted	001122334455
MAC Address*	SEP001122334455
Description	HQ_CapeTown
Device Pool*	< None >
Common Device Configuration	Standard 7975 SCCP
Phone Button Template*	Standard Manager
Softkey Template	Standard Common Phone Profile
Common Phone Profile*	< None >
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Location*	Hub_None
AAR Group	< None >
User Locale	< None >
Network Locale	< None >
Built In Bridge*	Default

Figure 7-24 Manual Phone Configuration

All these mandatory parameters have to be configured, but some of them have default values (Device Pool and Phone Button Template). Any configuration item on the screen with an asterisk (*) next to it is a required field, but you might want to use the default value if there is one.

Note It is recommended that you insert a meaningful description for each configured IP phone. The default description is the MAC address plus a prefix of SEP (Selsius Ethernet Phone). It helps include some type of site identifier in the Description field. The site identifier assists you with BAT update procedures in the future. If you want to make an update to every phone configuration at a site, you can quickly search BAT by the site identifier in the Description field of the phone.

Follow this procedure to configure the directory number for the manually added IP phone:

Step 1. After the phone configuration is saved, the left side of the Phone Configuration window will have an Associated Information column. Click the

Line [x] - Add a new DN link to configure the first directory number. Click this link to add a new directory number.

- Step 2.** When the Directory Number Configuration window appears (see Figure 7-25), enter the DN of the Cisco IP phone in the appropriate field.
- Step 3.** Click Save.

The screenshot displays the 'Directory Number Configuration' window. At the top right, there is a 'Related Links' button labeled 'Configure Device (SEP012345012388)'. The main area is divided into several sections:

- Directory Number Information:** Contains fields for 'Directory Number' (set to '11001'), 'Route Partition' (set to '< None >'), 'Description', 'Alerting Name', 'ASCII Alerting Name', and a checked 'Active' checkbox.
- Directory Number Settings:** Includes dropdowns for 'Voice Mail Profile' (set to '< None >'), 'Calling Search Space' (set to '< None >'), 'Presence Group' (set to 'Standard Presence group'), 'User Hold MOH Audio Source' (set to '< None >'), 'Network Hold MOH Audio Source' (set to '< None >'), and 'Auto Answer' (set to 'Auto Answer Off').
- AAR Settings:** A table with columns for 'AAR', 'Voice Mail', 'AAR Destination Mask', and 'AAR Group'. The 'AAR' column has a radio button for 'or'. The 'AAR Group' dropdown is set to '< None >'. Below the table is a checked checkbox for 'Retain this destination in the call forwarding history'.

Figure 7-25 Manual Phone Configuration

Use the same procedure to configure additional lines if the phone has more than one line.

Endpoint Registration Verification

Figure 7-26 shows an example of a phone listing from the Find and List Phones function available by clicking the **Find** button at the **Device > Phone** menu. Successful phone registration can be verified by looking at the following two criteria:

- Verify that the phone is registered in the Status column.

Note If the phone is displayed as unregistered, it has previously registered but is no longer registered. If a phone is being reset, it is shown as unregistered during the short time that it reregisters with CUCM. If the phone status is displayed as unknown, the phone has never successfully registered to CUCM. If the phone is registered, its IP address is shown in the Status column. The IP address is used for CUCM to send signaling to. Clicking the IP Address link will browse the web server component that is turned off by default beginning with CUCM 8.0.

- Click the device name of a phone in the list, and the configuration page of the phone will be displayed. The directory number configuration parameters can be verified by clicking a directory number on the Phone Configuration page.

	Device Name(Line)	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
<input type="checkbox"/>	SEP012345012345	SEP012345012345	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	SEP012345012346	SEP012345012346	Default	SIP	Unknown	Unknown		
<input type="checkbox"/>	SEP012345012349	SEP012345012349	Default	SIP	Unknown	Unknown		
<input type="checkbox"/>	SEP012345012388	SEP012345012388	Default	SCCP	Unknown	Unknown		

Figure 7-26 Phone Registration Verification

Third-Party SIP Phone Configuration

The example used here is based on a third-party, freeware SIP phone called X-Lite. Google “X-Lite” and you’ll find a site where you can download and install this software-based phone for free. Recall that CUCM requires three device license units (DLU) for a one-line, third-party SIP phone and six DLUs for a multiline, third-party SIP phone. DLUs are covered in Chapter 1, “Cisco Unified Communications Manager Architecture.” Step 4 that follows will vary based on the vendor of the SIP phone, but the first three steps are the same for other third-party SIP phones.

The high-level steps for adding a third-party SIP phone are as follows:

- Step 1.** Configure the end user in CUCM.
- Step 2.** Configure the device in CUCM.
- Step 3.** Associate the device to the end user as a digest user.
- Step 4.** Configure the third-party SIP phone to register with CUCM.

Figure 7-27 displays the addition of an end user in CUCM to be used for the third-party SIP phone. Third-party SIP phones register with CUCM by sending their username and password in a process called *digest authentication*. Digest authentication is an authentication mechanism with minimal security. Third-party SIP phones do not send their MAC addresses to CUCM like Cisco IP Phones using SCCP or SIP.

The SIP standard mandates that the digest authentication mechanism be used as the “standards-based” authentication mechanism between third-party SIP components. The first step of the process in adding a third-party SIP phone is adding a user that will be configured with digest credentials. The user is then applied to the Cisco IP Phone as a digest user.

The screenshot shows the 'End User Configuration' window with the following fields filled in:

User Information	Value
User ID *	mpolo
Password	*****
Confirm Password	*****
PIN	*****
Confirm PIN	*****
Last name *	Polo
Middle name	
First name	Marco
Telephone Number	
Mail ID	
Manager User ID	
Department	
User Locale	< None >
Associated PC	
Digest Credentials	*****
Confirm Digest Credentials	*****

Figure 7-27 End-User Configuration

The first step is to add a new user. Assuming that you are not performing Lightweight Directory Access Protocol (LDAP) synchronization, the following procedure would be used to add a new user. In CUCM Administration, choose **User Management > End User**. Click the **Add New** button. Be sure to configure the optional Digest Credentials and Confirm Digest Credentials fields. Click **Save**.

Note The Digest Credentials field is used to define the password that can be used for authentication of the SIP phone. This password will only be used for authentication if the third-party SIP phone configuration is using a device security profile with enabled digest authentication. The device security profile configuration can be found in CUCM Administration by choosing **System > Security Profiles > Phone Security Profile**. Find the phone by typing **SIP** in the blank field to the right of the Name and Contains drop-down menus. Click the Third-party SIP Device (Basic or Advanced) SIP Non-Secure Profile **<sip profile name>**. Change the name of the profile and select the Enable Digest Authentication check box. Apply this device security profile to the third-party SIP phone configuration later.

Some third-party SIP phones do not have a separate user ID and auth ID. In this case, the user ID has to be set to the directory number at the third-party SIP phone. The end user's username has to be identical to the directory number of the IP phone in CUCM Administration.

Figure 7-28 displays the addition of a new third-party SIP phone using X-Lite. Navigate to **Device > Phone** and click the **Add New** button. Choose **Third-Party SIP Device (Basic)**. A basic third-party SIP phone can only have one line and will use three DLUs in

CUCM licensing. Third-party SIP devices must have a SIP profile applied. The standard SIP profile can be used in most cases.

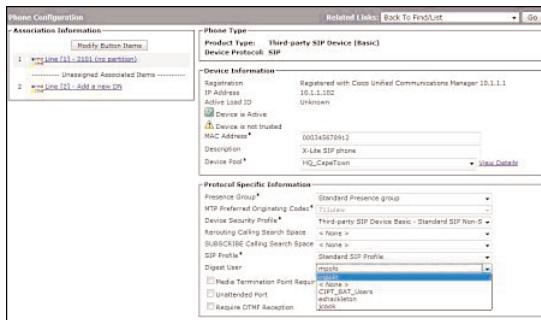


Figure 7-28 Third-Party SIP Phone Configuration

Third-party SIP devices usually support RFC 2833 dual-tone multifrequency (DTMF)-Relay, which can cause compatibility issues with older Type A Cisco IP Phones. Type A Cisco IP Phones require a Media Termination Point (MTP) to communicate keypad digits with a device that requires in-band DTMF Relay (RFC 2833). Type A Cisco IP Phones are only capable of passing digits out of band in their signaling path (SIP or SCCP). RFC 2833 uses in-band DTMF Relay, which passes DTMF digits in the RTP media channel (UDP port 16384–32767). MTPs convert the out-of-band keypad digits into in-band RFC 2833-compatible DTMF-Relay. MTPs are covered in more detail in Chapter 13, “Media Resources.”

The Digest User drop-down field must be populated with the end user configured. After the phone has been configured with the digest user, update the end-user configuration by associating the end user with the third-party SIP phone.

The final step to adding a third-party SIP phone takes place on the third-party phone itself. The configuration depends on the product that is used. Figure 7-29 shows the configuration of the freeware third-party SIP softphone X-Lite. In the Proxy Address field of X-Lite, specify the IP address or fully qualified domain name (FQDN) of CUCM. The User Name field has to be set to the directory number that is assigned to the IP phone in CUCM. The Authorization User Name field has to match the digest user’s username that was associated to the phone. The password only needs to be set if the digest credentials have been configured for the end user and if a phone security profile with selected Enable Digest Authentication has been assigned.

Note If the Enable Digest Authentication check box has not been selected in the phone security profile, only the username of the digest authentication is verified; the password (digest credentials in CUCM end-user configuration) is not checked.



Figure 7-29 Third-Party SIP Phone Configuration

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- Some IP configuration settings are applied directly to the device; others are applied by referencing configuration elements such as a device pool.
- IP phone auto-registration automatically adds new Cisco IP Phones to the configuration database and assigns one DN to the IP phone.
- Auto-registration configuration includes the configuration of a DN range and the activation of the feature on some servers of a CUCM group.
- The CUCM Tool for Auto-Registered Phone Support requires a Cisco CRS server on the network.
- CUCM BAT can be used to add and delete IP phones or to change their configuration.
- Manually adding IP phones is time consuming.

References

For additional information, refer to these resources:

CUCM Administration Guide, Release 8.0(1), at
www.cisco.com/en/US/docs/voice_ip_comm/cucm/drs/8_0_1/drsag801.html.

CUCM Bulk Administration Guide 8.0(1), at
www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/bat/8_0_1/bat-801-cm.html.

CUCM SRND, Release 8.0(1), at
www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8xsrnd.pdf.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. Which of the following is not an option to set the time for a Cisco IP Phone?
 - a. Manual settings configuration
 - b. Phone NTP reference
 - c. Cisco Unified Communications Manager registration
2. Which of the following configuration parameters are required only for SIP phones?
 - a. Security profile
 - b. SIP NTP reference
 - c. Device pool
 - d. SIP profile
3. Which phone NTP reference option generates a packet to the all hosts broadcast address?
 - a. Unicast
 - b. Multicast
 - c. Anycast
 - d. Directed broadcast
4. The date/time group is configured to which value by default?
 - a. CMLocal
 - b. NTP Reference
 - c. Cisco Unified Communications Manager Publisher
 - d. Eastern Standard Time (EST)
5. What parameter is not available in the device pool in CUCM 8.0?
 - a. Softkey template
 - b. Date/time group
 - c. Region
 - d. Cisco Unified Communications Manager group

- 6.** How many CUCM servers can be configured in a CUCM group?
 - a.** 2
 - b.** 3
 - c.** 4
 - d.** 5
- 7.** What functionality does the region support?
 - a.** Call admission control
 - b.** Collection of configuration parameters
 - c.** Date and time configuration
 - d.** Audio codec selection
- 8.** What functionality does the location support?
 - a.** Call admission control
 - b.** Collection of configuration parameters
 - c.** Date and time configuration
 - d.** Audio codec selection
- 9.** Where must auto-registration be enabled in CUCM? (Choose two.)
 - a.** CallManager Group Configuration
 - b.** Device Settings Configuration
 - c.** Device Configuration
 - d.** CallManager Configuration
- 10.** The Bulk Administration Tool does not require which parameter of the IP phone?
 - a.** IP address
 - b.** Phone type
 - c.** Phone protocol
 - d.** MAC address

Chapter 8

Implementing PSTN Gateways in Cisco Unified Communications Manager

To place external calls, Cisco Unified Communications Manager (CUCM) deployments need a connection to the public switched telephone network (PSTN). PSTN connections are provided through gateways, which connect traditional time-division multiplexing (TDM) telephony interfaces (digital T1/E1 or analog FXO ports) and VoIP domains. Gateways can be integrated in Cisco Unified Communications Manager by using different protocols such as Media Gateway Control Protocol (MGCP), H.323, or Session Initiation Protocol (SIP) for signaling on VoIP call legs.

This chapter describes the role and implementation of MGCP, H.323, and SIP gateways to provide PSTN access to a Cisco Unified Communications Manager environment.

Chapter Objectives

Upon completing this chapter, you will be able to describe the implementation of PSTN gateways in CUCM and be able to meet these objectives:

- Describe the types of gateways that can interact with CUCM and describe their differences
- Describe how to integrate MGCP gateways with CUCM
- Describe how to integrate H.323 gateways with CUCM
- Describe how to integrate SIP gateways with CUCM

A gateway is a device that can translate between different types of signaling and media. One type of gateway is a voice gateway. Voice gateways are used anytime that a Cisco IP Phone communicates with a TDM interface (for example, the PSTN, traditional PBX, analog phone, analog fax, security system remote monitoring, and so on). The gateway router converts VoIP Real-Time Transport Protocol (RTP) media packets to analog or digital TDM signals.

Note TDM interfaces are commonly referred to as trunks in telecommunications. CUCM uses the word *gateway* to refer to the PSTN accesses from CUCM while using the word *trunk* to indicate call routing using SIP, H.323 (H.225), or CUCM original signaling between a CUCM cluster and another Unified Communications (UC) system (for example, another CUCM cluster).

TDM interfaces were supported on various Cisco Catalyst 6000 switch modules in the past, but all of these TDM interfaces reached end of sale (EoS) status many years before the writing of this book. Gateway functionality is normally configured on Cisco routers, and Cisco router TDM interfaces have been the only TDM interfaces available for purchase for a good number of years now.

Analog and Digital Gateways

One call can be active at any one time on a Cisco gateway. There are two types of Cisco gateways:

- **Cisco access analog gateways:**
 - **Analog station gateways:** Analog station gateways connect CUCM to plain old telephone service (POTS) analog telephones and other systems that use analog interfaces, such as fax machines and smaller voicemail and interactive voice response (IVR) systems. Foreign eXchange Station (FXS) ports are used to connect to analog devices. Devices such as analog telephones and fax machines are normally plugged into FXS ports. FXS ports generate dial tone and battery, while the devices that are plugged into them expect dial tone and expect –48 volts of DC current to be delivered over the copper cabling. FXS ports provide 2-pair (4-pin) connectors terminated with an RJ-11 head. Only two pins are used in the cable, and they're commonly referred to as Tip and Ring.
 - **Access analog trunk gateways:** Access analog trunk gateways connect CUCM to PSTN central office (CO) or PBX trunks. Trunk gateways provide Foreign Exchange Office (FXO) ports for PSTN or PBX access and E&M ports for analog trunk connection to a traditional PBX. (E&M ports are known by various names, primarily recEive and transMit, ear and mouth, and Earth and Magneto.) E&M ports are not common anymore, but you might come across them. Analog direct inward dialing (DID) is also available to provide DID information for inbound calls. Analog DID trunks cannot be used for outbound calls to the PSTN. FXO ports can provide both inbound and outbound dialing functionality, but FXO ports do not supply DID information to CUCM when calls originated from the gateway are sent to CUCM.

Note FXO ports are normally connected to the PSTN for analog trunk functionality, but they could also be used to integrate with any device with an FXS port. For example, an FXO port on a Cisco gateway could be connected to a traditional PBX FXS port to integrate the CUCM solution to the traditional PBX that will be migrated.

- **Cisco access digital trunk gateways:** A Cisco access digital trunk gateway connects CUCM to various TDM destinations through much higher capacity than analog interfaces. T1s can send up to 24 calls (23 for T1-PRI) per interface and E1 interfaces can send up to 30 calls. ISDN uses common channel signaling (CCS), leveraging the ITU Q.931 signaling protocol. ISDN Basic Rate Interface (BRI) also used CCS/Q.931, but ISDN BRIs only offer the ability to trunk two phone calls at a time. ISDN BRIs are popular in Europe but are almost never used in North American-based deployments. Older T1 and E1 interfaces use channel associated signaling (CAS)/robbed bit signaling (RBS) to send their signaling information. CAS interfaces allow every port to be used for voice bearer traffic but do not have the same level of features as ISDN (for example, inbound and outbound Automatic Number Identification [ANI] and Digital Number Identification Service [DNIS] information).

Note Calling party information is presented to the called party as caller ID information. Caller ID is a standard that includes both the calling party name and calling party number. ANI is a PSTN standard for presenting the phone number of the calling party. DNIS is a public standard for called party information that is forwarded with call signaling. DNIS information is required to perform call routing at the customer network if direct inward dial (DiD) is used.

Core Gateway Requirements

IP telephony gateways must meet these core feature requirements:

- **Dual-tone multifrequency (DTMF) relay:** DTMF signaling tones must be processed by the gateways. DTMF relay is performed in band (IB) using the RTP capabilities (RFC 2833) or out of band (OOB) using the call-signaling protocol (SCCP/SIP/H.323).
- **Supplementary services:** Supplementary services are Cisco IP Phone features such as hold, transfer, and conferencing. Most features that require the end user to select a softkey button are supplementary services.
- **CUCM redundancy support:** CUCM clusters provide redundant CUCM servers to provide call-processing high availability. Gateways must support the ability to use multiple CUCM servers running the CallManager service for call-processing redundancy. Redundant CUCM servers are specified in the CM group that is applied to the device pool. The device pool with the CM group providing call-processing redundancy is then applied to the Cisco IP Phone.
- **Call survivability:** Call survivability (call preservation) is the concept that a voice gateway will preserve active calls when the CUCM server that set up the call goes down. End users will see the following message on the LCD of their IP phone during the CUCM outage: “CM Down, Features Disabled.” Supplementary services will not work for the duration of the active call. Call survivability is built in to MGCP, but the default switchback mechanism of graceful could cause some challenges. When the CUCM server that set up a call over an MGCP gateway goes down, the active calls over the gateway stay up. All future calls to or from the MGCP gateway will fail until the MGCP gateway has reregistered with the MGCP call agent (CUCM).

Redundant MGCP gateways can use different CM groups with different primary servers to minimize the impact of this call-survivability limitation. MGCP gateway 1 can register with CUCM 1 as its primary, and MGCP gateway 2 can register with CUCM 2 as its primary call-processing server. During a CUCM outage, CUCM will reroute inbound and outbound calls through the gateway that is active.

MGCP gateways have another call survivability pitfall. Branch sites in a centralized call-processing deployment leverage Survivable Remote Site Telephony (SRST) for backup call processing when reachability to CUCM is lost (for example, during a WAN outage). The MGCP gateway router will need to fall back to local call processing while CUCM is unreachable. All active calls will be dropped immediately on the MGCP gateway when it falls back to local call processing.

None of the preceding call-survivability challenges exist with H.323 gateways. H.323 gateways have supported call preservation (call survivability) since Cisco IOS Release 12.4(9T). The call preservation feature is not enabled by default. Use the following procedure to enable call survivability on all VoIP dial peers on the router:

```
Voice service voip  
H323  
Call preserve
```

All Cisco gateways support these core gateway requirements.

Gateway Communication Overview

Most gateway devices support multiple gateway protocols. Gateway protocol selection is normally based on the capabilities of the communicating devices. You might prefer MGCP to H.323 because of the simpler configuration, but beware of the limitations. My preference is to use the H.323 gateway protocol because of the availability concerns with MGCP around call survivability/call preservation. The features of the various protocols are outlined in the list that follows:

- **H.323:** H.323 uses a peer-to-peer call-processing model. Most of the configuration of H.323 is done in the Cisco IOS command-line interface (CLI) on the voice gateway. In a peer-to-peer call-routing model, CUCM has no control over the gateway. Calls are routed from CUCM to the gateway, and an independent call-routing decision is performed in the call-routing database of the H.323 (or SIP) gateway. Dial peers comprise a large portion of the call routing on a Cisco H.323 (or SIP) gateway. Most Cisco gateways support H.323 as a call-signaling option. H.323 gateways do not register with CUCM and will always show up as unknown.
- **MGCP:** MGCP uses a client/server model. The server is the call agent (CUCM), while the endpoint (TDM interface on the router) is the client. MGCP simplifies the configuration of voice gateways through centralized administration through the CUCM GUI. MGCP gateways require only two Cisco IOS commands. The rest of the MGCP gateway configuration is performed in CUCM Administration. When a

gateway is reset, the TFTP server pushes a new configuration file to the Cisco IOS gateway, and the gateway will load any necessary Cisco IOS configuration changes based on the GUI administration performed.

- **SIP:** The Internet Engineering Task Force (IETF) developed the Session Initiation Protocol (SIP) standard for multimedia calls over IP. SIP is a peer-to-peer protocol that leverages Session Description Protocol (SDP) to perform media negotiation (for example, audio and video codecs). SIP uses requests and responses to establish, maintain, and terminate calls between two or more endpoints. CUCM supports SIP trunk and SIP line side support beginning with CUCM 5.0. SIP gateways require a SIP trunk in CUCM (directing calls to the gateway), while MGCP and H.323 gateways are provisioned as gateways in CUCM.
- **Skinny Client Control Protocol (SCCP):** SCCP (skinny) is a client/server protocol (similar to MGCP) used to communicate between the Cisco IP Phone and CUCM. The Cisco IP Phone registers with CUCM in a manner similar to MGCP gateways. Cisco IP Phones and gateways receive their configuration file from the TFTP server in CUCM (similar to MGCP).

Gateway Protocol Functions for Cisco Unified Communications Manager Integration

The three main gateway-signaling protocols—MGCP, H.323, and SIP—provide slightly different feature support. Tables 8-1 and 8-2 provide an overview of the features and functions that each signaling protocol provides as well as the pros and cons of these protocols.

Table 8-1 *Gateway Protocol Functions*

Function	MGCP	H.323	SIP
Clients	Nonintelligent	Intelligent	Intelligent
Non-Facility Associated Signaling (NFAS)	Not supported	Supported	Supported
QSIG signaling	Supported	Supported (basic call functionality)	Supported
Fractional T1/E1	More difficult to implement; requires manual configuration	Easy to implement	Easy to implement
TCP/IP Transport Layer Protocol	TCP and User Datagram Protocol (UDP)	TCP	TCP or UDP (UDP by default)

Table 8-1 *Gateway Protocol Functions*

Function	MGCP	H.323	SIP
Code basis	ASCII	Abstract Syntax Notation Level One (ASN. 1) (same encoding as SNMP)	ASCII
Call survivability	Yes (except ISDN)	Yes (with additional configuration)	Yes
FXO caller ID	Yes (CUCM 8.0 or later)	Yes	Yes
Call applications (TCL/VXML)	No	Yes	Yes

Table 8-2 *Protocol Comparison*

	MGCP	H.323	SIP
Pros	Centralized dial plan configuration Centralized gateway configuration Simple gateway configuration Easy implementation	Dial plan directly on the gateway More specific call routing Advanced fax support Third-party integration support	Dial plan directly on the gateway Third-party telephony integration support Third-party end-device support
Cons	Extra SRST-related call-routing configuration	Complex configuration	Complex configuration

Each of the three gateway protocols has advantages and disadvantages when compared to the others. There is no one-size-fits-all gateway protocol, but you are not limited to one gateway protocol per gateway or per CUCM. CUCM and gateways support the simultaneous use of all the gateway protocols. CUCM provides signaling conversions between the gateway protocols for calls between devices utilizing different gateway protocols.

Note The Cisco Press book *Implementing Cisco Unified Communications Voice over IP and QoS (CVOICE) Foundation Learning Guide* provides detailed configuration information and features of the H.323, MGCP, and SIP protocols.

MGCP Gateway Implementation

MGCP is a plain-text protocol that call-control devices use to manage IP telephony gateways. MGCP (IETF RFC 2705) is a client/server protocol that allows a call agent (CA) to take control of a specific gateway endpoint (port). MGCP has the advantage of centralized gateway administration in the CUCM Administration GUI. CUCM controls the state of each port on the gateway (endpoint). SIP and H.323 gateways cannot be controlled on a per-endpoint (TDM port) level, but MGCP gateways can. MGCP endpoints can have a different configuration per endpoint. For example, each endpoint can have a different device pool, inbound calling search space, and significant digits. MGCP outbound signaling (CUCM to gateway) is transmitted over UDP port 2427, while inbound calls (gateway to CUCM) are transmitted over TCP port 2727 if Q.931 backhaul is used. Q.931 backhaul is automatically configured when using the automatic download MGCP mechanism and the endpoint is ISDN based (T1-PRI, E1-PRI, BRI).

The MGCP gateway must be supported in CUCM. Use the Cisco Software Advisor tool to make sure that the platform and version of Cisco IOS Software or Cisco Catalyst Operating System is compatible with MGCP for CUCM.

Endpoint Identifiers

The MGCP call agent (CUCM) sends commands to and receives commands from the gateway to manage individual endpoints. Endpoint identifiers address individual endpoints.

Endpoint identifiers consist of two logical parts. The endpoint identifier is separated by the @ symbol that is often used with email addresses. The first portion of the name is a local ID that indicates the individual port on the gateway router, while the last part of the endpoint identifier is normally a fully qualified domain name (FQDN). The FQDN can also be a host name if a domain name is not specified on the router.

Figure 8-1 is an example of MGCP device identifiers on a Cisco gateway router. The **show voice port summary** Cisco IOS command can be used to view the port device identifiers of all configured voice ports. All configured voice interfaces will be displayed. Notice the MGCP device identifiers of the T1 and Foreign Exchange Station (FXS) voice interfaces in Figure 8-1. Slot 1, subslot 1, port 1 (1/1/1) is a T1 interface. (DS1 indicates Digital Signal level 1, which is the digital signaling standard for T1 interfaces.) The FXS analog interface in slot 2, subslot 1, port 1 (2/1/1) is displayed with the Analog Access Line Number (AALN) prefix. The configuration of all voice interfaces on an MGCP gateway is performed in the GUI administration of CUCM. MGCP gateways did not support caller ID services on Foreign Exchange Office (FXO) ports, but this feature has been introduced in CUCM version 8.0.

Both MGCP and SCCP are client/server protocols. CUCM performs server functionality for both protocols, while the gateway performs client functionality. SCCP and MGCP endpoints are nonintelligent.

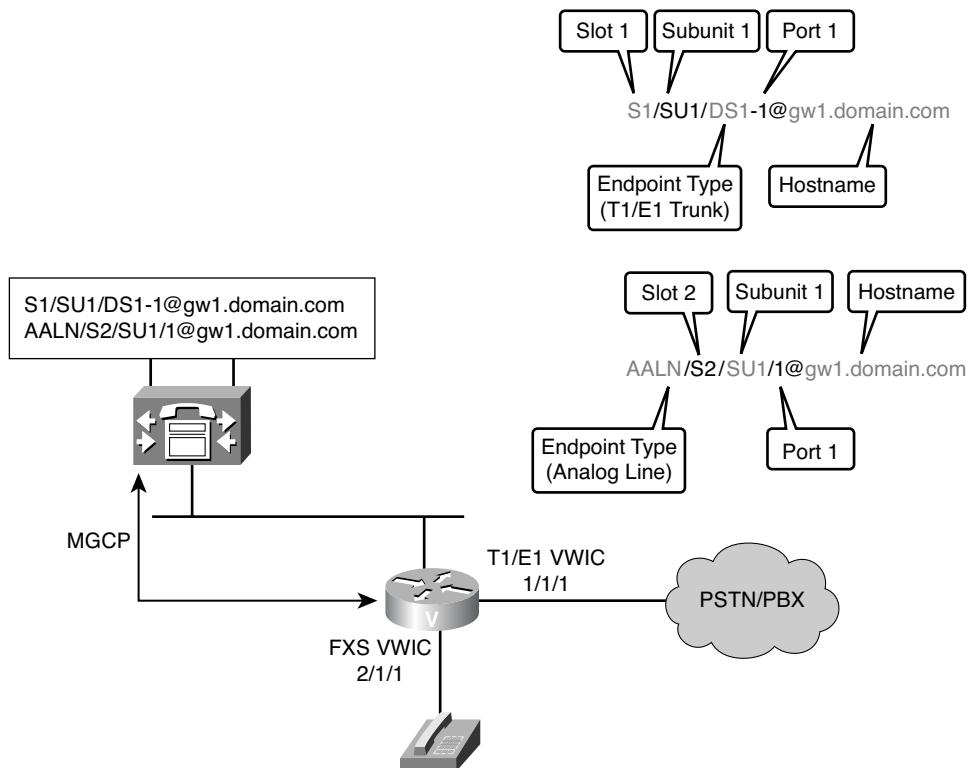


Figure 8-1 MGCP Endpoint Nomenclature

Figure 8-2 displays a call between an MGCP gateway and an SCCP-controlled Cisco IP Phone. MGCP communication is used between CUCM and the MGCP gateway. CUCM performs digit analysis (DA) against the dialed digits and routes the call to the proper destination. CUCM sends call progress signaling to the gateway, allowing the gateway endpoint to play a ringback tone to the calling party. CUCM simultaneously sends ring-down signaling to the Cisco IP Phone through SCCP. When the called party Cisco IP Phone user answers the phone, CUCM coordinates the communication of the media path between the Cisco IP Phone and the MGCP gateway. The voice bearer traffic from the gateway to the IP phone uses Real-Time Transport Protocol (RTP). RTP uses an even port number in the UDP port range of 16384 through 32767. The phone suggests an even UDP port number to use during signaling with CUCM. The next highest odd port is used to send quality of service (QoS) statistics for the call through Real-Time Control Protocol (RTCP). The information captured through RTCP is similar to the metrics that are written to the call management record (CMR) in CUCM at the end of a phone call. CMRs are turned off by default, but they can be turned on by setting the CUCM service parameter Call Diagnostics to True.

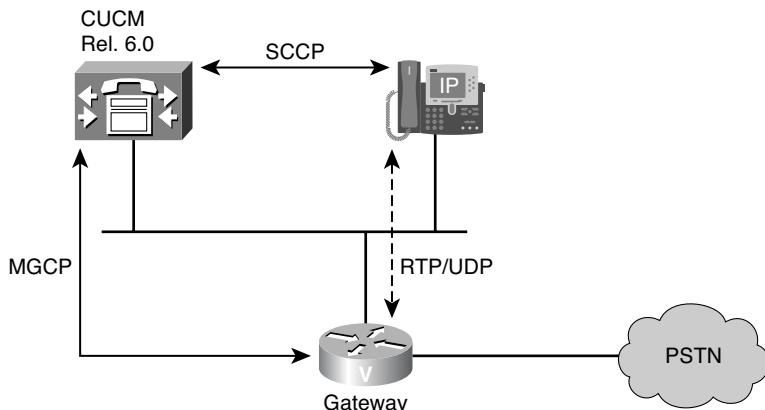


Figure 8-2 MGCP Call Flow

MGCP Gateway Support

MGCP support in CUCM includes a wide range of analog and digital interfaces that can be used on several Cisco router and switch platforms. FXO, FXS, T1-CAS, T1-PRI, E1-CAS, and E1-PRI are supported, but some voice ports are not supported by MGCP (for example, E&M voice ports).

CUCM pushes the Cisco IOS MGCP gateway configuration from the Cisco TFTP server to the gateway when automatic configuration is configured.

CUCM also supports Q.931 backhaul. Q.931 backhaul is only supported on ISDN voice ports. MGCP backhaul allows CUCM to process the Q.931 messaging from the ISDN circuit. The gateway router encapsulates the Q.931 signaling from the gateway over TCP port 2727.

MGCP Configuration Server

The Configuration Server feature allows all MGCP configurations to be administered through the GUI in CUCM. The Cisco IOS commands are downloaded automatically from the TFTP server to the MGCP gateway. This method is the recommended approach to integrate Cisco IOS MGCP gateways with CUCM. The Cisco IOS gateway dynamically loads the necessary MGCP configuration commands from the XML-based configuration file downloaded from the TFTP server. Cisco MGCP gateways translate the content of the XML configuration file into specific Cisco IOS commands.

Figure 8-3 illustrates the configuration communication between CUCM and the MGCP gateway. The Cisco router must be programmed with the two **ccm-manager** commands before this communication can occur. The **config server** command can be configured with multiple TFTP server IP addresses to provide TFTP high availability using the command **ccm-manager config server 10.1.1.1 10.1.1.2**. Note that Figure 8-3 shows only one TFTP server configured.

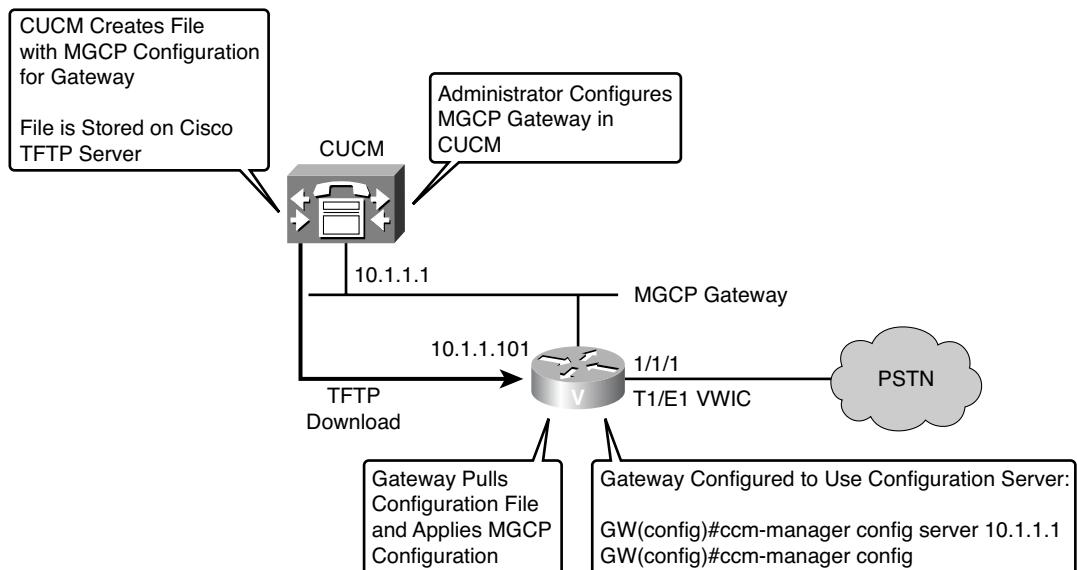


Figure 8-3 MGCP Configuration Server Communication

Q.931 Backhaul

Q.931 backhaul is a reliable TCP transport layer TCP/IP connection between CUCM and the Cisco MGCP gateway. Q.931 backhaul is an encapsulation of the Q.931 signaling in the D channel of the ISDN TDM interface. Q.931 backhaul carries the raw Q.931 signaling to CUCM to be processed natively. Instead of answering the call on the gateway and generating a new call leg to CUCM, the MGCP gateway router passes through the native Q.931 signaling to CUCM.

The gateway is still responsible for the termination of the Layer 2 Q.921 Link Access Protocol D-Channel (LAPD) signaling, but all ISDN Layer 3 call setup/call teardown signaling (Q.931) is sent to CUCM for processing.

MGCP Gateway Configuration: CUCM

Follow these steps to add an MGCP gateway to CUCM:

Step 1. In CUCM Administration, choose Device > Gateway.

Step 2. Click the Add New button.

Step 3. Choose the appropriate MGCP gateway by gateway or router name (see Figure 8-4).

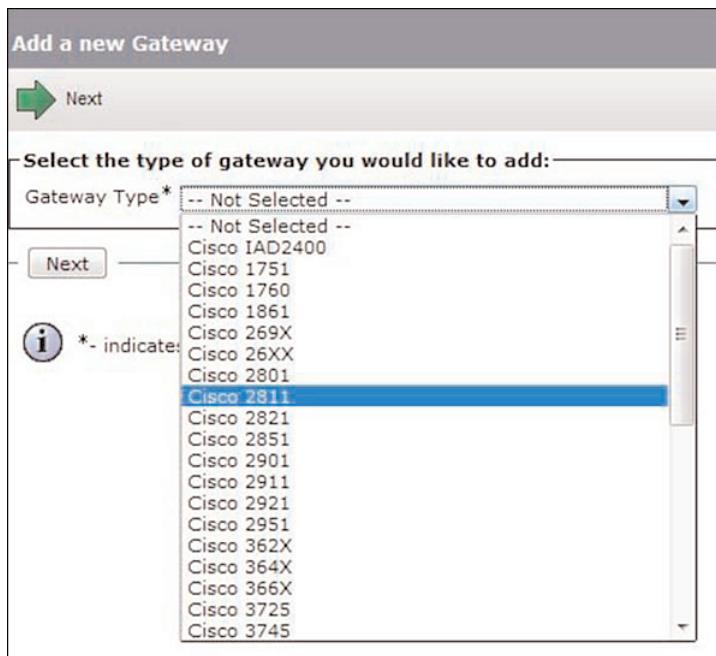


Figure 8-4 MGCP Gateway Configuration

Step 4. Click Next.

Step 5. Choose MGCP from the Protocol drop-down menu and click Next (see Figure 8-5).

Figure 8-5 displays the selection of the MGCP protocol for the gateway configuration.

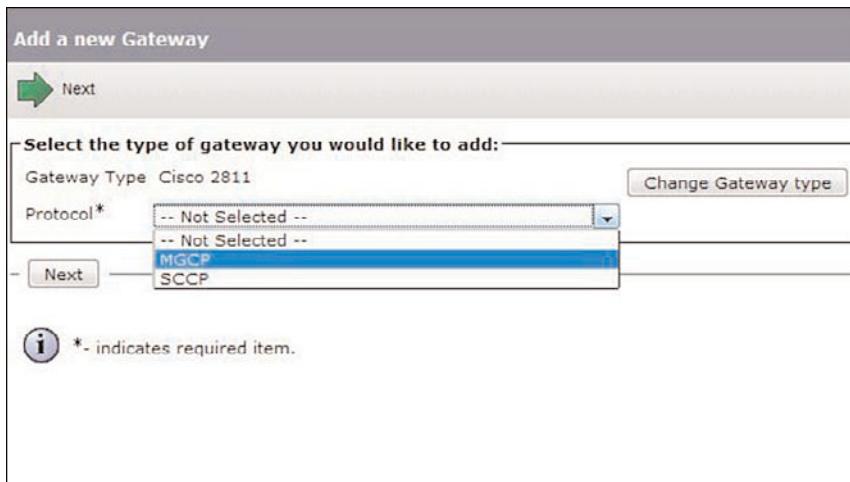


Figure 8-5 MGCP Gateway Protocol Selection

Note Most Cisco routers support SCCP and MGCP as signaling protocols. SCCP supports the *81 through *85 feature codes on analog phones connected to FXS interfaces, while MGCP does not. SCCP is only supported for FXS ports on Cisco routers.

The configuration of the MGCP gateway includes the following steps:

- Step 1.** Enter the host name or fully qualified domain name (FQDN) of the gateway in the Domain Name field. If a domain name is specified in the Cisco router, you must provision an FQDN. If the FQDN specified in CUCM does not match the “host name” dot “domain name” of the Cisco IOS router, the endpoint will never register. A router with the host name of Router1 and a domain name of highpoint.com would have an FQDN of Router1.highpoint.com.
- Step 2.** Enter a description for the gateway.
- Step 3.** Select a CUCM group.
- Step 4.** Configure the IDSN switch type.
- Step 5.** Locate the Configured Slots, VICs and Endpoints section, and select the voice hardware module placed in the slot (see Figure 8-6).
- Step 6.** Click Save. Reset the gateway (or click Apply Config) for the configuration changes to apply. The Apply Config option was not available prior to CUCM 7.1.

Figure 8-6 displays the MGCP Gateway Configuration page.

Figure 8-6 MGCP Gateway Configuration

Endpoints are added by selecting voice modules and voice interface cards at the Gateway Configuration page. To add endpoints to a gateway, follow these steps:

- Step 1.** Locate the Configured Slots, VICs and Endpoints section, and select the voice hardware module placed in the slot.

Note Only voice modules have to be specified. If data network modules are used in a slot, you do not have to specify them.

- Step 2.** The subunits (VIC slots) of the selected voice module will display. Select the subunit (voice interface card) (see Figure 8-7).

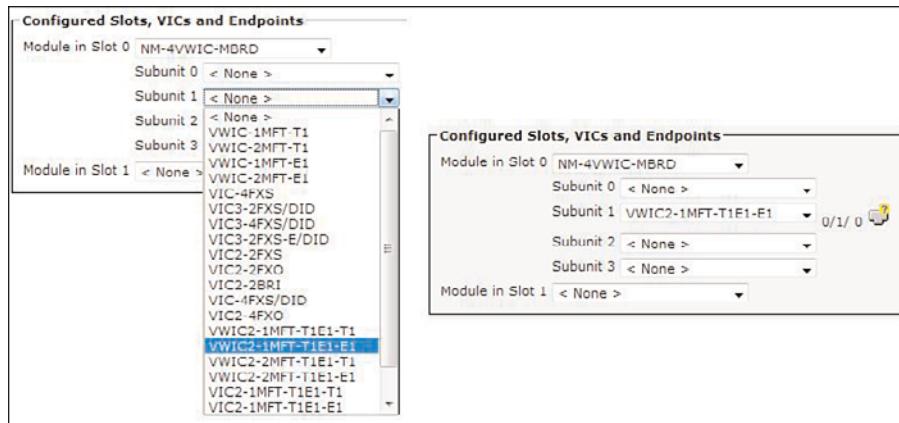


Figure 8-7 MGCP Configuration

- Step 3.** Click **Save**. The endpoints of the selected voice interface card will display with a written notation and a small port logo and yellow question mark in the graphical depiction of the port (see Figure 8-7).
- Step 4.** Repeat the process to indicate all the voice interface cards of the gateway.

Note The Cisco IOS command **show diagnostic** will display the voice modules and voice interface cards (VIC) with which the gateway is equipped.

To configure the MGCP endpoint, follow these steps:

- Step 1.** Click the endpoint identifier (0/1/0 in Figure 8-8).

- Step 2.** Select the device protocol or signaling for the endpoint. T1 and E1 interfaces support channel associated signaling (CAS) or common channel signaling (CCS) if the interface is an ISDN Primary Rate Interface (PRI). Analog interfaces support ground-start (GS) and loop-start (LS) signaling. Select the signaling mechanism that should be used on the endpoint and click **Next**.
- Step 3.** Enter a description for the endpoint.
- Step 4.** Select the device pool for the endpoint.
- Step 5.** Choose a Calling Search Space (CSS) and Significant Digits under the Inbound Call Routing section. The PSTN carrier might be sending ten digits, but the local site might be using an abbreviated dial plan that maps to the ten DID numbers that the PSTN carrier is sending. Set the Significant Digits field to equal the number of digits used in the internal dial plan. CSSs are covered in Chapter 9, “Call Routing Components.”
- Step 6.** Click **Save**. Click **Reset** to reset the gateway. The reset functionality will push configuration changes to the gateway.
- Step 7.** Many other optional parameters can be configured on the gateway. Most gateway configuration parameters are specific to the PSTN carrier requirements. Requirements differ by carrier, country, and general region. Some other parameters, including the Media Resource Group List (media resource selection) and Location (CAC), are general device-level configuration parameters that are not specific to gateway configuration.

Figures 8-8 through 8-10 are MGCP endpoint configuration screen captures from CUCM Administration.

Device Information	
Device Name*	Cisco MGCP E1 Port
Gateway	HQ_1
Device Protocol	Digital Access PRI
Device is not trusted	<input checked="" type="checkbox"/>
End-Point Name*	SIP/SU1/HQ1-0B#H2-L
Description	42/421/1/H1-0B#H2-1
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Network Locale	< None >
Packet Capture Mode*	None
Packet Capture Duration	0
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Line Information	
Use Trusted Relay Point*	Default
<input type="checkbox"/> Transmit UTI=0 for Calling Party Name	
<input type="checkbox"/> V150 (subset)	
<input type="checkbox"/> Enable Protected Facility IE	
<input checked="" type="checkbox"/> PSTN Access	

Figure 8-8 MGCP Endpoint Configuration: Device Information

MGCP Gateway Configuration: Cisco IOS Configuration

Only the two following commands are required to configure an MGCP gateway (where the TFTP server IP address is 192.168.1.200):

```
ccm-manager config
ccm-manager config server 192.168.1.200
```

Interface Information

- PRI Protocol Type *: PRI EURO
- QSIG Variant *: No Changes
- ASN.1 ROSE OID Encoding *: No Changes
- Protocol Side *: User
- Channel Selection Order *: Bottom Up
- Channel IE Type *: Use Number when 1B
- PCM Type *: A-law
- Delay for first restart (1/8 sec ticks) *: 32
- Delay between restarts (1/8 sec ticks) *: 4
- Inhibit restarts at PRI initialization
- Enable status poll
- Unattended Port
- Enable G.Clear

Figure 8-9 MGCP Endpoint Configuration: Interface Information

Call Routing Information - Inbound Calls

- Significant Digits *: All
- Calling Search Space: < None >
- AAR Calling Search Space: < None >
- Prefix DN

Call Routing Information - Outbound Calls

- Calling Party Presentation *: Default
- Calling Party Selection *: Originator
- Called party IE number type unknown *: Cisco CallManager
- Calling party IE number type unknown *: Cisco CallManager
- Called Numbering Plan *: Cisco CallManager
- Calling Numbering Plan *: Cisco CallManager
- Number of digits to strip *: 0
- Caller ID DN
- sMDI base Port *: 0
- Called Party Transformation CSS: < None >
- Use Device Pool Called Party Transformation CSS
- Calling Party Transformation CSS: < None >
- Use Device Pool Calling Party Transformation CSS

Figure 8-10 MGCP Endpoint Configuration: Call Routing Information

The Cisco IOS router will pull its MGCP gateway configuration file from the CUCM TFTP server. MGCP signaling is used between the Cisco IOS router with time-division multiplexing (TDM) ports, while CUCM translates signaling events from MGCP to SCCP or SIP for the Cisco IP Phones.

The **ccm-manager config server ip-address** command specifies the IP address of one or more TFTP servers in the CUCM cluster that have a configuration file from the MGCP-enabled Cisco router. If more than one CUCM TFTP server is deployed in the cluster, a list of IP addresses can be specified using a space between each IP address. The Cisco IOS MGCP gateway prioritizes the IP addresses from left to right. In the following example, the Cisco router will pull its configuration file from 192.168.1.100 but will use 192.168.1.200 if 192.168.1.100 was not available:

```
ccm-manager config server 192.168.1.100 192.168.1.200
```

The **ccm-manager config** command enables the Configuration Server feature. The **ccm-manager config server** command is ignored without this command.

For the Configuration feature to work, the following prerequisites must be met:

- The MGCP gateway and the CUCM TFTP server must have IP connectivity between each other. It's important to ensure that TCP and UDP ports 2427, 2428, and 2727 can communicate between the MGCP gateway and CUCM TFTP server. If there is a firewall or security appliance (ASA) between the MGCP gateway and CUCM server, ensure that these communication ports are enabled.
- The MGCP gateway and endpoints are configured in CUCM. The configuration has been saved and the Reset or Apply options have been applied.
- The host name or fully qualified domain name (FQDN) of the Cisco IOS MGCP gateway must match the CUCM MGCP gateway configuration. If the router's running configuration file has the **ip domain-name** command in it, an FQDN must be used (for example, Router1.highpoint.com).

If all these conditions are met and the gateway is configured with the **ccm-manager config** and **ccm-manager config server** commands, the gateway can download its XML configuration file from the TFTP server. I have seen situations where the MGCP gateway would not register unless the **no ccm-manager config server** command is executed, followed by the **ccm-manager config server** command. Certain situations also call for the MGCP gateway to be reset in CUCM Administration and then reset the MGCP functionality in the router using the aforementioned method. The command **no mgcp** followed by **mgcp** will also reset MGCP functionality. Be aware that resetting MGCP gateway functionality from Cisco IOS or the CUCM Administration will result in the immediate dropping of all existing calls. Using these commands in the middle of the day can be a Career Limiting Event (CLE). Use the Cisco IOS command **show voice port summary** before resetting a gateway. The **show voice port summary** command will display all active TDM interfaces on the router, and it's normally logical to deduce that there is an active phone call on every active TDM interface.

The gateway processes the configuration file by parsing the XML-based configuration file, converting the XML to Cisco IOS configuration commands for MGCP operation.

After a successful configuration download, the MGCP gateway saves the running configuration to the startup configuration. Any manually added configuration parameters not previously committed to the startup configuration will also be saved to the startup configuration when this occurs. Manually added configuration parameters are updates to the configuration that were made in the router using the Cisco IOS CLI.

Example 8-1 shows the resulting Cisco IOS configuration entries that are made based on the two following commands:

```
ccm-manager config server 10.1.1.1  
ccm-manager config server
```

Example 8-1 Configuring MGCP Gateway Registration

```
controller E1 0/3/0  
framing crc4
```

```

linecode hdb3
pri-group timeslots 1-31 service mgcp
!
interface Serial0/3/0:15
  isdn switch-type primary-4ess
  isdn incoming-voice voice
  isdn bind-l3 ccm-manager
!
ccm-manager mgcp
ccm-manager music-on-hold
!
mgcp
mgcp call-agent 10.1.1.1 2427 service-type mgcp version 0.1
mgcp rtp unreachable timeout 1000 action notify
mgcp modem passthrough voip mode nse
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp package-capability pre-package
no mgcp package-capability res-package
no mgcp package-capability fxr-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp rtp payload-type g726r16 static

```

MGCP Gateway: Registration Verification

MGCP gateways register with CUCM in a manner similar to SCCP phones. Each endpoint's registration status can be verified both in CUCM Administration and by Cisco IOS commands entered directly on the MGCP gateway. The **show ccm-manager** command in Example 8-2 shows that the MGCP gateway is registered. Other useful parameters and statistics can be verified with this command, but it's important to verify the importance of the MGCP gateway's registration status. There is only one good registration state to be in—and that's definitely registered. If "Registering" is displayed for longer than one minute, there is probably an FQDN configuration mismatch or communication problem between the Cisco router/gateway and CUCM TFTP server.

Example 8-2 Verifying MGCP Gateway Registration

```

Router# show ccm-manager
MGCP Domain Name: Router
Priority Status Host
=====
Primary Registered 10.16.240.124
First Backup None

```

```

Second Backup None
Current active Call Manager: 10.16.240.124
Backhaul/Redundant link port: 2428
Failover Interval: 30 seconds
Keepalive Interval: 15 seconds
Last keepalive sent: 00:45:31 (elapsed time: 00:00:04)
Last MGCP traffic time: 00:45:31 (elapsed time: 00:00:04)
Last failover time: None
Switchback mode: Graceful
MGCP Fallback mode: Not Selected
Last MGCP Fallback start time: 00:00:00
Last MGCP Fallback end time: 00:00:00
PRI Backhaul Link info
  Link Protocol: TCP
  Remote Port Number: 2428
  Remote IP Address: 10.16.240.124
  Current Link State: OPEN
  Statistics:
    Packets recv'd: 32
    Recv failures: 0
    Packets xmitted: 32
    Xmit failures: 0
  PRI Ports being backhauled: Slot 1, port 0
!
Configuration Auto-Download Information
=====
No configurations downloaded
Current state: Automatic Configuration Download feature is disabled
Configuration Error
  History:
  FAX mode: cisco

```

Although the MGCP gateway is registered, the endpoint in question might not be registered. The **show mgcp endpoints** command is useful to see which endpoints have registered. The output in Example 8-3 indicates that the T1 in slot 1/0 has registered all 24 channels of a T1 interface as a CCS ISDN PRI.

Example 8-3 Verifying Endpoint Registration

```

Router# show mgcp endpoints
Interface T1 1/0
!
ENDPOINT-NAME          V-PORT   SIG-TYPE ADMIN
S1/ds1-0/1@AV-2620-4 1/0:23 none up

```

```
S1/ds1-0/2@AV-2620-4 1/0:23 none up
S1/ds1-0/3@AV-2620-4 1/0:23 none up
S1/ds1-0/4@AV-2620-4 1/0:23 none up
S1/ds1-0/5@AV-2620-4 1/0:23 none up
S1/ds1-0/6@AV-2620-4 1/0:23 none up
S1/ds1-0/7@AV-2620-4 1/0:23 none up
S1/ds1-0/8@AV-2620-4 1/0:23 none up
S1/ds1-0/9@AV-2620-4 1/0:23 none up
S1/ds1-0/10@AV-2620- 1/0:23 none up
S1/ds1-0/11@AV-2620- 1/0:23 none up
S1/ds1-0/12@AV-2620- 1/0:23 none up
S1/ds1-0/13@AV-2620- 1/0:23 none up
S1/ds1-0/14@AV-2620- 1/0:23 none up
S1/ds1-0/15@AV-2620- 1/0:23 none up
S1/ds1-0/16@AV-2620- 1/0:23 none up
S1/ds1-0/17@AV-2620- 1/0:23 none up
S1/ds1-0/18@AV-2620- 1/0:23 none up
S1/ds1-0/19@AV-2620- 1/0:23 none up
S1/ds1-0/20@AV-2620- 1/0:23 none up
S1/ds1-0/21@AV-2620- 1/0:23 none up
S1/ds1-0/22@AV-2620- 1/0:23 none up
S1/ds1-0/23@AV-2620- 1/0:23 none up
```

Fractional T1/E1 Configuration on an MGCP Gateway

In some situations, not all time slots of a T1 or E1 connection will be used. This type of PRI is called a fractional T1 or E1, depending on what part of the world you're in. You can specify the number of usable B channels in Cisco Unified Communications Manager by setting the Cisco CallManager service parameter Change B-Channel Maintenance Status for the individual B channels on the ISDN PRI. Five PRI endpoints can be configured to have B channels in maintenance status. The B-Channel Maintenance Status setting has no effect on the XML configuration file that is received through the MGCP configuration server. The PRI group on the Cisco IOS MGCP gateway will always allocate the maximum number of B channels that are available for a specific controller type, but CUCM will never route a phone call to one of the configured B channels because the CUCM configuration indicates that certain B channels are out of service.

To configure fractional T1 or E1 on the Cisco IOS gateway, a manual gateway configuration would need to be performed that only specified the number of active time slots in the respective **ds0-group** (T1/E1 CAS) or **pri-group** (T1/E1 PRI) Cisco IOS commands. The configuration server functionality can be disabled in the router, and the preexisting MGCP configuration received from the TFTP server will be maintained. The fractional PRI group on the corresponding T1 or E1 controller is then configured. Anytime that Cisco IOS or CUCM versions are upgraded, I recommend testing the **ccm-manager config server** commands in a lab environment to see whether the new versions enabled any

new MGCP commands (MGCP package capabilities and so on) that might be required for the new version of Cisco IOS and CUCM to communicate properly. It's always best to use the automatic configuration commands unless there's a requirement for a fractional T1 or E1. Fractional circuits are not very common anymore in North America and other technically advanced countries because of dropping circuit costs.

Note The maximum number of PRI group B channels that can be supported in the gateway router depends on the number of installed voice interfaces and digital signal processors (DSP). T1 and E1 interfaces share DSP resources with hardware media resources configured in CUCM (transcoding, conferencing, and media termination point).

Fractional T1/E1 Configuration on Cisco Unified Communications Manager

To put specific time slots of an MGCP T1 or E1 PRI into the maintenance state, you need to retrieve the MGCP endpoint ID (for example, S0/SU1/DS1-0@HQ-1) and select the Enable Status Poll check box in the Interface Information configuration section on the MGCP Endpoint Configuration page.

From Cisco Unified Communications Manager Administration, choose **System > Service Parameter** and then choose the Cisco CallManager Service from the Service drop-down menu. Click the **Advanced** button at the top of the configuration page to view hidden advanced configuration options on the MGCP gateway that are required to change the B-Channel Maintenance Status parameter.

This parameter allows CUCM to change individual B-channel maintenance status for the time slots on the T1/E1 interface. The input format of the parameter is device name = B-channel maintenance status. The device name must match the gateway name retrieved from the gateway CUCM configuration. To avoid any data entry mistakes, copy the device name from CUCM's gateway configuration web page and paste it into this service parameter. The equal sign (=) is mandatory and unique and distinguishes the device name from the B-channel maintenance status. A T-1 B-channel maintenance status takes the form of xxxx xxxx xxxx xxxx xxxx xxxx, where each x represents one of the 24 channels in the T1 interface. Each x is used as a placeholder for one of three numerical values that indicate the following functions:

- 0: In service
- 1: Graceful out of service
- 2: Forceful out of service

Graceful out of service (1) changes channel status after any active calls are gracefully ended by the calling or called party. Forceful out of service (2) will forcefully disconnect any active calls without any indication to the end users on the active phone calls. Make sure that the total number of digits is either six groups of four values for a T1 (24 channels) or eight groups of four values for an E1 (32 channels). Any other length is treated as

an error and, no B-channel-maintenance-related action will be performed for that particular gateway device.

The following is an example of a fractional T1 interface that has four active channels with top-down channel selection order:

```
0000 1111 1111 1111 1111 1111
```

MGCP Gateway Verification

An easy way to check the operation of an MGCP-controlled T1/E1 ISDN PRI interface is by using the `show isdn status` command and checking the Layer 1 and Layer 2 status, as demonstrated in Example 8-4. The Layer 2 state of `MULTIPLE_FRAME_ESTABLISHED` is normally what you're looking for here. This message indicates that Layer 1 (T1/E1 controller) functionality is active and Layer 2 (Q.921 LAPD signaling) communication between the carrier equipment and the Cisco router is operational. Any Layer 2 status other than `MULTIPLE_FRAME_ESTABLISHED` normally indicates a problem with Layer 1 and/or Layer 2 communication.

Example 8-4 Verifying T1/E1 Interface Status

```
HQ-1# show isdn status
Global ISDN Switchtype = primary-net5
ISDN Serial0/1:0:15 interface
    dsl 0, interface ISDN Switchtype = primary-net5
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
        Active dsl 0 CCBs = 0
        The Free Channel Mask: 0x8000000F
        Number of L2 Discards = 0, L2 Session ID = 4
        Total Allocated ISDN CCBs = 0
```

MGCP Gateway Considerations

A constant logical IP session (connection) must be present between the Cisco IOS MGCP gateway and CUCM. If the connection between CUCM and the MGCP gateway is unavailable, the following can happen:

- If the gateway was configured for failover (by using the `ccm-manager fallback-mgcp` command), the MGCP gateway can fail over to local call control mode. All active calls are dropped (no call survivability/call preservation), and a complete local dial plan must be present. Fallback-MGCP functionality is normally enabled on branch

gateway routers configured with SRST in centralized call-processing architectures. Fallback-MGCP can be configured on headquarters routers as well, but this functionality is normally not present because the MGCP gateway's CUCM group defined in the gateway's device pool can include up to three CUCM servers to register the MGCP gateway to. Local MGCP registration failovers will not result in disconnected calls at the headquarters because of the graceful switchover feature that enables call survivability. No softkey features will be available during the duration of the survived calls, and new inbound and/or outbound calls will not work until the gateway reregisters with a CUCM server.

- If no failover configuration is present, all calls are dropped, and the PRI interface goes down.

H.323 Gateway Implementation

This section describes the signaling and media exchange between the H.323 gateway and CUCM.

Figure 8-11 demonstrates how CUCM and H.323 gateway configurations relate to each other. In the figure, the voice-enabled router is the H.323 gateway that allows devices registered to CUCM to make and receive calls from the PSTN. H.225 call control is carried over TCP port 1720 and is converted by CUCM to SCCP or SIP signaling used by the Cisco IP Phone. CUCM is acting as a proxy between the Cisco IP Phone and the gateway to instruct call setup/teardown events. The resulting voice media stream using Real-Time Protocol (RTP) is direct between the Cisco IP Phone and the H.323 gateway, where the digital signal processors (DSP) on the gateway convert the RTP media stream into a TDM format required for the gateway.

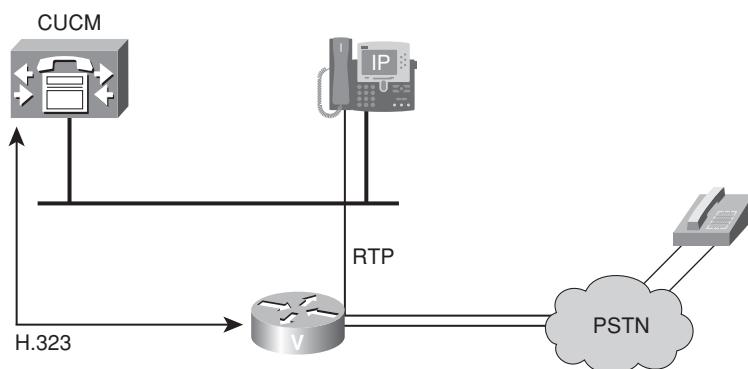


Figure 8-11 MGCP E1 Endpoint Configuration

When calls are made from the IP phone to the PSTN, the dial plan configuration on CUCM must direct inbound calls to the H.323 gateway. If ten dialed digits are received from the PSTN carrier, but the internal dial plan is abbreviated (five-digit internal dialing), digit manipulation will be performed. The Significant Digits gateway configuration

option can be used to enable this functionality. Future chapters will cover some fancier digit-manipulation techniques that can be leveraged in the CUCM configuration.

Cisco Unified Communications Manager H.323 Gateway Configuration

A gateway will need to be provisioned in CUCM Administration to enable communication between CUCM and another IP address using the H.323 protocol suite. Here are the steps from CUCM Administration:

- Step 1.** Choose Device > Gateway.
- Step 2.** Click Add New.
- Step 3.** Choose H.323 Gateway from the Gateway Type drop-down list, as shown in Figure 8-12. This option will be toward the bottom of the Gateway Type drop-down menu. Router models are used for MGCP and SCCP (FXS only) configurations of gateways. All router models are selected as “H.323 Gateway” if H.323 is the protocol to be used for signaling between CUCM and the gateway.

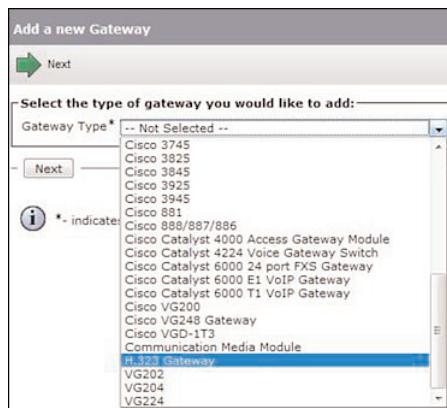


Figure 8-12 Selecting an H.323 Gateway

- Step 4.** Click Next to continue.
- Step 5.** Enter the H.323 gateway IP address or name. Figure 8-13 is using an IP address to avoid the reliance of using Domain Name System (DNS) to resolve the name to an IP address. Enter a descriptive name in the Description field (optional).



Figure 8-13 Configure the H.323 Gateway Settings

Step 6. From the Device Pool drop-down list, choose the device pool to which this gateway should belong. Recall that the device pool indicates the CUCM server registration prioritization. Ensure that the device pool selected includes a CUCM group with up to three servers to provide triple call-processing redundancy.

Step 7. Click Save. The H.323 configuration has many optional parameters that are similar to the MGCP gateway configuration, but there are far fewer configuration parameters because the bulk of H.323 and SIP provisioning occurs in the Cisco IOS configuration of the gateway. The router at IP address 10.1.1.101 can include any combination of FXS, FXO, T1-CAS, T1-PRI, E1-CAS, E1-PRI, or E&M voice interfaces. CUCM includes detailed configuration information of the MGCP gateways (client/server architecture) and far less information for SIP and H.323 gateways (peer-to-peer call-routing architecture).

Step 8. Verify the necessary configuration settings for the added H.323 gateway, as shown in Figure 8-14.

H.323 gateways configured in CUCM leverage H.245 media negotiation channels by default, which requires an additional TCP port in the range of 11000 to 11999 by default. I recommend enabling Inbound Faststart and Outbound Faststart, which will tunnel H.245 communication over H.225 call control's active TCP 1720 session. If a firewall is in between the communication of CUCM and the gateway, this configuration change will result in a much lower number of ports that must be enabled in the firewall.

After communication between the H.323 gateway and CUCM takes place, the H.323 gateway's source IP address is displayed on the Gateway Configuration page. Be aware that an H.323 gateway will never register with CUCM, so the registration status will never change from Unknown. Oddly enough, Unknown is the normal state. The registration status is somewhat useless for H.323 and SIP gateways that perform peer-to-peer call routing where the devices expect the destination to have a full call-routing configuration. MGCP gateways operate differently based on their reliance on CUCM. SIP and H.323 devices make independent call-routing decisions.

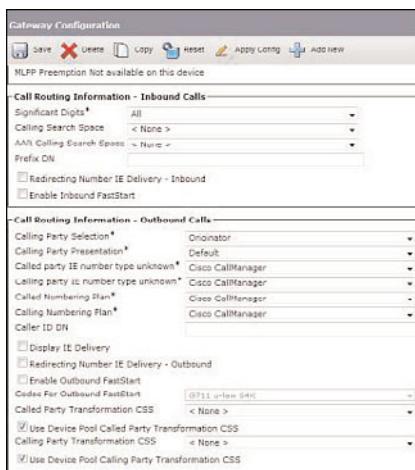


Figure 8-14 Configure the H.323 Gateway Settings (Continued)

Configure Basic Cisco IOS H.323 Functionality

After you add the IP address of the H.323 gateway in CUCM, the gateway will only accept inbound calls from the specified IP address. Cisco IOS H.323 gateways do a recursive route table lookup for the destination network and use the router's closest interface as the source IP address of the communication to CUCM by default. The H.323 bind command ensures that the Cisco router always uses the same IP address every time the gateway communicates with CUCM (inbound PSTN call routing). Example 8-5 includes a configuration where the source IP address is locked down to the logical loopback interface of the router. Loopback interfaces never go down because they are not tied to the link status of a physical interface.

Example 8-5 Basic H.323 Configuration

```
interface LoopBack0
ip address 10.1.1.101 255.255.255.0
h323-gateway voip interface
h323-gateway voip bind srcaddr 10.1.1.101
```

To route calls from the H.323 gateway to CUCM, you must configure at least one VoIP dial peer. In Example 8-6, all calls with a called party number that starts with 2 and is four digits long will be routed to the CUCM that has the IP address 10.1.1.1. This configuration assumes that the carrier circuit is only routing the last four digits to the customer's gateway router. If the carrier was routing ten digits for the called party digits, a translation profile could be directly attached to the incoming TDM interface. The translation profile would match on the customer's ten-digit DID range and convert the dialed digits from ten digits to four digits. The default signaling protocol for Cisco IOS VoIP dial

peers is H.323, so no further configuration is needed to implement the inbound call-routing functionality.

Example 8-6 VoIP Dial-Peer Configuration

```
dial-peer voice 1 voip
  destination-pattern 2...
no vad
ip qos dscp cs3 signaling
codec g711ulaw
  session target ipv4:10.1.1.1
```

Example 8-6 includes the **destination-pattern** command, which is matching on any four-digit patterns that begin with the number 2. The **no vad** command turns off Voice Activity Detection (silence suppression). The **ip qos** command maps call setup and tear-down signaling operations to the diffserv codepoint (DSCP) marking of CS3 to align to the QoS deployment based on the QoS 3.3 Solution Reference Network Design (SRND) requirements that have been used in CUCM since version 4.0. The Cisco IOS command default has not changed in IOS Release 15.x at press time. The default audio codec of G.729 has been changed to toll-quality G.711 with the **codec** command.

Configure CUCM Redundancy on H.323 Gateways: Calls from the H.323 Gateway to the CUCM Cluster

Dial peer hunting can be configured on the Cisco IOS H.323 gateway by using the **preference dial peer** command to indicate the relative priority of each VoIP dial peer that is the closest match for the evaluated string of digits. Dial peer hunting configurations are often used to enable redundancy for inbound call routing. If the preferred CUCM server becomes unreachable, the Cisco IOS gateway tries to set up the call with a different CUCM call-processing node within the cluster.

To configure dial peer hunting, create a second dial peer that has the same destination pattern but a different session target (IP address) and a lower-priority preference. Dial peer 2 in Example 8-7 has a preference of 1, which is subordinate (a lower priority) to that of dial peer 1. Dial peer 1 is using the default preference value of 0, which is a higher priority than a value of 1. Higher values normally indicate a higher priority, but it works the opposite way here. Think of this as a “cost” instead of a preference, and the logic makes sense. The **preference** command has ten options (0 through 9). The highest priority is 0 and the lowest priority is 9 in exact linear order.

Example 8-7 H.323 Voice Class Configuration

```
!
voice class h323 1
h225 timeout tcp establish 2
```

```

h225 timeout setup 2
!
dial-peer voice 1 voip
destination-pattern 2...
voice-class h323 1
session target ipv4:10.1.1.1
!
dial-peer voice 2 voip
preference 1
destination-pattern 2...
voice-class h323 1
session target ipv4:10.1.1.2
!
```

To reduce the failover-detection time for dial peer hunting, Example 8-7 has an H.323 voice class with the commands **h225 timeout tcp establish** and **h225 timeout setup** values that are lower than the defaults of 10 seconds. The default timeout value is a challenge (to say the least) because the T310 timer associated with most carriers' SETUP messages are 10 seconds. In other words, if it takes the gateway router 10 seconds to decide to reroute the call to a backup CUCM server, the carrier has already disconnected the call because it did not see a call-proceeding result from the setup message that it routed to the gateway. The following two **timeout** commands will be used to change this default that does not work very well in real-world deployment scenarios:

- **h225 timeout tcp establish *seconds*:** If the H.323 gateway cannot establish a TCP connection to the CUCM within the specified number of seconds, the next dial peer with an inferior preference will be used.
- **h225 timeout setup *seconds*:** An H.225 setup message will be sent to CUCM only after the TCP connection is established. If CUCM does not respond within the specified time, the next dial peer with inferior preference will be used.

If the H.323 voice class is used only to apply the two **h225 timeout** parameters, the class does not need to be applied to the dial peer that has the worst preference (the last dial peer of the hunt configuration). The **voice-class** command is optional for dial peer 2 but has been left in for the sake of consistency.

Configure CUCM Redundancy on H.323 Gateways: Calls from CUCM to the H.323 Gateway

The H.323 gateway is associated with a device pool in CUCM. The device pool of the H.323 gateway specifies a CUCM group that contains an ordered list of CUCM servers used for call processing. CUCM is therefore always responsible for gateway selection in outbound call routing but not inbound call routing.

H.323 Gateway Call Survivability

H.323 call survivability describes the behavior of active calls if communication between CUCM and the H.323 gateway is lost. A signaling session between the H.323 gateway and CUCM must be maintained for the duration of the call traversing the gateway or the call will be lost by default. H.323 gateways began supporting the call preservation/call survivability feature beginning with Cisco IOS Release 12.4(9T), but the feature is not enabled by default.

The TCP session between CUCM and the H.323 gateway is monitored using H.225 keepalives. To avoid the dropping of active calls during a communication failure between the H.323 gateway and CUCM, configure the global H.323 `no h225 timeout keepalive` parameter, as shown in Example 8-8, which will preserve TDM-to-VoIP calls.

Example 8-8 Keepalive Configuration

```
!
voice service voip
h323
no h225 timeout keepalive
!
```

The global H.323 `no h225 timeout keepalive` command has no effect on IP-to-IP calls traversing the Cisco Unified Border Element (CUBE) router. CUBE functionality was first branded as an “IP-to-IP gateway,” and the industry normally refers to this functionality as session border control (SBC) functionality. To configure call survivability for CUBE configurations, create an H.323 voice class, set the call preserve parameter, and bind the voice class to VoIP dial peers, as shown in Example 8-9.

Example 8-9 CUBE Call Survivability

```
!
voice service voip
allow-connections h323 to h323
!
voice class h323 1
h225 timeout tcp establish 2
h225 timeout setup 2
call preserve
!
```

SIP Gateway Implementation

SIP gateways are integrated with CUCM by using SIP trunks provisioned from CUCM Administration. The voice-enabled router in Figure 8-15 is the SIP gateway that connects devices in CUCM to the PSTN. CUCM establishes a SIP trunk to the IP address of the loopback or FHRP interface on the router. To route calls from the cluster toward the

PSTN network, the SIP trunk requires that the gateway router is configured with dial plan information. MGCP gateways only require two lines of Cisco IOS code, but H.323 and SIP gateways require an extensive dial peer configuration to enable PSTN dial plan functionality.

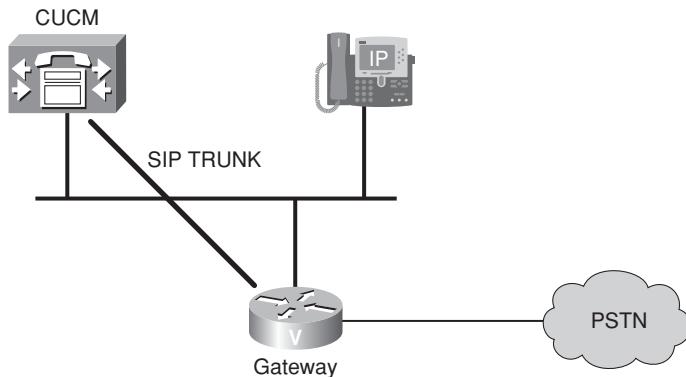


Figure 8-15 SIP Trunk

CUCM SIP Gateway Configuration

To configure a SIP gateway in CUCM, follow these steps:

- Step 1.** Add a SIP trunk.
- Step 2.** Configure the SIP trunk parameters.

To configure SIP gateway functionality on the Cisco IOS router, follow these steps:

- Step 1.** Configure Cisco IOS SIP functionality.
- Step 2.** Configure Cisco IOS call-routing information.
- Step 3.** Configure the SIP user agent parameters.

Add a SIP Trunk

Follow these steps, shown in Figure 8-16, to add a new SIP trunk to CUCM:

- Step 1.** In CUCM Administration, choose Device > Trunk.
- Step 2.** Choose the following:
 - SIP Trunk from the Trunk Type drop-down menu
 - SIP from the Device Protocol drop-down list
 - None (Default) from the Trunk Service Type drop-down list
- Step 3.** Click Next to continue with the SIP trunk parameter configuration.

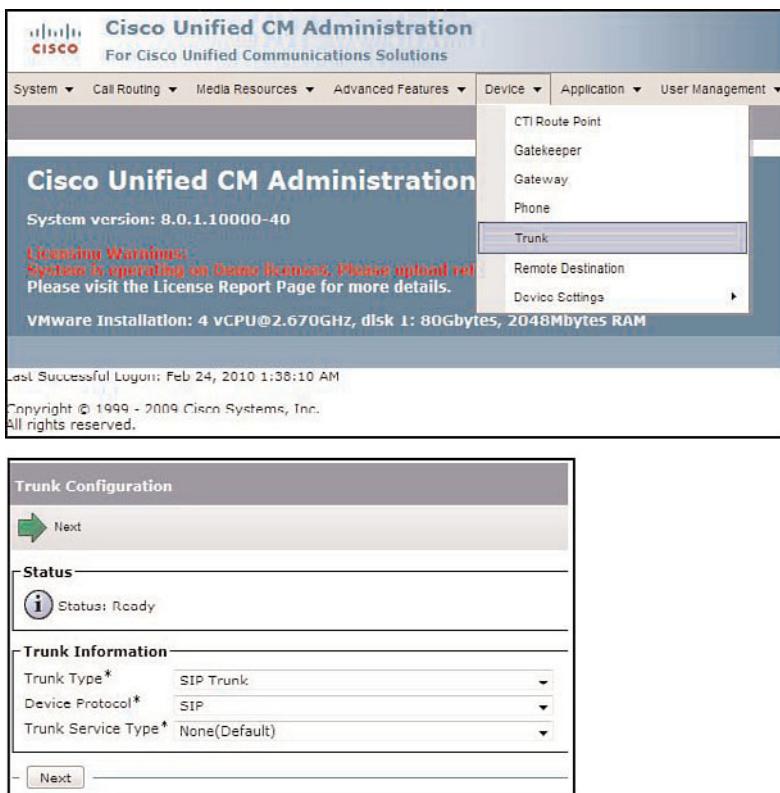


Figure 8-16 SIP Trunk Configuration

Note The trunk service types Call Control Discovery (CCD), Extension Mobility Cross Clusters (EMCC), and Cisco Intercompany Media Exchange (IME) are discussed in the Cisco Press book *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide*.

Configure SIP Trunk Parameters

The following steps outline the process to configure the parameters for a SIP trunk:

- Step 1.** From the Device Information section of the Trunk Configuration page, as shown in Figure 8-17, enter a unique SIP trunk name in the Device Name field and optionally enter a descriptive name in the Description field.

The screenshot shows the 'Trunk Configuration' page for a SIP Trunk. The 'Device Name' field is set to 'SIP-Trunk_01'. The 'Device Pool' dropdown is set to 'Default'. Other fields include 'Product' (SIP Trunk), 'Device Protocol' (SIP), 'Trunk Service Type' (None(Default)), 'Call Classification' (Use System Default), 'Media Resource Group List' (< None >), 'Location' (Hub_None), 'AAR Group' (< None >), 'Packet Capture Mode' (None), and 'Packet Capture Duration' (0).

Parameter	Value
Product	SIP Trunk
Device Protocol	SIP
Trunk Service Type	None(Default)
Device Name*	SIP-Trunk_01
Description	
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Packet Capture Mode*	None
Packet Capture Duration	0

Figure 8-17 SIP Trunk Parameters

- Step 2.** Choose the device pool from the Device Pool drop-down list. The physical location is a large determinant of which device pool to place the device in. Recall that the CUCM group is configured at the device pool level along with other parameters, such as the Location, Media Resource Group List, and SRST Reference.
- Step 3.** Enter the IP address or fully qualified domain name (FQDN) of the SIP gateway.
- Step 4.** From the SIP Information section of the Trunk Configuration page, as shown in Figure 8-18, choose a security profile from the SIP Trunk Security Profile drop-down list. The first SIP trunk might not require the custom configuration of a SIP trunk security profile because one of the default SIP trunk security profiles might work, but each subsequent SIP trunk will always require its own SIP trunk security profile. CUCM requires each SIP integration to have a unique TCP and/or UDP source port. The SIP trunk security profile is where the source port of the connection is administered.
- Step 5.** Choose a SIP profile from the SIP Profile drop-down list. The SIP profile allows the tweaking and tuning of timers and signaling variables in SIP. The SIP profile enables easy integration with other vendors' SIP proxy servers. IETF specifications have many options in them. The SIP profile allows administrators easy access to these variable timers, allowing quicker and easier integrations with third-party vendor platforms like Avaya, Nortel (now Avaya), Siemens, Microsoft, NEC, and so on.
- Step 6.** Click Save.
- Step 7.** Click Apply Config or Reset.

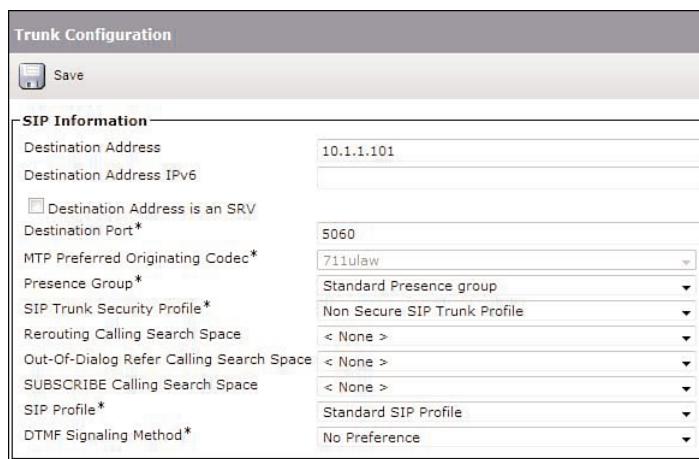


Figure 8-18 SIP Trunk Parameters (Continued)

Configure Basic Cisco IOS SIP Functionality

Unlike the source interface for H.323 traffic, the source interface (IP address) for SIP traffic and other parameters are configured as global SIP parameters. SIP signaling uses UDP 5060 by default, but the transport layer protocol can be changed to TCP. Some environments experience better reliability with the reliable TCP transport layer functionality when compared to the application layer reliability of the SIP signaling protocol stack over the unreliable UDP transport layer. Example 8-10 demonstrates the Cisco IOS configuration commands required to accomplish the following:

- Change the transport layer to TCP
- Configure the gateway router to use the Loopback 0 interface IP address of 10.1.1.101 on the router as a source IP address when communicating with CUCM

Example 8-10 Source IP Interface Binding

```
!
voice service voip
sip
bind control source-interface LoopBack0
bind media source-interface LoopBack0
session transport tcp
!
interface LoopBack0
ip address 10.1.1.101 255.255.255.0
!
```

Configure Cisco IOS Call Routing on SIP Gateways

The default signaling protocol on VoIP dial peers is H.323. Using the previously discussed voip dial-peer we used for H.323, we would need to change the dial peer configuration to specify SIP signaling. Example 8-11 includes the **session protocol sipv2** command, which converts the VoIP dial peer from the default of H.323 to SIP. The **dtmf-relay** command specifies the use of RFC 2833 in-band DTMF Relay (first priority) and out-of-band DTMF Relay using the SIP Notify method (second priority). The **rtp-nce** command is confusing, but it indicates that the VoIP dial peer will attempt to first use RFC 2833 as a signaling mechanism and then fall back to out-of-band SIP Notify signaling packets if the primary method was not successful. DTMF Relay parameters are negotiated over Session Description Protocol (SDP).

Example 8-11 DTMF Relay Method Configuration

```
!
dial-peer voice 1 voip
destination-pattern 2...
session protocol sipv2
session target ipv4:10.1.1.1
codec g711ulaw
dtmf-relay rtp-nce sip-notify
!
```

At this point, inbound call routing from the PSTN to CUCM would work. If the integration was with a third-party vendor, additional tuning of some optional parameters might be required. CUCM has the SIP profile and the Cisco IOS gateway has a SIP UA (user agent) configuration mode that can be used to configure various SIP signaling parameters.

Many signaling parameters, including the number of times to send a SIP Invite message, response timers, retry times, and authentication server settings, can be configured through the SIP user agent configuration on the Cisco IOS gateway:

```
!
sip-ua
retry invite 5
retry response 10
sip-server ipv4:10.1.1.1
!
```

Note There are many parameters and settings related to advanced SIP configuration. The Cisco Press book *Implementing Cisco Unified Communications Voice over IP and QoS (CVOICE) Foundation Learning Guide* describes how to configure Cisco IOS SIP gateway advanced features.

SIP Trunking

SIP trunks in CUCM originally used out-of-band signaling (SIP) to indicate dialed digits entered during an RTP media session (phone call) in CallManager 4.0, but CUCM 5.0 introduced RFC 2833 (in-band DTMF Relay) into the SIP trunk. RTP-NTE/RFC 2833/in-band DTMF signaling is configurable from the DTMF Signaling Method drop-down menu on the SIP trunk.

CUCM 7.0 uses an early offer (EO) SDP message in its outbound signaling by default. This is important because most IP Telephony Service Providers (ITSP) require an EO SDP message. CUCM versions before version 7.0 followed a delayed offer (DO) SDP model, where the outgoing SIP Invite message did not have an SDP offer. The SDP offer in a DO model is initiated by the destination. Most service providers do not support a delayed offer model, but integration was still supported in CUCM versions 4.x, 5.x, and 6.x by provisioning a Media Termination Point (MTP) with the SIP trunk.

SIP Trunk: MTP Allocation Configuration

To statically allocate an MTP for all calls on a SIP trunk, select the Media Termination Point Required check box on the SIP Trunk Configuration page. After the MTP is statically enabled for all calls, also choose a codec from the MTP Preferred Originating Codec drop-down list. This audio codec is normally G.711 because the communication between CUCM and the gateway takes place over the high-speed LAN running at speeds measured in gigabits. Only the VoIP side of the call includes an audio codec because the TDM side uses pulse code modulation (PCM) techniques, where the voice channel is given up to 64 kbps. Recall that the default VoIP dial peer audio codec is G.729, so the audio codec will need to be manually provisioned on the Cisco gateway router.

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- Gateways are essential components in an IP telephony environment and provide functions such as conversion from TDM voice to VoIP, DTMF Relay, and so on.
- CUCM can act as an MGCP call agent and thereby control voice interfaces of Cisco IOS routers. MGCP allows centralized dial plan configuration. With T1/E1 PRI, the backhaul functionality transparently passes Q.931 messages to CUCM.
- H.323 gateways provide an easy and flexible way to connect VoIP calls to the PSTN. Call-routing configuration needs to be applied on the gateway as well as on Cisco Unified Communications Manager.
- SIP gateways are implemented in CUCM by using SIP trunk configuration. Call-routing configuration needs to be applied on the gateway and on CUCM.

References

For additional information, refer to these resources:

- Session Description Protocol, at www.ietf.org/rfc/rfc2327.txt.
- Media Gateway Control Protocol, at www.ietf.org/rfc/rfc2705.txt.
- Session Initiation Protocol (SIP), at www.ietf.org/rfc/rfc3261.txt.
- Cisco NetPro Forums, at www.cisco.com/go/netpro.
- Cisco Feature Navigator, at www.cisco.com/go/fn.
- Cisco Systems, Inc. Cisco Unified Communications System Release 8.x SRND, at www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_0_1/ccmcfg/bccm.pdf.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

- 1.** Which type of protocol is MGCP?
 - a.** Proprietary
 - b.** Master/slave
 - c.** Peer-to-peer
 - d.** Clustered
- 2.** MGCP is closest in operation to which of the following protocols?
 - a.** H.323
 - b.** SIP
 - c.** SCCP
 - d.** Megaco/H.245
- 3.** What technology or protocol does an SCCP phone use to send media to an MGCP gateway?
 - a.** SCCP
 - b.** MGCP
 - c.** RTP
 - d.** Transcoder

- 4.** Which of the following interfaces now supports caller ID with MGCP gateways using CUCM 8?
 - a.** FXO
 - b.** FXS
 - c.** PRI
 - d.** T1-CAS
- 5.** What parameter is not available in the device pool in CUCM 8.0?
 - a.** Softkey template
 - b.** Date/time group
 - c.** Region
 - d.** CUCM group
- 6.** What two commands are required to configure MGCP for automatic configuration from the CUCM?
 - a.** ccm-manager config server
 - b.** mgcp
 - c.** ccm-manager redundant-host
 - d.** ccm-manager call-agent ip-address
 - e.** ccm-manager config
- 7.** Q.931 backhaul opens which socket with CUCM?
 - a.** UDP 2427
 - b.** UDP 16384
 - c.** TCP 2000
 - d.** TCP 2428

Chapter 9

Call-Routing Components

The dial plan is the essence of a Unified Communications (UC) system. The dial plan is at the core of the end user experience because it defines the rules that govern how a user can dial a public switched telephone network (PSTN) destination.

Endpoint addressing is an important part of the internal dial plan, which is normally segregated but directly related to the external PSTN dial plan required when calling from devices external to the organization.

Digit analysis and path selection are also important components of a dial plan. This chapter describes endpoint addressing, digit analysis (DA), and call-routing path selection in a Cisco Unified Communications Manager (CUCM) deployment.

Chapter Objectives

Upon completing this lesson, you will be able to describe and configure CUCM numbering plans, directory numbers, route groups, route lists, route patterns, route filters, digit analysis, and urgent priority to place PSTN calls. You will also be able to meet these objectives:

- Describe the components and importance of a dial plan
- Describe the concept of endpoint addressing, including On-Net versus Off-Net dialing and the uniform On-Net dial plan length
- Describe the concept of call routing in CUCM
- Describe how CUCM analyzes digits
- Describe features that relate to call routing
- Describe how CUCM performs path selection
- Describe how to configure CUCM path selection

Dial Plan Components

Although most people are not acquainted with dial plans by name, they use dial plans on a daily basis when communicating over a telephone (office/home/cellular/fax/modem). A dial plan is a numbering plan for a voice-enabled network. The dial plan is the way in which the PSTN carrier networks know how to perform its call routing. Individual blocks of telephone numbers (E.164 addresses) from public dial plans are normally assigned to one or more physical lines/circuits that the customer pays a carrier for. The North American Numbering Plan (NANP) telephone network is based on a ten-digit dial plan that consists of three-digit area codes, three-digit exchanges (NNX), and four-digit subscriber numbers. Telephone numbers within an area code sometimes only require a seven-digit dial plan. The NANP is one of the most scalable dial plans in existence. Many large voice deployments use the NANP as an example scalable network, and our PSTN direct inward dialing (DID) plan will need to align to the internal dial plan in some way. Deployments without DID will normally direct all inbound calls to an automated attendant (AA) or interactive voice response (IVR) server like Cisco Unity Connection (AA) or Cisco Unified Contact Center eXpress (UCCX=IVR).

Internal dial plans can be as few as three digits, but typical small to medium organizations use a four- or five-digit internal dial plan. The number of digits is normally determined by the number of people at each site. A four-digit dial plan can accommodate up to eight sites with 1000 phone numbers per site, which might sound large to a small organization, but it is nothing within the context of organizations that have campus networks with thousands of individuals and locations throughout the world. Most medium-to-large-size organizations leave a lot of room in their dial plan for the purpose of internal call routing. This is required because the organization might have hundreds or thousands of sites distributed throughout the world. A three-digit site code identifier per physical location would allow an organization to have up to 1000 sites (800 to avoid overlapping dial plans with leading digits of 0 or 9). Organizations benefit from transporting intersite national and international phone calls over their own private IP network by avoiding toll charges of the PSTN for intersite calls (toll bypass).

A dial plan consists of these components:

- **Endpoint addressing (internal numbering plan):** Assigning directory numbers to internal endpoints (Cisco IP Phones, fax machines, and analog phones) and applications (voicemail systems, auto-attendants, and conferencing systems) enables you to access internal and external destinations.
- **Call routing and path selection:** Depending on the calling device, you can select different paths to reach the same destination. You can also use a secondary path when the primary path is unavailable. Call routing will reroute calls over the PSTN during an IP WAN failure or when the call admission control (CAC) mechanism denies the call because there is not enough bandwidth available to accommodate the call quality.
- **Digit manipulation:** Calling and called patterns normally require digit manipulation to reflect a calling party that is accessible on the PSTN. An access code is normally

used to indicate to the local phone system that an outside (PSTN) call is going to be made. An access code of 9 will be used in this book. PSTN dial plan requirements require the stripping of the access code. Internal abbreviated dialing is sometimes used to reach externally reachable destinations through the use of digit manipulation. Number normalization and number globalization are digit manipulation techniques that are used in E.164 call routing in international systems (and Microsoft integrations). CUCM version 7.0 added E.164 internationalization support through number normalization and number globalization features that will be discussed. Another example of abbreviated dialing is using an operator code of 0 for people to get help over the phone system. The 0 key is normally routed to a hunt pilot, where the call is distributed to an available agent that is not logged out of his/her hunt group. The Cisco IP Phone supports an optional softkey parameter called HLog that can be used to log in and out of line groups (since CUCM 6.0). Digit manipulation can occur before or after a call-routing decision has been made by CUCM or the gateway router (translation profiles).

- **Calling privileges:** You can assign different groups of devices to different classes of service (CoS) by granting or denying access to certain destinations. Most organizations have a policy where lobby and other publicly accessible phones can only reach destination numbers that are routed internally or 911 emergency calls. Most employees require local PSTN destinations, but maybe they don't need access to long-distance numbers. Senior employees might need access to long-distance numbers, while only the executive team should be granted access to make an international call. This configuration will require many different partitions for the pieces of the dial plan that must be logically segregated. Devices will be assigned Calling Search Spaces (CSS) that will allow them to access (call) the phone numbers in the partitions assigned to the called party. The called party can be a directory number assigned to an internal Cisco IP Phone or a publicly accessible phone on the PSTN accessed through the dial plan in CUCM.
- **Call coverage:** You can create special groups of devices to process incoming calls for a certain service. This operation helps distribute the inbound calling load to a department or group among the members in adherence to the distribution algorithm selected (top-down, circular hunt, longest idle, or broadcast). A final forwarding rule should always be configured on the hunt pilot to ensure that the call is processed after the maximum hunt timer expires. The maximum hunt timer ensures that the calling party will not hear ringback for too long. The call coverage technique built into CUCM does not support any queuing technology like that in Unified Contact Center (UCC) or Unified Contact Center eXpress (UCCX).

CUCM, Cisco IOS gateways, Cisco Unified Communications Manager Express (CUCME), and Cisco Unified Survivable Remote Site Telephony (SRST) dial plan components are outlined and compared in Table 9-1.

These analogies only make sense if you understand one of the technologies, but understanding one of the dial peer technologies provides a comparison to understand the other.

Table 9-1 Dial Plan Components of CUCM and IOS Gateways

Dial Plan Component	Cisco IOS Gateway	CUCM
Endpoint Addressing	POTS dial peers for FXS ports and ephone-dn	Directory number
Call Routing and Path Selection	Dial peers	Route patterns, route groups, route lists, translation patterns, partitions, and CSSs
Digit Manipulation	Voice translation profiles, prefix, digit-strip, forward-digits, and num-exp	Translation patterns, route patterns, global transformations, and calling and called party settings
Calling Privileges	Call of restriction (COR) and COR lists	Partitions, CSSs, and Forced Authorization Codes
Call Coverage	Dial peers, hunt groups, and call applications	Line groups, hunt lists, and hunt pilots

If it is your first time reading about either one, you can ignore the comparisons for now because they might be confusing.

Endpoint Addressing

Reachability of internal destinations is provided by assigning directory numbers (DN) to all the internal endpoints (Cisco IP Phones, fax machines, and analog phones) and applications (voicemail, auto-attendants, and conferencing systems).

The number of dialable extensions determines the quantity of digits needed to dial extensions internally. A four-digit abbreviated dial plan cannot accommodate more than 10,000 extensions (from 0000 to 9999), but a leading digit of 0 is normally not used in dial plans because it is dedicated to route calls to the company operator or for operator functionality (AA/IVR). A leading digit of an 8 or 9 is also normally restricted because either one of these digits is normally used to make outgoing calls to the PSTN. If we assume that access code 9 is used, the access code and operator functionality reduce the number range to 8000 dialable patterns (1000 to 8999). Customers normally want to distinguish each site by a different leading digit as well, which limits the scalability of the system to eight sites if each site would receive a different leading digit (1 to 8). Each site could have 1000 directory numbers (1000 to 1999). A four-digit dial plan is not very popular with large organizations. Most large organizations use at least a five-digit dial plan but can use as many as seven digits internally and ten digits for all intersite calls (modeled after the PSTN).

Direct inward dial (DID) is used in most organizations. The PSTN service provider maps a range of phone numbers to one or more circuits on the customer's behalf. The DID range

offered from the service provider usually determines the abbreviated dialing range for that particular site. If a customer were taking in a range of numbers in the 1-800-555-XXXX block, the customer would probably use a five-digit dial plan for this site to accommodate the 10,000 possible DID phone numbers that the provider is going to map to the customer circuits. The gateway router at the edge of the network will normally collect all ten digits for the called party information. The ten-digit dialing received from the gateway is then translated into an abbreviated internal dialing plan. The five-digit range of numbers would be 5XXXX to map directly to the DID range from the provider.

Endpoints dial each other using the internal abbreviated dial plan. Each call routed by CUCM is categorized as one of two types: On-Net and Off-Net. Call forwarding information on the Cisco IP Phone is segregated as internal and external. As an example, call forward no answer (CFNA) can ring my second line if I'm busy on the first for external callers (PSTN), but I would like internal callers to hear my voicemail greeting if I'm busy on my primary line (internal). On-Net and Off-Net call classification can also be useful for call-blocking service parameters that can help limit toll fraud in the system. The Block Off-Net to Off-Net Transfers Call Manager service parameter can be turned on and the system would then block a PSTN-sourced call from being forwarded back out to the PSTN. This service parameter is turned off by default. Here are some details of how CUCM determines whether a call will be classified as On-Net or Off-Net:

- **On-Net:** These calls remain within the CUCM system (private network). An example of an On-Net call is a call from an internal Cisco IP Phone to another internal Cisco IP Phone. On-Net calls can be routed over intercluster trunks (ICT) or Session Initiation Protocol (SIP) trunks to integrate with remote CUCM clusters or third-party SIP vendor equipment (ITSP, Microsoft integration, Avaya/Nortel VoIP integration). The administrators have control over how calls are classified, but all route patterns and all calls to or from a gateway are classified as Off-Net by default.
- **Off-Net dialing:** Off-Net calls are normally calls that are routed outside the private telephony system to the PSTN. Most Off-Net calls are routed across gateways to the PSTN.

Abbreviated dialing is not a configuration parameter in CUCM. Abbreviated dialing is the idea that employees do not need to dial the full ten-digit phone number of a PSTN destination if it's a resource that's constantly being leveraged. A good example of this can be a travel agency that works closely with the company to provide travel arrangements, where there might be 300 instructors flying around the country (global knowledge). A four-digit internal dialing pattern could be configured to translate the dialed digits into the full ten-digit phone number.

Figure 9-1 includes the following three call scenarios:

- A Cisco IP Phone with extension number 2003 (calling party) dials extension 3001 (called party). The called party is a Cisco IP Phone that is natively registered with CUCM over IP but physically located in a remote IP subnet across the WAN. CUCM will route the call to the endpoints directly based on the IP address that CUCM has associated with the Cisco IP Phone registration information. The IP address can be verified in CUCM Administration by choosing **Device > Phone** and searching for the phone. The display output will have an IP address associated with it. The IP address appears as if it is a hyperlink, and it is. CUCM 8.0 has shut off the web server components of the Cisco IP Phones by default for security reasons. The phone configuration page allows this functionality to be turned back on so that it can be used for remote troubleshooting purposes. The call is routed internally over the private IP network (Multiprotocol Label Switching [MPLS] Virtual Private Networks [VPN] are by far the most popular WANs at the time of this writing), and the call is classified as an On-Net call.

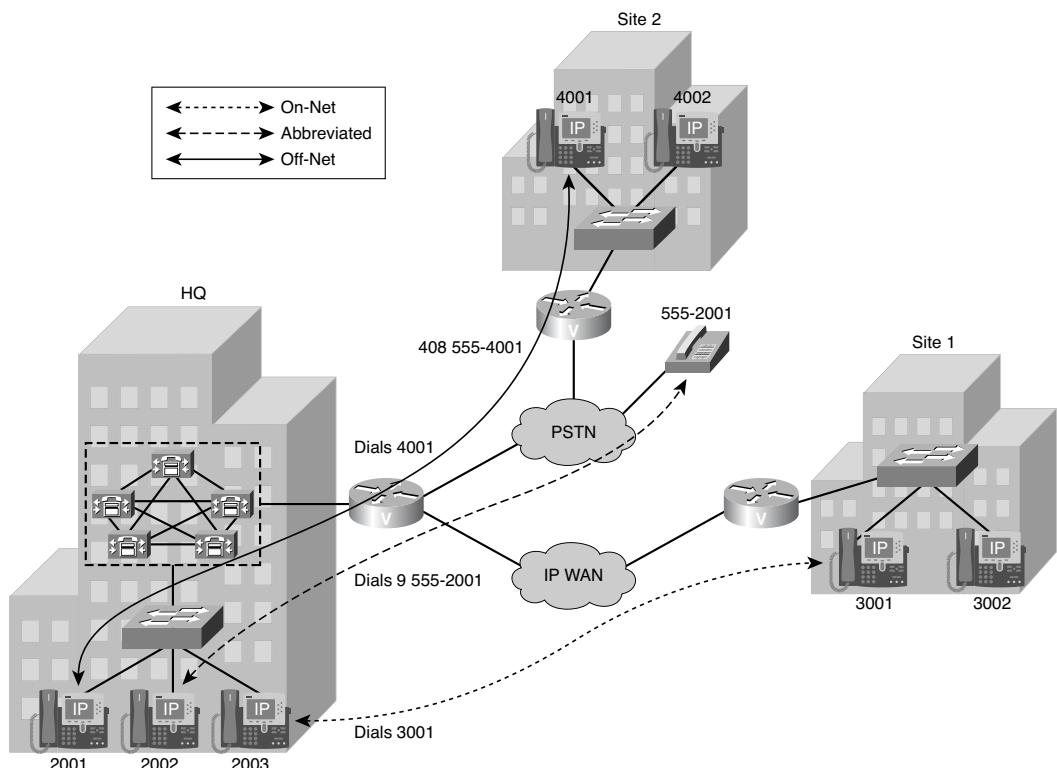


Figure 9-1 Endpoint Dialing

- A Cisco IP Phone calling party (2002) dials 9-555-2001 (called party), and the call is routed to a PSTN destination through a PSTN gateway. The call is classified as an Off-Net call. All route patterns “provide outside dial tone” and are classified as “Off-Net” by default. If you deselect the Provide Outside Dial Tone check box on the route pattern configuration page, the call classification default changes to On-Net.
- A Cisco IP Phone with extension 2001 (calling party) dials 4001 (called party). The Cisco IP Phone with extension 4001 is physically located at Site 2. CUCM Express (CUCME) is used for local call processing at Site 2, and no IP WAN link connects the sites. Because Site 2 cannot be reached over an IP WAN and the service provider (PSTN) requires ten-digit dialing to properly route the call, a CUCM translation pattern is used to manipulate the called party digits that were received. The translated pattern will match a route pattern, and the call will be routed to a PSTN gateway on the network. Translation patterns (TP) and route patterns (RP) are covered in more detail later in this chapter and in Chapter 10, “Calling Privileges.”

Uniform On-Net Dial Plan Example

A dial plan should be designed so that all extensions within the system are reached in a uniform way. A fixed number of digits are used to reach a given extension from any internal Cisco IP Phone or other device integrated into the Unified Communications system. Uniform dialing is desirable because of the simplicity it presents to end users. An end user does not have to remember different ways to dial a number when calling from various locations, as long as they understand the underlying dial plan. An example of such a dial plan could be four-digit internal dialing, while all interoffice dialing requires seven-digit dialing. The three additional digits are the three-digit site code identifier used for interoffice mail and distribution (retail).

Table 9-2 provides an example of a four-digit uniform On-Net dial plan. Unfortunately, most dial plans in the real world do not look like the one in the table because of moves, adds, changes, deletions, DID blocks offered by the carriers, and so on. Most internal dial plans align closely with the DID blocks that can be purchased from the carriers. Table 9-2 offers a view of what you can strive for in your internal dial plan for a small organization. Larger organizations normally require some type of site prefix identifier like the example in the previous paragraph.

Table 9-2 Dial Plan Example

Directory Number Range	Usage	DID Ranges	Non-DID Ranges
0XXX	Excluded: 0 is used to reach the operator.	—	—
1XXX	Site A extensions	418 555 1XXX	Not applicable
2XXX	Site B extensions	919 555 2XXX	Not applicable
3XXX	Site C extensions	415 555 30XX	3[1-9]XX

Table 9-2 Dial Plan Example

Directory Number Range	Usage	DID Ranges	Non-DID Ranges
4[0–4]XX	Site D extensions	613 555 4[0–4]XX	Not applicable
4[5–9]XX	Site E extensions	450 555 4[5–9]XX	Not applicable
5XXX	Additional Site A extensions	418 555 5XXX	Not applicable
6XXX	Site F extensions	514 555 6[0–8]XX	69XX
7XXX	Future extensions	—	—
8XXX	Future extensions	—	—
9XXX	Excluded: 9 is used as an access code.	—	—

Table 9-2 represents an example of a multisite dial plan with each number range divided for a logical listing to cover a four-digit extension range:

- Site A in Table 9-2 requires more than 1000 extensions. Two ranges of numbers have been reserved for this site because the company had previously decided on an internal dial plan and configured many devices with the following four-digit block of numbers: 1XXX. The 5XXX range was selected as the second range because Sites B, C, and D were already deployed at the time. The corresponding DID ranges in the 5XXX block just happened to be available from the local exchange carrier (LEC). What luck!
- Site B in Table 9-2 has been assigned the four-digit block of 2XXX, allowing up to 1000 extensions. A corresponding DID block was purchased from the LEC.
- Site C was assigned a four-digit range, but it has been split between 100 DID extensions (415 555-30XX) and up to 900 non-DID extensions. If growth requires more than 100 extensions (directory numbers), the additional lines will not be able to leverage DID.
- Sites D and E were each assigned 500 numbers from the 4XXX range. Note that their corresponding DID ranges must match each of the site's respective portions of the 4XXX range. Because the DID ranges are for different sites (probably from different PSTN service providers), more coordination effort is required to split ranges between sites. This can be nearly impossible to do in the real world, where we are simply running out of phone numbers with our existing ten-digit dialing system. I don't believe the original developers of the North American Numbering Plan (NANP) imagined each human being having multiple phone numbers, and if they did, we're still running out. The future might bring a 13- or 14-digit dial plan to us as the NANP continues to run out of phone numbers.

- Site F's range is split between 900 DID numbers (6[0–8]XX) and 100 non-DID numbers (69XX).
- The ranges 7XXX and 8XXX are reserved for future use.

Medium- to large-sized organizations with more than eight sites would need to have a more complicated intersite call-routing paradigm to ensure proper call routing and ease of use. The Cisco Press book *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide* goes into more detail on larger centralized call-processing and distributed call-processing deployments, but the call-routing information from this book is considered a prerequisite for reading the CIPT2 book.

E.164 Overview

E.164 is an ITU-T recommendation that defines the international public telecommunication numbering plan that is used in the PSTN.

The E.164 specification defines the format of telephone numbers. An E.164 phone number can have a maximum of 15 digits, and international phone numbers are represented with a plus sign (+) before the phone number to represent the international call prefix. International operator codes and country codes are not required if the system is programmed to understand the + character to indicate an international call. Cisco IP Phones do not have a + character on them, so the + character cannot be dialed natively from the Cisco IP Phone keypad. The + character can be dialed on a keyboard when using a software-based phone like Cisco IP Communicator (CIPC) or Cisco Unified Personal Communicator (CUPC). CUPC requires the Cisco Unified Presence (CUP) server to register, but CUPC can also be used to remotely control a Cisco IP Phone over a Computer Telephony Interface (CTI) connection.

Dialing international phone numbers from a Cisco IP Phone normally requires dialing an access code (9), international code (011 in the United States), country code (variable in length), and subscriber code (variable). Some countries, such as the U.K. and Germany, have a unified dial plan, but each country's dial plan is very unique and it might not be uniform over carriers or geographical barriers.

CUCM can route calls that have been placed to E.164 numbers using a plus sign (+) as a prefix. Support for + dialing is implemented by recognizing the plus sign as dialable pattern that can be part of call-routing entries such as route patterns or translation patterns. This configuration might be required if international calls are being received with the + character in the called party number information in the call setup. Integrations with Microsoft Unified Communications products (LCS, OCS, Lync) require the support of the + character because these platforms use and pass the + character in all call routing.

Cisco IP Phones can place calls to PSTN destinations by using destination numbers in E.164 format with a + prefix. The user cannot manually enter the plus sign on the Cisco IP Phone keypad though. + dialing is supported on Cisco IP phones when calling from call lists (placed, received, and missed calls), directories, speed dials, and web-based applications like “click to dial.”

Call-Routing Overview

CUCM performs call routing (steering) to get calling parties connected to called parties. Call routing is destination based because the call is normally directed to a particular destination by performing digit analysis (DA) against the called party (dialed digits) information. Figure 9-2 displays three different types of calls that are explained as follows:

- **Intrasite routing:** A call that is routed from one device to another device within a single site. This call is classified as an On-Net call.

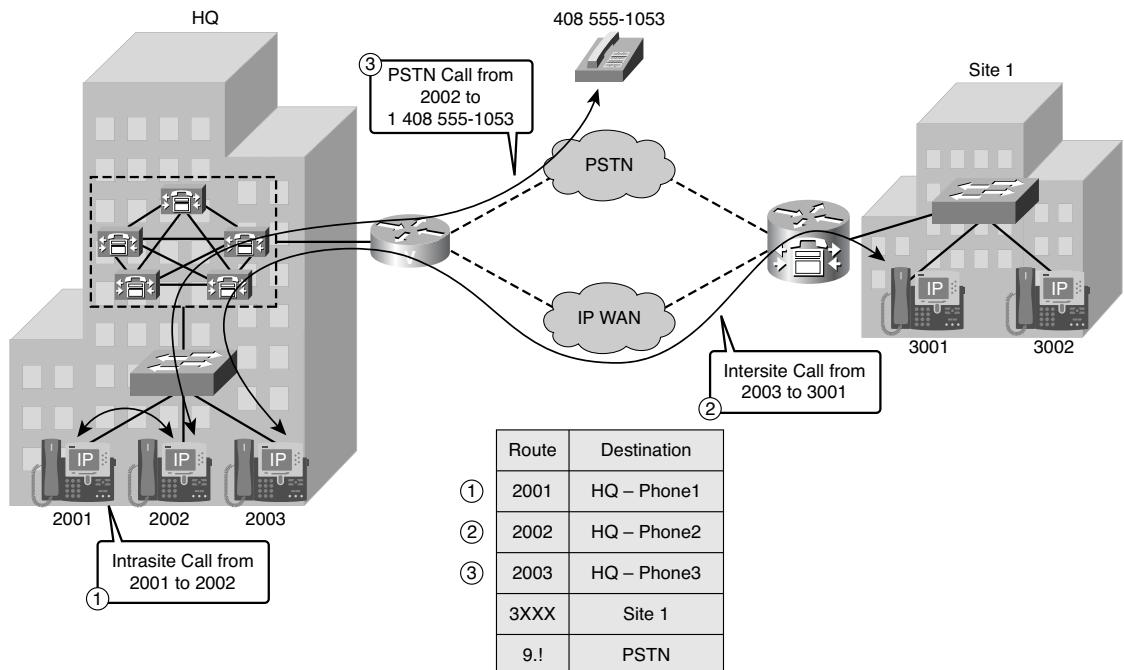


Figure 9-2 Call Routing

- **Intersite routing:** A call that is routed between multiple devices that are physically located at separate geographical sites that are logically interconnected by the WAN links of the data communications network (IP). The call is also classified as an On-Net call because the call is routed between two devices that are natively registered to CUCM over a TCP/IP network. CUCM does not know whether two IP subnets are connected to the same data network switch in two different VLANs or whether the two subnets are across the world. CUCM merely sends call setup/teardown (SCCP/SIP) over the network and relies on the network to route the data packets.
- **PSTN routing:** Call routing from a device internal to the CUCM cluster to a device on the PSTN. PSTN calls are routed out gateways (Cisco routers with time-division

multiplexing [TDM] interfaces) instead of trunk cards. A trunk card on a PBX has functionality that is very close to that provided by gateway routers.

CUCM has an IP address associated with every registered phone that has one or more registered directory numbers (DN). The directory number information is part of the call-routing database and can be seen if a call-routing report is run from the Call Routing menu in CUCM Administration. Bulk Administration Tool (BAT) also has a way to export the call-routing database. Route patterns must be configured to route calls to the PSTN because CUCM does not natively know about any of the DID ranges of the PSTN (seven-digit, ten-digit, and 11-digit dialing mostly, but we'll get into far more detail). Call routing is synonymous with static route IP routing if you're reading this book coming from a data network routing background. A large portion of CUCM's call-routing table is built of registered endpoints and statically entered route patterns that point to external destinations. Any phone number programmed anywhere in CUCM Administration becomes part of the underlying call-routing database stored in the IBM Informix Database Server (IDS).

Figure 9-2 has a basic routing table that consists of the following entries:

- **Headquarters:** 2001, 2002, and 2003 are directory numbers (DN) of phones configured in CUCM. All the DNs within the 2XXX range are located at the headquarters site.
- **Site 1:** CUCM Express (CUCME) is running on the Cisco router/gateway at Site 1. CUCME has a dial plan that is independent of CUCM. CUCM treats CUCME as if it were an external destination reachable through the PSTN or through H.323 or SIP. Media Gateway Control Protocol (MGCP) could be used as a gateway protocol, but then the devices at the remote site would natively be registered to CUCM, not CUCME. CUCME is a good choice over unreliable or low-bandwidth WAN links, or between sites that are very geographically separated (for example, CUCM in San Jose, CA, and Cisco IP Phones in India).

CUCME requires up to three VoIP dial peers configured with the four-digit directory number range of devices at the headquarters (2... because dots are used in Cisco IOS to indicate dialed digits. The CUCME VoIP dial peers will point to the IP addresses of two or three CUCM servers in the cluster. CUCM requires a route pattern configured as 3XXX because CUCM uses X as a wildcard parameter indicating any dialed digit. Dial peers are required in Cisco IOS on the Cisco router if the H.323 or SIP gateway protocols are used.

The CUCM cluster will need to have an H.225 intercluster trunk (ICT) configured that is pointing to an IP address used for H.323/H.225 call signaling on the CUCME router. The trunk will require a Media Termination Point (MTP) provisioned on the H.225 trunk because CUCME and CUCM support different H.323 standard options to provide supplementary services (call hold, park, conference, and so on). CUCM uses the H.323v2 Empty Capability Set (ECS), while CUCME uses the H.323v2 H.450.X standards. ECS and H.450.X standards are not compatible with each other, so the MTP is used as the translation device between the two different options. MTPs will be discussed further in Chapter 13, "Media Resources."

The example uses 9.! as a route pattern example because we have not yet discussed the various wildcard parameters used in CUCM route patterns (RP). Using 9.! in your dial plan is normally not recommended because it will lead to a very complex overlapping dial plan in which you will continuously wait 15 seconds for the system to route phone calls (unless you lowered your T.302 intersite digit timeout in the CallManager service parameters). The exclamation point (!) is a wildcard character that matches on one or more digits. The 9.! route pattern basically matches on every dialable pattern, as long as the digit string only includes 15 digits plus the access code. The dot (.) character is normally used purely for digit-stripping purposes. Called party digit discard instruction (DDI) rules are normally configured to strip out any digits that appear before the dot (.) in the digit string. In our example, this will ensure that the provider only gets up to 15 digits dialed from the phone, not the access code that was dialed to route a phone call to the outside world (PSTN). Usage of the dot and the ! are further explained later in this chapter.

Three calls are part of the example shown in Figure 9-2:

- (1) **2001 to 2002:** This is an internal On-Net call. The called party number of 2002 is connected with calling party 2001.
- (2) **2003 to 3001:** The dialed number 3001 matches a route pattern that is routed across the H.225 intercluster trunk (ICT) to CUCME at Site 1. In an H.323 integration using the H.225 trunk, a Q.931-derived SETUP message is sent from CUCM to CUCM Express (CUCME). This call is classified as On-Net because the “provide outside dial tone” was deselected from the 3XXX route pattern configured in CUCM. Call classification defaults to On-Net for all calls routed with a route pattern that does not have the Provide Outside Dial Tone check box selected.
- (3) **2002 to 9 1-408-555-1053:** This call is routed to the PSTN by means of the gateway. The gateways DSPs are responsible for converting the Real-Time Transport Protocol (RTP) media used on the IP network to the TDM PCM format required for PSTN compatibility. Gateways are increasingly becoming IP based with the advent of IP trunking services from IP Telephony Service Providers (ITSP). The gateway is still a gateway in the ITSP model, but the gateway functionality is referenced as the Cisco Unified Border Element (CUBE). CUCM’s called party DDI is set to pre-dot, and the access code of 9 will be stripped out before the call is routed to the PSTN. This classification of the call is Off-Net in CUCM by default (as long as the “provide outside dial tone” is at the default (selected)). Call classification can be manually controlled at any time, but most of us do not change it often.

Call-Routing Table Entries

Table 9-3 shows a list of possible call-routing table destinations (called party). A call-routing lookup might be destined to any of the call-routing table entries in Table 9-3. Some of these call-routing components have not been discussed yet, but each call-routing component will be covered in more detail as you progress through this book.

Table 9-3 Call-Routing Destinations

Routing Component	Description
Directory numbers	Numbers assigned to endpoints and applications. Used for internal routing within a cluster.
Translation pattern	Used to translate the called party number to a different number.
Route pattern	Used to route calls to remote destinations (PSTN, remote CUCM cluster, and so on).
Hunt pilot	Used for call coverage capabilities (call distribution similar to that provided by automatic call distribution [ACD]). Cisco reserves the ACD terminology for its call center products (UCC/UCCX).
Call-park numbers	Allows the holding of a call on a number to be retrieved by any other Cisco IP Phone in the cluster.
Meet-me numbers	Allows a conference call that easily accommodates four or more parties on one call.

Route Patterns

The CUCM call-routing database includes the directory numbers of Cisco IP Phones and various items configured in the CUCM cluster. CUCM does not know about any phone numbers external to CUCM. Gateway and trunks allow CUCM to communicate with other systems using traditional TDM interfaces (FXO/FXS/T1-CAS/T1-PRI/E1-CAS/E1-PRI) or a gateway protocol for CUBE (H.323, SIP) as the communication integration. CUCM always uses a gateway protocol to communicate to the gateway router, but the gateway needs to convert that signaling in the case of both traditional gateways and CUBE. CUCM is configured with route patterns that route calls to a prioritized list of gateways and/or trunks. Call-routing logic in CUCM requires various wildcard parameters to implement robust call-processing logic. Table 9-4 is a listing of the various wildcard parameters that route patterns can use in CUCM.

The @ wildcard is a special macro function that expands into a series of patterns representing the entire national numbering plan for a certain country. A route pattern of 9.@ will load a complex 166-route-pattern North American Numbering Plan (NANP) by default.

It is possible to configure CUCM to accept other national numbering plans. When this is done, the @ wildcard can be used for different numbering plans, even within the same CUCM cluster, depending on the value selected in the Numbering Plan field on the Route Pattern Configuration page.

Table 9-4 Route Pattern Wildcards

Wildcard	Description
X	Single digit (0–9, *, #)
@	North American Numbering Plan
!	One or more digits (0–9, *, #)
[x–y]	Generic range notation
[^x–y]	Exclusion range notation
.	Terminates access code
#	Terminates interdigit timeout
<wildcard>?	Matches zero or more occurrences of any digit that matches the previous wildcard
<wildcard>+	Matches one or more occurrences of any digit that matches the previous wildcard
\+	Matches the + sign as part of a number. (The \ denotes a delimiter, telling CUCM to process the + as its own character +, rather than the wildcard as previously shown.) The + is used for globalized E.164 call routing.

The @ wildcard is not practical for the simple reason that it is impossible to perform a class of service (CoS) deployment with it. CoS is the idea that certain devices should be restricted from making certain types of calls that are a possibility in the NANP. International, long-distance, and toll service numbers are normally restricted from devices that don't need to be making these types of calls that can incur high costs. The @ wildcard has many other disadvantages that normally precludes its use, but it is there and you can use it. I would urge you to continue reading, learn the dial plan, and never use the @ route pattern, but that's just my opinion.

International destinations are usually configured using the ! wildcard, which represents one or more digits. In North America, the route pattern 9.011! is typically configured for international calls. The same result is accomplished in Germany with the use of the 0.00! route pattern because Germany uses different access codes and international dialing codes.

The ! wildcard is also used for deployments in countries where the dialed numbers can be of varying lengths. In such cases, CUCM does not know when the dialing is complete and waits for 15 seconds (by default) before sending the call. This delay can be reduced in any of the following ways:

- **Reduce the T.302 timer service parameter.** A best practice is to set this value to 4 to 5 seconds to prevent premature transmission of the call before the user is finished dialing.

- Configure a 9.011# second route pattern to include the T.302 timeout expiration code. The # symbol is normally used to indicate that the system should stop analyzing the dialed digits (called party) against the call-routing database and to choose the closest route immediately (even if an overlap exists in the call-routing database). The second route pattern of 9.011# requires that the end user dials the # at the end of the entered digits so that the system will not wait for up to 15 seconds (default) for the T.302 interdigit timeout to perform the call routing. This action is analogous to pressing the Send button on a cell phone, and it's a well-known trick among those that make international calls.

The Urgent Priority check box in the route pattern configuration is often used to force immediate routing of certain calls as soon as a match is detected. The system will not wait for any more digits even if an overlapping dial plan exists. Emergency call-routing patterns are used in many countries throughout the world, but they differ by part of world. Inside the European Union, the emergency telephone number of 112 is often used. 112 is also the emergency call-routing number used in GSM cellular networks throughout the world. 911 is the emergency call-routing number used in North America that this book will cover. The same information can be applied to emergency call-routing patterns used throughout the world. If 9 is used as an access code to get an outside line, it makes sense to configure a 9.911 route pattern in addition to a 911 route pattern. The 911 route pattern must have the Provide Outside Dial Tone check box selected if a 9 is used as an access code to the system. When the outside dial tone is played to the calling party, it could get very interesting if every pattern that includes that leading digit does not have the “provide outside dial tone” selected. Try this in a lab if you get a chance. Take your 911 route patterns and deselect the Provide Outside Dial Tone check box. Try dialing a ten-digit pattern that begins with a 9 and see when you get your secondary dial tone. If the following dialed digits were entered into a Cisco IP Phone registered to CUCM, the end user would hear a secondary dial tone when the 8 is dialed because that is when the system knows that all patterns that begin with 918 have “provide outside dial tone” selected. After 911 was removed from the call-routing match potentiality logic, the system believed it was time to play secondary dial tone:

9-1-800-268-7737

The short end of this story goes back to the original statement: Ensure that the Provide Outside Dial Tone check box is selected for any route pattern that has the access leading digit (9 in this example).

Let's look at a scenario that's more closely connected to the Urgent Priority check box. We take a scenario where local call routing can still be performed with seven-digit dialing. Seven-digit dialing seems to be going the way of the dinosaur, but at the time of this writing, I can still use it locally in Hopewell Junction, NY. The same scenario would happen with ten-digit dialing; here's the scenario: An end user feels a pounding in his chest and dials 9911 as fast as he can (properly trained employees can dial 9911 and not 911 (or vice versa). It's best to be conservative here because we're talking about a system designed to save lives. It's best to support both patterns in your system. If a lot of calls

are being improperly routed to the public safety answering point (PSAP)/911 center, the access code for outside calls should be changed to an 8. This would limit end users' ability to improperly route a 911 call.

Because both route patterns 9.911 and 9.[2–9]XXXXXX are configured for emergency call routing and local seven-digit dialing, respectively, CUCM would normally have to wait for the T.302 timer to expire before routing the 9.911 call because further digits might result in a match against the 9.[2–9]XXXXXX 7 digit pattern. This represents an overlapping dial plan because both patterns are a match, but one pattern might include more digits. CUCM must wait for more digits or wait for the T.302 to expire—whichever one happens first—and then call routing can happen. If the Urgent Priority check box is selected for the 9.911 route pattern, CUCM would have made its call-routing decision as soon as the user finished dialing 9911. CUCM would ignore any overlapping patterns and the T.302 timer because urgent priority instructs CUCM to route the call as soon as there is a match.

Translation patterns always have the Urgent Priority check box enabled. CUCM versions before 7.0 could not disable this check box, but this capability has not been in place since CUCM 7.0. The check box on the configuration page will be grayed out in versions prior to 7.0. This can be best understood through an example. In a dial plan consisting of a translation pattern of 100 and a directory number of 1001, extension 1001 would never receive a call from a Cisco IP Phone that sends digits in real time, as they are dialed.

Cisco Type A phones converted to SIP use enbloc signaling by default, so this scenario would not take place because CUCM would evaluate all four digits as one pattern. Enbloc signaling is used with T1/E1 ISDN services and various gateway protocols (H.323, SIP, MGCP). Skinny Client Control Protocol (SCCP) and most Cisco SIP devices send their digits as they're dialed for digit-by-digit analysis against the call-routing database.

CUCM matched on 100, which is a translation pattern that had the Urgent Priority field selected. CUCM routed the phone call even though a subsequent 1 could have been received and the call would have been routed to another Cisco IP Phone. This did not happen because of the urgent priority call-processing logic in CUCM.

Route Pattern Examples

Table 9-5 includes examples of call-routing logic used in CUCM. The X wildcard matches on any dialed digits, including the * and # that can be dialed from a standard phone keypad. The [X–Y] generic range notation matches only one digit within the brackets. A range of [13–59] using the brackets would match on exactly one digit (1, 3, 4, 5, or 9). This range does not match on two digits, even though the human brain is more apt to evaluate this string as 13 through 59. The range notation uses Boolean regular expressions, and this is the way it works. A comma is an illegal character in the regular expression language. A range of digits that are not in sequence cannot include a comma. 1,3–5,9 might be a more natural way of evaluating the pattern to humans, but Boolean programming requires 13–59 to achieve the resulting match digits (1, 3, 4, 5, or 9).

Table 9-5 Route Pattern Matching

Route Pattern	Result
1234	One exact dialed digit: 1234.
1*1X	Matches dialed digits 1200 to 1299, 12**, 12*#, 12#*, and 12##.
12XX	Matches dialed digits 1200 to 1299, 12**, 12*#, 12#*, and 12##.
13[25-8]6	Matches dialed digits 1326, 1356, 1366, 1376, and 1386.
13[13-59]X	Matches dialed digits 1310–1319, 1330–9, 1340–9, 1350–9, or 1390–9. The * and # have been excluded for brevity.
13[^3-9]6	Matches dialed digits 1306, 1316, 1326, 13*6, or 13#6.
13!	Matches the string 13 followed by one or more digits.
13!#	Matches the string 13 followed by one or more digits and then ended with a #.
\+!	Matches a phone numbers staring with + and is followed by one or more digits, as used by E.164 numbers.

13! is shown in Table 9-5 with a pound sign (#) and without it, and the exclamation point carries with it an interesting call-routing challenge. CUCM will never know when the user is done dialing digits because the exclamation point can match on a nearly infinite number of patterns (up to 15 digits are evaluated). CUCM routes all calls that include ! when the T.302 interdigit timeout expires or when the pound/octothorpe (#) key is dialed. The T.302 timer is 15000 milliseconds (15 seconds) by default. CUCM does not implicitly know how to process the interdigit timeout, so it must be configured in the route pattern. This normally means that all route patterns that include the exclamation point are probably going to be in the dial plan with and without the pound sign. The pound sign must be in the route pattern for it to be dialed. The only exception to this rule is if the frequently unknown “PreDot IntlAccess IntlDirectDial” called party digit discard instruction (DDI) is used. I normally make the assumption that this is not set because it’s not covered in any of the CCNP Voice certification-related classes at the time of this writing. The current CCNP Voice (formerly CCVP) certification requirements are available online at the following URL: www.cisco.com/go/certifications.

Digit Analysis

When there are multiple digit analysis results for the same dialed pattern (and none of the patterns require additional digits), CUCM performs closest-match routing. This routing is explained further in the examples that follow using the simple dial plan illustrated in Figure 9-3.

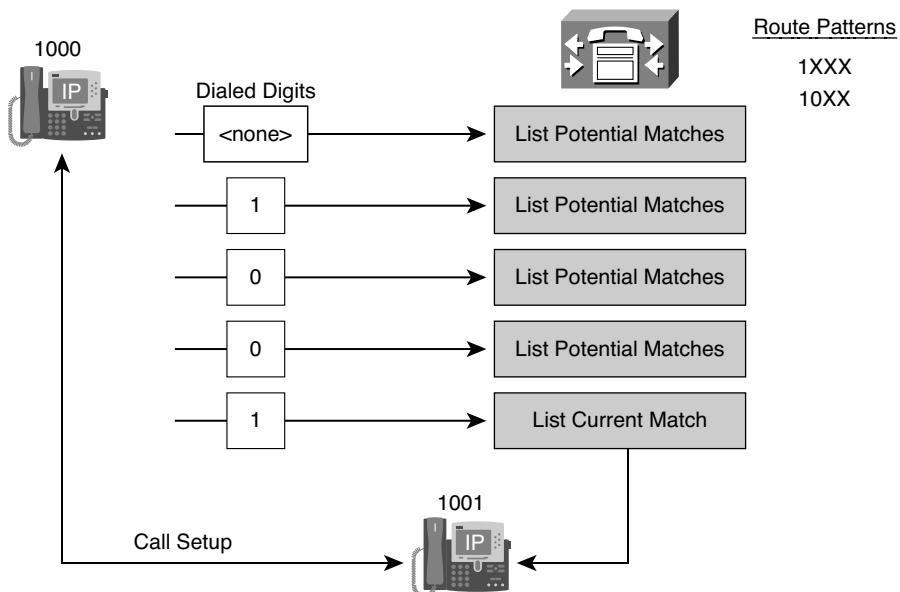


Figure 9-3 *Digit-by-Digit Analysis*

The dial plan in Figure 9-3 includes a directory number of 1001 and two route patterns of 1XXX and 10XX. The dialed digits (called party) of 1001 match on one directory number and two route patterns. Each route pattern in Figure 9-3 can match on a range of 1000 phone numbers, but directory number 1001 is an exact match. The call is routed to the Cisco IP Phone with extension 1001. The call setup information includes the IP addresses and ports that will be used in the RTP media communication between the Cisco IP Phones. The Cisco IP Phones randomly use an even port number in the UDP port number range of 16384 through 32767 (16K through 32K).

Consider the dial plan in a similar way to the call-processing logic in CUCM. CUCM in Figure 9-3 has three potential matching patterns when the first three digits are received. The call would not be routed until the T.302 timer expired or there was an exact match in the call-routing database. Digit analysis can be performed in the trace file on CUCM. Search through the trace file for the keyword *Potential*, and you're very likely to see the "Potential Matches Exist" state that the call routing is in after the third digit is received. When the fourth and final digit is received, there is only one pattern that matches the dialed digits exactly, and no other patterns would cause the system to wait for more digits. Call routing takes place within milliseconds (thousands of a second), but Cisco does not guarantee call setup times as is done in Inter-Process Communication (IPC) turret systems. I have seen CUCM and Cisco IP Phones used in financial environments because of the high cost of the IPC turret systems. A turret-based phone will have call setup times guaranteed in microseconds (millionths of a second), but each handset can cost up to \$10,000.

Digit collection is stopped as soon as an entry in the call-routing table is matched in its full length and no other (longer) potential matches exist. Figure 9-4 will be used in the next example in which an end user dials 1111. Because the call came from an SCCP or SIP phone using Keypad Markup Language (KPML), CUCM receives, interprets, and analyzes the dial plan on a digit-by-digit basis. After the first two digits in Figure 9-4 have been analyzed, only one potential match is left because all other entries in the call-routing table require a different second digit. CUCM continues collecting digits until it receives all four digits of 1111.

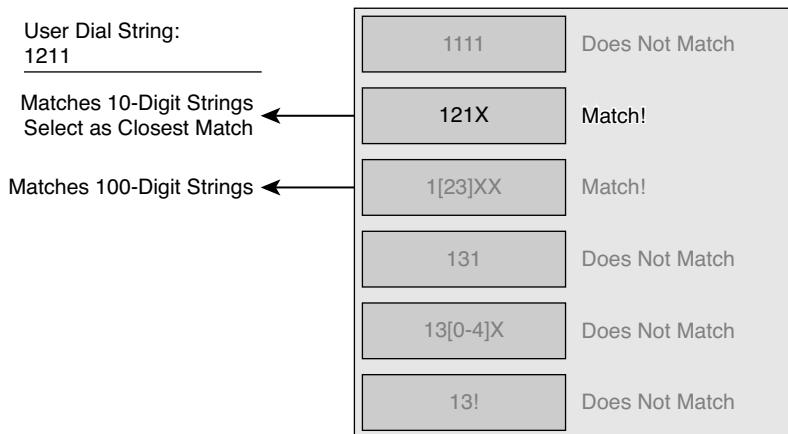


Figure 9-4 Digit Collection Example

Consider the following two additional call-routing scenarios against the basic call-routing database in Figure 9-4:

1. Dialed digits of 1200 are received and CUCM performs digit analysis. There are two potentially matching patterns in this scenario: route patterns 1XXX and 12XX. Both route patterns match the dialed digits of 1111, but 12XXX is a closer match. The call will be routed in the way intended for the route pattern of 12XXX, which can be routed to a different final destination when compared to route pattern 1XXX. 1XXX matches a total of 1000 potential strings (1000 to 1999), whereas 12XX only matches on 100 potential strings (1200 to 1299). 12XX is selected and CUCM performs call routing to the intended destination.
2. Dialed digits of 1212 are dialed against the dial plan in Figure 9-4. There are three potentially matching patterns: 1XXX, 12XX, and 121X. 121X matches only ten strings, whereas the other two route patterns match 1000 and 100 possible strings, respectively. 121X is chosen as the closest match, and the call-processing logic for this pattern continues.

When an endpoint goes off-hook, CUCM begins the digit analysis process immediately without a single digit being dialed. Every number in the call-routing database is a potential match by default. Cisco IP Phones can be configured as private line automatic

ringdown (PLAR) devices that will dial a number as soon as the handset is lifted (similar to a hoot-and-holler line). PLAR is associated with the primary line on a Cisco IP Phone by configuring a calling search space (CSS) that includes only one partition that is in a translation pattern. The configuration of this feature is done in Chapter 13 after we talk about partitions and CSSs that are required for a class of service (CoS) deployment in which certain types of phone numbers cannot be dialed by certain devices. For example, a lobby phone should not be allowed to make international calls without the use of a Forced Authorization Code (FAC).

Hotdial functionality on the Cisco IP Phone is the idea that a pattern can be dialed and then the end user clicks the Dial softkey. Cisco Type A phones (SCCP) send their SCCP signaling enbloc (all at once) when hotdial functionality is used, even though SCCP uses digit-by-digit pulsing by default. Analog gateway voice interfaces (Foreign Exchange Office [FXO], Foreign Exchange Station [FXS]) and T1-CAS voice interfaces send their digits digit by digit, but H.323, SIP, and ISDN send their digits in one Q.931 setup message (enbloc) by default. The method of forwarding digits is important to understand to determine how digit analysis will match on a route pattern when there is an overlapping dial plan. The Dialed Number Analyzer (DNA) tool is a great tool built into Cisco Unified Serviceability that will enable administrators of the system to analyze call-routing results without physically dialing the phone and diving into the technical complexities of reading a CUCM trace file.

I highly recommend using the Triple Combo GUI tool to analyze CUCM trace files that can be next to impossible to read in an application like Microsoft Word. Triple Combo is not officially supported by the Cisco Technical Assistance Center (TAC), but it is widely used in the Cisco Unified Communications community:

www.employees.org/~tiryaki/tc

Note Cisco SIP phones that support KPML use digit-by-digit dialing by default. KPML is not supported on older Cisco Type A SIP phones. Type A phones only support enbloc dialing when using SIP firmware.

If a user dialed 1211 in the call-routing database that's shown in Figure 9-5, CUCM would have two potentially matching patterns: 121X and 1[23]XX. Recall that there cannot be any potential matches that represent a longer number of digits that overlap with the digits of another pattern. Digit collection is stopped after receiving four digits in this scenario because there is no pattern that matches these first four digits. Closest-match routing logic is applied and route pattern 121X is chosen because there are only ten potential matches using the 121X route pattern. The route pattern 1[23]XX could have been selected as well, but this pattern represents 100 potential matches (all patterns beginning with 12).

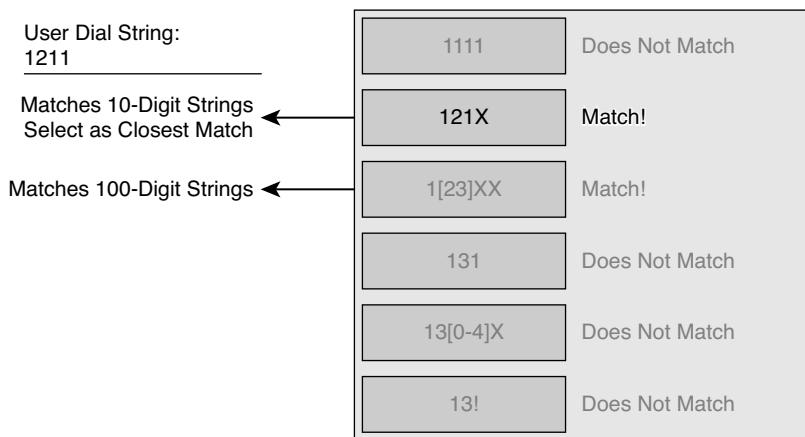


Figure 9-5 Closest-Match Routing Example

The next dial plan analysis scenario uses the example dial plan shown in Figure 9-6. CUCM received the dialed digits of 1311. After performing digit analysis, there are three potential matches based on the number of digits received at that point in time. The route patterns 13[0–4]X, 1[23]XX, and 13! all match the dialed digits, but CUCM waits for the T.302 interdigit timeout to expire before routing the call because of the 13! route pattern. Any route pattern including the exclamation point (!) represents variable-length dialing because the pattern can match any digit string starting with 13. The route pattern of 13[0–4]X is the closest match because there are only ten potential number combinations for a digit string of 1311 against the route pattern 13[0–4]X. The 1[23]XX route pattern has 100 potential matches, and 13! matches on a near infinite (up to 15 digits) number of potential numbers.

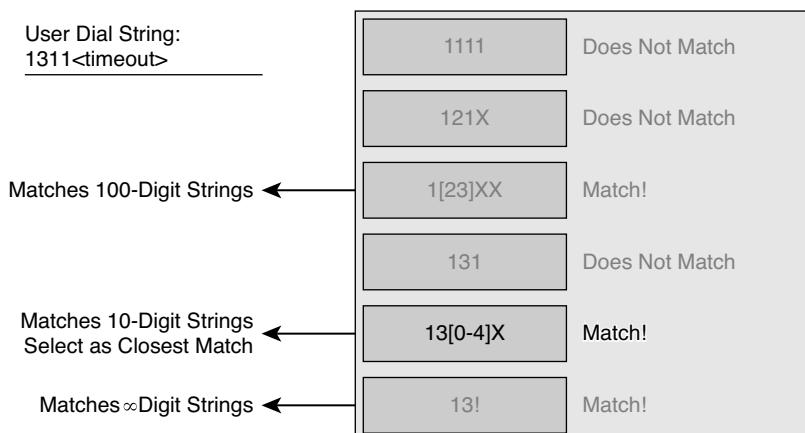


Figure 9-6 Interdigit Timeout

Using the dial plan shown in Figure 9-6, assume that only three digits were received by CUCM: 131. CUCM would match the same three route patterns as the previous example, but if no more digits were received, the T.302 interdigit timeout would expire and the route pattern of 13! would be matched.

Wildcards digits are useful to have in the call-routing database. Table 9-6 shows an example PSTN dial plan that could be used in North America with the NANP. All the route patterns begin with an access code of 9 because this is typically used in North American deployments. An 8 works even better as an access code, and I highly encourage its use in greenfield (new) installations. Many UC deployments are an upgrade or replacement of an existing solution, and the dial plan should be similar to that of the system that's being replaced. Each route pattern in Table 9-6 also has the Provide Outside Dial Tone check box selected (default) to ensure that secondary (stutter) dial tone is always played at the appropriate time (after the 9 is dialed). Every route pattern will also have a called party digit discard instruction (DDI) of Pre-Dot to strip out the access code before routing the call. The 911 does not have a dot, so the called party DDI will not apply to that pattern.

Table 9-6 NANP Dial Plan Example

Route Pattern	Description
911	Emergency call routing without access code
9.911	Emergency call routing with access code
9[2-8]11	Three-digit service codes (for example, 411 for information)
9[2-9]XX XXXX	Seven-digit local dialing
9[2-9]XX [2-9]XX XXXX	Ten-digit local dialing
9.1[2-9]XX [2-9]XX XXXX	11-digit long-distance dialing
9.011!	International dialing (variable length)
9.011!#	International dialing (variable length with interdigit timeout termination code [#])

The following list further explains these route patterns:

- **911 and 9.911 (emergency dialing):** The first two route patterns of 911 and 9.911 are both used for emergency call routing in North America. These route patterns are both configured with the Urgent Priority check box to avoid any delay in routing emergency calls if an overlapping dial plan is created in error. These are the only patterns in the table that have the Urgent Priority field set, but recall that translation patterns are all set to Urgent Priority (UP) by default. Translation patterns (TP) will be discussed in the next chapter.

- **9.[2–8]11 (three-digit service codes):** The three-digit route pattern (plus access code) is used for service codes in the NANP (for example, 411 for information and 511 for traffic information).
- **9.[2–9]XX XXXX (seven-digit dialing):** This seven-digit route pattern (plus access code) is used for local calling. Seven-digit dialing has been removed from the PSTN dial plan by the carriers in most metropolitan environments. New York City; Washington, DC; and other large metropolitan areas require ten-digit dialing even if the person you're calling lives across the street. Seven-digit dialing is not a requirement for some customers.
- **9.[2–9]XX [2–9]XX XXXX (ten-digit dialing):** This ten-digit route pattern (plus access code) is used to match on ten-digit dialing patterns. Most providers do not support ten-digit dialing to any area code, but not necessarily. The PSTN dial plans deployed are going to closely align with the service provider requirements for the geographical region and carrier selected. Ten-digit dialing is almost always supported in geographically local area codes. Within a 50-mile circumference of New York City, there must be close to a dozen area codes in use. Most providers support ten-digit dialing among these area codes. Because the PSTN requirements for ten-digit dialing in this scenario only support 12 local area codes, ten local area codes should be provisioned in the ten-digit dialing to meet the local dialing requirements. If a provider supports ten-digit dialing to any area code in the NANP, the exact ten-digit pattern from Table 9-6 could be used. The generic ten-digit pattern would cause an overlapping dial plan with seven-digit dialing if both were deployed. If a user dials a seven-digit pattern, CUCM cannot route the call for 15 seconds because of the overlap between seven- and ten-digit dialing. CUCM will wait for more digits or until the T.302 interdigit timeout expires. Removing seven-digit dialing is an easy way to remove the overlapping dial plan, but you might find yourself in a situation where a PSTN provider supports seven-digit and ten-digit dialing to any area code (usually not the norm).
- **9.1[2–9]XX [2–9]XX XXXX (11-digit long-distance dialing):** This route pattern will be required in almost every North American deployment. Some AT&T dedicated long-distance (LD) circuits only support ten digits for the called party. To a carrier ten-digit forwarding requirement, we can move the placement of the dot after the 1 so that the digit discard instructions (DDI) strip out the 9 and 1, resulting in a ten-digit pattern forwarded to the carrier. The pattern would be 91.[2–9]XX[2–9]XXXXXX. Notice that the dot placement has been moved from before the 1 to after the 1 to ensure that the 1 digit gets stripped out before the call is routed to the carrier.
- **9.011! and 9.011!# (international dialing):** International dialing from North America requires the international dialing code of 011. International dialing requires a country code next in the dial string. The country code is sometimes referred to as a two-digit code, but international country codes can be three or four digits long, depending on the country being dialed. Because each country has one or more independent dial plans, detailed knowledge of the destination country dial plan is required to configure robust international dial plans. If the deployment has a requirement of international

dialing only to the United Kingdom, I would configure these two patterns instead of the previous two: 9.01144! and 9.01144!#. The two patterns with the U.K.'s country code of 44 would guarantee that no one international country could be dialed.

Digit Forwarding

Table 9-7 summarizes the digit-forwarding methods supported in CUCM for different endpoint devices.

Table 9-7 *Digit-Forwarding Behavior*

	Signaling Protocol	Addressing Method
IP phone	SCCP SIP	Digit-by-digit Enbloc KPML (default on newer phones) SIP dial rules
Gateway	MGCP/SIP/H.323	Enbloc (default) Overlap sending and receiving (ISDN PRI only)
Trunk	H.323/SIP	Enbloc (default) Overlap sending and receiving (ISDN PRI only)

Most SIP devices support enbloc dialing, but enbloc dialing from SIP devices changes the end user experience. End users on older Cisco Type A phones will not hear dial tone by default on a device converted to SIP. Enbloc dialing sends the entire dialed string in one single SIP INVITE message. This is the way digits are always sent and received on SIP trunks, H.323 gateways, and SIP Type A phones (default).

KPML is an IETF standard that supports sending digits as they're dialed (digit by digit) to be sent one by one. All Cisco Type B (79x1, 79x2, 79x5, 7970, 7906) and newer Cisco IP Phones support KPML, and it's turned on by default. KPML enables the same end user experience that the end user had with a traditional PBX system when a Cisco phone is converted to use a SIP firmware image.

SIP dial rules offer another option that can be used on all Cisco SIP devices. SIP dial rules are downloaded to the phone at the time of registration. The local dial rules allow CoS rejections to be done at the handset level. SIP dial rules reduce the amount of network traffic sent back and forth between the Cisco IP Phone and CUCM because dialed digits are processed locally against the SIP dial rules and then sent to CUCM enbloc (all at once). SIP dial rules are advantageous when the Cisco IP Phone endpoints are geographically separated from CUCM or there is a lack of bandwidth between a branch site in a centralized call-processing architecture.

CUCM trunks and ISDN PRIs send their digits en bloc by default, but they can both be configured for overlap sending and receiving. Overlap sending and receiving allows digits to be sent or received one by one in multiple setup messages. Overlap sending is not normally required for an NANP deployment but might be required in countries like Germany and Sweden, where the carrier equipment only supports overlap sending and receiving with digit-by-digit analysis.

SCCP Phones: User Input

Cisco IP Phones using SCCP (TCP port 2000) report every user input event to CUCM immediately. As soon as the user goes off-hook, a signaling message is sent from the phone to the CUCM server with which it is registered, as illustrated in Figure 9-7. The phone is the client device, and CUCM is the server.

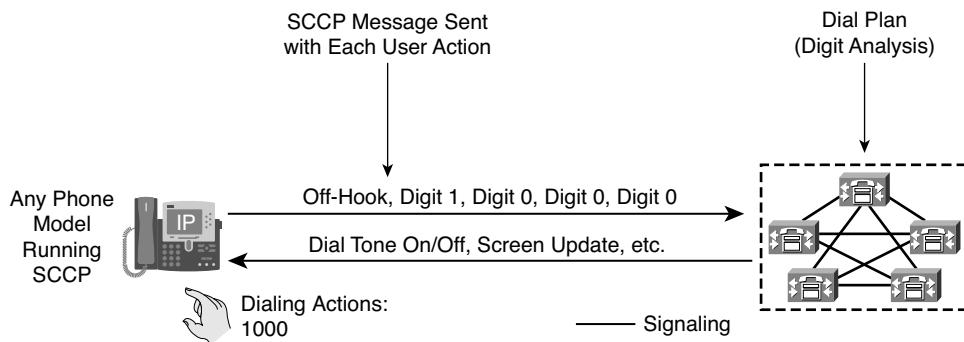


Figure 9-7 SCCP Phones: User Input

A user goes off-hook and then dials extension 1000. Each event is reported to CUCM in real time. All the call progress feedback provided by CUCM to the end user on the Cisco IP Phone (screen display messages showing calling or called party, dial tone, secondary dial tone, ringback, reorder tone, and so on) is initiated by an SCCP message sent from CUCM to the Cisco IP Phone. Skinny Client Control Protocol (SCCP) is a stimulus/response protocol where the endpoint sends user input (stimulus) and expects some type of response from the server instructing the endpoint about what to do.

It is not possible to configure dial plan information (dial rules) on Cisco IP Phones using SCCP. All dial plan functionality is contained in the CUCM cluster with an SCCP phone.

A user dialing an international pattern that is denied by the end user's CoS deployed in CUCM will result in a reorder tone (busy signal) that is played to the calling party letting the party know that the call could not be completed as dialed. If calls to the 976 area code are denied based on the calling party's configured CoS, a reorder tone is sent to the calling party phone as soon as the user dials 91976.

Cisco SIP IP Phones: User Input

Type A phones (Cisco Unified IP Phone Models 7905, 7912, 7940, and 7960) do not support KPML. Type A phones support SIP dial rules, which are configured in CUCM and downloaded to the IP phone at boot time. SIP dial rules will enable dial tone and traditional phone functionality on CUCM. Type A phones converted to SIP will lose a number of telephony features based on the limited amount of DRAM on the older Type A phones and the additional memory requirements of the SIP protocol stack.

Type B (and newer-model phones) support KPML and SIP dial rules. KPML is turned on by default on all Type B phones (Cisco IP Phone Models 79x1, 79x2, 79x5, 7970, and 7960). The 8000 and 9000 phones have not been called Type C phones at press time, but these phones definitely represent newer hardware architectures. It's fairly safe to assume that any feature supported on the Type B phones is also supported on the newer 8000 and 9000 Series Cisco IP Phones.

Type A SIP Phones: No Dial Rules

Type A Cisco IP Phones using SIP firmware without SIP dial rules (default) do not deliver a dial tone to the calling party when the calling party goes off-hook with the handset, speakerphone, or headset. All digits are sent to CUCM en bloc after the user completes dialing and presses the Dial softkey. This function is similar to the Send button used on cellular phones.

Figure 9-8 illustrates a user making a call to extension 1000. The user dials 1000 followed by pressing the Dial softkey. The Cisco IP Phone sends a SIP INVITE message to CUCM with all dialed digits (en bloc). CUCM performs digit analysis and provides a call progress message to the Cisco IP Phone.

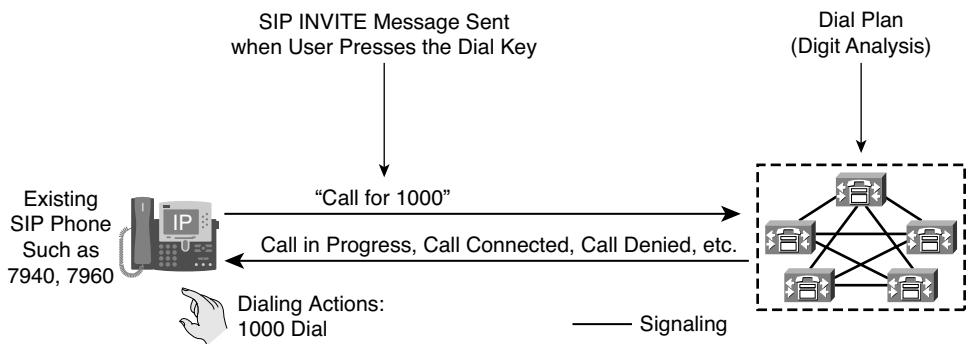


Figure 9-8 SIP Type A Phones: No Dial Rules

Cisco Type A SIP IP Phones: Dial Rules

SIP dial rules allow SIP phones to emulate the functionality of an SCCP phone (dial tone and digit-by-digit pattern analysis). When SIP dial rules are leveraged, a user receives dial tone when going off-hook. This functionality is different than the default functionality on

Cisco Type A phones converted to SIP, where there are no local dial rules. Dialed digits are processed against the local SIP dial rule in real time. If a user dials a phone number that is rejected by the local SIP dial rules (for example, pay dialing beginning with 9 1-900), the call is quietly dropped without being forwarded to CUCM. Users might be accustomed to hearing a reorder tone when a call cannot be routed. SIP dial rule pattern rejection does not result in a reorder tone. SIP dial rules can help minimize overhead bandwidth consumption and CUCM processor overhead. SCCP is a chatty protocol that uses many small SCCP signaling messages between the Cisco IP Phone and CUCM. The constant nature of SCCP messages can result in postdial delay when a Cisco IP Phone and CUCM are separated by large geographical boundaries. SCCP (less than 500 bps) and SIP (approximately 500 bps) communication uses up a very small amount of bandwidth (under 500 bps per call) across WAN circuits, but the overhead can be minimized by using SIP dial rules. SIP dial rules eliminate the need to send constant signaling across the network between the Cisco IP Phone and CUCM.

A SIP INVITE message with enbloc signaling is sent from the Cisco SIP IP Phone to CUCM when the SIP dial rule of the Cisco IP Phone recognizes and permits the dialed pattern. End users do not need to press the Dial key like they had to on Cisco SIP Type A phones. SIP dial rules allow Type A phones to emulate SCCP and traditional phone systems, while also providing processing and signaling overhead benefits.

Figure 9-9 illustrates a phone configured to recognize all four-digit patterns beginning with a leading digit of 1. This pattern has an associated timeout value of 0. All user input actions matching the pattern will trigger the sending of the SIP INVITE message to CUCM immediately, without requiring the user to press the Dial key.

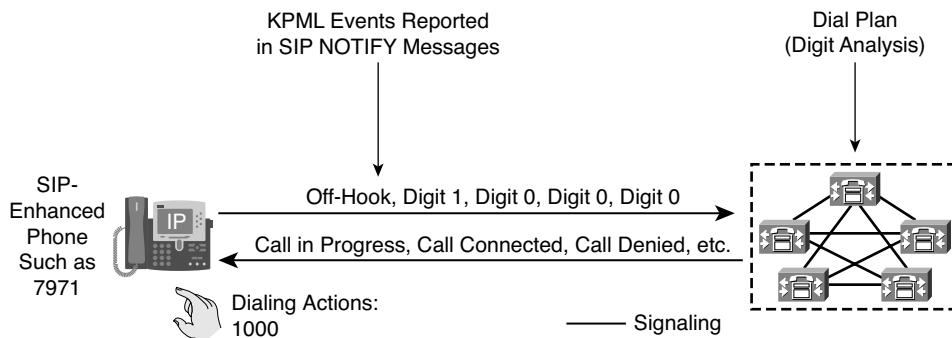


Figure 9-9 SIP Type A Phones: Dial Rules

Cisco Type B SIP Phones: No Dial Rules

Cisco Type B SIP IP Phones offer functionality based on the KPMI standard to report user activities. Each user input event (dialed digit or softkey/button) generates a KPMI message to CUCM. This mode of operation emulates a similar end-user experience to that of phones using SCCP.

Every key the end user presses triggers an individual SIP message. The first event is communicated with a SIP INVITE, but subsequent messages use SIP NOTIFY messages. The SIP NOTIFY messages send KPML events corresponding to any buttons or softkeys pressed by the user. Cisco Type B SIP IP Phones with SIP dial rules operate in the same manner as Cisco Type A phones with dial peers. Figure 9-10 illustrates the enbloc signaling used with SIP dial rules.

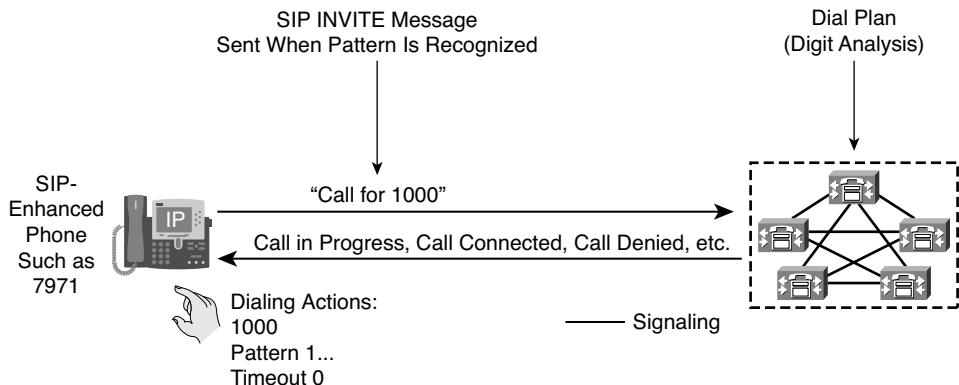


Figure 9-10 SIP Type B Phones: SIP Dial Rule

Special Call-Routing Features

The @ wildcard is a special macro function that expands into 166 individual route patterns in the CUCM call-routing database. This @ symbol is easy to configure but causes a lot of processor overhead on the CUCM server because of the large dial plan/call-routing database it sets up.

CUCM can be configured to accept other national numbering plans, but the NANP dial plan adds 166 route patterns. The @ wildcard can then be used for different numbering plans, even within the same CUCM cluster if an international dial plan has been installed on CUCM. The Numbering Plan field on the Route Pattern configuration page would need to be set appropriately to interact with international dial plans.

Route Filters

Route filters can be used only with the @ route pattern to match certain elements or special numbers of a numbering plan. A route filter that is applied to a pattern that does not contain the @ wildcard is ignored. Even if the deployment is not looking to use the @ route pattern, the @ route pattern can be leveraged by attaching a route filter to the route pattern. This configuration allows certain area codes that carry premiums to be removed from the call-routing database while preserving the ability to make calls to any other area code. The logical expression that is entered with the route filter can include up to 12 clauses and include as many as 1024 characters (excluding the NOT-SELECTED fields).

Tags serve as the core component of a route filter. A tag applies a name to a subset of the dialed-digit string. For example, the NANP number 972 555-1234 comprises the LOCALAREA-CODE (972), OFFICE-CODE (555), and SUBSCRIBER (1234) route filter tags. Calls can be denied based on any of the previous criteria in the dialed digits. Table 9-8 includes all the different route filters. I try to keep my route filters simple by matching on items such as Area-Code == 900 and Area-Code == 976.

Table 9-8 NANP Route Filter Tags

Tag	Description
AREA-CODE	This three-digit area code in the form of [2–9]XX identifies the area code for long-distance calls. Area codes are also referred to as numbering plan area (NPA).
COUNTRY-CODE	Country codes are variable in length, but most Western European-block countries have two-digit country codes. A country code specifies the destination country for international calls.
END-OF-DIALING	This single character identifies the end of the dialed-digit string. The # character serves as the end-of-dialing signal for international numbers that are dialed within the NANP.
INTERNATIONAL-ACCESS	This two-digit access code specifies international dialing. Calls that originate in the United States use 01 for this code.
INTERNATIONAL-DIRECT-DIAL	This one-digit code identifies a direct-dialed international call. Calls that originate in the United States use 1 for this code.
INTERNATIONAL-OPERATOR	This one-digit code identifies an operator-assisted international call. This code specifies 0 for calls that originate in the United States.
LOCAL-AREA-CODE	This three-digit local area code in the form of [2–9]XX identifies the local area code for ten-digit local calls.
LOCAL-DIRECT-DIAL	This one-digit code identifies a direct-dialed local call. NANP calls use 1 for this code.
LOCAL-OPERATOR	This one-digit code identifies an operator-assisted local call. NANP calls use 0 for this code.
LONG-DISTANCE-DIRECT-DIAL	This one-digit code identifies a direct-dialed, long-distance call. NANP calls use 1 for this code.
LONG-DISTANCE-OPERATOR	These one- or two-digit codes identify an operator-assisted, long-distance call within the NANP. Operator-assisted calls use 0 for this code, and operator access uses 00.
NATIONAL-NUMBER	This tag specifies the nation-specific part of the digit string for an international call.

Table 9-8 NANP Route Filter Tags

Tag	Description
OFFICE-CODE	This tag designates the first three digits of a seven-digit directory number in the form of [2-9]XX.
SATELLITE-SERVICE	This one-digit code provides access to satellite connections for international calls.
SERVICE	This three-digit code designates services such as 911 for emergency, 611 for repair, and 411 for information.
SUBSCRIBER	This tag specifies the last four digits of a seven-digit directory number in the form of XXXX.
TRANSIT-NETWORK	This four-digit value identifies a long-distance carrier. Do not include the leading 101 carrier access code prefix in the TRANSIT-NETWORK value. Refer to TRANSIT-NETWORK-ESCAPE for more information.
TRANSIT-NETWORK-ESCAPE	This three-digit value precedes the long-distance carrier identifier. The value for this field specifies 101. Do not include the four-digit carrier identification code in the TRANSIT-NETWORK-ESCAPE value. Refer to TRANSIT-NETWORK for more information.

In my boilerplate CUCM deployments, I use two 9.@ route filters to block the following 20 area codes that carry toll premiums, where each clause in the route filter AREA-CODE == 900. Table 9-9 provides an illustration of 20 area codes you might want to consider removing from your dial plan (or strongly control with a CoS deployment).

Table 9-9 Area Codes Frequently Blocked in North American Deployments

Country	Area Code
Anguilla	264
Antigua/Barbuda	268
Bahamas	242
Barbados	246
Bermuda	441
British Virgin Islands	284
Cayman Islands	345
Dominica	767

Table 9-9 Area Codes Frequently Blocked in North American Deployments

Country	Area Code
Dominican Republic	809
Grenada	473
Jamaica	876
Montserrat	664
Puerto Rico	787
St. Kitts & Nevis	869
St. Lucia	758
St. Vincent & the Grenadines	784
Toll Charge	900 976
Trinidad & Tobago	868
Turks & Caicos	649
U.S. Virgin Islands	340

Route patterns and translation patterns can also be configured to block individual route patterns, but I have found it easier to configure a couple of route filters and attach them to generic 9.@ route patterns for the exclusive purpose of removing patterns from the dial plan. Patterns that are associated with a block action must be provided with a cause code that is written to the call detail record (CDR) as part of the call teardown.

The ! Wildcard

International destinations are usually configured by using the ! wildcard, which represents up to 15 digits. The route pattern of 9.011! is typically configured for international calls in North American locations. In Germany, an access code of a 0 is typically used, and the international code is 00.

The ! wildcard is also used for deployments in countries in which dialed digits can be of varying lengths. CUCM does not know when the end user is done dialing and will wait for 15 seconds by default before sending the call. This delay can be reduced in one of the following ways:

- Reduce the T.302 timer (CallManager service parameter) to indicate the end of dialing. It is not recommended to set this timer to less than 5 seconds. Values lower than 5 seconds can result in end users becoming frustrated. Calls could be attempted before the end users are done dialing if 5 seconds have elapsed since the last keypress.
- Configure a second route pattern that ends with the # wildcard (9.011!# for North America or 0.00!# for Europe). Train end users to dial # to indicate the fact that they are done dialing. This action is analogous to pressing the Send button on a cell phone.

The support of the pound/octothorpe as the interdigit timeout termination pattern is supported differently in Cisco IOS dial peers. Route patterns in CUCM must be explicitly configured to support the #, while the Cisco router using H.323 or SIP implicitly knows that the # (pound) should terminate the interdigit timeout. MGCP gateways follow the same rules as CUCM processing because the MGCP endpoints (TDM interfaces) on the router are explicitly controlled by CUCM on MGCP gateways.

Call Classification

Route patterns can be classified as On-Net or Off-Net. The configuration at the route pattern is used for outgoing calls, whereas there is a global setting for gateway and trunk devices used for incoming calls.

All route patterns have the Provide Outside Dial Tone check box selected by default, resulting in an Off-Net call classification. The Allow Device Override parameter can be turned on as well to change the classification method for outgoing calls when the primary path is not available and the call is to be routed out. When this parameter is activated, the classification of the outgoing device, rather than the route pattern classification, is used for a call. This parameter is useful when the route pattern refers to a route list that has multiple options for path selection. Assume that the first path is an intercluster trunk, which should be considered an On-Net call, but the second path using a PSTN gateway is leveraged for the call. The call would be classified as an On-Net call over the trunk and an Off-Net call when the call is routed over the gateway (if the Device Override option is selected).

The following features leverage the call classification:

- **Call forward settings:** Call forward can be configured differently for internal (On-Net) and external (Off-Net) calls. External calls are normally calls that were routed from a gateway.
- **Block Off-Net to Off-Net transfers:** This CallManager service parameter toll-fraud prevention feature ensures that the UC infrastructure is not misused by an internal facilitator to connect two external parties.

- **Drop conference when no On-Net party remains:** This toll-fraud prevention feature drops a conference call when only external parties remain in the conference. If the setting is not enabled, an internal facilitator can try to connect two external parties by setting up a conference and then drop out of the call. The entire call would be billed to the company on the CUCM cluster because the conference was initiated by a Cisco IP Phone on the cluster. This service parameter would stop this toll-fraud scenario.

Secondary Dial Tone

The secondary dial tone typically indicates a call to the PSTN after the country-specific access code has been dialed.

The secondary dial tone function can be enabled on route patterns and translation patterns. The dial tone will change only if all possibly matching route or translation patterns have the secondary dial tone enabled.

Consider this example:

Route pattern: 9.@ (secondary dial tone enabled)

Route pattern: 9.[2-9]XXXXXX (secondary dial tone enabled)

After a user dials 9, the dial tone will immediately change because both matching route patterns have the secondary dial tone enabled. Or, consider another example:

Route pattern: 9.@ (secondary dial tone enabled)

Route pattern: 9.[2-9]XXXXXX (secondary dial tone disabled)

After a user dials 9, the dial tone does not change because only one matching route pattern has the secondary dial tone enabled. If the user dials a 1 after the 9, the stutter dial tone will be heard because only the route pattern that has the secondary dial tone enabled remains as a possible match.

The secondary dial tone is configured by selecting the Provide Outside Dial Tone check box on the Route Pattern or Translation Pattern configuration page.

CUCM Path Selection

Path selection is an essential dial plan element. CUCM selects how and where to route the call after it has matched a pattern in the call-routing database. External calls are normally routed across IP trunks or gateways. CUCM allows multiple paths to be configured for a route pattern for high-availability purposes. Figure 9-11 displays the high-level concept of path selection. In the figure, a 408 area code is matched in the 11-digit pattern and the call is routed across the H.225 trunk pointed to the gatekeeper as the primary path. If the WAN is down (or the H.323 gatekeeper's call admission control [CAC] rejects the call), the backup path over the gateway router is used.

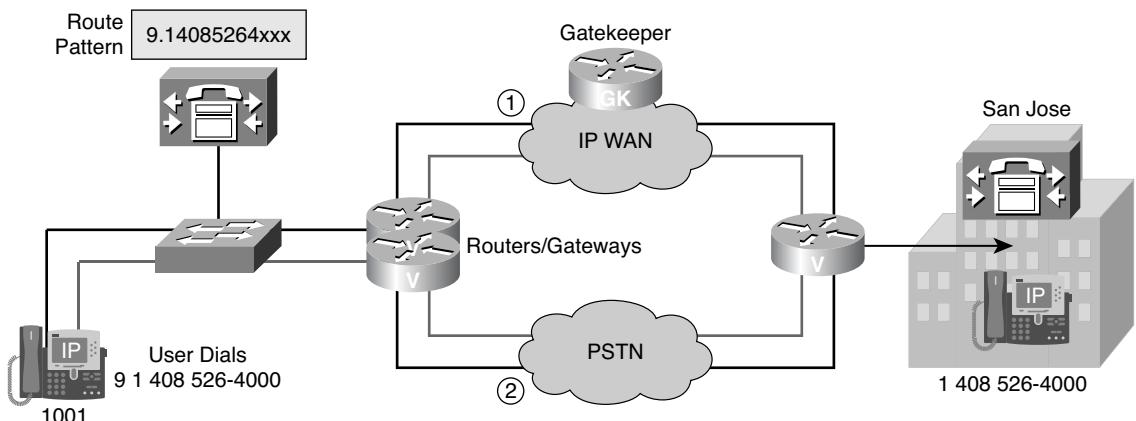


Figure 9-11 CUCM Call-Processing Logic

Path Selection Elements

Route patterns are strings of digits and wildcards configured in CUCM. Route patterns can point directly to a trunk or gateway device, but the device would not be available for any other route patterns. Most CUCM administrators never point route patterns directly to gateways or trunks. Gateways are instead put into a logical grouping called route groups that one or more route lists can leverage. Route lists are logical groupings of route groups. Route lists always use top-down processing of route groups to perform call routing. Call routing within a route group is controlled by one of the two call distribution algorithms: top-down or circular. The route list and route group elements provide the greatest level of flexibility for call routing and digit manipulation. Gateways, route groups, route lists, and route patterns are normally built from the bottom up, but the processing order is top down.

Path Selection Configuration

To configure call routing, follow these steps:

- Step 1.** Add and configure the gateway and trunk devices (covered in Chapter 8, “Implementing PSTN Gateways in Cisco Unified Communications Manager”).
- Step 2.** Create route groups (RG) and add required devices to the route groups.
- Step 3.** Create route lists (RL) and add available route groups in the proper order.
- Step 4.** Create route patterns (RP) and point the route patterns to route lists.

Route Group

A route group is a list of devices (gateways and trunks). It is recommended to put similar devices (gateways or trunks) that have a similar purpose into the same route group. Digit manipulation in this model happens on the Route List configuration page, under the Route List Details for the selected route group in the route list. The gateways must have identical digit-manipulation requirements.

Note A route group can be configured for circular distribution (round robin) or for top-down distribution (first entry in the list has the highest priority). The circular distribution is used for load-sharing scenarios; the top-down distribution is used to implement backup paths if the preferred path is unavailable.

Figure 9-12 displays the call-routing logic of CUCM. Notice that there are two gateway resources to the PSTN in the second-choice route group (PSTN_RG). The route group can be configured with the top-down distribution algorithm to use the resources of gateway 1 first and then the resources of gateway 2. If each gateway were connected to a different carrier circuit with different digit-manipulation requirements, two route groups would be required. Because both circuits have the same requirements, one route group will suffice for our example. This configuration would prove useful in a scenario where gateways 1 and 2 are pointed to different service providers with different negotiated rates. Gateway 1 would be connected to the cheaper carrier. Circular routing is a good solution that allows load-sharing calls across both gateways. Circular is a good option when the rates are the same regardless of which carrier circuit is used.

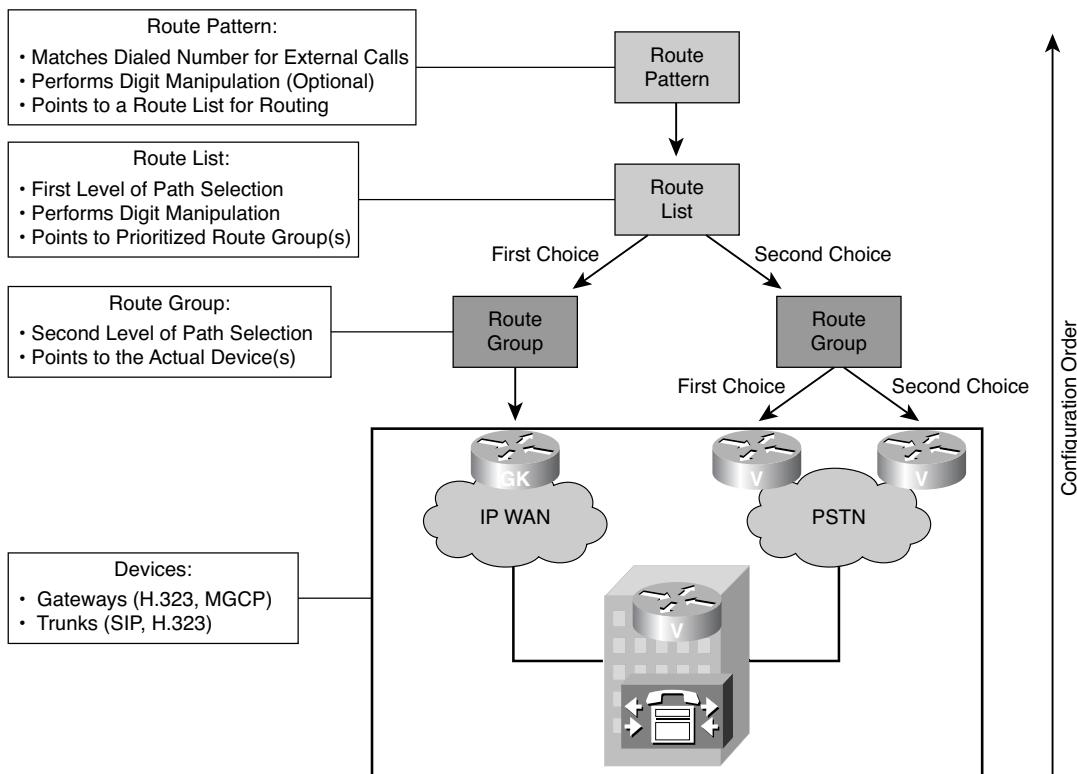


Figure 9-12 Route Groups

Figure 9-13 shows a screen capture of the Route Group Configuration page in CUCM Administration. Choose Call Routing > Route/Hunt > Route Group. Click Add New. The route group should be given a descriptive name. If all the resources in the route group will be used to access the PSTN and there is only one PSTN route group in the CUCM cluster, a name of PSTN_RG might be descriptive enough. Best practice is to use a naming nomenclature that includes the configuration item's functionality. The PSTN_RG route group name ends with _RG to signify that the configuration item is a route group. In a large, centralized call-processing architecture, you might want to include the location of the gateways in the route group naming, but this might not be required. Choose the distribution algorithm of Top-Down or Circular from the Distribution Algorithm drop-down menu. Select the gateway or trunk resource that you want to add to the route group from the Available Devices section of the page and click the Add to Route Group button. Click Save.

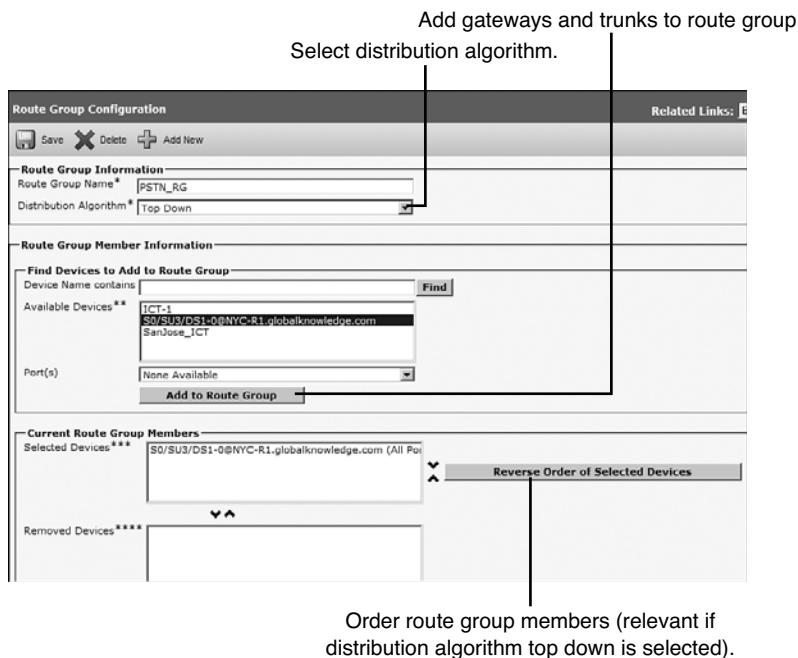


Figure 9-13 Route Group Configuration

Local Route Group

Local route groups decouple the selection of a PSTN gateway or trunk for Off-Net dialing from the route patterns that are used to access the gateway. This action can greatly reduce the complexity and size of dial plans in CUCM.

The Local Route Group Device Pool parameter was a new call-routing element introduced with CUCM 7.0. The standard local route group is a new call-routing element that always appears in the list of available route groups that can be added to a route list. A route list can only include this entry one time. The local route group is selected by the calling device's device pool Local Route Group setting.

The Local Route Group parameter is set to <None> by default.

Route patterns that use the local route group are routed to the gateways that are associated with the local route group configured at the device pool level of the calling device. The local route group call-routing option decouples the dial plan from the site. Each site will use one global dial plan that points to a local route group. The local route group is a dynamic call-routing configuration element based on the device pool configuration of the calling device. The device pool specifies a local gateway router at the site, and the call is routed to a local gateway. Each site in a centralized call-processing deployment normally had a local PSTN dial plan requirement per site before the local route group configuration element. Calls using static route groups will always route the call to the same gateway, regardless of the device that originated the call.

The route pattern 9.555XXXX in Figure 9-14 points to a route list that contains only the standard local route group. Gateway A is associated with Route Group A, which is the local route group of Device Pool A. Gateway B is associated with Route Group B, which acts as the local route group to Device Pool B. The gateways can be on opposite sides of the country. Gateway A could be the New York gateway, while Gateway B is the San Jose, CA, gateway. It's always best to use a local gateway if one is available. If a phone that is associated with Device Pool A places a call to 95550815, the standard local route group for this device pool will be used to place the call to the PSTN from Gateway A. Phones in Device Pool B will have their calls routed to Gateway B because of the device pool B's configured local route group.

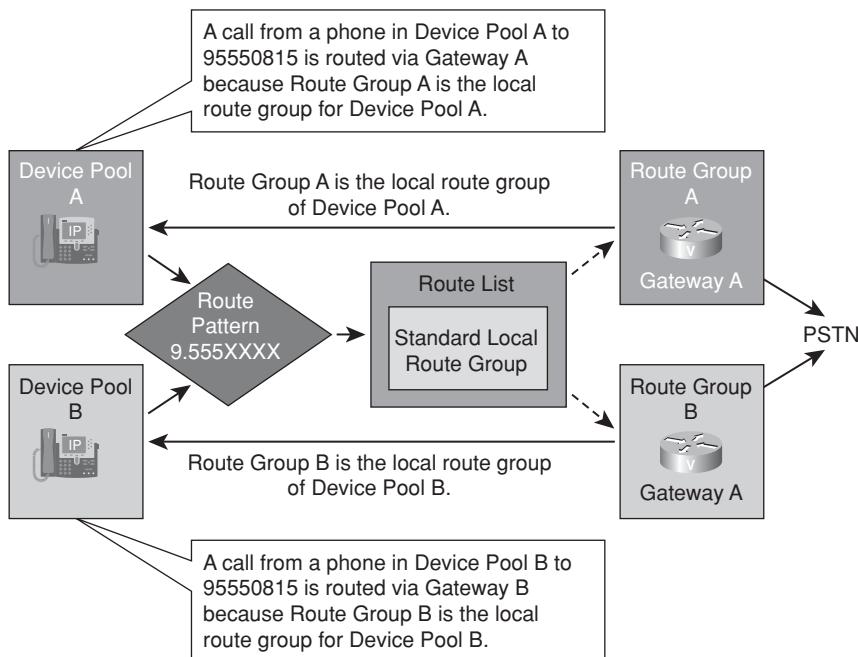


Figure 9-14 Local Route Group Functionality

Route List

A route list is a list of prioritized route groups. Route groups are always processed in a top-down prioritization order. Digit manipulation can be set up per route group within the route list by clicking the Route List Details link toward the bottom of the Route List Configuration page. Figure 9-15 is an example of call routing where the first route group

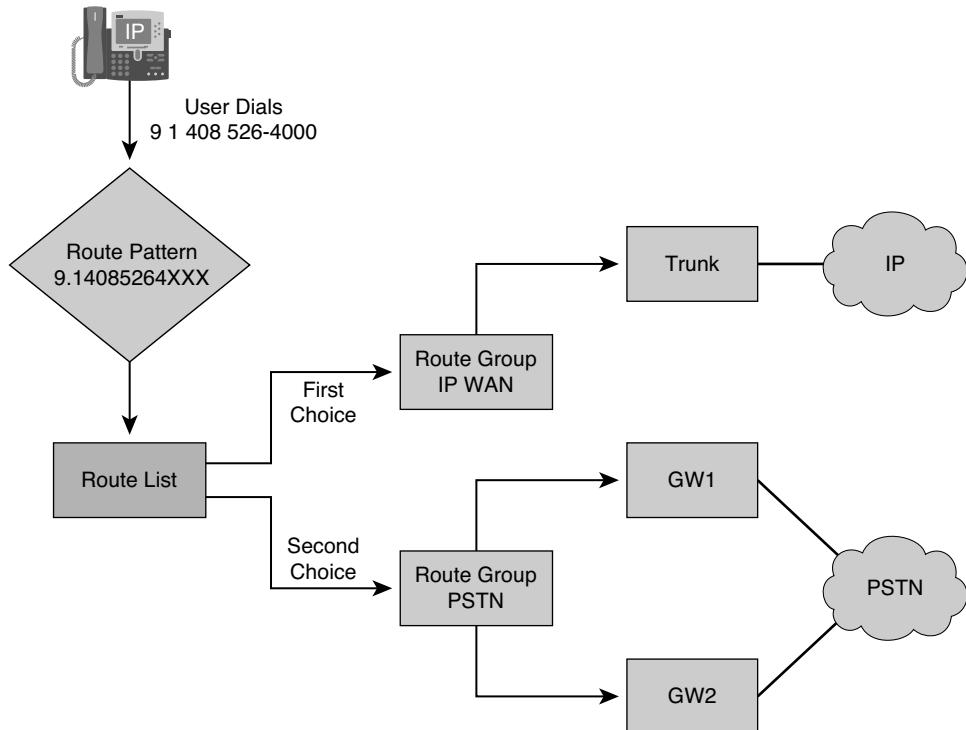


Figure 9-15 Route Lists

is the IP WAN route group, which is routing calls to a different CUCM cluster over a trunk (H.225, SIP, nongatekeeper-controlled intercluster trunk or gatekeeper-controlled intercluster trunk). Gatekeeper-controlled intercluster trunks exist for backward compatibility because they were replaced by H.225 trunks in CallManager 3.2. H.225 trunks can direct calls to an H.323 gateway or an H.323 gatekeeper, whereas gatekeeper-controlled intercluster trunks only supported gatekeepers.

CUCM trunks are used to route calls to IP destinations, where traditional PBXs have traditionally used trunk cards to route calls to a time-division multiplexing (TDM) circuit. If five-digit dialing is used internally and between sites, no digit manipulation is needed at the IP WAN route group level for this call. Intersite call routing can require digit manipulation to strip a site code from the call routing. Calls rerouted over the PSTN gateway require digit manipulation to comply with the public PSTN dial plan. Digit manipulation can occur at the route pattern, route list, or translation pattern level. If a route pattern is

pointed to a route list and digit manipulation is attempted at the route pattern level, the digit manipulation will be ignored. Digit manipulation can only occur at the route pattern level if the route pattern is pointed directly to a gateway or trunk (not a route list). Most digit manipulation of outbound calls occurs at the route list detail level. Route list detail is provided at the route list level for each individual route group. This allows calling and called party information to be presented differently depending on the call-routing target.

Figure 9-15 displays a route list configuration in which the 9.14085264XXX range of phone numbers are being routed across a trunk utilizing the IP WAN as a first priority. If the WAN link is down or the H.323 gatekeeper rejects the call, the call will be rerouted over the PSTN route group. The PSTN route group has a prioritized list of two gateways it can use, providing gateway redundancy. Call-routing distribution algorithms of top-down and circular call routing can be configured at the route group level. Use good naming nomenclature when configuring route lists that identify the functionality of the route list. If the route list is being used to route intersite calls between New York and San Jose over the IP WAN, a name of SanJose_RL would work well.

Two route groups have been added to the route list example shown in Figure 9-16. The WAN route group is listed first and has highest priority. If calls cannot be set up by using any trunk devices in the WAN route group, the next route group in the list (PSTN) is used to route the call. Cisco Unified Communications Manager tries all devices in that route group, according to the route group distribution algorithm (circular or top-down). If a route list is disabled, the route list configuration remains in the database, but it is not used.

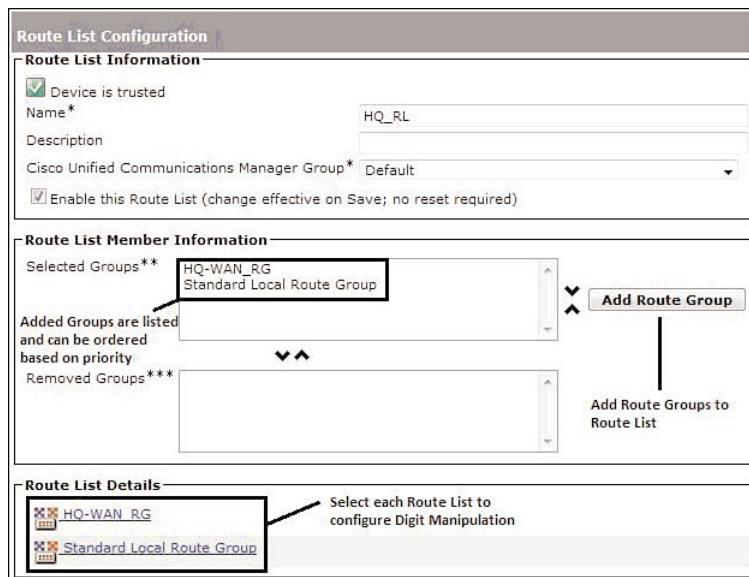


Figure 9-16 Route List Configuration

Notice the links to the route list details at the bottom of the Route List Configuration page. Route list details are configured on an individual route group basis. Figure 9-17 illustrates two sites of an enterprise (San Jose and Philadelphia) in which each phone has a five-digit extension and a corresponding ten-digit PSTN DID phone number. CUCM has replaced an existing system in which users dialed seven digits for all intersite calling. The dial plan is capable of using five-digit dialing to call between the locations, but five-digit intersite dialing would limit the scalability of the dial plan. The solution will use seven digits and a two-digit site code. The site code limits the number of sites that can be used in this deployment, but seven-digit intersite dialing might be easier for the end users (in North America) to understand because they might have been using local seven-digit PSTN dialing for most of their life. This assumption might not be true in metropolitan areas, where local dialing has required ten digits for some time.

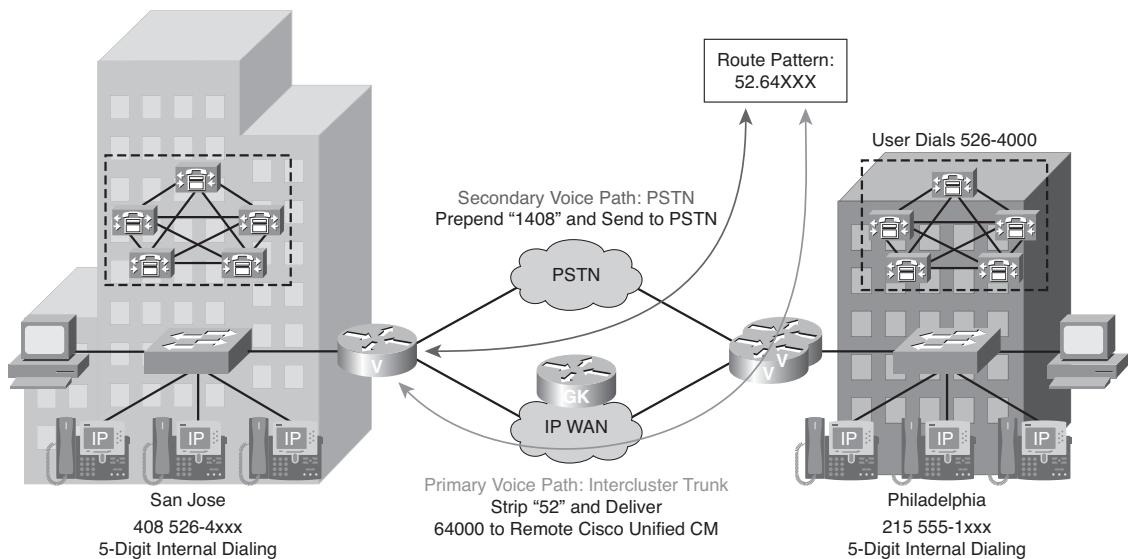


Figure 9-17 *Intercluster Call Routing Example*

A route pattern of 52.64XXX is configured in the Philadelphia CUCM cluster for intersite calls from Philadelphia to San Jose. The route pattern points to a route list with two route groups. The primary route group includes a trunk, and the secondary route group includes one or more PSTN gateways. The following digit-manipulation requirements apply for a call placed from Philadelphia to 526-4000:

- **Calls routed over the intercluster trunk:** The first two digits (52) of the called number (526-4000) represent the site code used for intersite call routing. The site code must be stripped out of the dialed digits so that the CUCM cluster in San Jose evaluates the five-digit number and properly routes the call to the directory number 64000. The calling party number must also be changed from a five-digit extension to a seven-digit intersite route pattern (prefix 55 to calling party number). This will

allow proper caller ID presentation so that the called party can use the missed and received call history list on the Cisco IP Phone to place calls. The placement of the dot (.) delimiter is critical in Figure 9-17. The called party digit discard instruction (DDI) rule will be configured as pre-dot to remove the 52 from the dialed number. The result will forward only the dialed digits 64000 to San Jose for digit analysis.

- **Calls routed over the PSTN:** The called number routed to the PSTN carrier must adhere to local PSTN standards for that particular carrier. The carrier used in Figure 9-17 requires 11-digit long-distance numbers to any nonlocal area codes. Figure 9-17 conforms to this requirement by prefixing 1408 to the dialed seven-digit number. The called party DDI will be set to the default of None for calls routed over the PSTN. This is only possible because the site codes used for intersite call routing have been designed to conform to the NXX exchange number (the leading three digits of the last seven digits). The resulting called party is an 11-digit long-distance number of 1 408 526-4000. Calling party digit manipulation can be configured with the “Use Phone’s External Phone Number Mask” to manipulate the five-digit internal caller ID to a ten-digit caller ID that can be dialed back from a phone on the PSTN.

Inbound call routing on both gateways (San Jose and Philadelphia) can be configured with an inbound call-routing significant digits value set to 5. This setting causes CUCM to only analyze the last five digits of the called party information provided by the carrier. Most providers will customize the number of dialed digits forwarded from the PSTN to the company’s dial plan requirements, but it’s a best practice to receive all the digits from the carrier so that the enterprise can provide intelligent rerouting of calls in larger deployments. More information about digit-manipulation configuration is provided in the next chapter.

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- A dial plan consists of different elements and functions, such as endpoint addressing, path selection, digit manipulation, and so on. It is the core of the call-processing logic used in Cisco Unified Communications Manager.
- A uniform On-Net dial plan provides unique endpoint addressing by fixed-length directory numbers.
- Call routing is when Cisco Unified Communications Manager processes incoming call requests by looking up the dialed number in its call-routing table.
- Cisco Unified Communications Manager can receive dialed digits one by one or enbloc.
- Cisco Unified Communications Manager allows multiple, prioritized paths to be selected for a given route pattern.

- Route lists, route groups, and devices are configured to implement path selection.
- Cisco Unified Communications Manager configuration includes special call-routing features, such as numbering plans and route filters, a wildcard for variable-length numbers, blocked patterns, patterns with urgent priority, and classification of calls.

References

For additional information, refer to these resources:

Cisco Systems, Inc. Cisco Unified Communications System Release 8.x SRND, at www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8xsrnd.pdf.

Cisco Systems, Inc. Cisco Unified Communications Manager Administration Guide, at www.cisco.com/en/US/docs/voice_ip_comm/cucm/drs/8_0_1/drsag801.html.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. Which of the following is not a dialing method?
 - a. PSTN
 - b. On-Net
 - c. Off-Net
 - d. Abbreviated
2. What dial plan element is used to match the dialed digits for call routing to another cluster or the PSTN?
 - a. Route pattern
 - b. Route list
 - c. Route group
 - d. Gateway
 - e. Trunk
3. What dial plan element is responsible for changing the dialed digits?
 - a. Directory numbers
 - b. Translation pattern
 - c. Route pattern
 - d. Hunt pilot
 - e. Meet-me numbers

4. Which of the following wildcards represents the North American Numbering Plan (NANP)?
 - a. @
 - b. !
 - c. X
 - d. T
 - e. #
5. Which of the following wildcards represent one or more digits?
 - a. @
 - b. !
 - c. X
 - d. T
 - e. #
 - f. ()
6. Which of the following wildcards represents the termination of the interdigit timeout?
 - a. @
 - b. !
 - c. X
 - d. T
 - e. #
7. Which of the following two patterns does the route pattern 13[13–49]X match?
 - a. 13130
 - b. 13199
 - c. 1310
 - d. 1319

This page intentionally left blank

Chapter 10

Calling Privileges

Upon completing this chapter, you will be able to explain the need and uses for calling privileges and to implement them in Cisco Unified Communications Manager (CUCM). You will also be able to meet these objectives:

- Describe the tools that CUCM supports for call-privilege implementation
- Describe how partitions and calling search spaces work and how they are configured
- Describe how time schedules and time periods work and how they are configured
- Describe how CMC and FAC work and how they are configured
- Identify applications for calling-privileges configuration elements
- Describe how to implement CoS
- Describe how to implement 911 emergency calls and vanity numbers
- Describe how to implement time-of-day-based carrier selection
- Describe how to implement PLAR

Calling privileges are an important dial plan component. They are used to implement class of service (CoS), which restricts calling capabilities to authorized personnel. Calling restrictions are based on the calling device. Other applications of CoS include time-of-day call routing, vanity numbers, client matter codes (CMC), forced authorization codes (FAC), and private line automatic ringdown (PLAR).

This chapter describes the configuration tools used to implement calling privileges and discusses different usage scenarios.

Calling Privileges

Calling privileges control the available components of a call-routing database that are accessible to an endpoint. The primary application of calling privileges is the implementation of class of service (CoS). CoS is used to control toll fraud by blocking costly numbers. Many organizations block international calls, toll services, and

long-distance dialing on common area phones. CoS can also be used to restrict who can call managers, executives, and other important figures internally in the organization. Some environments restrict calls to executives but allow calls to executive administrative assistants who can transfer calls to executives. Call-forwarding actions override the original calling party's calling privilege with the calling privileges of the party that has forwarded the call.

Calling privileges can also be used to implement special applications such as tail-end hop off (TEHO). TEHO allows organizations to save money on public switched telephone network (PSTN) toll charges by routing long-distance and international calls across the private IP WAN network before hopping off at the destination site gateway to route a local PSTN call. TEHO is an application of least-cost routing (LCR), which has been in telephony networks for a long time.

TEHO can complicate a dial plan because of the additional configurations required to properly route calls on a per-site basis based on the area code of the called party number. In a multisite environment with PSTN gateways at each site, area codes are analyzed in the route patterns and the call is sent to a gateway where the call can be routed to the PSTN as a local call. The same route patterns can exist in the call-routing database multiple times. Some cities only have one local area code, while larger metropolitan areas like New York City could have over ten local area codes. In the case of New York City, ten area codes would be routed to the local New York City gateway regardless of which site made the phone call.

Another application of CoS is time-of-day routing, where calls are routed along different paths depending on the time of day and day of year in which the call is placed.

Table 10-1 provides a typical CoS implementation, where the internal CoS only allows internal and emergency calls while the local CoS includes all the destinations of the internal CoS and local PSTN calls. The long-distance CoS allows all the destinations of the local CoS and long-distance PSTN calls. The international CoS allows all the long-distance CoS destinations and international calls.

Table 10-1 *CoS Example*

CoS	Allowed Destinations
Internal	Internal Emergency
Local	Internal Emergency Local PSTN
Long-Distance	Internal Emergency Local PSTN Long-distance PSTN
International	Internal Emergency Local PSTN Long-distance PSTN International PSTN

Table 10-2 briefly describes the various call privilege configuration elements that this chapter covers. The chapter focuses on the partition and Calling Search Space (CSS) before proceeding to the other call privilege elements.

Table 10-2 Call Privileges Configuration Elements

Element	Characteristic
Partition	A group of numbers with similar reachability characteristics. Every phone number (route patterns, directory numbers, translation patterns, and so on) in CUCM can be applied to a partition.
Calling Search Space	An ordered list of accessible partitions applied to devices to permit calls.
Time periods	Static days or recurring time intervals.
Time schedules	An ordered list of time periods.
CMCs	Tracks calls to certain destinations.
FACs	Restrict outgoing calls to certain numbers.

Partitions and Calling Search Spaces

A partition is a group of dialable patterns with similar accessibility. Any dialable pattern in CUCM can be assigned to a partition. All phone numbers are in the null partition by default. All devices have access to the null partition. Any number assigned to a partition is logically segmented from the rest of the dial plan. Only devices that are configured with a CSS that has access to the partition will be allowed to call the number.

A CSS defines which partitions are accessible to a particular device. A device can only call patterns that are in partitions accessible by the calling device. The calling party (device) must have a CSS that includes the partition of the called pattern. Any entry in the call-routing database (voicemail ports, directory numbers [DN], route patterns, translation patterns, meet-me conference numbers, and so on) can be assigned to a partition.

CSSs are assigned to devices, which are the source of a call-routing request (phones, phone lines, gateways, trunks, voicemail ports, and Computer Telephony Integration [CTI] ports). Inbound calls inherit the CSS assigned to the gateway or trunk. Gateway and trunk CSSs normally restrict calls to any PSTN destination unless TEHO is configured in

the cluster. TEHO requires the trunk that received the call to have a CSS that allows local calls or the TEHO operation will fail.

Entities that do not have a CSS assigned can only access numbers that are in partition <None>. Partition <None> is commonly referred to as the *null partition*.

Partitions can be thought of as logical locks. All phone numbers are accessible by all devices by default. After a partition has been applied, a lock has been placed on the phone number restricting who can dial it. A CSS is like a key ring that includes multiple keys (partitions). When evaluating whether a call is being restricted because of the CSS configuration, evaluate the CSS of the calling party and the partition of the called party. The CSS configuration applied to the calling party must include the partition of the called party.

Figure 10-1 is an example CoS deployment where internal calls are being restricted with one of four different CSSs:

- **Phone 1:** Phone 1 can dial the directory numbers that are in the null partition, lobby partition, or employee partition. Phone 1 can dial the directory number on Phone 2 and Phone 4. Phone 1 cannot dial Phone 3's or 5's DN because each phone's DN is in the Manager partition. Phone 4 is accessible through any device because Phone 4's DN has not been assigned to a partition.
- **Phone 2:** Phone 2 can access Phone 1, Phone 3, Phone 4, and Phone 5. Phone 2's CSS includes the Manager partition, while Phone 1's CSS does not.
- **Phone 3:** Phone 3 can access Phone 1, Phone 2, Phone 4, and Phone 5.
- **Phone 4:** Phone 4 can access Phone 1 only, because Phone 1's CSS only has access to the lobby partition.

Partitions:	Lobby_PT	Employee_PT	Manager_PT	No Partition Assigned	Manager_PT
Phones	Phone 1	Phone 2	Phone 3	Phone 4	Phone 5
CSSs:	Lobby_PT Employee_PT	Lobby_PT Employee_PT Manager_PT	Lobby_PT Employee_PT Manager_PT Executive_PT	Lobby_PT	No CSS Assigned

Figure 10-1 Calling Privileges: Partitions and Calling Search Spaces

- **Phone 5:** Phone 5 does not have a CSS configured. Phone 5 can only dial the DN of Phone 4 because this DN is not assigned to a partition. The <None> (null) CSS only has access to the <None> (null) partition.

Figure 10-2 illustrates a phone with a CSS that contains the Chicago and San Jose partitions. The Atlanta partition is not included in the CSS, so the phone configured with this CSS will not be able to dial DN 4001 in the Atlanta partition.

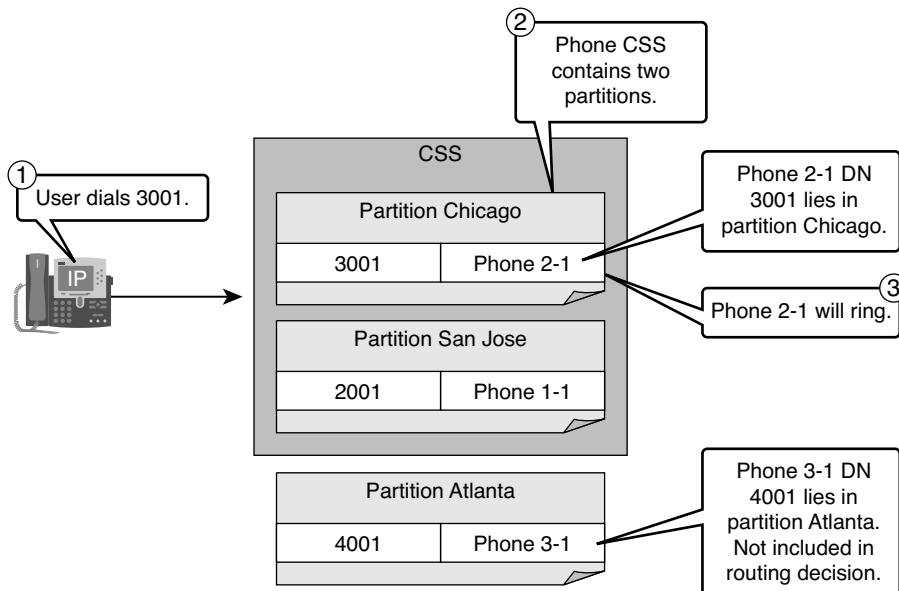


Figure 10-2 Calling Search Space Example

The user at the phone dials 3001, which is the DN of Phone 2-1. CUCM performs digit analysis against the dialed digits of 3001. The call-routing lookup will search only through the partitions configured in the CSS of the calling phone (Chicago and San Jose). CUCM finds a match in partition Chicago because the DN 3001 of Phone 2-1 is assigned to this partition. Partitions logically segment the dial plan, while CSSs provide access to the logically segmented portions of the dial plan (partitions).

A CSS is an ordered list of partitions. The CSS is processed in a top-down fashion in CUCM, which will prioritize partitions in the order in which they are listed out.

Multiple identical entities can exist in the call-routing table, but they must be in different partitions or CUCM will treat the numbers as if they were a shared line assigned to multiple devices. Shared lines will be covered later in this book. It is advisable to route emergency calls through a local gateway in multisite centralized call-processing deployments. Assuming that the deployment is done in North America, 911 and 9.911 are the emergency number patterns that can exist in the call-routing database once per site unless the

local route group call-routing element is leveraged. The local route group was a new configuration element beginning in CUCM version 7.0 and has been covered in Chapter 9, “Call-Routing Components.” If the UC deployment involves at least two sites in a centralized call-processing architecture without the use of the local route group, there will be many iterations of the emergency route patterns in the system. Site-specific CSSs and partitions would be used to create local call routing at each site. This configuration would guarantee the use of local PSTN resources at the site, but local route groups would greatly simplify the deployment configuration.

Figure 10-3 illustrates a CSS scenario in which the same called party number matches multiple partitions. The CSS processing is based on the following order:

1. **Best match:** A route pattern of 3XXX would not be considered in Figure 10-3 because the 3001 DN is a closer match than the four-digit 3XXX wildcard range of numbers.
2. **CSS is processed in a top-down fashion:** A call will never be routed to Phone 1-1 in Figure 10-3 unless Phone 2-1 was not registered and extension 3001 at Phone 2-1 did not have a call forward unregistered (CFUR) field configured.

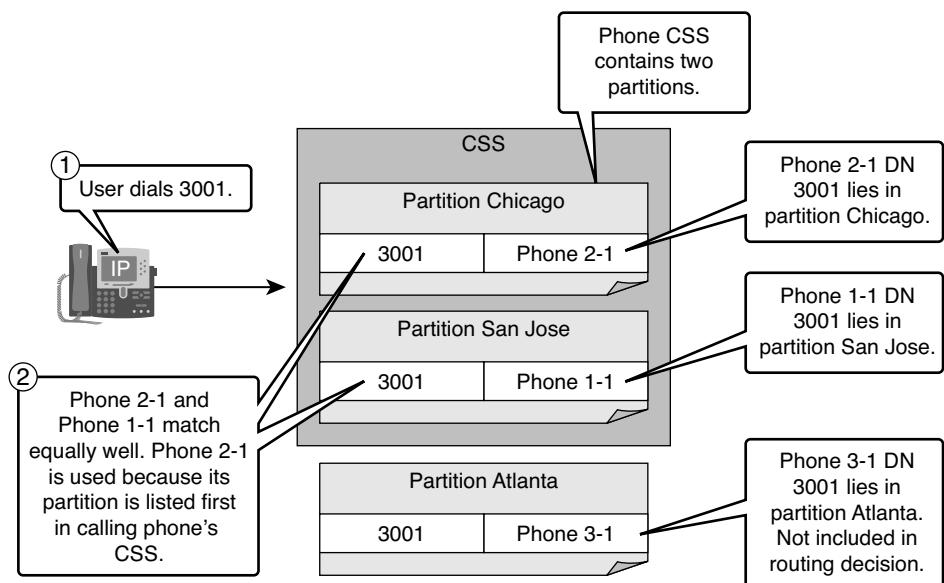


Figure 10-3 Multiple Best Matches Example

If CSSs are configured at both the device and line (DN) level, the line from which the call is placed is considered first in the call-processing logic. CUCM concatenates the line and device CSSs, resulting in the line/device CSS approach. The line/device CSS approach increases the scalability of the dial plan in a centralized call-processing architecture. Each CSS is processed in a top-down manner, but the line CSS will be analyzed before the device CSS. If a call is explicitly permitted or rejected at the line level, the device CSS will not be considered.

The CSSs considered so far in this chapter follow the traditional CSS approach, where a call is explicitly permitted if the partition of the called party is included in the calling party's CSS. The line/device approach takes the CSS configuration to a higher complexity level, but offers the benefit of having only one device-level CSS per site and globally configured translation patterns that explicitly block calls at the line level. Figure 10-4 illustrates the line/device CSS approach. The line/device approach is covered at the end of this chapter.

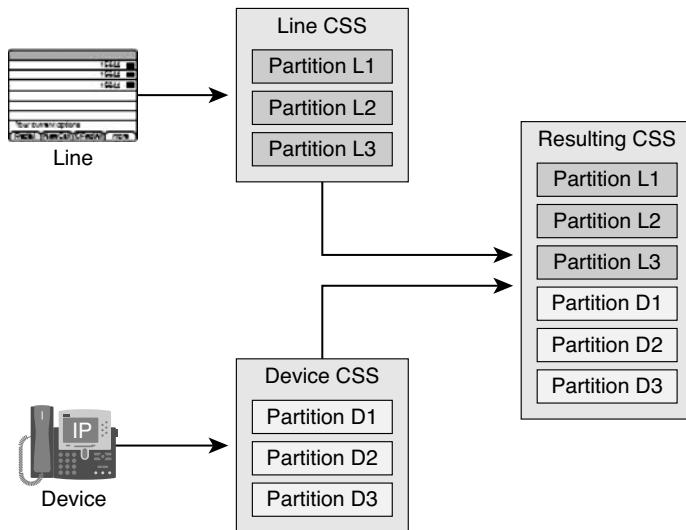


Figure 10-4 Line/Device Calling Search Space Example

Note On CTI ports, the line and device CSSs are processed in reverse order; the partitions of the device CSS are processed before the partitions of the line CSS.

The line CSS of Figure 10-5 includes partitions San Jose and Chicago, while the device CSS of the calling party includes partition Atlanta.

CUCM interprets the dialed digits to the called party number 3001 and searches for the closest match first. The two DN entries in the call-routing table are more specific than the route pattern of 300X, so the route pattern will not be considered as a potential match in the call-routing database after digit analysis (DA) is performed against the fourth digit. Phone 2-1 is chosen as the best (closest) match because the Chicago partition is configured in the line CSS, while the Atlanta partition is part of the device CSS. The CSS order is used as a tie breaker if there are multiple patterns that qualify as the closest match.

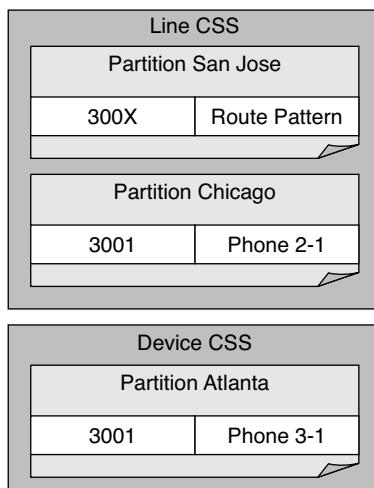


Figure 10-5 CSS Partition Order Example

Figure 10-6 is using partitions and CSSs to implement four different CoSs:

- **Internal:** Allows internal calls only
- **Local:** Allows internal and local PSTN calls
- **Long-Distance:** Allows internal, local PSTN, and long-distance PSTN calls
- **International:** Allows internal, local, long-distance, and international PSTN calls

The following partitions are applied as described:

- **Phones:** This partition is applied to all phone lines.
- **Local-PSTN:** This partition is applied to route pattern 9.[2-9]XXXXXX. Ten-digit dialing to local area codes can also be included in the Local-PSTN partition.
- **LD-PSTN:** This partition is applied to long-distance numbers. Route pattern 9.1[2-9]XX[2-9]XX XXXX is normally used in the North American Numbering Plan (NANP).
- **Intl-PSTN:** This partition is applied to the international route patterns of 9.011! and 9.011#!.

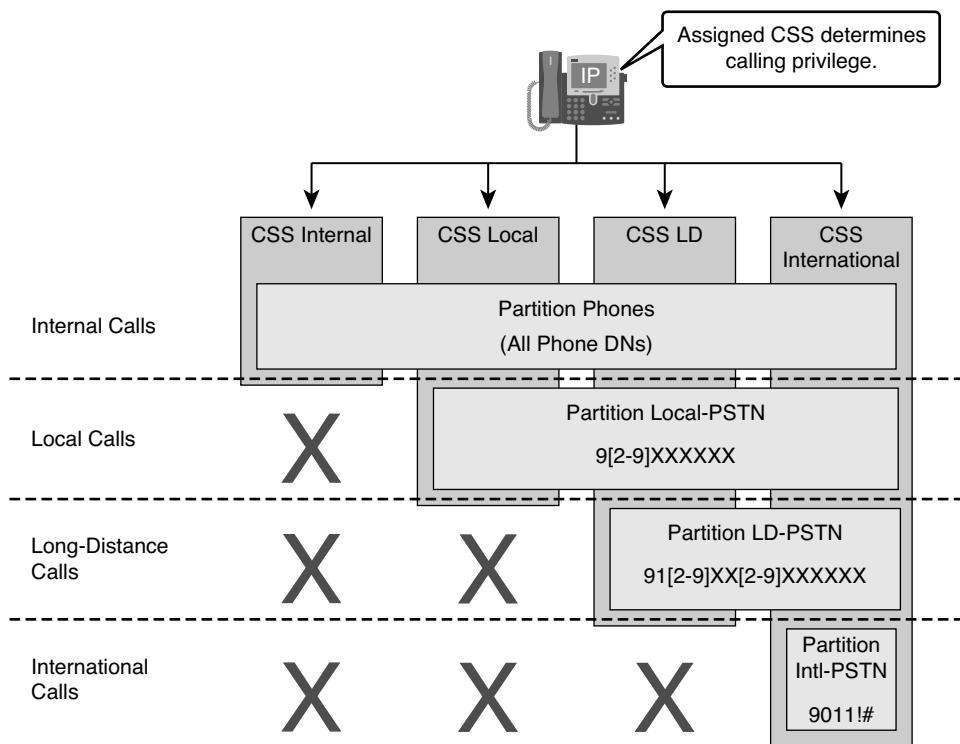


Figure 10-6 Calling Search Space Example

The following CSSs are configured to meet the CoS requirements:

- **CSS-Internal:** Phones partition
- **CSS-Local:** Phones and Local-PSTN partitions
- **CSS-LD:** Phones, Local-PSTN, and LD-PSTN partitions
- **CSS-International:** Phones, Local PSTN, LD-PSTN, and Intl-PSTN partitions

Note CSSs take on an inverted logical approach when assigned to devices such as Session Initiation Protocol (SIP) trunks, intercluster trunks, and gateways. Calls received from a trunk or gateway take on the CSS applied at the gateway or trunk device. It is normally a requirement in distributed multicluster call-processing environments to restrict emergency calls from being routed across trunk links. Emergency calls should be routed to the local public safety answering point (PSAP).

Configuring Partitions and Calling Search Spaces

Configuration of partitions and CSSs includes the following steps:

- Step 1.** Create partitions.
- Step 2.** Assign directory numbers, translation patterns, CTI ports, voicemail ports, meet-me conference bridge numbers, call-park ranges, and any other numbers in the system to their respective partitions based on the deployment's CoS requirements.
- Step 3.** Create Calling Search Spaces.
- Step 4.** Add partitions in the desired order into each newly created CSS.
- Step 5.** Assign CSSs to the devices that can request lookups to the call-routing table. Phones, directory numbers, trunks, gateways, and translation patterns can all request a call routing lookup.

Note A translation pattern is both a calling and called pattern in the call-routing table. When a translation pattern is first matched, it is treated as the called party but invokes a new call-routing request for the translated pattern (calling party). The partition of the translation pattern (called party) limits the devices that can access the translation pattern, while the CSS of the translation pattern limits the patterns that a translation pattern can be rerouted to.

Step 1: Creating Partitions

To add partitions in CUCM Administration, navigate to **Call Routing > Class of Control > Partition**. Click the **Add New** button. Figure 10-7 shows the Partition Configuration page in CUCM. You can add up to 75 partitions in one insertion of partitions with a limitation of 1475 characters. If more than 75 partitions are required, you can perform multiple insertions into the database.

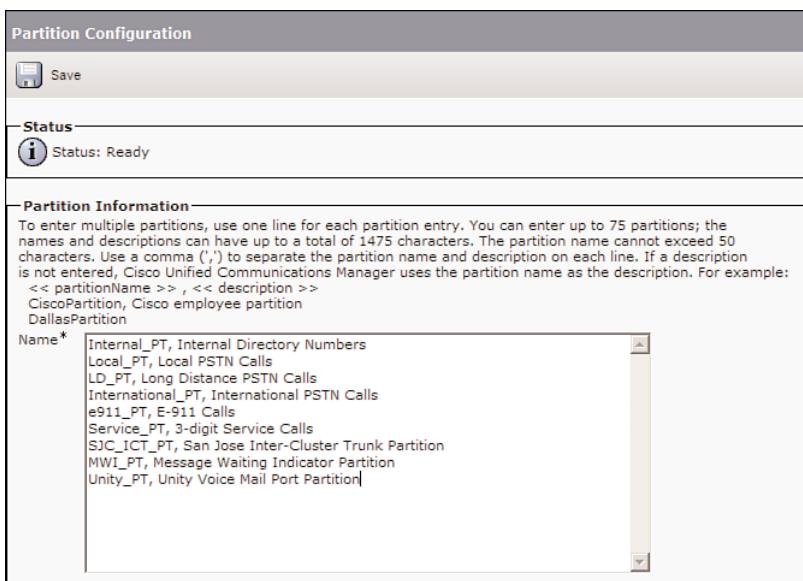


Figure 10-7 Partition Configuration

A CSS is a string of partition names internally in CUCM's database. The partition string can be verified when analyzing a CUCM trace file. Partition names should not be lengthy because the CSS has a length restriction of 1024 characters. Add two characters to each partition name if you feel that you're approaching this limit because the colon and the space in between each partition name are counted as two characters. (The CSS in CUCM is configured as follows: partition_1:partition_2:partition_3.) The maximum number of partitions in a CSS varies depending on the length of the partition names and the number of partitions. If individual CSSs are used on both the device and line level, the maximum character limit for each individual CSS (line and device) is 512 (half the combined CSS clause limit of 1024 characters). Figure 10-7 shows the Partition Configuration page in CUCM, which is somewhat akin to a basic text editor. A comma can only be used once per line. The comma is analyzed to separate the partition name and the description. If a comma is used after the partition description, CUCM will return an error when the Save button is clicked.

Step 2: Assigning Numbers, Patterns, and Ports to Partitions

Figure 10-8 shows a partition being applied to a directory number. If a large number of directory numbers will be placed in the same partition, the Bulk Administration Tool (BAT) will greatly reduce provisioning time.

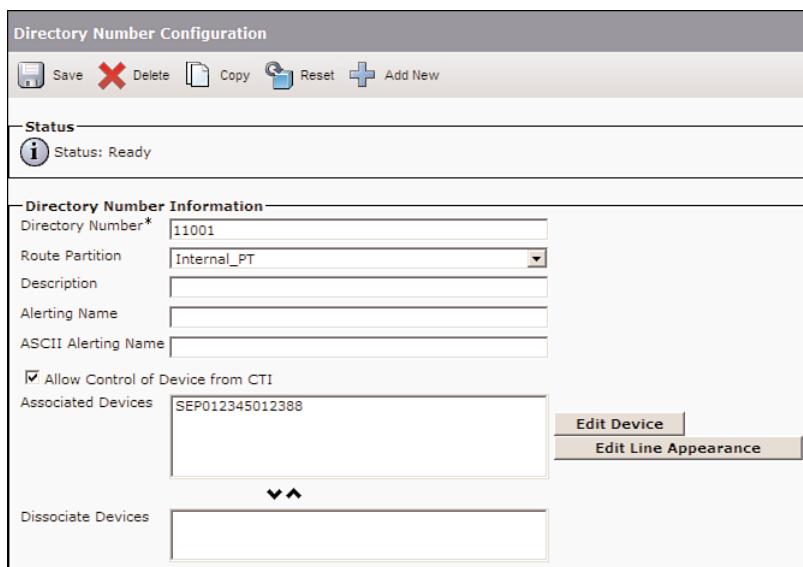


Figure 10-8 Partition Application: Directory Number

Figure 10-9 is a screen capture of an 11-digit long-distance route pattern that is being placed in the long-distance partition (LD_PT). Route patterns cannot be assigned to partitions by using BAT.

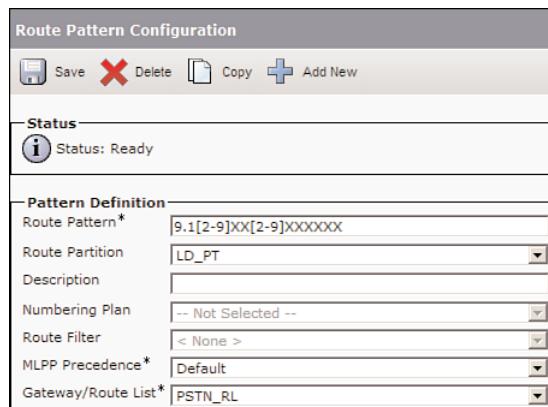


Figure 10-9 Partition Application: Route Pattern

Steps 3–5: Configuring Calling Search Spaces

Figure 10-10 is a screen capture of a CSS configuration, which you can get to through CUCM Administration by choosing Call Routing > Class of Control > Calling Search Space. Click the Add New button. The LD_CSS describes the functionality of this CSS configuration that allows long-distance, local, emergency, and internal PSTN dialing. Click a partition in the Available Partitions section of the configuration page and use the down arrow to move the partition from the Available Partitions to the Selected Partitions

section. Use the up and down arrows to the right of the Selected Partitions section to change the priority of the selected partition. The CSS is processed in a top-down fashion. The emergency call-routing partition should normally be at the top of the list, ensuring that emergency calls receive priority treatment.

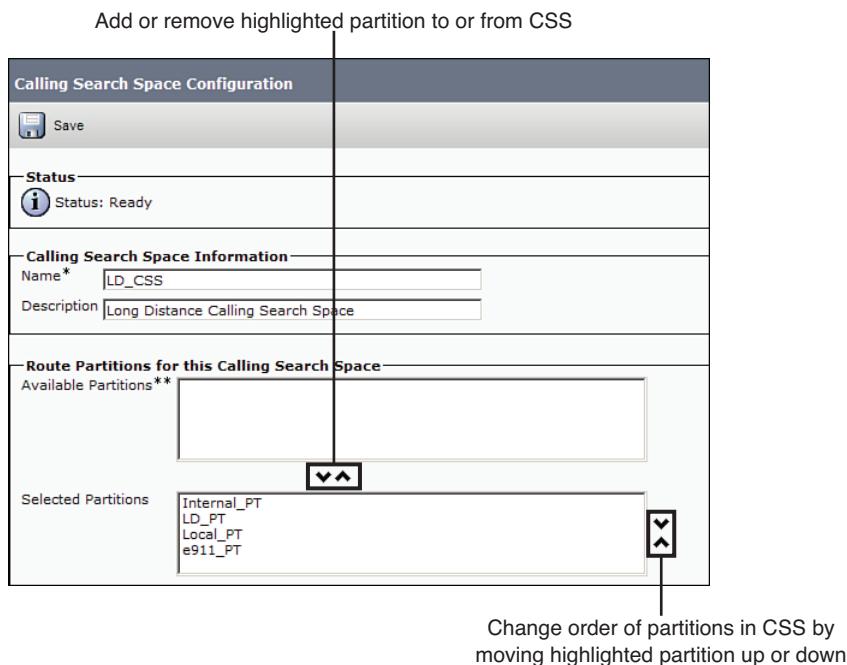


Figure 10-10 CSS Configuration

Figure 10-11 displays the phone configuration page where a CSS would be applied. CSSs can be assigned to phones, phone lines (DNs), gateways, trunks, voicemail pilot points, voicemail ports, CTI route points, CTI ports, translation patterns, and any other source of a call-routing request (calling party). If a CSS is only applied at the phone configuration level, all directory numbers on that phone will inherit the phone configuration settings.

Time-of-Day Call Routing

Time-of-day call routing can be configured in CUCM by applying time and date attributes to partitions using a time period and time schedules. A time schedule consists of one or more time periods. Time periods define time ranges or static dates and are grouped into time schedules, which are in turn assigned to partitions.

A CSS that includes a partition that is associated with a time schedule can use the partition only if the current date and time match the information specified in the time schedule that is associated with the partition. If the configured time schedule is not within the current date and time ranges specified, the partition is not evaluated by CUCM.

Phone Type:	Cisco 7961
Device Protocol:	SIP
Device Information	
Registration	Unknown
IP Address	Unknown
MAC Address*	012345012345
Description	SEP012345012345
Device Pool*	Default
Common Device Configuration	< None >
Phone Button Template*	Standard 7961 SIP
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >

Figure 10-11 Calling Search Space Phone Application

Note It is highly advisable that you use Network Time Protocol (NTP) when using time-of-day call routing to guarantee that the system has the accurate date and time.

Time-of-day call routing can be used to route calls to different locations in the following way:

- Identical route patterns are created and put into different partitions.
- Different time schedules are applied to the different partitions so that calls will match on different route patterns depending on the time of day.
- If the current time does not match the configured time schedule, the partition is not considered.

Examples of when time-of-day routing can be used include the following:

- Allowing international calls only during office hours.
- Blocking international calls on holidays.
- Using time-of-day routing for support functions. The San Jose, CA, Cisco Technical Assistance Center (TAC) might pick up calls during daylight hours in the United States, while calls after 5 p.m. are routed to ASIAPAC and calls after 1 a.m. are routed to EMEA.
- Time-of-day call routing can be used to route calls to different providers if the service providers charge different rates based on the time of day. Most service providers incur the same costs regardless of the time of day, but this paradigm can still exist in other parts of the world outside of North America.

The CiscoAustin_PT partition in Figure 10-12 is only accessible Monday through Friday from 8 a.m. to 5 p.m. (0800 to 1700).

Figure 10-13 is an example where international calls will be blocked on weekends and holidays (New Year's Day in the example). Forced authorization codes (FAC) might be a more useful way of restricting calls based on the time of day unless there is a requirement that certain types of calls are always restricted based on the time of day. Nurses' stations in hospitals provide a good case study for this feature. The nurses' stations need to make international calls between the hours of 8 a.m. and 8 p.m., but you might want to create a restriction for these types of calls after 8 p.m. Two international route patterns could be used to accommodate this need. One long-distance route pattern will be mapped to a time schedule that only makes the pattern available between 8 a.m. and 8 p.m. The second international route pattern will be available from 8 p.m. to 8 a.m., but will require the end user to dial a FAC to route the call. FACs are discussed in more detail later in this chapter.

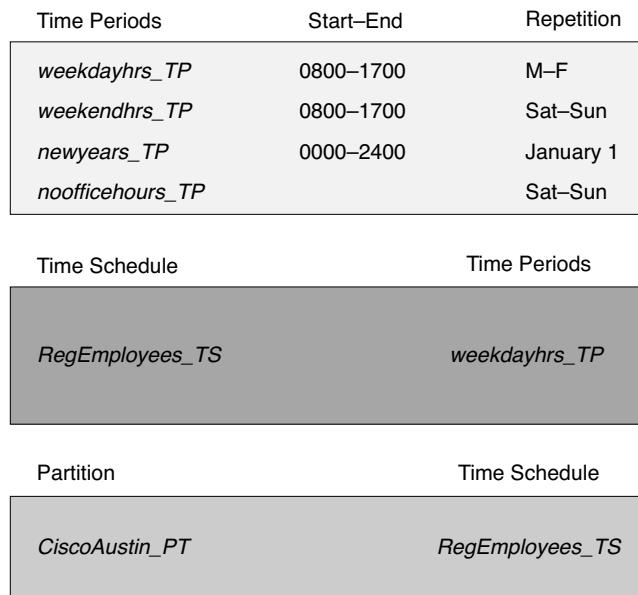


Figure 10-12 Time Periods and Schedules

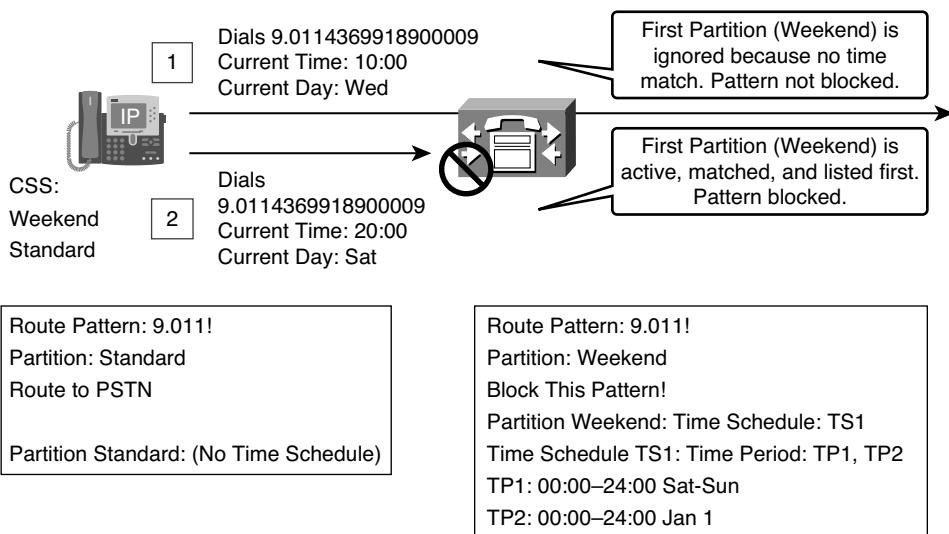


Figure 10-13 Time-Based Call-Routing Example

Note Route patterns and translation patterns can be configured with the Block This Pattern parameter to explicitly deny calls to certain patterns if the pattern is selected by the call-routing logic.

The steps to implement time-of-day routing are as follows:

Step 1. Create time periods.

Step 2. Create a time schedule and associate one or more time periods with it.

Step 3. Assign the time schedule to a partition that should be active only during the time specified in the time schedule.

The following sections describe the tasks involved with each step in more detail.

Step 1: Create Time Periods

In CUCM Administration, choose **Call Routing > Class of Control > Time Period**. Click the **Add New** button. Use descriptive names in your time period configurations and append “_TP” to the name (for example, weekdays_TP). Figure 10-14 is an example of a time period configuration with a recurring time range every week from Saturday to Sunday.

TP1 is active Saturday and Sunday from 0:00 to 24:00

Time Period Configuration		Related Links: Back		
Save				
Status				
(i) Status: Ready				
Time Period Information				
Name*	OfficeHours_TP			
Time Of Day Start*	09:00			
Time Of Day End*	17:00			
Repeat Every*	<input checked="" type="radio"/> Week from*	Mon	through*	Fri
	<input type="radio"/> Year on*	None		None

Figure 10-14 Recurring Time Period

Figure 10-15 shows a static time period that will be active every year on January 1.

TP2 is active Jan 1 from 0:00 to 24:00

Time Period Configuration		Related Links: Back To First		
Save Delete Copy Add New				
Status				
(i) Add successful				
Time Period Information				
Name*	NewYears_TP			
Time Of Day Start*	No Office Hours			
Time Of Day End*	No Office Hours			
Repeat Every*	<input type="radio"/> Week from*	None	through*	None
	<input checked="" type="radio"/> Year on*	Jan		1

Figure 10-15 Static Time Period

Step 2: Create a Time Schedule and Associate One or More Time Periods with It

Time schedules are created by adding one or more time periods to a time schedule. In CUCM Administration, choose Call Routing > Class of Control > Time Schedule. Click the Add New button. Figure 10-16 shows a time schedule that includes two time periods.

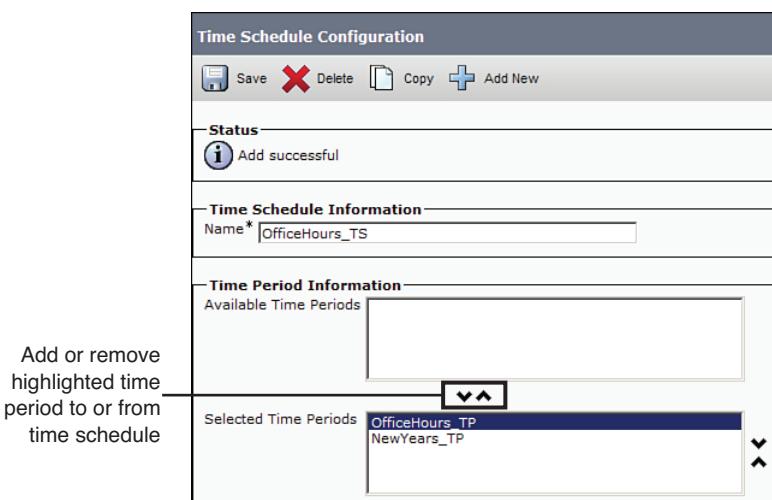


Figure 10-16 Time Schedule Configuration

Step 3: Assign the Time Schedule to a Partition That Should Be Active Only During the Time Specified in the Time Schedule

Time schedules are then assigned to partitions. The time schedule OfficeHours_TS is applied to the international partition in Figure 10-17. International_PT will only be included in the CSS during office hours. When initially configuring a partition, there is no option for setting a time schedule. This setting will only be available after the partition is initially configured.

Client Matter Codes and Forced Authorization Codes

Client matter codes (CMC) and forced authorization codes (FAC) can be applied to route patterns.

CMCs are typically used in professional organizations where a great deal of business is transacted over the phone and clients are billed for the time spent with them on the phone. CMC detail is added to call details records (CDR) to allow accounting and billing of calls based on the client matter code used after initially dialing the phone number. If a route pattern that has a CMC applied is matched, the user is prompted to enter a CMC. CMCs are created in the system and associated with route patterns that are used to call customers. Environments that are heavy users of CMCs might require a CMC for any PSTN-bound phone call. These environments normally have a CMC that is not billed back to customers (overhead). If a route pattern requires a CMC, the call will not be routed unless a valid CMC is entered when prompted by a tone in the system.

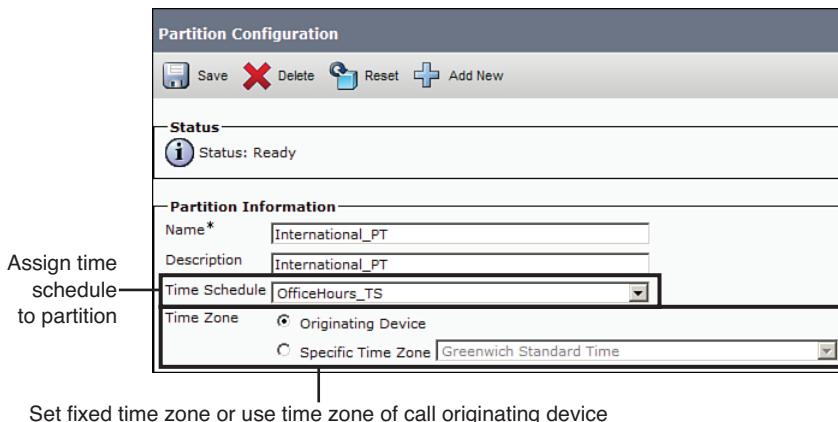


Figure 10-17 Time Schedule: Partition Application

Forced authorization codes (FAC) are implemented in a similar manner to CMCs, but their goal is very different. FACs are implemented to prevent calls from being placed by unauthorized users (similar to CSSs). Some organizations use unique FACs for every user in the system for legal or accounting purposes. We will investigate using FACs as an alternative way of restricting calls similar to using CSSs. FACs have the advantage of tracking users' calls regardless of the physical phone used to make the phone call. The end user dialing the phone receives a tone from CUCM after dialing a number, prompting the user to enter a FAC for the call to be completed. CSSs and FACs can be used together, as mentioned in the nurses' station example used earlier in this chapter.

FACs are added to CUCM's call-routing configuration, and each FAC will have an associated authorization level assigned. Route patterns are configured to require a FAC with an associated minimum authorization level. Users have to enter a FAC with an authorization level that is equal to or greater than the authorization level required in the route pattern configuration.

Figure 10-18 illustrates a CMC application where UserA dials a number that matches a route pattern that has the Require Client Matter Code parameter selected. CUCM plays a tone to prompt the user for a CMC. The end user enters a valid CMC and the call is routed. CMCS 1234, 1244, and 3489 are configured in Figure 10-18. The end user in Figure 10-18 enters the code 1234. If the user does not terminate the CMC with a #, the user will have to wait until the T.302 interdigit timeout expires (15 seconds by default) for the call to be routed. As long as a valid CMC is entered, CUCM successfully routes the call. The CMC will be mapped to the call in the call detail records (CDR) of CUCM.

Figure 10-19 uses the same configuration as the preceding example. UserA enters 5555 when receiving the tone prompting the user to enter a CMC and/or FAC. The call is rejected because 5555 is not a valid CMC. A CDR is generated for the attempted call if the CDR Log Calls with a Zero Duration Flag CallManager service parameter has been enabled. Calls with zero-duration flags are not logged in CDRs by default.

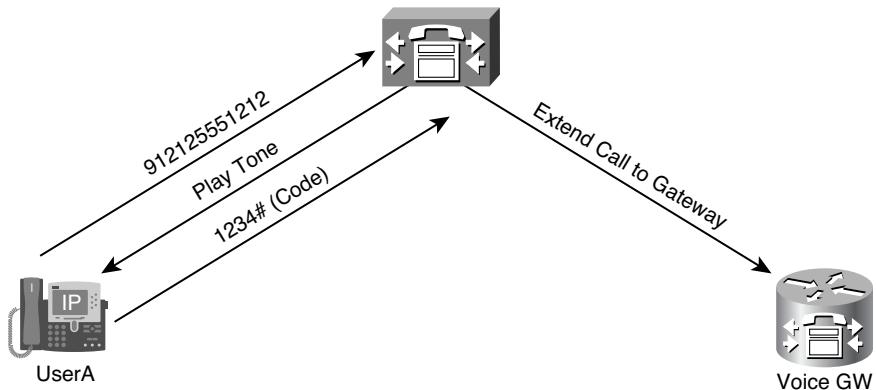
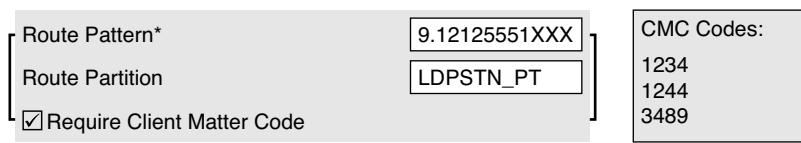


Figure 10-18 Client Matter Code: Successful Operation

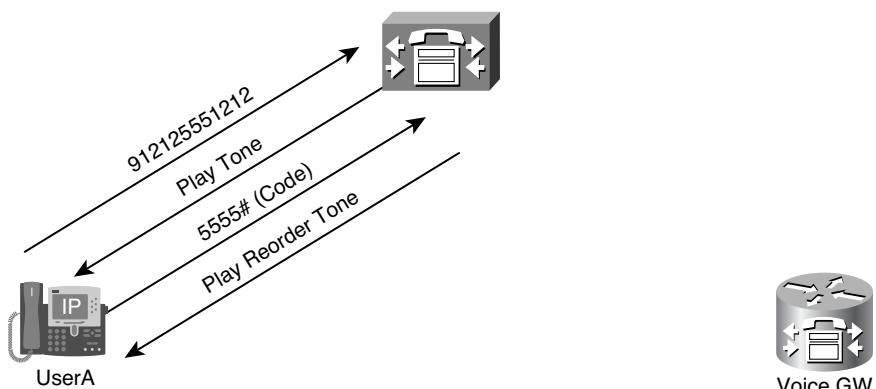
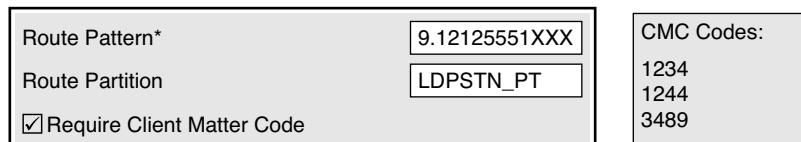


Figure 10-19 Client Matter Code: Call Failure

Figure 10-20 shows an example involving the use of FACs. UserA dials a number that matches a route pattern in this example where the Require Forced Authorization Code parameter is selected and the Authorization Level field is set to 3. CUCM prompts the user with a tone that a FAC and/or CMC has to be entered. The user enters 1888, which is configured with an authorization level of 7. The FAC level of the code was equal to or higher than the required authorization level (3), so the call is routed successfully. The name of the entered FAC is included in the generated CDR.

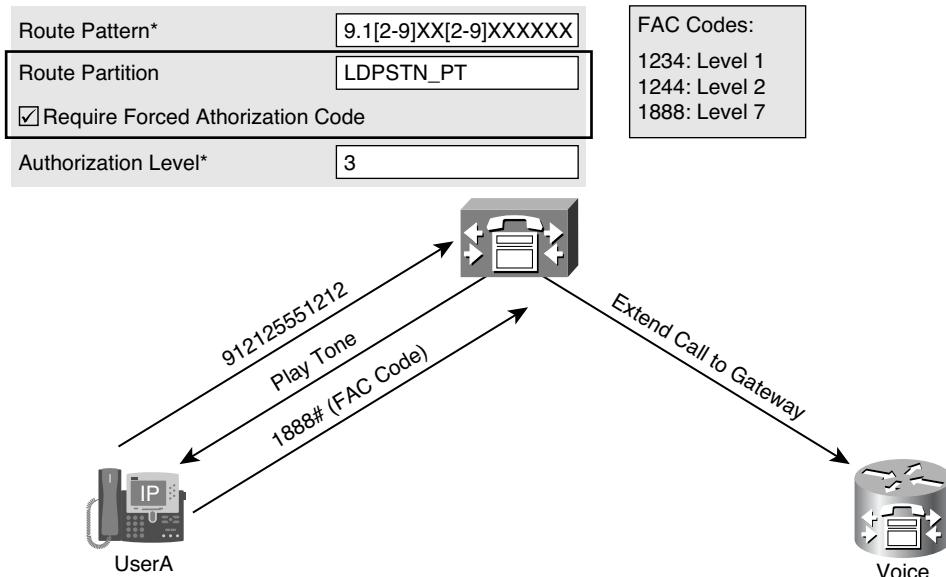
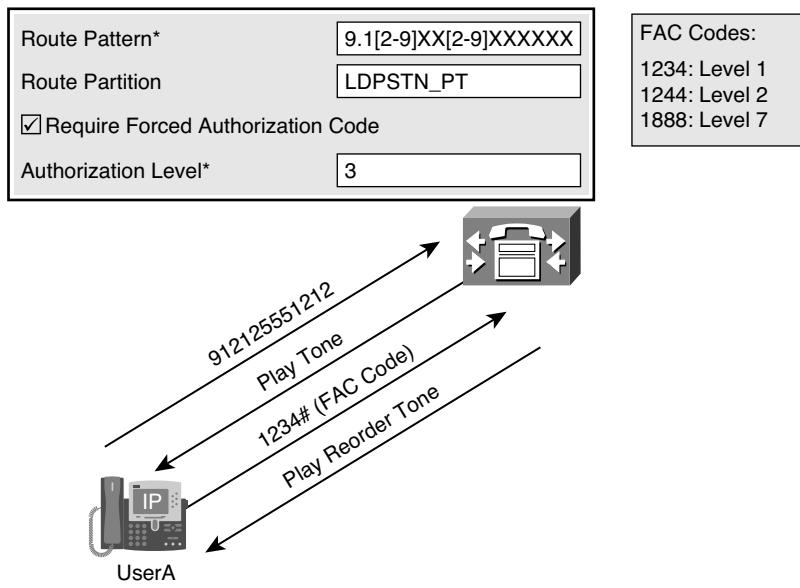
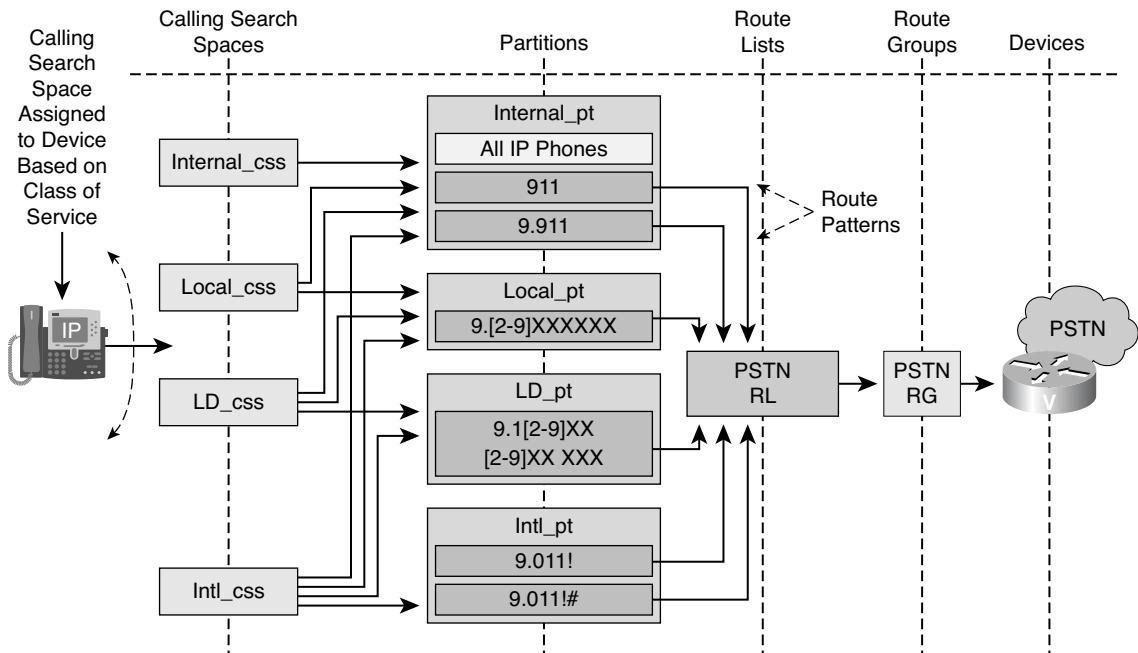


Figure 10-20 Forced Authorization Code: Successful Operation

Figure 10-21 has the same configuration as Figure 10-20, but UserA enters 1234 at the FAC prompt. The call is denied because the authorization level of FAC 1234 is 1 and an authorization level of 3 is required to route the call. A CDR is generated, logging the attempted call.

Class of Service Approaches

Figure 10-22 illustrates a single-site CoS deployment with four distinct classes of service. Four partitions and four CSSs have been created to implement the customer requirements. The route patterns for each call type have been put into their respective partitions. The CSSs will be assigned to various devices in the infrastructure. Figure 10-22 follows what Cisco refers to as the “Traditional Calling Search Space” approach.

**Figure 10-21** Forged Authorization Code: Call Failure**Figure 10-22** Single Site with Four Calling Search Spaces

Each additional site in a centralized call-processing model will result in four more site-specific partitions and four more CSSs. The PSTN route patterns will need to be duplicated and put into the site-specific partitions that will all be part of the device-level unrestricted CSS. The challenge in this scenario is that partitions and CSSs need to provide three functions:

- Call routing (determining the best possible match)
- CoS (control who is allowed to dial what number)
- Path selection (select the local PSTN gateway)

A much lower number of route patterns will be required if the CUCM Local Route Group option is used. The Local Route Group call-routing construct will enable the routing of calls to a local gateway based on the local route group associated with the device pool instead of creating an unrestricted site-specific CSS for each site.

Figure 10-23 illustrates a summary of the partitions, CSSs, and route patterns necessary to achieve a traditional CSS deployment without the use of a local route group. The solution includes four partitions and four CSSs per site. The number of required partitions and CSSs will be slightly different in every deployment, but the number of configuration elements could become unwieldy in large centralized call-processing deployments.

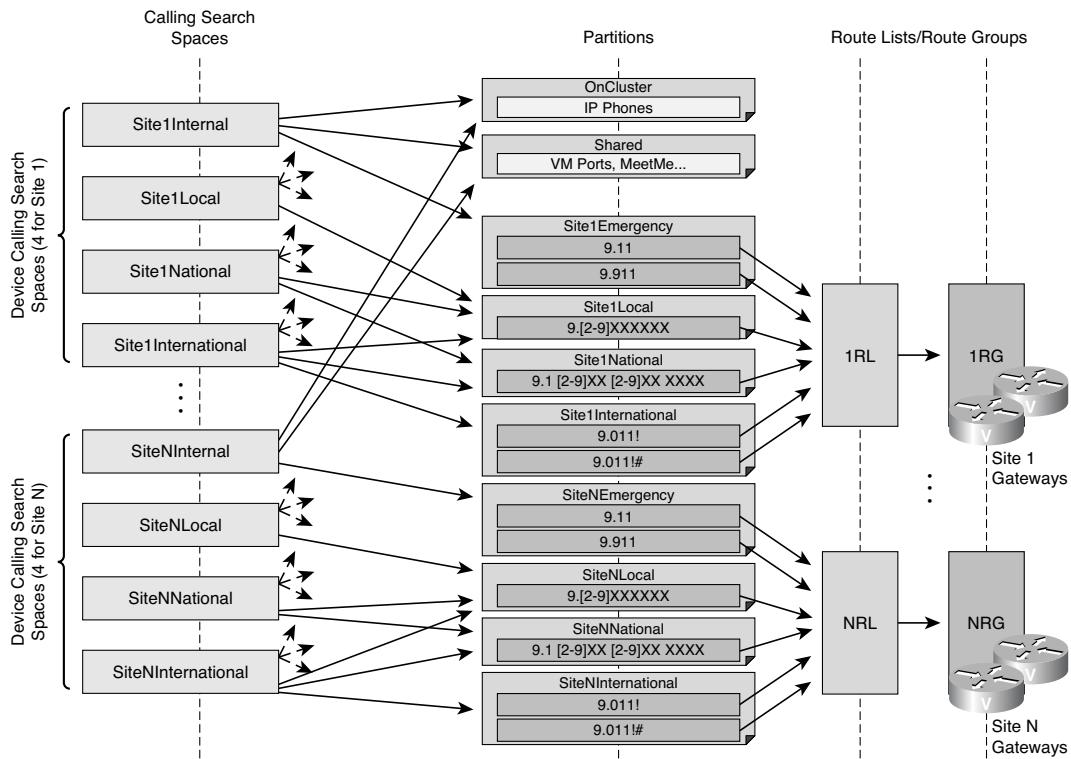


Figure 10-23 Centralized Call Processing with Four Calling Search Spaces

Note Traditional CSSs are not scalable for medium- to large-size centralized call-processing deployments.

It is possible to significantly decrease the total number of partitions and CSSs required for the deployment by dividing the functions of site-specific routing (call steering) and performing CoS-based restrictions by using a line CSS to perform CoS restrictions and a device CSS to perform call routing. The use of both a line CSS and a device CSS is called the line/device CSS approach.

CUCM performs a concatenation of both the line and device CSSs for each IP phone and then performs top-down processing of the line CSS and then the device CSS. As soon as there is an explicit action associated with routing or rejecting the call, the processing of the line/device CSS stops.

The device CSS provides unrestricted, site-specific call routing to one or more local gateways. The device CSS is unrestricted, allowing all types of PSTN calls.

The line CSS only has access to partitions that explicitly block patterns using translation patterns. The blocking translation patterns are put into blocking partitions that only line CSSs will have access to. The line CSSs are configured globally and assigned on a per-directory number basis.

Figure 10-24 illustrates the use of the line/device CSS approach, where a phone has a line CSS that restricts international calls. The translation pattern of 9.011! has an explicit action of Block This Pattern configured. As soon as the translation pattern is matched in the line CSS, CUCM stops processing and explicitly rejects the call. Although the device CSS permits the international call, the line CSS has explicitly rejected the call.

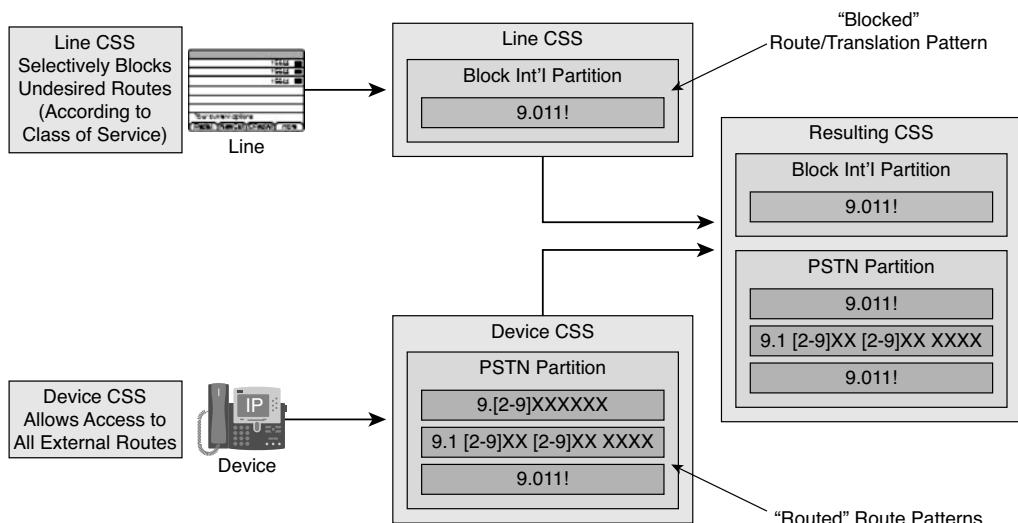


Figure 10-24 Line/Device Calling Search Space Approach

Figure 10-25 illustrates the scalability of the line/device CSS approach with two sites. This approach results in a significantly simpler configuration with many fewer partitions and CSSs. Each site will only need one device-level CSS, and the blocking CSSs only need to be configured once in the global configuration.

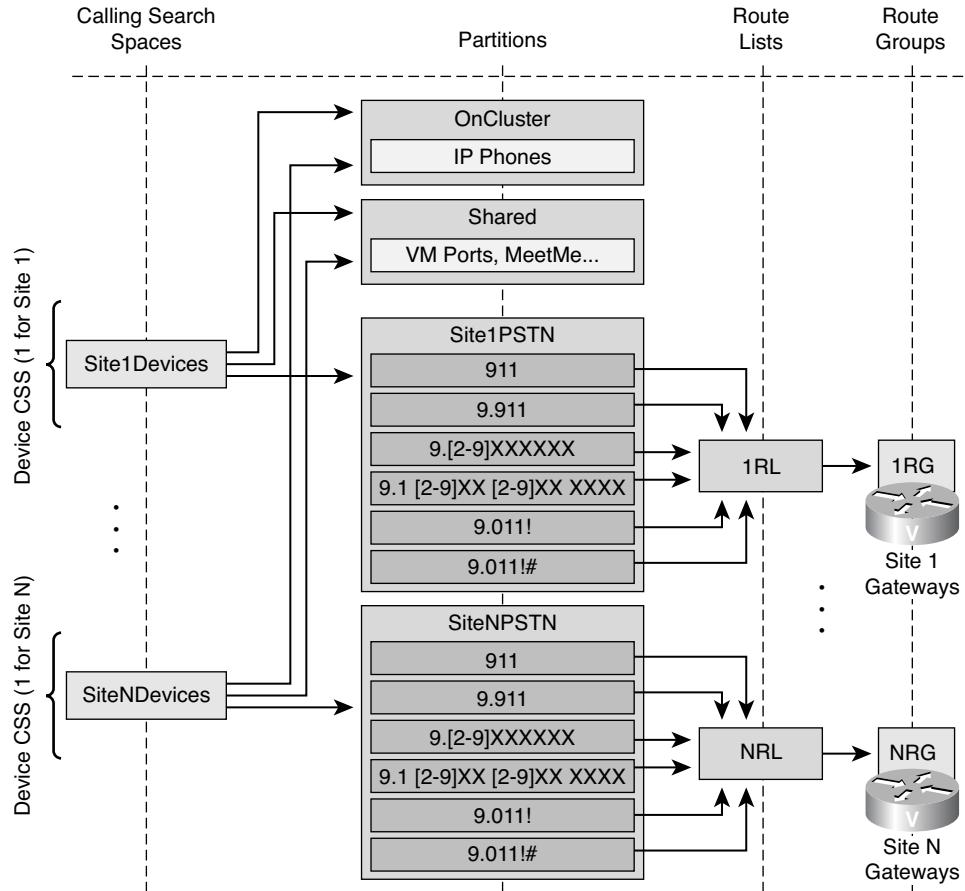


Figure 10-25 Line/Device CoS with Multiple Sites

This approach has the significant advantage that only a single, site-specific partition (and device CSS) is required for each site to allow local gateway selection, and only one partition per CoS (independent of the site) is required to perform CoS enforcement.

Instead of requiring the number of partitions determined by multiplying classes of service and sites, the number of partitions is determined by adding the required sites and CoSs.

A deployment with four sites and four CoSs using the traditional approach would result in 16 partitions, whereas the line/device approach results in only eight required partitions.

The line/device CSS approach contains a line CSS and a device CSS. CUCM concatenates the two CSSs and performs top-down processing of the line CSS and then the device

CSS. The line CSS blocks certain type of calls on a cluster-wide basis. There would be three different blocking CSSs based on the examples used previously where there is a requirement for four different CoS levels. The three line CSSs would be as follows:

- **Long-Distance-CoS-CSS:** This CSS would only include the Block-International partition. Two translation patterns matching on 9.011! and 9.011#! would be members of this partition. Each translation pattern would have a configured action of Block This Call.
- **Local-PSTN-CoS-CSS:** This CSS would include the Block-International and Block-LD partitions. A 9.1[2-9]XX[2-9]XXXXXX translation pattern would be placed in the Block-LD partition with a configured action of Block This Call. The Block-International partition was configured in the last paragraph.
- **No-PSTN-CoS-CSS:** This CSS would include the Block-Local partition, which includes 9.[2-9]XXXXXX and 9.[2-9]XX[2-9]XXXXXX translation patterns with Block This Call actions.

Device requiring international PSTN access would not need a line CSS because all calls from these devices would be permitted.

The device CSS would be site specific but completely unrestricted. As soon as there is a match at the line level blocking a pattern that should not be allowed, CUCM stops analyzing the CSSs and performs the action. If the call is permitted, the device CSS will route the call to the local gateway at the site.

Additional information on the Cisco line/device CSS approach is available through the CUCM Solution Reference Network Design (SRND) guide available through the Cisco Design Zone at www.cisco.com/go/srnd.

Click the Unified Communications link, and then click the Unified Communications Systems link.

Emergency Call Routing and Vanity Numbers

911 is the NANP emergency phone number for medical, fire, and police emergencies in North America. Other countries have different emergency numbers in which this information can apply. Calls to 911 are routed to a public safety answering point (PSAP). The PSAP is the call center used for emergency calls in North America. Emergency calls should always be routed to a local PSAP through a local gateway if available. The 911 and 9.911 route patterns will be created once per site in either a traditional CSS approach or a line/device CSS approach. These patterns could be configured once (system-wide) if the local route group call-routing option is leveraged. The local route group will route all PSTN calls to the local gateway router, which metes out the 911 call-routing goal.

Note Emergency calling includes many additional aspects that are not covered in this book. The National Emergency Number Association (NENA) should be contacted to verify the 911 requirements for your deployment.

Vanity numbers provide access to a certain local service within an enterprise. Users should be able to dial the same number to access the appropriate locally provided service no matter where they are located. Some companies, for example, use the dual-tone multi-frequency (DTMF) keypad word HELP (4357) to dial the IT help desk.

An example of vanity services is a number that connects users to local IT support. Vanity numbers are not limited to internal services. They could also be configured to reach external local services (taxis, travel agencies, and so on) by using abbreviated dialing within the corporate dial plan.

A vanity number can be configured as a DN, a route pattern, a hunt pilot, or a translation pattern.

Implementing vanity numbers is similar to configuring selective PSTN outbreak (always using the local gateway for PSTN or emergency calls) and consists of the following steps:

- Step 1.** Create a site-specific partition per site.
- Step 2.** For each service, configure the same vanity number (route pattern, DN, hunt pilot, or translation pattern) once per site and put it into the site-specific partition created earlier.
- Step 3.** Put the appropriate site-specific partition into the CSS of the phones located at a site.

Note If abbreviated dialing is used to reach external local services (such as a local travel agency by dialing 7998), a translation pattern is used for the vanity number.

Figure 10-26 shows a vanity number for IT support that is configured as 7999. Both the New York and San Jose sites will use this same IT support vanity number. The DN of 7999 located in San Jose is put into the San Jose partition. The same DN is configured in the New York partition. Phones located in New York have partition New York listed first in their CSS; phones located in San Jose have partition San Jose listed first in their CSS.

If a San Jose user dials 7999, the call is routed to the IT help desk in San Jose because the New York DN of 7999 is not accessible by the San Jose phone. The San Jose CSS does not include the New York partition. The same call-routing theory applies to users in New York. Calls placed to 7999 in New York are routed to the local New York IT help desk.

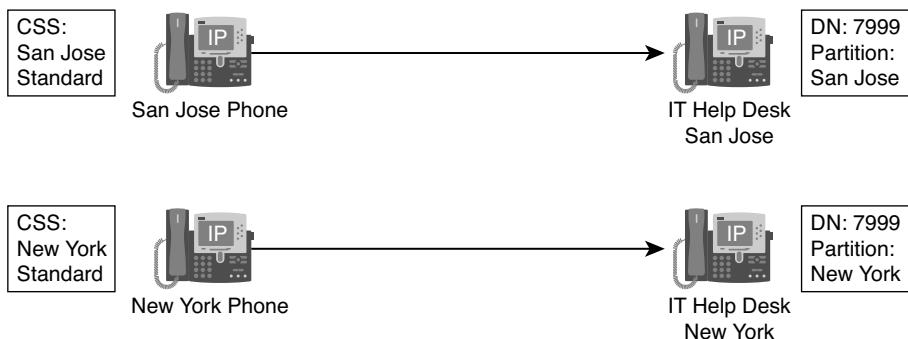


Figure 10-26 *Vanity Number Example*

If the desired services are provided externally, a translation pattern is configured to translate the appropriate vanity number. Users can be given a phone number that aligns to the internal corporate dial plan even if the call will be routed to the PSTN using a longer number. The translation pattern will match on the dialed digits of 7998 and manipulate the digits to 1 914 555-1212 by using a called-party transformation mask. Over time, if there are changes to the external number, users will not need to know the new phone number. The CUCM administrator can reconfigure the called-party transformation mask. By creating the vanity number once per site and putting it into a site-specific partition, you can ensure that users always match the vanity number translation pattern for their respective site. This is achieved by including the site-specific partition in the phone CSS.

Figure 10-26 would use two translation patterns to achieve this objective. Each translation pattern would be placed in a site-specific partition. Configure the San Jose translation pattern with the PSTN number of the San Jose travel agency; configure the New York translation pattern with the PSTN number of the New York travel agency. Make sure that the translation patterns have CSSs assigned that allow them to use the local PSTN gateway for routing the calls out to the translated PSTN numbers.

Private Line Automatic Ringdown

Private line automatic ringdown (PLAR) is used when a phone should dial a predefined number as soon as the phone goes off-hook. PLAR is typically used with button-free security phones in elevators and stairways.

Implement PLAR in CUCM by following these steps:

- Step 1.** Configure a translation pattern where the pattern is empty (null string pattern), and put it into a partition.
- Step 2.** Configure the number to be dialed by the PLAR-enabled phone in the called-party transformation mask of the translation pattern.

- Step 3.** Configure the first line of the phone that should use PLAR with a CSS that includes only the partition that was applied to the translation pattern.
- Step 4.** Make sure that the CSS of the translation pattern has access to the transformed number. The translation pattern CSS is used when making the call-routing decision for the translated number.

When the phone goes off-hook, the off-hook event triggers call processing (digit analysis) on CUCM, where the null dialed string matches the translation pattern and is translated to the PLAR number. The call is then extended toward the PLAR destination. CUCM performs digit analysis as each digit is received from the phone, starting with the off-hook event. Different call-processing protocols (SIP, Skinny Client Control Protocol [SCCP], H.323) and calling methods send their dialed digits in different manners (en bloc or digit by digit) and thus the way in which a call is routed with an overlapping dial plan. This information is covered in more detail in Chapter 5, “Cisco Unified Communications Manager Endpoints.”

In Figure 10-27, a null-string translation pattern is created and put into partition PLAR1234. The called-party transformation mask is 1234. The translation pattern has a CSS assigned that includes partition Phones (the partition of destination 1234).

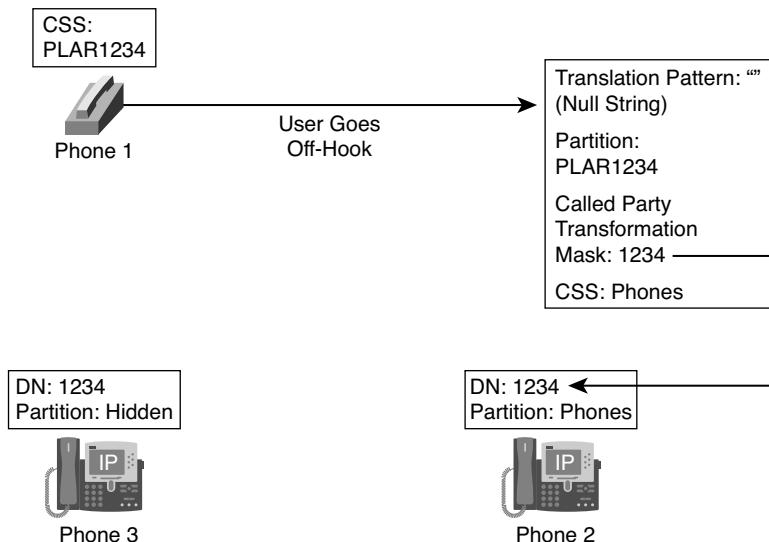


Figure 10-27 PLAR Example

Phone 1 is configured with a CSS that contains the PLAR1234 partition (the partition of the translation pattern).

Two phones exist with DN 1234: Phone 2 is in partition Phones, and Phone 3 is in partition Hidden.

When Phone 1 goes off-hook, the null-string pattern is matched, and the translation pattern transforms the dialed null string to 1234 and sends a call-routing request to CUCM. This request uses the CSS of the translation pattern (Phones) and therefore finds only a single match (Phone 2). The call is extended to Phone 2.

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- Calling privileges are configured to implement class of service (CoS) or special applications that require calls to be treated differently depending on the caller.
- Partitions are groups of called numbers with identical reachability characteristics. Calling Search Spaces (CSS) are lists of partitions that the owner of the CSS has access to.
- Time schedules and time periods are used to activate or deactivate partitions within a CSS depending on time or date information.
- Client matter codes (CMC) are used to track calls to certain clients by requesting the CMC to be entered and adding it into call detail records (CDR). Forced authorization codes (FAC) are used to allow access to route patterns only if an authorization code with a high-enough level is entered when requested.
- Calling-privileges applications include implementation of CoS, vanity numbers, time-based route or carrier selection, and PLAR.
- Complexity of CoS implementation at IP phones can be reduced by using the line/device approach, which allows the effective CSS to be composed of a line and device CSS (in this order).
- Vanity numbers provide access to local services by dialing the same number from any physical location.
- Time schedules and time periods can be used to route calls through different gateways or carriers depending on the time of the day or date to take advantage of the cheapest rate at any time.
- PLAR, a function where a phone is automatically connected to a predefined number when it goes off-hook, is implemented by using null-string translation patterns, partitions, and CSSs.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. What are the calling privileges of a user in the telephony system called?
 - a. Class of service
 - b. Calling Search Space
 - c. Partition
 - d. Capabilities
2. Phone numbers (directory numbers, partitions, translation patterns) are assigned to which dial plan element to achieve calling privileges?
 - a. Calling Search Space
 - b. Partition
 - c. Class of service
 - d. Route list
3. What is assigned to a phone or line to implement calling privileges?
 - a. Calling Search Space
 - b. Partition
 - c. Class of service
 - d. Route list
4. Which two elements are used to control how calls are routed based on the time of day?
 - a. Time-based ACLs
 - b. Time period
 - c. Time schedule
 - d. Time interval
 - e. Time list
5. Which element is used to verify the calling privileges of a user after the digits have been dialed?
 - a. Client matter code
 - b. Partition
 - c. Calling Search Space
 - d. Forced authorization code

- 6.** If a device contains both a device and a line CSS, how will they be processed by CUCM?
 - a.** Line CSS overrides device CSS.
 - b.** Device CSS overrides line CSS.
 - c.** Both are concatenated. Line CSS is processed before device CSS.
 - d.** Both are concatenated. Device CSS is processed before line CSS.
- 7.** Calling Search Spaces are not applied to which one of the following?
 - a.** Directory numbers
 - b.** Phones
 - c.** Translation patterns
 - d.** Voicemail ports
 - e.** Route patterns
 - f.** Trunks
 - g.** Gateways
- 8.** In the line/device CSS approach, the device CSS achieves which objective?
 - a.** Class of service
 - b.** Least-cost routing
 - c.** Site-specific call routing
 - d.** Tail-end hop off
- 9.** A phone number that is used in the system to abbreviate the numbers that users need to remember is referred to as what?
 - a.** Hunt pilot
 - b.** Route pattern
 - c.** Translation pattern
 - d.** Vanity number
- 10.** A PLAR line uses which of the following dial plan elements?
 - a.** Route pattern
 - b.** Route list
 - c.** Translation pattern
 - d.** Directory number

Chapter 11

Digit Manipulation

Upon completing this chapter, you will be able to use digit manipulation techniques to change calling party (caller ID) and called party (dialed digits) information, and be able to meet the following objectives:

- Describe when to use digit manipulation in CUCM
- Describe CUCM digit manipulation operation
- Identify CUCM digit manipulation configuration options
- Describe how to use external phone number masks
- Describe how to use translation patterns
- Describe how to use transformation masks in CUCM
- Describe how to use digit stripping and digit prefixes in CUCM
- Describe how to use significant digits in CUCM
- Describe how to use global transformations in CUCM
- Describe how to use incoming number prefixes in CUCM

Users of a phone system need to communicate with a variety of destinations.

Destinations might be located within the same site, different sites within the same company, and other companies located within the same country or different countries.

Completing various types of calls often requires dialing access codes or prefix numbers. It is often prudent to restrict users from dialing certain destinations that could incur high costs, such as 1-900 pay service phone numbers and international dialing.

Users should be provided with a dial plan with the lowest amount of complexity. Cisco Unified Communications Manager (CUCM) has the capability to provide digit manipulation, which achieves the goal of adding or subtracting digits to comply with a private or public numbering plan. Toll bypass calls that are routed over the data network should be

transparently rerouted across the public switched telephone network (PSTN) when WAN resources are not available or are fully utilized.

This chapter describes digit manipulation tools that allow a CUCM administrator to implement flexibility and transparency in the dial plan of the company. The chapter covers external phone number masks, digit prefixing, digit stripping, transformation masks, translation patterns, and significant digits.

CUCM Digit Manipulation

Digit manipulation is often used to change calling party numbers for caller ID purposes on outgoing PSTN calls. Digit manipulation is also used to strip PSTN access codes before CUCM routes calls to the gateway (PSTN). Digit manipulation is required for abbreviated dialing and to properly route inbound calls from the PSTN where an abbreviated internal dial plan exists. Inbound calls from the PSTN can be received with a ten-digit called party length, but the internal dial plan might use only a subset of those numbers (four or five digits). These inbound calls would need to have the called party number transformed to the digit length used in the internal dial plan. PSTN access codes do not adhere to public standards, so they need to be stripped from the called party number before routing the call to the PSTN. Most organizations use the number 0, 8, or 9 as the access code for PSTN dialing. The calling party number also needs to be changed from the abbreviated internal extension number to a full E.164 PSTN number to allow easier redial.

Mechanics of CUCM Digit Manipulation

An IP phone with extension 1002 in Figure 11-1 calls a phone on the PSTN with a called party number of 408 555-111. The user at extension 1002 must first dial a PSTN access code of 9 to route a call to the PSTN. The PSTN Class 5 switch will not be able to route the call unless the access code is dialed before the PSTN number. The calling party number is transformed into a ten-digit pattern so that the PSTN is presented with a routable caller ID of 706 555-1002, not the extension of 1002. Four-digit dialing is not possible in the North American Numbering Plan (NANP).

Note In some countries, the calling party number must be set to the correct PSTN number of the used PSTN subscriber line or trunk.

Table 11-1 displays some often-used digit manipulation requirements and the methods in which they are handled in CUCM.

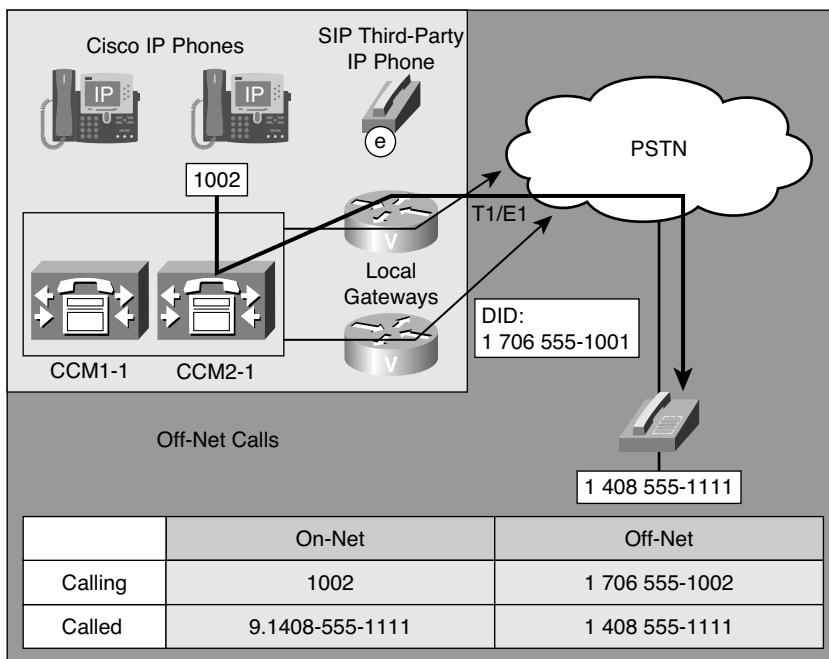


Figure 11-1 *Digit Manipulation Overview*

Table 11-1 *Digit Manipulation Methods*

Requirement	Call Type
Expand calling party directory number to full E.164 PSTN number	Internal to PSTN
Strip PSTN access code	Internal to PSTN
Expand abbreviated number	Internal to internal
Convert E.164 PSTN called party directory number to internal number	PSTN to internal
Expand endpoint directory numbers to accommodate overlapping dial plan	Internal to internal PSTN to internal

Figure 11-2 illustrates an internal caller at extension 1005 dialing a PSTN number using a PSTN access code of 9 followed by the 11-digit PSTN number. The process of digit manipulation occurs as follows:

1. Extension 1005 dials 9-1-303-555-6007.

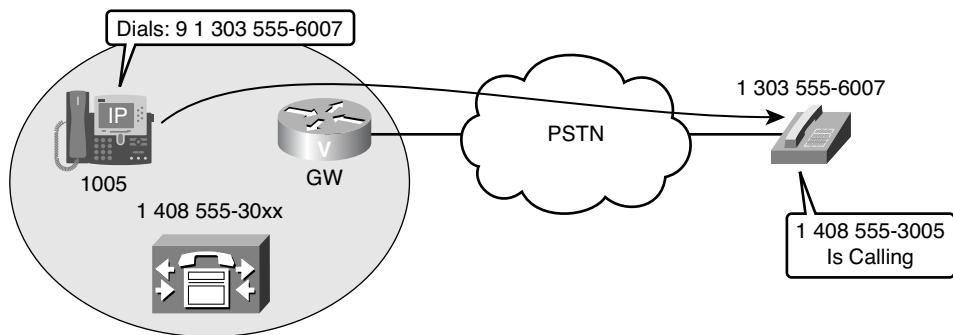


Figure 11-2 Outgoing Call to the PSTN

2. The dialed number (called party) matches the 9! route pattern, where digit manipulation is taking place. For the sake of simplicity, let's imagine that there is only one gateway with this very simple dial plan. The route pattern is pointed directly to the gateway where the following is configured:
 - Called party transformations > Discard digits: PreDot
 - Calling party transformations: 40855530XX
 - Route the call to the gateway
3. CUCM provides digit stripping of the access code from the called party and sends 11 digits (1-303-555-6007) to the PSTN through the gateway. The calling party number is modified from 1005 to 408 555-3005.
4. The PSTN phone at (303) 555-6007 rings and sees 4085553005 as the calling number.

Calling and called party transformations are configured at the route pattern level in the example, but these digit manipulation techniques are normally preferred at the route list detail level of the route list (per route group). The calling party transformation is often performed first at the external phone number mask configuration level. The external phone number mask is a directory number (DN) configuration parameter that will display a phone's ten-digit PSTN phone number to the end user at the phone. External phone number masks are also used when Automated Alternate Routing (AAR) reroutes a call over a call admission control (CAC) call rejection in a centralized call processing model. AAR is covered in detail in the Cisco Press book *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide*.

Figure 11-3 illustrates a call coming from the PSTN to an internal phone. The call-routing process from the gateway is as follows:

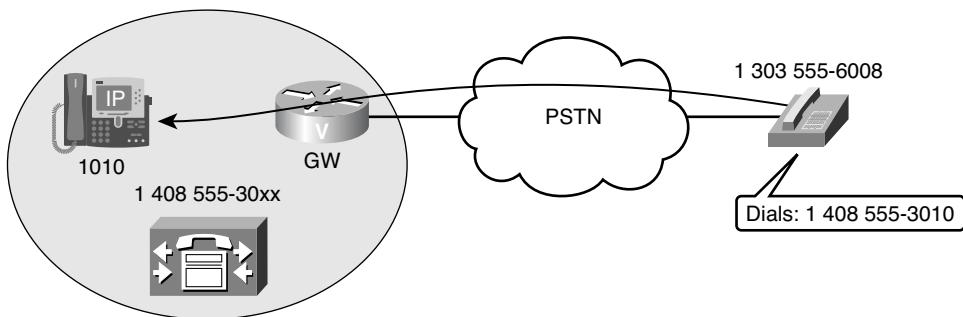


Figure 11-3 Incoming Call from the PSTN

1. The PSTN phone calls the full E.164 number of the destination. The call is received at the PSTN gateway with a called party number ten digits in length. Digit manipulation is performed to convert the inbound ten-digit called number to a four-digit number matching the internal dial plan. Digit manipulation might occur in the translation configuration of the gateway if the gateway is an H.323 or Session Initiation Protocol (SIP) gateway. Media Gateway Control Protocol (MGCP) gateways can perform digit manipulation on an individual endpoint basis using called party transformation patterns. Digit manipulation can be configured in CUCM if the gateways are H.323 or SIP using the same called party transformation patterns beginning with CUCM version 7.0.
 2. The called party number received from the PSTN can also be manipulated to align to the internal dial plan using a translation pattern that matches the called party number digits received from the provider. The translation pattern then applies any calling and called party digit manipulations in a manner very similar to the digit manipulation performed at the route list detail level of the route list. Translation patterns are unique in the respect that they do not forward calls to a trunk or gateway device. Translations are leveraged only to perform digit manipulation.

Translation patterns are normally not necessary to change the incoming called party E.164 number to an internal directory number unless the digits received from the carrier don't map directly to the internal dial plan. The calling party transformation mask of the translation pattern can be used to insert 91 into the calling party number, enabling callback functionality from the Cisco IP Phone's call history (missed and received calls). Calling party digit manipulation can be more granular if the call is coming in over ISDN Q.931 signaling or H.323 Q.931 signaling. At the time of this writing, SIP trunks do not support the passing of numbering plan type (subscriber, national, international, or unknown). Q.931 signaling used in ISDN and H.323 supports the passing of numbering plan type, allowing the calling party number to be transformed as follows:

- Calling number (prefix 9) for seven- or ten-digit dialing indicated by the “subscriber” numbering plan type.
 - Calling number (prefix 91) for 11-digit dialing indicated by the “national” number plan type.
 - Calling number (prefix 9011) for international dialing indicated by the “international” numbering plan type.

- Calling number (prefix 91) to the “unknown” numbering plan type. If most calls are received from international locations, or local seven- or ten-digit callers, change the unknown field to match the highest percentage of inbound call sources.

This step is optional because the Cisco IP Phone user can use the Edit softkey and edit the phone number from a call history list and manually dial the required codes to properly route the call.

3. The Cisco IP Phone receives the call or the call is forwarded as a result of the application of the call-forwarding configuration.

External Phone Number Mask

The external phone number mask is a directory number (DN) configuration attribute. The external phone number mask is leveraged in call routing to manipulate the internal directory number to digits that can be routed over the PSTN. The external phone number mask is configured on the Directory Number configuration page in CUCM Administration. The use of the external phone number mask is enabled in the route list detail calling party number digit manipulations. The external phone number mask can also be leveraged at the route pattern, translation pattern, calling party transformation pattern, and hunt pilot configurations. Automated alternate routing (AAR) uses the external phone number mask to change the internal dial plan into a PSTN-routable dial plan when rerouting intersite calls from the WAN to the PSTN. The external phone number mask of the first DN of the phone is also used for the following functions:

- To change the display of the main phone number at the top of the LCD screen. A DN of 15001 with an external phone number mask of 21255XXXX would result in a displayed phone number of 2125515001. Any user on the phone can instantly identify his PSTN direct inward dialing (DID) number by viewing the LCD of the phone.
- AAR technology uses the external phone number mask to manipulate digits for PSTN outbound dialing when bandwidth is not available for a guaranteed-quality call over the WAN (CAC). The AAR call will be rerouted out the PSTN using the full PSTN phone number of the destination as determined by the application of the external phone number mask.
- To change the display of the caller ID for all calls in which the call classification is Off-Net. The calling party number (caller ID) is changed to the full ten-digit DID phone number of the calling party.

Figure 11-4 displays the configuration of the external phone number mask at the Directory Number Configuration page. This page is accessed by navigating to the following in CUCM Administration:

Step 1. Choose Device > Phone.

Step 2. Insert the search criteria and click the Find button.

Step 3. Click the phone that has the required directory number (DN).

Step 4. Click the directory number.

Figure 11-5 displays the configuration option that is normally used at the route list detail level. The Calling Party Transformations section includes a check box to use the calling party's external phone number mask for the calling party presentation on the PSTN. This same option can be seen in various call-routing configuration elements.

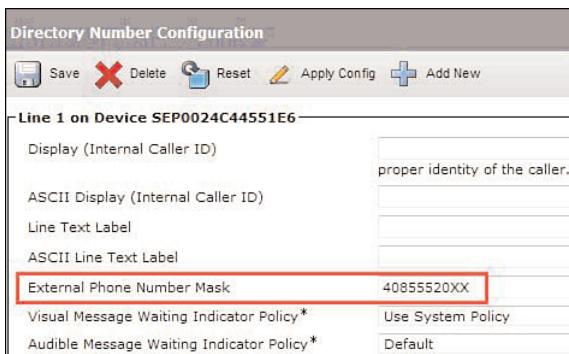


Figure 11-4 Directory Number Configuration: External Phone Number Mask

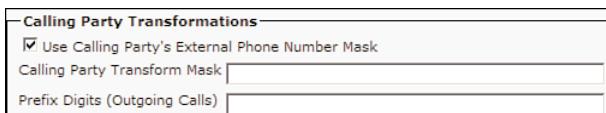


Figure 11-5 Route Pattern Configuration: External Phone Number Mask

Translation Patterns

CUCM uses translation patterns to manipulate digits before forwarding a call. A translation pattern normally requires another digit analysis attempt. Translation patterns and route patterns can be used to block patterns, but the default action is to attempt call routing.

Digit manipulation and translation patterns are used frequently in geographically distributed systems where office codes might not be the same for all locations. A uniform dialing plan can be created and translation patterns applied to accommodate the unique office codes at each location. Here are some additional examples where translation patterns can be leveraged:

- Security and operator desks (abbreviated dialing to PSTN locations enabling more productivity)
- Hotlines with a need for private line automatic ringdown (PLAR) functionality (security phones in elevators, phones used to access lab facilities, college campuses, financial trading markets, and so on)
- Extension mapping from a public to a private network

Translation patterns use route pattern style matching and transformation mask-based digit manipulation. The pattern resulting after the translation pattern is applied is then rerouted by the system, causing a second round of digit analysis. The new pattern can match another translation pattern where digit transformation can occur once again. Eventually, the call is routed to a device or blocked by CUCM. CUCM passes digits through translation patterns for only ten iterations to prevent call-routing loops. There are various call-routing loop-deterring mechanisms that are in the system by default.

Figure 11-6 illustrates the operation of a translation pattern. A translation pattern matches the called party number in a similar manner to the matching of a route pattern. The primary difference between route patterns and translation patterns is that translation patterns do not have a final path selection destination (route list, gateway, or trunk).

Translation patterns exist only to manipulate digits; they do not perform call routing.

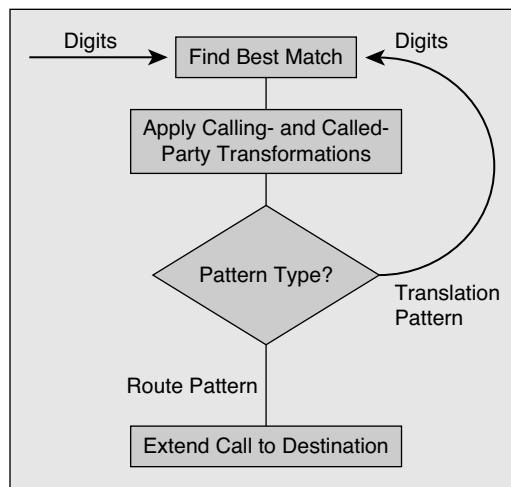


Figure 11-6 Translation Patterns

To configure a translation pattern, navigate to **Call Routing > Translation Pattern** in CUCM Administration.

Figure 11-7 is a screen capture of a translation pattern configuration. The translation pattern identifies the dialed digit string to match and the calling or called party transformation settings that should be applied.

If the **Block This Pattern** radio button is selected, a cause code must be selected. Choose a value from the drop-down menu:

- No Error
- Unallocated Number
- Call Rejected
- Number Changed

- Invalid Number Format
- Precedence Level Exceeded

Pattern

Route option

Transformation settings

Pattern Definition	
Translation Pattern	40855530XX
Partition	< None >
Description	(empty)
Numbering Plan	< None >
Route Filter	< None >
MLPP Precedence*	Default
Calling Search Space	< None >

Route Option	
<input checked="" type="radio"/> Route this pattern	
<input type="radio"/> Block this pattern	No Error
<input checked="" type="checkbox"/> Provide Outside Dial Tone <input type="checkbox"/> Urgent Priority	

Calling Party Transformations	
<input type="checkbox"/> Use Calling Party's External Phone Number Mask	
Calling Party Transform Mask	(empty)
Prefix Digits (Outgoing Calls)	(empty)
Calling Line ID Presentation*	Default
Calling Name Presentation*	Default

Connected Party Transformations	
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default

Called Party Transformations	
Discard Digits	< None >
Called Party Transform Mask	(empty)
Prefix Digits (Outgoing Calls)	(empty)

Figure 11-7 Translation Pattern Configuration

The transformation settings are not applicable if the Block This Pattern radio button is selected.

If the translation pattern contains an @ sign, a numbering plan and route filter can be selected to match certain number patterns of the selected numbering plan.

Translation patterns are processed as urgent priority by default. The Urgent Priority check box can be disabled beginning with CUCM 7.0. Prior versions of the product did not allow the urgent priority option to be disabled at the translation pattern configuration. An overlapping dial plan involving a translation pattern could result in call-routing issues. Translation patterns are ignored when performing analysis of the dial plan with the Dialed Number Analyzer (DNA) tool that is integrated into the Cisco Unified Serviceability web pages.

When the direct inward dialing (DID) range from the provider does not match the internal DN range, a translation pattern can be used to map the PSTN number to the internal DNs.

Figure 11-8 illustrates a scenario in which a company has a PSTN DID range of 408 555-1XXX, but the internal four-digit extensions use the four-digit range of 4XXX. The company uses a translation pattern that matches the assigned PSTN DID range of 408 555-1XXX. The called party transformation mask of 4XXX is applied to the translation pattern, resulting in a 4XXX called party number. CUCM applies the transformations and reanalyzes the resulting pattern. Eventually the call is routed to a device or explicitly rejected.

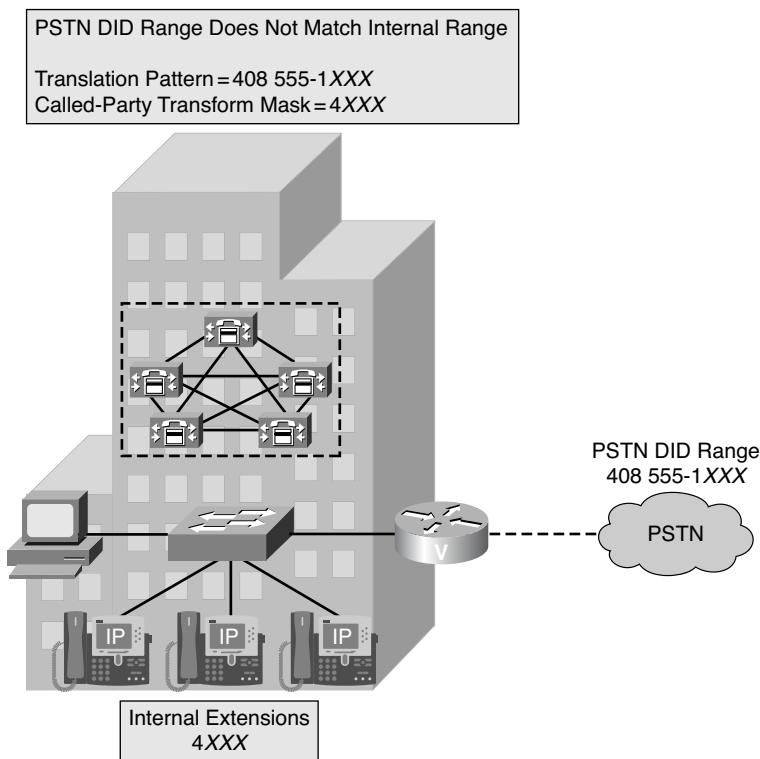


Figure 11-8 Translation Pattern Example

An additional translation pattern of XXXX with a called party transformation mask of 4111 can be used to route calls of unidentified internal extensions to the company operator. Many companies own large blocks of DID numbers that they are not currently using. Assume that the DN of 4333 no longer exists in the system because the person that had the phone number won the lottery and decided that he was not going to work anymore. Because of cost-cutting measures implemented, a replacement is not hired and the Cisco IP Phone is reused with a unique configuration for a different department. When a customer calls that user, the customer will receive a reorder tone unless a call forward

unregistered (CFUR) number has been configured for the DN that receives the call. If a called party number of 408 555-1333 is received from the PSTN, the call will be routed to DN 4333. If a DN of 4333 no longer exists in CUCM, the generic XXXX translation pattern will be matched and the call is routed to the company operator at extension 4111. The company operator instructs the outside caller that the employee no longer works for the company and tries to assist the caller in resolving his issue.

Transformation Masks

Dialing transformations allow the call-routing component to modify either the calling (initiator) or called (destination) digits of a call. Transformations that modify the calling number (automatic number identification [ANI]) are calling party transformations; transformations that modify the called party (dialed digits) are called party transformations. Dialed Number Identification System (DNIS) is a public standard implemented in the PSTN for modifying called party numbers.

Digit translation is possible in CUCM mainly through the Transformation Mask feature that can be found in various configuration options in CUCM (for example, route list details and translation pattern). CUCM overlays the calling or called party number with the transformation mask so that the last character of the mask aligns with the last digit of the calling or called party number. CUCM uses the original calling or called party digit of the source number anytime the mask contains an X. The X acts as a binary OR function. If the number is longer than the mask, the mask will add extra digits to the original calling or called party pattern.

Figure 11-9 illustrates an approach typically used to change the calling party (ANI) of internal directory numbers when he or she makes calls that are routed to the PSTN. The five-digit extension of 45000 in Figure 11-9 is transformed into a ten-digit pattern for the purposes of caller ID (ANI) on the PSTN. There is a distinction between ANI and caller ID that I would like to point out. Caller ID (CLID) refers to the presentation of the calling party name and number, whereas automatic number identification (ANI) refers only to the calling number. The mask of 8086236XXX has been applied to 45000 in Figure 11-9, resulting in 45 being replaced with 36, while the first five digits of 80862 are prefixed before the number so that users connected to the PSTN can return phone calls to the presented calling party number.

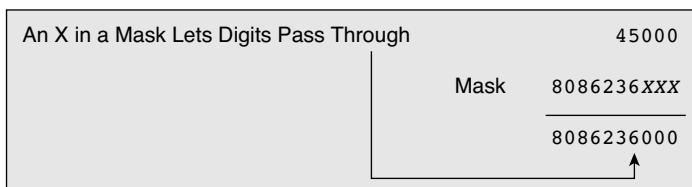


Figure 11-9 Transformation Mask Operation

Figure 11-10 illustrates the process in which a ten-digit number from the PSTN could be converted to a five-digit number using transformation masks. This process would be useful if the incoming called party from the PSTN gateway to CUCM was ten digits long, but incoming calls had to be converted to an abbreviated five-digit internal dial plan. Masks are always processed from right to left in CUCM. Transformation masks can be used to manipulate either the calling or called party number. A ten-digit pattern with a five-digit mask applied to it will result in a five-digit number. Figure 11-10 illustrates a ten-digit pattern with a five-digit pattern of 45XXX, which indicates that the last three digits will not change but the leading two digits will be set to 45, regardless of the incoming pattern.

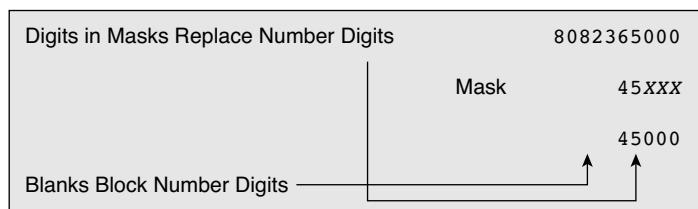


Figure 11-10 Transformation Mask Operation

Transformation masks are configurable at various CUCM configuration levels including route patterns, translation patterns, and route lists (per route group).

The calling and called party transformation settings are assigned to route groups in the route list details of the route list that the route pattern is pointed to. Route pattern transformations apply only when a route pattern is pointed directly to a gateway. Route patterns are normally pointed to a route list. Multiple route patterns can point to the same route list, but multiple route patterns cannot point directly to the same gateway.

Inserting gateways into route groups allows the gateways to be used for many different route patterns.

Most intersite calls in private companies are routed over WAN links as Voice over IP (VoIP) calls, but routed over PSTN links if the WAN is down or congested. Distributed Multi-Cluster Call Processing architectures require call routing to be configured for all intersite calls that cross cluster boundaries. Intercluster calls are routed over trunks in CUCM. H.225 trunks, SIP trunks, nongatekeeper-controlled intercluster trunks, and gatekeeper-controlled intercluster trunks are covered in more detail in *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide*.

The call routing between sites that belong to different CUCM clusters is normally configured to have a PSTN route group and an IP WAN route group. The IP WAN route group includes one or more intercluster trunks (ICT) or SIP trunks, while the PSTN route group contains one or more gateway endpoints (MGCP) or gateway devices (H.323/SIP) that connect the cluster to the PSTN. CUCM will forward the internal abbreviated dialing extension number if proper digit manipulation has not been configured. CUCM routes calls to a gateway in the PSTN route group. Proper digit manipulation requires that the

calling pattern reflect a phone number that can be called back on the PSTN and that the dialed digits are properly routed.

CUCM Digit Prefix and Stripping

The Digit Prefix feature prepends digits to the beginning of a dialed number. Any digits that can be entered from a standard phone (0 through 9, *, and #) can be prepended to the calling or called party numbers. Digit prefixing is available for either the calling or called party number and can be configured at the route pattern, route list, or translation pattern configuration levels.

Figure 11-11 displays the calling and called party prefix configuration available at the route pattern, route list, and translation pattern configuration levels.

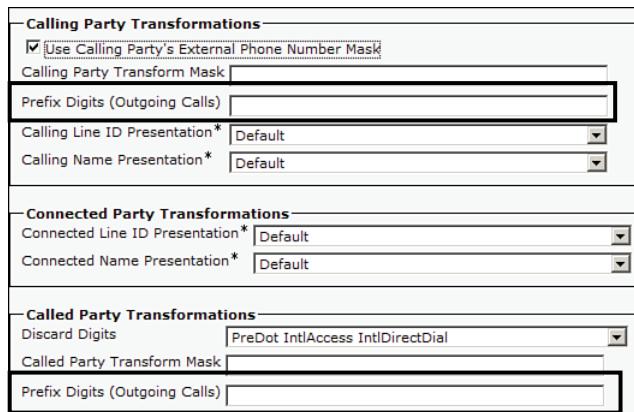


Figure 11-11 *Digit Manipulation: Prefix Digits*

Digit discard instructions (DDI) remove parts of the dialed digit string before passing the number on to the adjacent system. A DDI removes a certain portion of the dialed string (called party). Access codes are typically used to make a phone call that will be routed to the PSTN. The PSTN switch does not expect the access code, so the access code must be stripped out of the called party number before sending the call to the carrier.

Digit stripping is configured in the Called Party Transformations section by selecting a Discard Digits setting from the drop-down menu. Discard digits can be configured at the route pattern and at the route group details level of the route list.

The entire range of discard digits are supported if the @ wildcard pattern is used in the route pattern. If the @ wildcard is not used in the route pattern, only the <None>, NoDigits, PreDot, PreDot Trailing #, and Trailing # discard digits can be used.

Table 11-2 displays different digit discard instructions and their effects on dialed digits leveraging a route pattern of 9.5@. 9.5@ would not be used in most deployments, but it is

a good example that can use various DDIs that are not available without the @ wildcard character. The digits that would be discarded appear in bold in Table 11-2.

The PreAt, 11D/10D@7D, 11D@10D, IntlTollBypass, and 10-10-Dialing complex DDIs are not available without the @ symbol in the route pattern.

Table 11-2 *Digit Discard Instructions 9.5@*

Instructions	Discarded Digits	Used For
PreDot	95 1 214 555 1212	Removes access code
PreAt	95 1 214 555 1212	Removes all digits that are in front of a valid numbering plan pattern
11D/10D@7D	95 1 214 555 1212	Removes PreDot/PreAt digits and local or long-distance area code
11D@10D	95 1 214 555 1212	Removes long-distance identifier
IntlTollBypass	95 011 33 1234 #	Removes international access (011) and country code
10-10-Dialing	95 1010321 1 214 555 1212	Removes carrier access (1010) and following carrier ID code
Trailing #	95 1010321 011 33 1234 #	Removes the # sign for PSTN compatibility

Note Trailing # is automatically removed by default in CUCM. You can turn off this behavior by changing the Strip # Sign from Called Party Number CUCM service parameter to False.

Figure 11-12 illustrates a call in which CUCM applies the PreDot DDI to the 9.8XXX route pattern, resulting in the access code (9) being stripped out of the dialed digits. The resulting four digits of 8123 are routed to the traditional PBX across a gateway or trunk device. The PBX analyzes the called party number and forwards the call to the necessary device. If the 8123 pattern did not match on a device in the PBX, it is very probable that the PBX would route the call back to CUCM, causing a call-routing loop. The PBX can have a route pattern-like configuration that routes all calls four digits in length beginning with an 8 (8XXX) to CUCM to accommodate phones that have been migrated to CUCM. CUCM probably has a route pattern of 8XXX to accommodate phones that have not been migrated from the PBX yet. If neither system has line 8123 configured on a device, a call-routing loop will normally occur. CUCM has service provider call-loop protection mechanisms that will only process each call reference value a certain number of times within a time interval. Supplementary service actions (call forward, conference, park, and so on) result in a new call reference value.

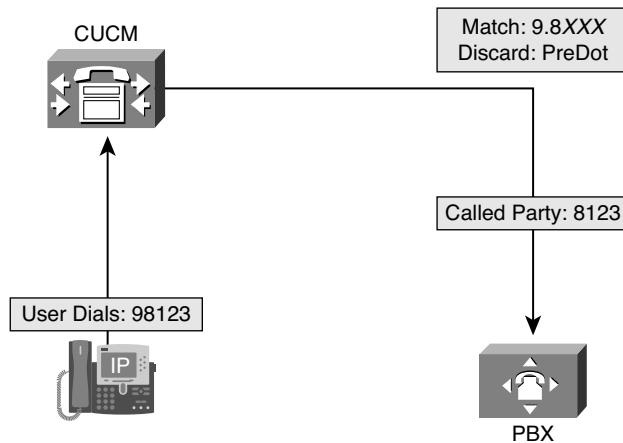


Figure 11-12 PreDot Digit Discard Instructions

Figure 11-13 illustrates the PreDot 10-10-Dialing DDI applied to the 9.@ route pattern. The PreDot 10-10-Dialing compound DDI strips the access code (9), the carrier selection code (1010), and the carrier identification code (288) from the called party number. The resulting 11-digit long-distance called party number of 1 214 555-1212 is then routed to the gateway device. Removing the 10-10 dialing parameters guarantees that long-distance calls will be billed by the preferred carrier. Most organizations contract a minimum number of long-distance minutes per month with the long-distance carrier. Although end users might believe that they are saving the company money by routing the call across an advertised carrier, they might be incurring additional costs to the organization. This compound DDI works only if the @ symbol is part of the route pattern. Translation patterns could perform similar functionality without introducing a route pattern with the @ symbol into the dial plan.

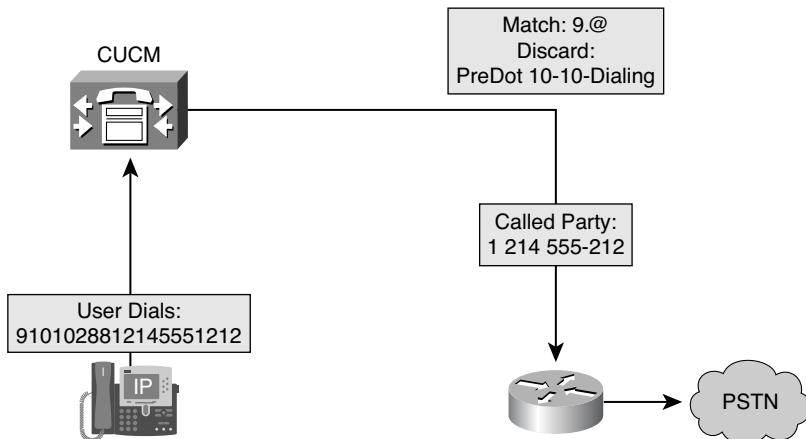


Figure 11-13 Compound Digit Discard Instructions

Significant Digits

The Significant Digits feature instructs CUCM to analyze the configured number of digits (from right to left) of the called number for incoming calls received by a gateway or trunk. Setting the significant digits to 5 on a PSTN gateway instructs CUCM to ignore all but the last five digits of the called party number for routing incoming gateway or trunk calls. The Significant Digits feature is the easiest approach to convert incoming PSTN called numbers to an internal extension, but the setting affects all calls received from the gateway. The Significant Digits setting also assumes that the internal dial plan is using the last five digits (or other number specified) of the DID block as the internal extension (directory number). The Significant Digits setting also cannot accommodate variable-length extension numbers on the internal network. Variable-length internal extensions could also lead to a variety of overlapping dial plan challenges.

The PSTN gateway illustrated in Figure 11-14 is using the Significant Digits setting in CUCM to instruct CUCM to only analyze the last four digits of the incoming call with a called party number of (408) 555-1010 received from the gateway. The significant digits configuration is available in the gateway or trunk CUCM Administration configuration pages under the Incoming Calls section (toward the bottom of the gateway/trunk web page).

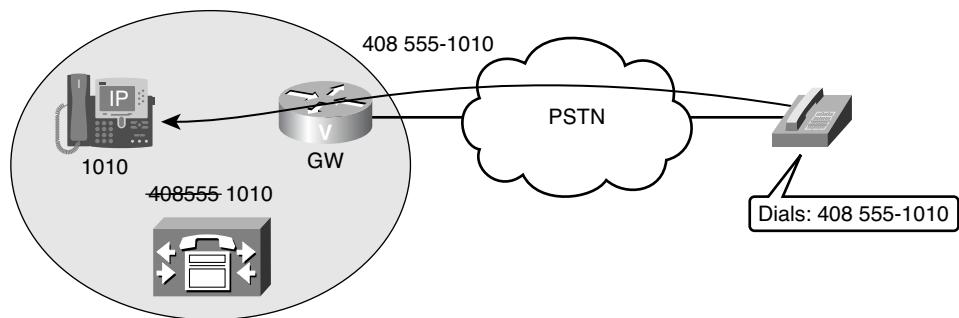


Figure 11-14 Significant Digits Example

Note In contrast to using translation patterns to map E.164 numbers to internal DNs on incoming PSTN calls, this solution performs only one call-routing table lookup. The Significant Digits feature is a more processor-friendly alternative than translation patterns, but this approach will not allow the same flexibility as translation patterns.

Cisco Unified Communications Manager Global Transformations

CUCM version 7.0 introduced number normalization and number globalization support for E.164-based call routing. Calling and called party transformation patterns extend the power of CUCM's digit manipulation. Calling and called party transformation patterns have the following characteristics:

- Transformations are implemented in the global CUCM configuration.

- Calling and called party transformation patterns are put into partitions.
- Identical transformation patterns with different transformation settings can exist if they are put into different partitions. Partitions separate dial plan elements so that each pattern will only be evaluated if that partition is in the calling party's Calling Search Space (CSS).
- Gateways and trunks can be configured with calling and called party transformation CSSs. Calling party transformations are supported at the Cisco IP Phone, but called party transformations are not supported on the Cisco IP Phone.
- The transformation CSS determines which transformation patterns are visible to the device.

Calling and called party transformation patterns are applicable only to calls from CUCM to gateways, trunks, and phones. A call to a phone is usually not considered to be an outgoing call from a user's perspective. Think of a phone as the outgoing call leg of an internal call from another phone or incoming call.

Instead of configuring an individual calling and called party transformation CSS at each device, you can configure the devices to use calling and called party transformation CSSs configured at the device pool level. No transformation is performed if the device and associated device pool are not configured with a transformation CSS.

Calling and called party transformations are not applicable to calls that CUCM receives from devices (incoming call legs). Figure 11-15 illustrates called party transformations for four different phone numbers.

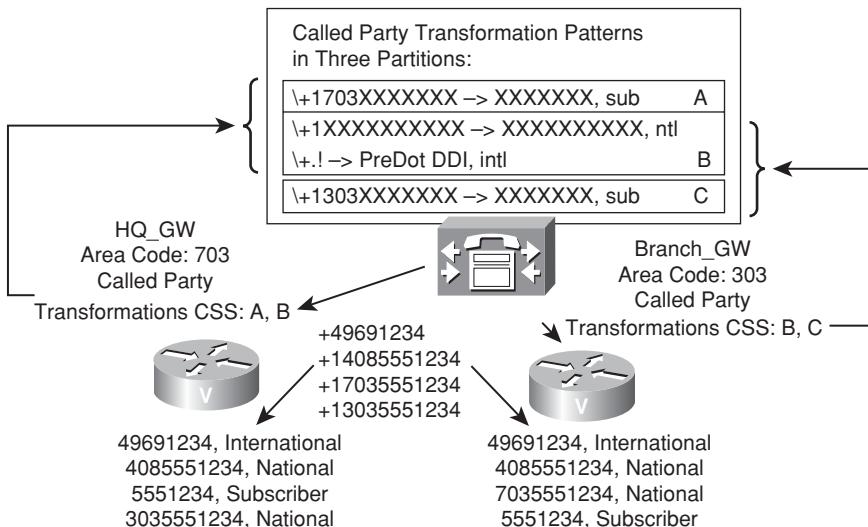


Figure 11-15 *Called Party Transformation Patterns*

Calling and called party globalized call routing has been configured in Figure 11-15, as indicated by the leading + character shown in the following four called party number strings:

```
+49691234  
+14085551234  
+17035551234  
+13035551234
```

Transformations patterns only apply to outgoing call legs. Figure 11-15 is an example of globalized outbound call routing. Only the localization of the called number at the selected outgoing gateway is considered in this example.

Figure 11-15 is an example with four called party transformation patterns in three partitions at headquarters (HQ_GW) and branch (Branch_GW) sites. Partition A is specific to HQ (local area code 703), while partition B includes generic transformation patterns used by both HQ and Branch. Partition C is specific to the Branch site (local area code 303). The HQ gateway is configured with a called party transformation CSS that includes partitions A and B. The Branch gateway is configured with a called party transformation CSS that includes partitions B and C.

The transformation pattern in partition A modifies all 11 called party number information into a seven-digit called party number. The pattern also configures the numbering plan type to subscriber. Ten- and 11-digit dialing is normally categorized with a numbering plan type of national. Some providers require the numbering plan type to be set to the proper numbering plan type or they will reject the call. The transformation pattern in partition C provides the same function for called party numbers that are within the Branch area code of 303. Partition B is a partition that is shared between both the HQ and Branch transformation CSSs. Partition B includes two transformation patterns:

```
\+1XXXXXXXXXXX  
\+.!
```

The first pattern matches on all 11-digit patterns beginning with the E.164 + character used to route international calls followed by a 1 and any ten digits. This pattern represents all U.S. area codes within a globalized route plan. The second pattern represents all other possible numbers that begin with the + character followed by two digits or more.

Calls to the following four called party numbers are transformed differently depending on the gateway to which they are routed:

- +49691234 is matched and transformed on both gateways to 49691234 with a numbering plan type set to international. If the ISDN provider does not support number types, a prefix of 011 must be used to indicate the fact that this is an international call.
- +14085551234 is matched and transformed on both gateways to 4085551234, with type national. If the ISDN provider does not support number types, a prefix of 011 must be used.

- +17035551234 is matched and transformed on the both gateways, but the outbound calls match on different transformation patterns because of the different CSSs used at the respective gateways. The +17035551234 called party number is routed out the HQ gateway as 5551234 with a numbering plan type of subscriber. The Branch gateway matches the \+1XXXXXXXXXX with a number plan type of national. If the ISDN provider does not support numbering plan types for international call routing, a prefix of 011 must be used to route an international call.
- +13035551234 is matched and transformed on the Branch gateway with the \+1303XXXXXXX transformation pattern. The called party number is sent out the HQ gateway with a called party number of 5551234 and a numbering plan type of subscriber. The called party number is sent out the Branch gateway as 303 5551234 and a number plan type of national. If the ISDN provider does not support number types, a prefix of 011 must be used.

Figure 11-16 shows an example of calling party number transformation using calling party transformation patterns in different partitions. The HQ and Branch gateways and phones are configured with different calling party transformation CSSs to change the calling number differently depending on which gateway processes the call. Only the localization of the calling party number at the HQ outgoing gateway is considered in this example.

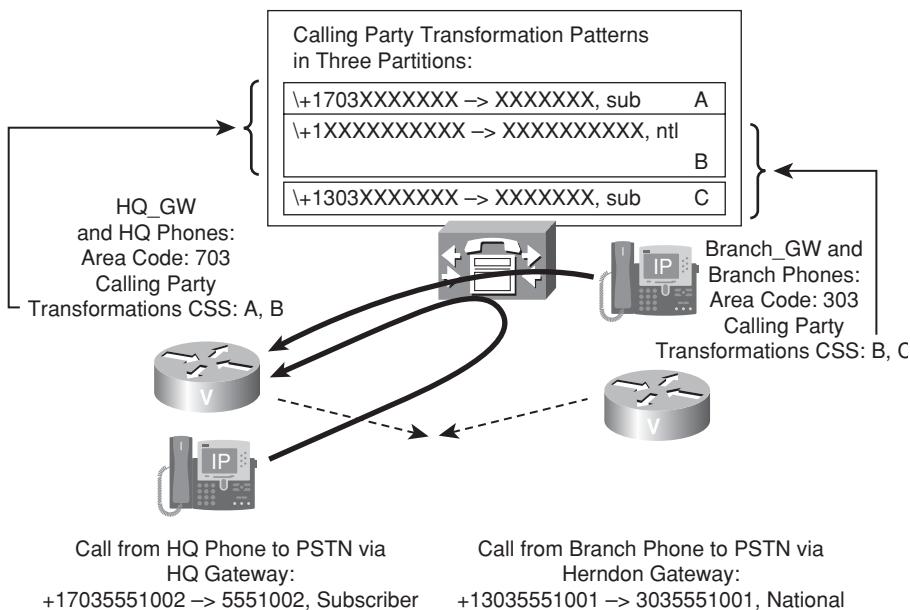


Figure 11-16 Calling Party Transformation Patterns in Partitions

There are three calling party transformation patterns in three different partitions. Partition A is specific to HQ (local area code 703), while partition B includes a generic transformation pattern for all 11 digit numbers in the North American Numbering Plan (NANP). Partition C is specific to the Branch (local area code 303).

The HQ gateway phones are configured with a calling party transformation CSS that includes partitions A and B, while the Branch gateway and phones have a calling party transformation CSS that includes partitions B and C. The transformation pattern in partition A modifies all HQ globalized numbers to a seven-digit number with a numbering plan type of subscriber. The transformation pattern in partition C provides the same functionality for local calls at the Branch site. Partition B is used by both the HQ and Branch transformation CSSs. Partition B includes the transformation pattern of \+1XXXXXXXXXX and represents all area codes in the NANP.

The calling party numbers will be transformed as follows:

- A +17035551002 call from an HQ phone to the PSTN through the HQ gateway is transformed to 5551002 with a numbering plan type of subscriber.
- A +13035551001 call from a Branch phone to the PSTN through the HQ gateway is transformed to 3035551001 with a numbering plan type of national.

Calling Party Transformation Pattern Configuration

Calling party transformation patterns are configured in CUCM Administration. Choose Call Routing > Transformation > Transformation Pattern > Calling Party Transformation Pattern. Click the Add New button to create a new calling party transformation pattern.

In the pattern configuration, define a matching pattern and assign a partition to this pattern. Specify calling party transformations in the same way as the route pattern, route list, and translation pattern configurations covered earlier in this chapter. Figure 11-17 is a screen capture of the Calling Party Transformation Pattern Configuration page in CUCM Administration.

Figure 11-17 Calling Party Transformation Pattern Configuration

Called Party Transformation Pattern Configuration

Called party transformation patterns are configured in CUCM Administration. Choose Call Routing > Transformation > Transformation Pattern > Called Party Transformation Pattern. Click Add New to create a new called party transformation pattern. Figure 11-18 is a screen capture of a Called Party Transformation Pattern Configuration page.

Pattern Definition	
Pattern*	\+.
Partition	DNIS-Trans_PT
Description	Localization of Called Number
Numbering Plan	< None >
Route Filter	< None >
<input checked="" type="checkbox"/> Urgent Priority	
Called Party Transformations	
Discard Digits	PreDot
Called Party Transformation Mask	
Prefix Digits	
Called Party Number Type*	International
Called Party Numbering Plan*	Cisco CallManager

Figure 11-18 Called Party Transformation Pattern Configuration

Transformation Calling Search Space

The transformation Calling Search Space (CSS) configuration is identical to the CSS configuration used to configure class of service (CoS) restrictions that was covered in the last chapter. The CSS is applied differently to restrict the patterns that are matched for the purpose of digit transformation. During digit analysis, CUCM treats transformation patterns similar to any other pattern in the call-routing database. Independent CSSs are normally created for the purpose of performing calling and called party digit transformation using transformation patterns. Calling and called party transformation CSSs can be applied in the phone, gateway, and device pool configuration locations of CUCM Administration.

Figure 11-19 is a screen capture of a CSS configuration that will be used as a transformation CSS. Transformation CSSs normally only have one partition.

Figure 11-20 illustrates the application of the CSS created in Figure 11-19 as a calling party transformation CSS on a Phone Configuration page in CUCM Administration.

Incoming Number Settings

Incoming transformation settings have the following characteristics:

- They allow the configuration of digit prefixes, digit stripping, and transformations to be applied to calling and called party numbers for calls inbound to the CUCM cluster. Different settings can be configured per number plan type (unknown, subscriber, national, and international) if this information is in the call signaling.

- Incoming calling and called party settings can be configured at the device, device pool, and/or global service parameter configuration levels in CUCM Administration.
- Incoming calling and called party setting apply to calls received from gateways and trunks. Incoming calling and called party settings are not applicable to calls that are received from phones. The external phone number mask of directory numbers is used to globalize the calling party number from Cisco IP Phones.

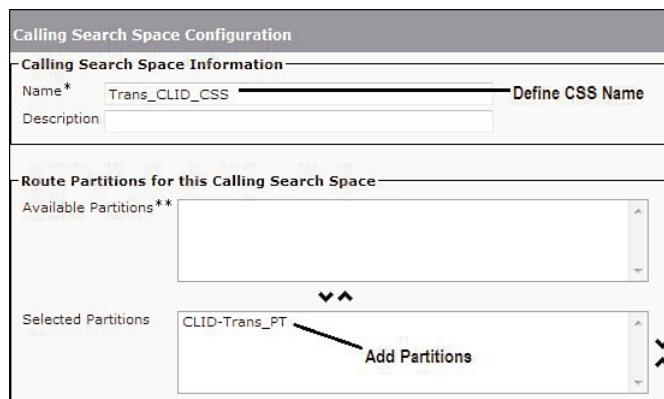


Figure 11-19 Transformation CSS

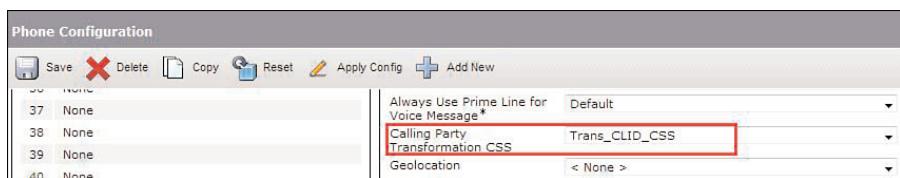


Figure 11-20 Transformation CSS Application

H.225 trunks and H.323 gateways support incoming calling and called party settings based on numbering plan type, but Media Gateway Control Protocol (MGCP) gateways support only incoming calling party settings based on numbering plan type. Session Initiation Protocol (SIP) does not support numbering plan types.

Incoming Calling Party Prefix Example: Globalization of Calling Number

Figure 11-21 shows an example of incoming calling party digit transformation for calling party number globalization using the E.164 + international operator pattern. Figure 11-22 is performing digit transformation based on the numbering plan type provided in the incoming call signaling from the provider in Hamburg, Germany.

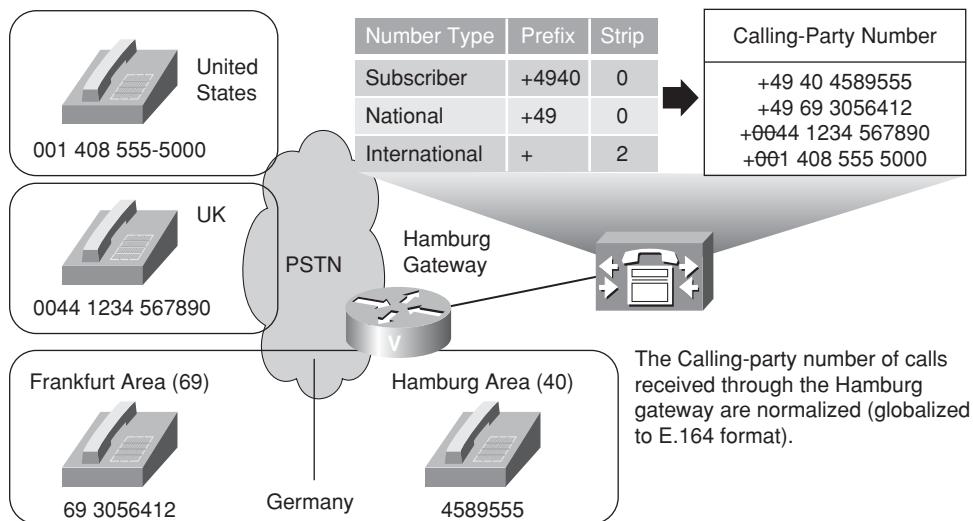


Figure 11-21 Globalization of Calling Number

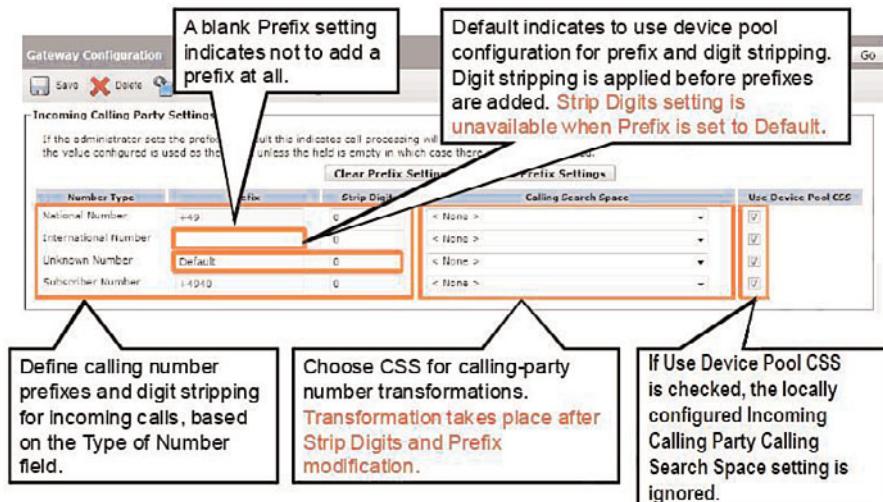


Figure 11-22 Gateway Calling Party Settings

Gateway Incoming Calling Party Settings Configuration

The gateway is configured with the following incoming calling party number digit manipulation:

- Prefix +4940 for calls that are received with a numbering plan type of subscriber.
- Prefix +49 for calls that are received with a numbering plan type of national.

- Prefix a + and strip the leading two digits of the calling party number for calls that are received with a numbering plan type of international.

Incoming calling party settings can be configured at the bottom of the gateway or trunk configuration level of CUCM Administration. Figure 11-23 is a screen capture of the configuration required to perform the digit transformation illustrated in Figure 11-22.

Device Pool Incoming Calling and Called Party Transformation Calling Search Space

Selecting the Use Device Pool CSS check box causes CUCM to ignore any transformation CSS configured at the gateway or trunk level. The transformation CSS defined at the device pool that is associated to the gateway or trunk is applied instead.

The configuration of incoming calling and called party settings in the device pool is nearly identical to the configuration of these settings on gateways or trunks.

The only differences are the following:

- The device pool does not include a Use Device Pool CSS check box.
- If the Default keyword is used in any Prefix field, the corresponding incoming calling or called party settings set at the Cisco CallManager service parameter configuration level are applied.

Transformation Examples

Multiple transformations can take place when placing a phone call. External phone number masks instructs the call routing of CUCM to apply the external phone number mask to the calling party directory number (DN) to pass caller ID information when calls are routed across a gateway to the PSTN. The external phone number mask is applied on an individual line basis through the DN configuration.

Figure 11-23 illustrates the multiple levels of calling party manipulations that are possible if the company wants to change the calling party number information so that a call appears to be coming from a main support number instead of an end user's extension (DN). The DN of 35062 will appear as 214 713-5062 when calls are routed through a gateway if only the external phone number mask is applied to the DN. The X character in the external phone number mask will pass through the original digits, while any digit specified in the mask will override the original number. If a mask applies more digits than the original number, a larger number will result. If the mask applies less digits than the original pattern, a smaller pattern will result. A calling party transformation mask has been applied at the route list detail level that changes the calling party number.

Figure 11-24 is an example of called party modifications where the user dials the pattern 10-10-321 before her phone number in an effort to save the company money on the phone call. The route pattern of 9.@ was matched by the dialed digits of 9 10-10-321 1 808 555-1221. The called party digit discard instruction (DDI) was configured to remove

the 10-10 dialing. The resulting number is applied to the called party transformation mask, which consists of ten X wildcard characters. The access code of 9 and long-distance code of 1 have also been removed from the dialed digits. An 8 is prefixed as a new access code because the call can be routed to another system like a traditional PBX where an 8 is required as an access code to route the call to the PSTN.

Directory Number	35062
External Phone Number Mask	21471XXXXX
	2147135062
Calling-Party Transformation Mask	40885XX000
Caller ID	4088535000

Figure 11-23 Calling Party Transformation Mask Example

Dialed Number	9 10-10-321 1 808 555-1221
Discard Digits	10-10-Dialing
	9 1 808 555-1221
Called-Party Transformation Mask	XXXXXXXXXX
	808 555-1221
Prefix Digits	8
Called Number	8 808 555-1221

Figure 11-24 Called Party Digit Manipulation

Figure 11-25 is an example where the Cisco Unified Communications (UC) TAC support group in Richardson, Texas, is placing calls to Cisco TAC in San Jose, California. The corporate policy is to not allow direct calls to members of either support team. The calling and called party numbers will be manipulated to reflect the main hunt pilot used to distribute calls (call coverage) to support group members at each site:

1. User A at extension 5062 dials 91234.
2. The route pattern of 9.1XXX is matched against the dialed digits (called party).
3. A DDI of PreDot is applied to the called party. The resulting called party number is 1234.
4. A calling party transformation mask of X000 is applied to caller 5062.
5. The caller ID at the destination will now appear as if the call were placed from the hunt pilot of 5000 in Richardson, Texas.
6. A called party transformation mask of X000 is applied to the dialed digits. 1234 is applied to the mask, and the resulting number is 1000.
7. San Jose receives a call destined for extension 1000 with a caller ID of extension 5000.

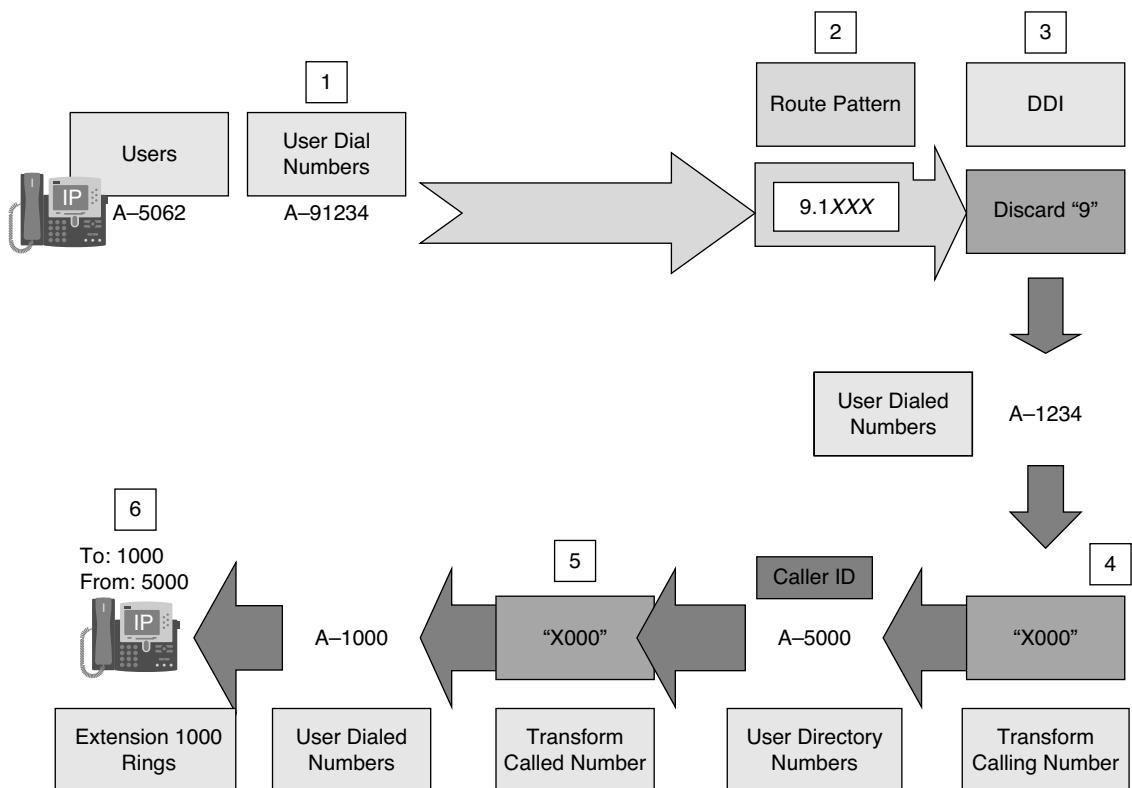


Figure 11-25 Complex Digit Manipulation

Three levels of digit-manipulation options are available for outbound calls:

- Digit manipulation that is configured on the route pattern (not used if the route pattern is routed to the route list)

- Digit manipulation that is configured at the route list detail level
- Digit manipulation that is configured by using a transformation CSS on the gateway/trunk or device pool

The three levels of digit manipulation are not cumulative. Only one level of digit manipulation will be applied. The hierarchy for these digit manipulations are as follows:

1. Digit manipulation settings on the route pattern take effect only when the route list details do not have any defined digit manipulations. A transformation CSS applied at the gateway/trunk or device pool will also cause the digit manipulations applied at the route pattern level to be skipped.
2. If the transformation CSS at the gateway or trunk matches, but the route list details have configured digit manipulations, the manipulations configured at the route list details are used. Route pattern digit manipulations are ignored.
3. If any manipulation matches through a gateway or trunk transformation CSS, all other digit manipulations are ignored.

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- Digit manipulation is an essential dial plan function. It is mandatory to provide the correct called number to the PSTN and present appropriate calling party numbers on IP phones.
- Depending on the call flow, different methods and configuration elements can be used to manipulate calling and called party numbers.
- CUCM provides a variety of digit manipulation configuration elements, such as transformation masks, translation patterns, incoming calling party prefixes, and so on.
- CUCM external phone number masks can be used to display the full DID number on Cisco IP Phones. The external phone number masks also provide calling party modification for calls sent out to gateways or trunks.
- CUCM translation patterns provide powerful functionality to manipulate dialed digits and calling party numbers for any type of call.
- CUCM transformation masks are an integral part of digit manipulation at route patterns, translation patterns, and so on.
- CUCM digit stripping provides an easy way to apply DDI to route patterns or translation patterns.
- CUCM significant digits functionality allows simple called party number length normalization on incoming calls from gateways or trunks.
- CUCM global transformations provide a flexible and scalable way to implement globalization and normalization for functions such as globalized call routing.

- CUCM incoming number prefixes are used to modify incoming called and calling party numbers, based on their Type of Number setting.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. The external phone number mask modifies which of the following for calls routed to the PSTN?
 - a. ANI
 - b. DNIS
 - c. Caller ID name
 - d. Route pattern
2. What dial plan element is used to manipulate digits when a route pattern can be routed to multiple devices?
 - a. Route pattern
 - b. Route list
 - c. Route group
 - d. Gateway
 - e. Trunk
3. Which of the following items do external phone number mask configurations not have an effect upon?
 - a. Automatic number identification
 - b. Automatic alternate routing
 - c. Extension mobility
4. Calling party modifications change which portion of a phone number?
 - a. ANI
 - b. DNIS
5. Called party modifications change which portion of a phone number?
 - a. ANI
 - b. DNIS
 - c. RDNIS
 - d. Original calling party

- 6.** Which of the following items is processed as urgent priority by default?
 - a.** Directory numbers
 - b.** 911
 - c.** Route patterns
 - d.** Translation patterns
- 7.** Which of the following patterns does the 10-10-Dialing digit discard instruction apply to?
 - a.** 9!
 - b.** 9.[2-9]XXXXXX
 - c.** 9.@
 - d.** 9.1[2-9]XX[2-9]XXXXXX
- 8.** Which of the following digit discard instructions can be applied to a route pattern of 9.1[2-9]XX[2-9]XXXXXX?
 - a.** 10-10-Dialing
 - b.** 11D@10D
 - c.** PreDot
 - d.** PreDot 11D@10D
- 9.** A directory number of 11001 with an external phone number mask of 212551XXXX would result in what phone number?
 - a.** 11001
 - b.** 212 551-1001
 - c.** 212 551-100X
 - d.** 212 551-1001
- 10.** A number of 212 555-1212 with a called party transformation mask of 646XXX3456 would result in which of the following numbers?
 - a.** 212 555-1212
 - b.** 646 555-1212
 - c.** 646 555-3456
 - d.** 212 646-1212

This page intentionally left blank

Chapter 12

Call Coverage

Upon completing this chapter, you will be able to describe and configure call-coverage components in Cisco Unified Communications Manager (CUCM) and be able to meet the following objectives:

- Identify call-coverage options in CUCM
- Describe call forwarding, shared lines, and call pickup
- Describe call-hunting implementation in CUCM
- Describe call-hunting options and line-group distribution algorithms
- Describe the process of call hunting
- Implement call hunting in CUCM

Many businesses have sales or service departments that handle inbound calls from customers. These businesses typically need several phone lines and a way to make the lines work together in a cohesive manner. If a representative is busy or not available, incoming calls to the group will rotate to available members of the group. The call is distributed in this way until it is answered or forwarded to an auto-attendant or voicemail. Hunt groups are the mechanisms that help these businesses manage inbound calls. A *hunt group* is a group of telephone lines that are associated with a common number. When a call comes in to the number associated with the hunt group, the call cycles through the group of lines until an available line is found. This process is known as *hunting*.

This chapter describes how to implement hunt groups and enable the other call-coverage features such as call forwarding, shared lines, and call pickup.

Call Coverage

Call coverage is part of the dial plan. It ensures that all incoming calls are answered. The following call-coverage features are typically implemented for individuals:

- **Call forwarding:** If the called phone does not answer the call, the call should be forwarded to another phone or voicemail.
- **Shared lines:** A shared line is a directory number (DN) that is assigned to more than one device, allowing the call to be accepted on more than one phone.
- **Call pickup:** Call pickup allows a call that is ringing on a phone to be picked up at another phone.

In addition, there is a more complex and highly flexible feature providing call coverage called *call hunting*. Call hunting is based on a pilot number, which if directly called or used as a call-forward target, allows hunting through multiple line groups. Several hunting algorithms exist, ranging from a round-robin selection of group members to a broadcast option that rings all members of a line group.

Call Forwarding

There are three primary types of call forwarding:

- **Call Forward All (CFA):** The CFA feature forwards all calls unconditionally. CFA can be configured by the phone user from either the user web page or at the phone itself. If CFA is configured, the call is forwarded immediately without ringing the originally dialed phone. The CUCM administrator can also configure the CFA target.
- **Call Forward No Answer (CFNA):** CFNA forwards calls if the call is not answered within a specified amount of time. CFNA can be configured by the administrator in CUCM Administration or by the phone user from the user web page.
- **Call Forward Busy (CFB):** CFB forwards calls that are received while the IP phone is in use with another call. CFB can be configured by the administrator in CUCM Administration or by the phone user from the user web page.

The administrator can configure separate Calling Search Spaces (CSS) for each call-forward type. For CFNA and CFB, different CSSs can be set for internal (on-net) calls and for external (off-net) calls. For CFA, a primary and a secondary CFA can be configured. These two get concatenated like a device and line CSS. For all call-forward scenarios, the corresponding call-forward CSSs are used; line and device CSSs are ignored. Therefore, if the system uses partitions, it is recommended to always set call-forward CSSs because otherwise forward operations are likely to fail. Figure 12-1 illustrates call forwarding.

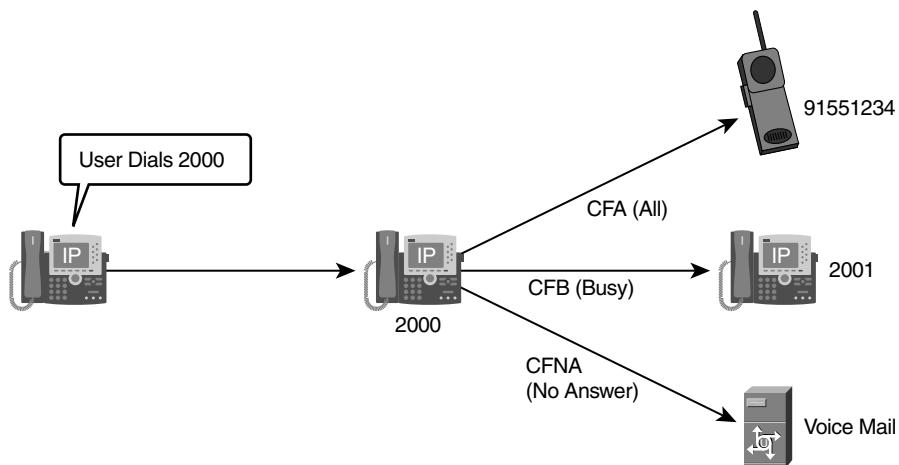


Figure 12-1 Call Forwarding

Shared Lines

A shared line is implemented by assigning the same DN to multiple phones within the same partition. If the number is called, all phones that are configured with this shared line number ring. The first user who accepts the call is connected to the caller, and all other phones stop ringing. Figure 12-2 illustrates shared lines.

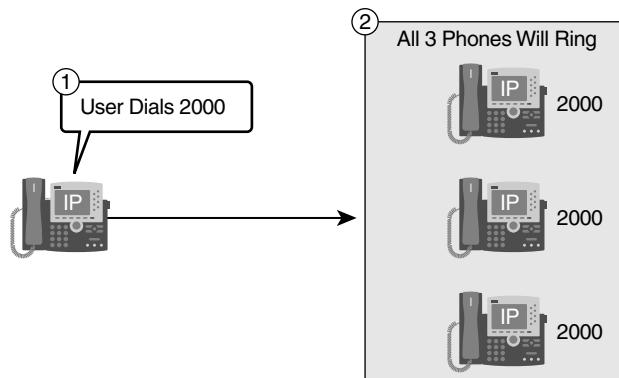


Figure 12-2 Shared Lines

Call Pickup

CUCM allows multiple lines to be grouped into call-pickup groups. Each pickup group is identified by a unique pickup group number. A phone line can be assigned to only one pickup group.

If a phone rings but no one is at the ringing phone to answer the call, another user can pick up the call by pressing the Pickup softkey if the ringing phone is in the same pickup group.

In the same situation, if the phone of the user who wants to pick up the call is not a member of the pickup group of the ringing phone, the user can use the *group pickup* feature (GPickup softkey) to pick up the call. When a user invokes the group pickup feature by pressing the corresponding softkey, the user has to enter the pickup group number of the ringing phone to be able to pick up the call.

Call-Hunting Components and Processes

CUCM call-hunting implementation is composed of the following components:

- **Line numbers/directory numbers (DN):** Number assignments to phones, Computer Telephony Integration (CTI), voicemail ports, and so on.
- **Line groups:** Phone DNs or voicemail ports are assigned to line groups.
- **Hunt lists:** Line groups are assigned to hunt lists. A hunt list can have one or more line groups. Line group hunt options and distribution algorithms can be specified to define how call hunting should be performed for the members of the line group.
- **Hunt pilots:** Hunt lists are assigned to hunt pilots. A hunt list is an ordered list of one or more line groups.

Hunt pilots are the numbers that will match on dialed digits to invoke the hunting process. A hunt pilot can be called directly or a call can be forwarded to the hunt pilot from an IP phone that received a call and is configured to forward calls to the hunt pilot to provide call coverage.

While hunting, the forwarding configuration of line group members is not used. If the hunting algorithm is ringing a phone and the call is not answered, the CFNA setting of that phone is ignored and the hunting algorithm goes on to the next line group member.

Figure 12-3 illustrates the call-hunting process and components. The hunt pilot in this example has been configured as 1 800 555-0111. Calls are distributed among the four DNs at the bottom of the figure.

In the following example, two line groups are configured:

- **Agents line group:** Contains the DNs 2001 and 2002
- **Operators line group:** Contains the DNs 2101 and 2102

The line groups are assigned to the hunt list HelpDesk:

- The first line group is Agents.
- The second line group is Operators.

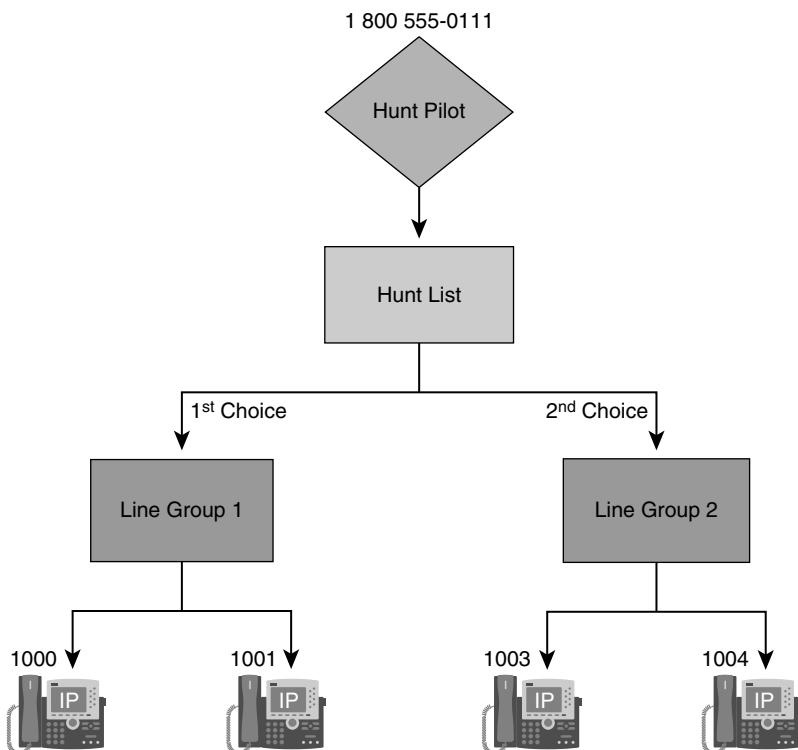


Figure 12-3 Call Hunting

A hunt pilot of HelpDesk with the pattern 2222 is configured to use hunt list HelpDesk for call coverage.

The following list and Figure 12-4 illustrate the call-coverage components involved in distributing a call from the hunt pilot:

1. A call is received for extension 2222. The CUCM digit analysis result matches the hunt pilot number of 2222. The hunt pilot distributes the call to the hunt list HelpDesk.
2. The hunt list uses top-down processing of the line groups. The first line group of Agents is processed.
3. The line group distributes the call to agent DNs. Assuming that the top-down call-distribution algorithm was selected, 2001 would ring and then 2002. The various call-distribution algorithms are covered later in this chapter.
4. If no agent answers, the hunt list sends the call to the second line group, Operators.
5. The line group Operators distributes the call to the operator DNs.

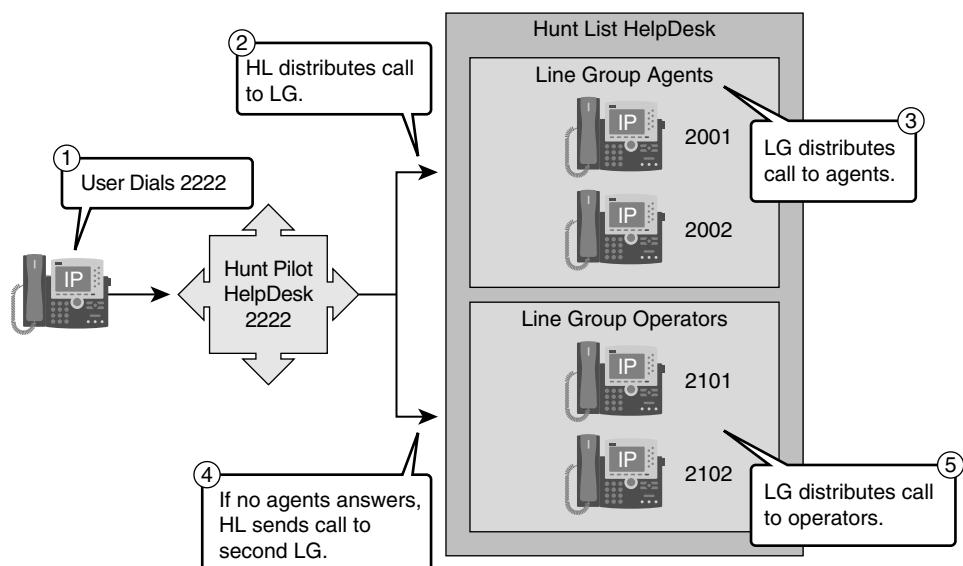


Figure 12-4 Call-Hunting Process

Hunt pilots are dialable patterns in the call-routing database (similar to route patterns, translation patterns, and DNs). The hunt pilot points to a hunt list. The hunt list points to one or more line groups, which include DNs.

Beginning with CUCM Release 4.1, calls can be redirected to a final destination when the hunting fails. Hunting can fail for one of the following reasons:

- All hunting options have been exhausted, and the call has not been answered.
- The maximum hunt timer has expired (configured at the hunt list level).

This call redirection is configured in the Hunt Forward Settings section of the Hunt Pilot Configuration page, and the destination for this redirect can be either of the following options:

- A specific destination configured globally at the hunt pilot.
- A personal preference, configured at the DN of the originally called number when hunting on behalf of that number fails. The personal preference is configured using the Call Forward No Coverage (CFNC) settings at the phone line.

You can implement the personal preferences option by configuring a user's phone so that the Forward No Answer field redirects the call to a hunt pilot, to search for someone else who can answer the call. If the call hunting fails, either because all the hunting options were exhausted or because a timeout period expired, the call can be sent to a destination personalized for the person who was originally called. For example, if the Forward No

Coverage field is set to voicemail, the call will be sent to that person's voicemail box when hunting fails.

The following considerations apply to calls handled by hunt pilots:

- Call Pickup and Group Call Pickup are not supported on calls distributed by a hunt pilot. A member of the line group cannot pick up the hunt pilot call offered to another member in the line group, even if the member belongs to the same call-pickup group.
- The hunt pilot can distribute calls to any of its line group members, regardless of the partition of the line group member. Class of service is not implemented in the call-coverage paradigm.

A hunt list is a prioritized list of line groups used for call coverage. Hunt lists have the following characteristics:

- Multiple hunt pilots can point to the same hunt list.
- Multiple hunt lists can contain the same line group.
- A hunt list is a prioritized list of line groups; line groups are hunted in the order of their configuration in the hunt list.

Line groups control the order in which a call is distributed, and they have the following characteristics:

- Line groups point to specific extensions, which are typically IP phone extensions or voicemail ports.
- The same extension can be present in multiple line groups.
- Line groups are configured with a global distribution algorithm that is used to select the next line group member for hunting.
- Line groups are configured with a hunt option that describes how hunting should be continued after trying the first member of the line group. The hunt option is configured per hunt failure event: No Answer, Busy, and Not Available.
- The Ring No Answer Reversion (RNAR) timeout specifies how long the hunting algorithm rings a member of the line group before it continues hunting according to the line group No Answer hunt option setting.

Line group members are the endpoints accessed by line groups, and they can be of any of the following types:

- Any Skinny Client Control Protocol (SCCP) endpoints, such as Cisco Unified IP Phone models VG248 or ATA 188
- Session Initiation Protocol (SIP) endpoints
- Voicemail ports

- H.323 clients
- Foreign Exchange Station (FXS) extensions attached to a Media Gateway Control Protocol (MGCP) gateway

Computer Telephony Integration (CTI) ports and CTI route points cannot be added to a line group. Therefore, calls cannot be distributed to endpoints controlled through CTI applications such as Cisco Customer Response Solution (CRS), Cisco Unified IP Interactive Voice Response (IVR), and so on.

Call-Hunting Options and Distribution Algorithms

Various hunt options are available at the line group configuration level. The default works for most implementations, but life is rife with options to accommodate the requirements of various organizations and collaborative groups. The following hunt options are available:

- **Try Next Member, Then, Try Next Group in Hunt List (Default):** Sends the call to the next idle or available member of this line group. If no more members are available in this line group, go to the next line group configured in the hunt list. If no more line groups are available, hunting stops.
- **Try Next Member, but Do Not Go to Next Group:** Sends the call to the next idle or available member of this line group. If no more members are available in this line group, hunting stops.
- **Skip Remaining Members, and Go Directly to Next Group:** Sends the call to the next line group. If no more line groups are available, hunting stops.
- **Stop Hunting:** Do not proceed to the next line group or next member.

The line group distribution algorithm specifies the order line in which group members should be used during the hunting process. The available algorithms are as follows:

- **Top-down:** If you choose a top-down distribution algorithm, CUCM distributes the call to idle or available members starting from the first idle or available member at the top of the line group to the last idle or available member (bottom of the list). In Figure 12-5, a top-down distribution algorithm would extend the next call to 1000, then to 1001, then to 1002, then to 1003, and back to 1000 depending on the line state of the destination DN. An important distinction in this model is that every new call attempts to use extension 1000, no matter how long the lines in the line group are idle. If extension 1000 is available every time there is a new call distributed, extension 1000 will receive the call. The user at extension 1000 would be very busy in this model.
- **Circular:** If you choose a circular distribution algorithm, CUCM distributes the call to idle or available members starting from the first member of the line group (1000). CUCM retains the most recently extended call target in memory and attempts to

place the second call to the second member of the line group (1001). The third call is distributed to the third member of the line group (1002), and the fourth call is extended to the fourth member of the line group (1003). The circular distribution algorithm might appear to be the same as the top-down distribution algorithm, but it is much fairer in its distribution of calls.

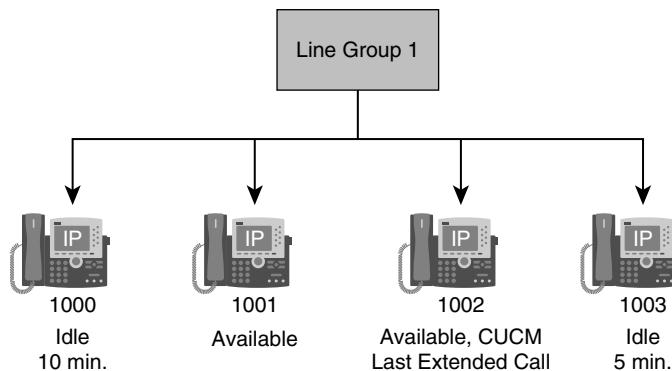


Figure 12-5 Line Group Distribution Algorithms

- **Longest idle time:** If you choose a longest idle time distribution algorithm, CUCM distributes the call to the member that has been idle for the longest amount of time. Only members in the idle call state are considered by this distribution algorithm. Available and busy call states do not receive calls. A phone in the available state is servicing a call but can manage a second call. Figure 12-5 assumes that 1000 has been idle for 10 minutes and 1003 has been idle for 5 minutes. A longest idle time distribution mechanism extends the call to extension 1000.
- **Broadcast:** If you choose a broadcast distribution algorithm, CUCM distributes the call to all idle or available members of a line group simultaneously.

Distribution algorithms are configured once per line group in CUCM Administration.

Call-Hunting Flow

The call-hunting flow in CUCM is as follows:

1. A direct call is placed to the hunt pilot number, or a call is forwarded to the hunt pilot number from a phone.
2. The hunt pilot starts the maximum hunt timer to monitor the overall hunting time. If the timer expires, hunting stops, and final forwarding is performed. The hunt pilot is logically associated with a hunt list.
3. The hunt list associated with the hunt pilot sends the call to the first line group configured in the hunt list.

The call is sent to the next line group member based on the distribution algorithm configured at the line group. Each line group is attempted until all resources are exhausted (or the maximum hunt timer expires).

- If the call to the hunt pilot goes unanswered, hunt failure has occurred. Possible hunt failure reasons include no one answered the phone or everyone is busy servicing other customers.

Figure 12-6 illustrates the call-coverage distribution of a call destined to a hunt pilot of 7000.

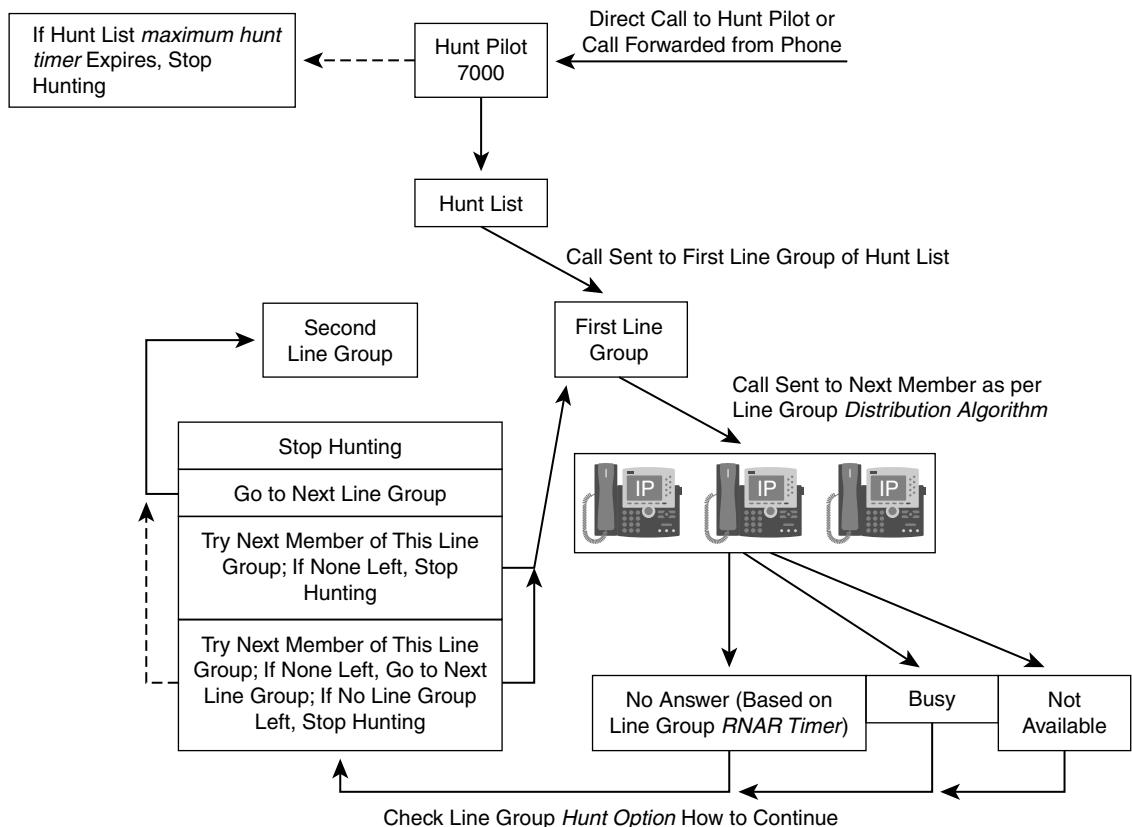


Figure 12-6 Call-Hunting Flow

Figure 12-7 illustrates the final forwarding options of the hunt pilot configuration.

If hunting stops (ring no answer or busy) and the hunt pilot is not configured for final forwarding, the call fails and a reorder tone is played.

If a final forwarding number is specified at the hunt pilot, the call is routed to the number.

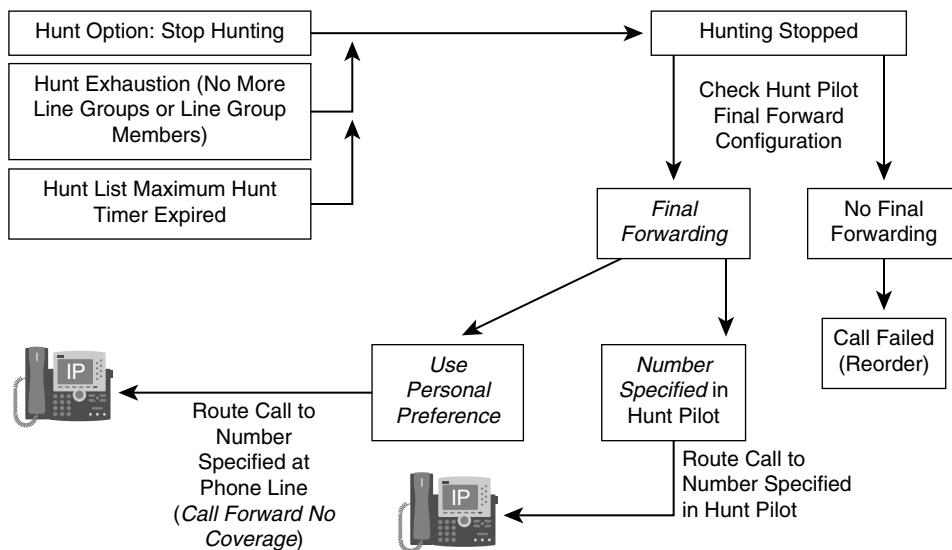


Figure 12-7 Call-Hunting Flow

If Use Personal Preference is selected, the call is routed as configured for Call Forward No Coverage at the phone line that invoked the call to the pilot number.

Call-Hunting Configuration

To access the line group, hunt list, and hunt pilot configuration windows in CUCM Administration, choose **Call Routing > Route/Hunt**.

When configuring hunting, follow these tasks:

Task 1: Create the line groups, add members, and configure the distribution algorithm and hunt options.

Task 2: Create the hunt list and add the line groups.

Task 3: Create the hunt pilot, associate the hunt list with the hunt pilot, and configure hunt forward settings.

Task 4: Configure personal preferences on phone lines in the event that hunting ends with no coverage.

These tasks are covered in more detail in the following sections.

Task 1: Create the Line Groups, Add Members, and Configure the Distribution Algorithm and Hunt Options

The DNs that will become the members of the line group must already exist in the database before you can complete this procedure. The following steps describe the creation of a line group. The configuration of the line group is illustrated in Figure 12-8.

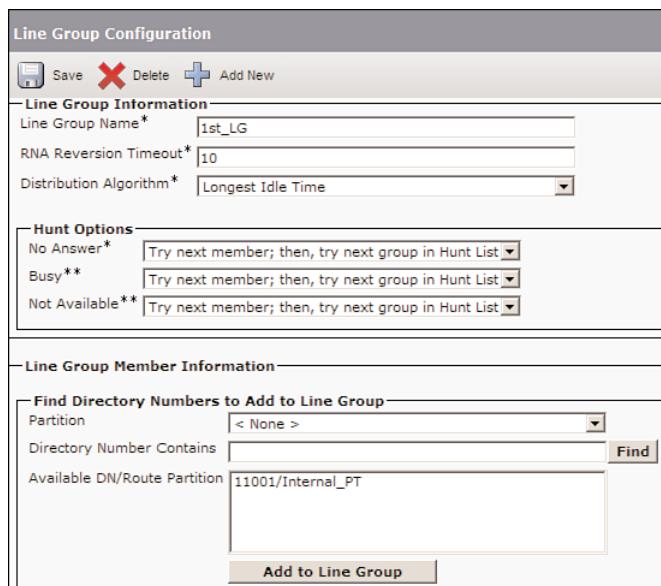


Figure 12-8 Line Group Configuration

- Step 1.** Choose Call Routing > Route/Hunt > Line Group from CUCM Administration.
- Step 2.** Click the Add New button.
- Step 3.** Enter a name in the Line Group Name field. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each line group name is unique to the route plan. Use a naming nomenclature that is brief and descriptive of the line group usage in the environment. It is good practice to append _LG to the line group name so that it can be easily identified.
- Step 4.** Configure the Distribution Algorithm, Hunt Options, and RNA (ring no answer) Reversion Timeout as desired. The RNAR parameter limits the amount of time (in seconds) that each DN in the line group rings before CUCM reports a No Answer condition.
- Step 5.** Add members to the line group. To locate a DN, choose a route partition from the Partition drop-down list, enter a search string in the Directory

Number Contains field, and click **Find**. To find all DNs that belong to a partition, leave the Directory Number Contains field blank and click **Find**. A list of matching DNs is displayed in the Available DN/Route Partition pane.

- Step 6.** In the Available DN/Route Partition pane, select a DN to add and click **Add to Line Group** to move it to the Selected DN/Route Partition pane. Repeat this step for each member that you want to add to this line group.
- Step 7.** In the Selected DN/Route Partition pane, choose the order in which the new DNs will be accessed in this line group. To change the order, click a DN and use the up and down arrows to the right of the pane.
- Step 8.** Click **Save** to add the new DNs and to update the DN order for this line group.

Task 2: Create the Hunt List and Add the Line Groups

To add a hunt list, follow these steps:

- Step 1.** Choose **Call Routing > Route/Hunt > Hunt List**.
- Step 2.** Click the **Add New** button.
- Step 3.** In the Name field, enter a descriptive name for the hunt list functionality and append **_HL** to indicate that the item is a hunt list. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Each hunt list name must be unique.
- Step 4.** Choose a CUCM group from the drop-down list.
- Step 5.** Click the **Save** button. The Hunt List Configuration window will display the newly added hunt list.
- Step 6.** Add at least one line group to the new hunt list. To add a line group, click **Add Line Group**. The Hunt List Detail Configuration window will open.
- Step 7.** From the Line Group drop-down list, choose a line group to add to the hunt list.

To add the line group, click **Save**. The pop-up window is shown stating that for the changes to take effect, you must reset the hunt list. Click **OK** to confirm the message.

The line group name is displayed in the Selected Group list on the right side of the window.
- Step 8.** To add more line groups to this list, click **Add Line Group** and repeat the preceding two steps.
- Step 9.** When you finish adding line groups to the hunt list, click **Save**.
- Step 10.** A pop-up window will open. Click **OK** to reset the hunt list.

CUCM accesses line groups in the order in which they are shown in the hunt list. The access order of line groups is changed by selecting a line group from the Selected Groups pane and clicking the up or down arrow on the right side of the pane to move the line group up or down in the list. Figure 12-9 illustrates the configuration order of the hunt list configuration.

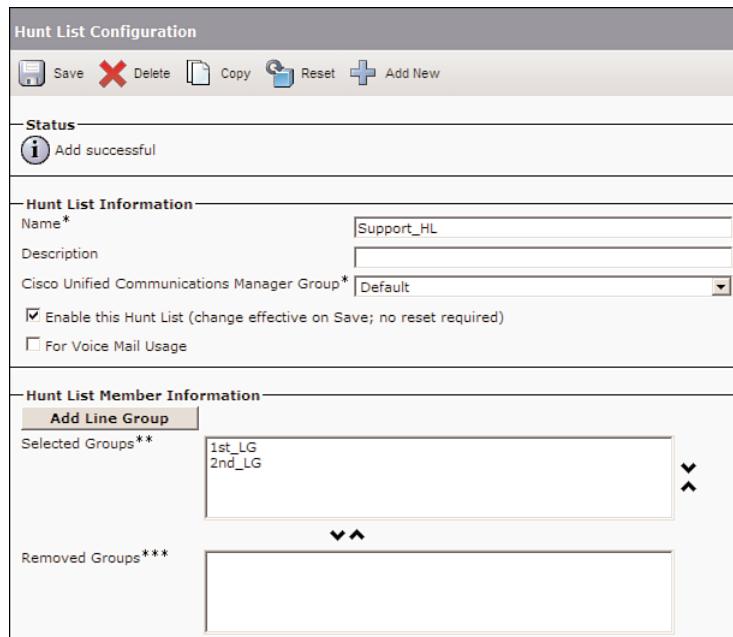


Figure 12-9 Hunt List Configuration

Task 3: Create the Hunt Pilot, Associate the Hunt List with the Hunt Pilot, and Configure Hunt Forward Settings

Follow these steps to create a hunt pilot:

- Step 1.** Choose Call Routing > Route/Hunt > Hunt Pilot.
- Step 2.** Click the Add New button.
- Step 3.** Enter the hunt pilot number in the Hunt Pilot field.
- Step 4.** Assign the hunt pilot to a hunt list using the Hunt List drop-down list.
- Step 5.** Scroll down to the bottom of the page to configure final forwarding settings and the maximum hunt timer.
- Step 6.** Click the Save button.

The hunt pilot configuration is illustrated in Figure 12-10.

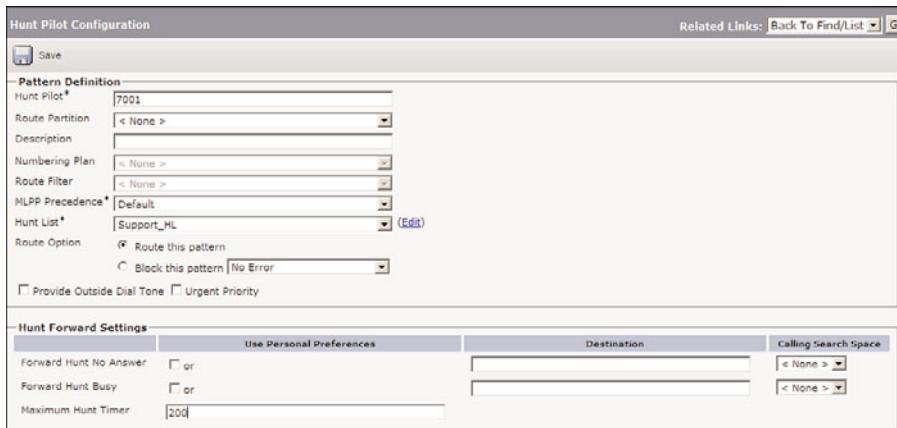


Figure 12-10 Hunt Pilot Configuration

Task 4: Configure Personal Preferences on Phone Lines in the Event That Hunting Ends with No Coverage

The Hunt Forward Settings pane of the Hunt Pilot Configuration window specifies the final forwarding settings and maximum timer values, as described in Table 12-1.

Table 12-1 Hunt Forward Settings

Setting	Description
Forward Hunt No Answer	<p>When the call distributed through the hunt list is not answered within a specific period of time, this field specifies the destination to which to forward the call. Choose from these options:</p> <p>Use Personal Preferences: Enables the CFNC settings for the original called number that forwarded the call to this hunt pilot.</p> <p>The CFNC setting specifies a call-forwarding reason that you administer in the Directory Number Configuration window.</p> <p>Calls are diverted based on the value in the Coverage/Destination field of the DN when a call to the DN first diverts to coverage, and coverage either exhausts or times out, and the associated hunt pilot for coverage specifies Use Personal Preferences for its final forwarding.</p> <p>When the Use Personal Preferences check box is selected, CUCM ignores the settings in the Destination and Calling Search Space fields.</p> <p>Destination: This setting indicates the DN to which calls are forwarded.</p> <p>Calling Search Space: This setting applies to all devices that are using this DN.</p>

Table 12-1 Hunt Forward Settings

Setting	Description
Forward Hunt Busy	<p>When the call distributed through the hunt list encounters only busy lines for a specific period of time, this field specifies the destination to which to forward the call. Choose from these options:</p> <p>Use Personal Preferences: Select this check box to enable the CFNC settings for the original called number that forwarded the call to this hunt pilot.</p> <p>When this check box is selected, CUCM ignores the settings in the Destination and Calling Search Space fields.</p> <p>Destination: This setting indicates the DN to which calls are forwarded.</p> <p>Calling Search Space: This setting applies to all devices that are using this DN.</p>
Maximum Hunt Timer	Specifies the maximum time for hunting (in seconds).

The Directory Number Configuration window provides configuration options for internal and external forwarding based on whether a call is CFA or CFNA, as specified in Table 12-2.

Table 12-2 Hunt Forward Settings

Field	Description
Forward All	<p>Specifies the forwarding treatment for calls to this DN if the DN is set to forward all calls.</p> <p>Voice Mail: Select this check box to use the settings in the Voice Mail Profile Configuration window.</p> <p>When this check box is selected, CUCM ignores the settings in the Destination and Calling Search Space fields.</p> <p>Destination: This setting indicates the DN to which all calls are forwarded. Use any dialable phone number, including an outside destination.</p> <p>Calling Search Space: This setting applies to all devices that are using this DN.</p>
Forward Busy Internal	<p>When the call distributed through the hunt list encounters only busy lines for a specific period of time, this field specifies the destination to which to forward the call. Choose from these options:</p> <p>Use Personal Preferences: Select this check box to enable the CFNC settings for the original called number that forwarded the call to this hunt pilot.</p> <p>When this check box is selected, CUCM ignores the settings in the Destination and Calling Search Space fields.</p> <p>Destination: This setting indicates the DN to which calls are forwarded.</p> <p>Calling Search Space: This setting applies to all devices that are using this DN.</p>
Forward Busy External	<p>When the call distributed through the hunt list encounters only busy lines for a specific period of time, this field specifies the destination to which to forward the call. Choose from these options:</p> <p>Use Personal Preferences: Select this check box to enable the CFNC settings for the original called number that forwarded the call to this hunt pilot.</p> <p>When this check box is selected, CUCM ignores the settings in the Destination and Calling Search Space fields.</p> <p>Destination: This setting indicates the DN to which calls are forwarded.</p> <p>Calling Search Space: This setting applies to all devices that are using this DN.</p>

Table 12-2 Hunt Forward Settings

Field	Description
Forward No	Specifies the forwarding treatment for internal or external calls to this DN if the DN does not answer.
Answer Internal	
Forward No	Voice Mail: Select this check box to use the settings in the Voice Mail Profile Configuration window.
Answer External	When this check box is selected, CUCM ignores the settings in the Destination and Calling Search Space fields. Destination: This setting indicates the DN to which an internal call is forwarded when the call is not answered. Use any dialable phone number, including an outside destination. Calling Search Space: This setting applies to all devices that are using this DN.
Forward No	This setting applies only if you configure one of the other forwarding fields (CFA, CFB, or CFNA) with a hunt pilot number in the Destination DN field.
Coverage Internal	
Forward No	
Coverage External	For the hunt pilot settings, you must also configure the Forward Hunt No Answer or Forward Hunt Busy fields and select the Use Personal Preferences check box under the Hunt Forward Settings section in the Hunt Pilot Configuration window; otherwise, the Forward No Coverage configuration in the Directory Number Configuration window has no effect.

Call-Forwarding Features

The following five examples explore the related call-forwarding options used at the Cisco IP Phone and the hunt pilot configuration.

Example: Call Forwarding Without Forward No Coverage Settings

Here, User A at DN 3000 has the DN configuration illustrated in Figure 12-11:

- **CFB:** Call Forward Busy has two settings: Forward Busy Internal and Forward Busy External. Both forwarding options are set to 3001. This setting forwards both internal and external (public switched telephone network [PSTN]) calls to 3001 when 3000 is busy. 3001 is probably the second line of the phone, but this cannot be determined from Figure 12-11 alone.
- **CFNA:** Call Forward No Answer has two settings as well: Forward No Answer Internal and Forward No Answer External. The CFNA setting in Figure 12-11 forwards internal calls to 3001 and forwards external calls to 303 555-0111 when 3000 does not answer.

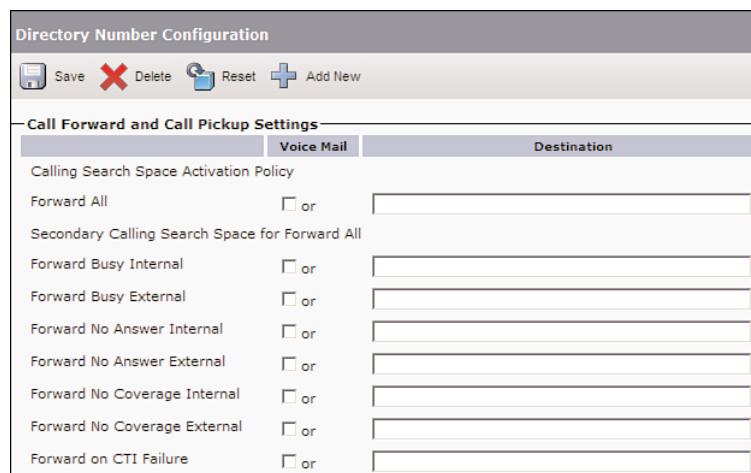


Figure 12-11 Call Hunting Call Forwarding Without Forward No Coverage Settings

- **CFNC:** Call Forward No Coverage does not have a configuration. Any calls that are sent back to this phone from the hunt pilot for personal treatment will result in a re-order tone.

The following examples will discuss scenarios where the hunt pilot final forwarding rules are used.

Example: Forward No Coverage

This example presents a scenario where no final forwarding rules were configured. User A at DN 3000 has the configuration shown in Figure 12-12 in the Directory Number Configuration window:

- **CFB:** When busy, incoming internal calls are forwarded to 3001 and external calls are forwarded to hunt pilot 7000.
- **CFNA:** When there is no answer, incoming internal calls are forwarded to 3001 whereas external calls are forwarded to hunt pilot 7000.

Hunt pilot 7000 is associated with hunt list abc and has four hunt parties equally distributed over Line Group 1 and Line Group 2. Hunt pilot 7000 has no final forwarding fields provisioned (default).

Question: What behavior results when an internal caller calls 3000 and user 3000 is busy?

Answer: The call forwards to line 3001.

Question: What behavior results when an external caller calls 3000 and user 3000 does not answer?

Answer: The call forwards to hunt pilot 7000, which will cause hunting to lines 3001, 3002, 4001, and 4002. If one of the hunt parties answers, the caller is connected to that party. If no hunt party answers, then, regardless of the reason, the caller receives a reorder tone (or an equivalent annunciator announcement).

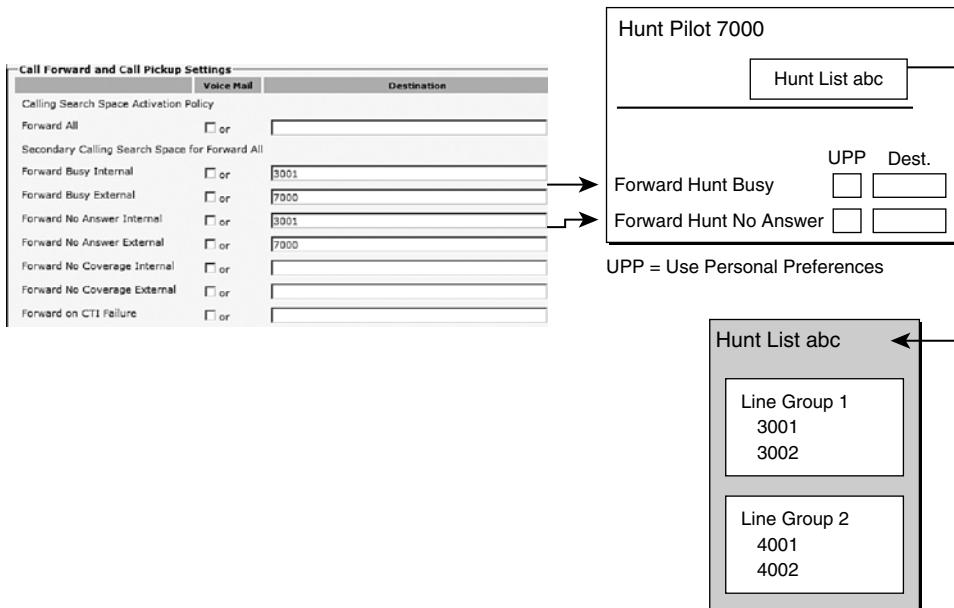


Figure 12-12 Call Hunting: Forward No Coverage

Example: Call Coverage—Forward Hunt No Answer

In this call-hunting example, illustrated in Figure 12-13, hunt pilot 7000 has the Forward Hunt No Answer field set to 3002, but all Forward Hunt Busy fields are empty.

If an external caller calls 3000 and user 3000 does not answer, the call forwards to hunt pilot 7000, which causes hunting to lines 3001, 3002, 4001, and 4002. If one of the hunt parties answers, the caller is connected to that party.

If all hunt parties are busy, the caller receives a reorder tone. The reorder tone was sent because of the missing Forward Hunt Busy configuration in the hunt pilot.

If at least one hunt party is alerted (phone rings) but does not pick up, the call forwards to 3002 because 3002 is the value configured for the Forward Hunt No Answer field.

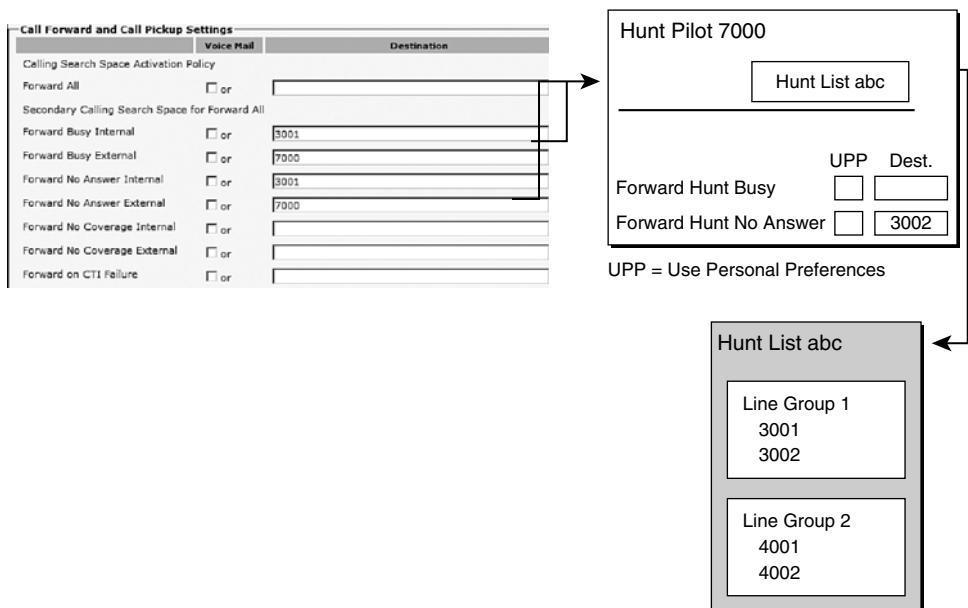


Figure 12-13 Call Hunting: Call Coverage—Forward Hunt No Answer

Example: Call Coverage—Forward Hunt Busy

This example presents a scenario where user personal preferences are used for the final forwarding for forward hunt busy. The forward hunt no answer calls to 3002. Figure 12-14 is different from Figure 12-13 because Forward Hunt Busy is configured at the hunt pilot level. The DN configuration also differs from previous examples because the DN has two Call Forward No Coverage numbers configured.

When an external caller calls 3000 and user 3000 does not answer, the call forwards to hunt pilot 7000, which hunts to lines 3001, 3002, 4001, and 4002.

If one of the hunt parties answers, the caller is connected to that party. If at least one party is alerted, but hunting exhausts the hunt list, the call is forwarded to 3002.

If all hunt parties are busy, the call is forwarded as configured by the DN that forwarded the call to the hunt pilot. The DN's Forward No Coverage External setting determines what happens to the call if the hunt pilot has Use Personal Preferences configured. In this case, the call will forward to 303 555-0111.

Note If the hunt pilot is configured to use personal preferences, the corresponding Forward No Coverage field should be set at the phone forwarding the call to the hunt pilot. A call forwarded from a phone to the hunt pilot leveraging personal preferences with no Forward No Coverage setting will result in a reorder tone. This is similar to the behavior when final forwarding settings are missing at the hunt pilot.

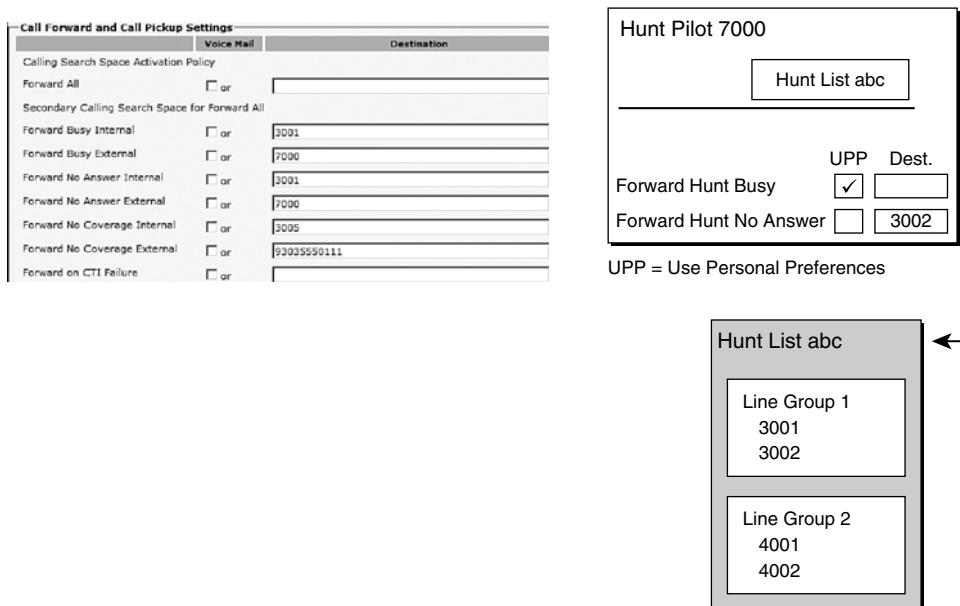


Figure 12-14 Call Hunting: Call Coverage—Forward Hunt Busy

Example: Call Coverage—Forward No Coverage External Missing

This example presents a scenario in which the Forward No Coverage External has not been configured. This missing configuration will cause any external calls forwarded to hunt pilots to result in a reorder tone. Figure 12-15 has a similar configuration to Figure 12-14, but the DN does not have a Forward No Coverage External provisioned.

The RNAR timer for a line group determines how long hunting will ring a hunt party before moving to the next party in its list (assuming that the customer did not select the broadcast algorithm). This timer has a default value of 10 seconds.

In Figure 12-15, there are four hunt parties. How long will it take before hunting exhausts? It will take 40 seconds before hunting exhausts (10 seconds RNAR default \times 4 hunt members).

Assume that the maximum hunt timer for hunt pilot 7000 is set to 25 seconds. The call must be answered within this hunt timer. In this example, the maximum hunt timer is 2.5 times the RNAR timer, which is 10 seconds.

If a user calls hunt pilot 7000, the call attempts to hunt for the four parties. If all the phones ring but no one picks up within 25 seconds, hunting terminates and the cause is treated as no answer. Hunting terminates after the third member has been alerted for 5 seconds (10 seconds RNAR on each of the first two members leaves 5 seconds before expiration of the 25-second maximum hunt time configured at the hunt pilot). The call forwards to 3002 because hunting failed with a No Answer condition.

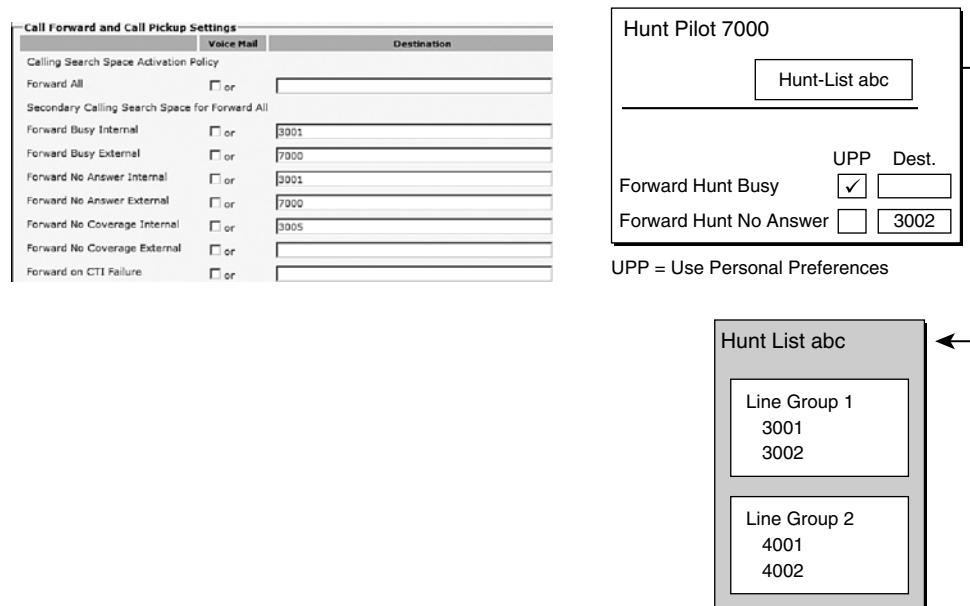


Figure 12-15 Call Hunting: Call Coverage—Forward No Coverage External Missing

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- CUCM offers several features for call coverage, including call forwarding, shared lines, call pickup, and call hunting.
- In CUCM, IP phone lines can be configured with Call Forward All, Call Forward Busy, Call Forward No Answer, Call Forward No Coverage, and Call Forward Unregistered.
- Call hunting in CUCM uses the following elements: hunt pilots, hunt lists, line groups, and endpoints (lines and voicemail ports).
- Call-hunting options are configured per line group and specify how to continue hunting when the selected line group member does not answer. The distribution algorithms, also configured per line group, specify how to select a line group member.
- During hunting, the hunt option, distribution algorithm, RNAR timeout, maximum hunt timer, and final forwarding settings are considered.
- Call-hunting implementation includes configuration of IP phone lines, line groups, hunt lists, and hunt pilots.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. Which of the following is not a call-forwarding option that can be configured at the directory number of a phone?
 - a. Call Forward Queue Exhaustion
 - b. Call Forward All
 - c. Call Forward Busy
 - d. Call Forward No Coverage
2. Which Calling Search Space will further restrict the Call Forward All capabilities of a phone?
 - a. Phone CSS
 - b. Directory Number CSS
 - c. CFA CSS
 - d. CFNA CSS
3. What two mechanisms will allow multiple phones to ring at the same time?
 - a. Shared lines
 - b. Hunt group
 - c. Route pattern
 - d. Route list
4. Which technology allows a call to be picked up on another phone in the same department?
 - a. Shared line
 - b. Call pickup
 - c. Call hunting
 - d. Group pickup
5. Which technology allows a call to be picked up on another phone in a different department?
 - a. Shared line
 - b. Call pickup
 - c. Call hunting
 - d. Group pickup

- 6.** If a device contains both a device and line Calling Search Space, how will they be processed by CUCM?
 - a.** Line CSS overrides device CSS.
 - b.** Device CSS overrides line CSS.
 - c.** Both are concatenated. Line CSS is processed before device CSS.
 - d.** Both are concatenated. Device CSS is processed before line CSS.
- 7.** Which component of call hunting does a hunt pilot point to?
 - a.** Line group
 - b.** Line group members
 - c.** Telephony call dispatcher
 - d.** Hunt list
- 8.** Which component of call hunting does a hunt list point to?
 - a.** Line group
 - b.** Line group members
 - c.** Telephony call dispatcher
 - d.** Hunt list
- 9.** Which call-forwarding option is used when calls forwarded to the hunt pilot exhaust (final forwarding)?
 - a.** CFA
 - b.** CFB
 - c.** CFNB
 - d.** CFNC
 - e.** CFUR
- 10.** Which line group distribution mechanism routes calls in a round-robin fashion between all the members of the line group?
 - a.** Broadcast
 - b.** Top-down
 - c.** Circular
 - d.** Longest idle

Chapter 13

Media Resources

Upon completing this chapter, you will be able to describe CUCM media resources, including conferences, transcoding, Media Termination Point (MTP), music on hold (MoH), and annunciator services. You will also be able to meet these objectives:

- Describe media resources and their functions
- Describe how CUCM supports media resources
- Describe conferencing
- Configure conferencing media resources
- Configure MeetMe conferences
- Describe and configure music on hold
- Describe annunciators
- Describe and configure media resources access control

This chapter describes available hardware and software media resources and discusses how they are configured in Cisco Unified Communications Manager (CUCM) to provide features such as conferences, transcoding, media termination, and MoH. It also explains how to perform access control to media resources using media resource groups and media resource group lists.

Media Resources

A media resource is a software- or hardware-based entity that performs media-processing functions on the data streams to which it is connected. Media-processing functions include converting an audio signal to IP packets and vice versa (voice termination), mixing multiple streams to create one output stream (conferencing), passing the stream from one connection to another (MTP), converting the data stream from one compression type to another (transcoding), echo cancellation, signaling, termination of a voice stream from a

time-division multiplexing (TDM) circuit (coding/decoding), packetization of a stream, and streaming audio (annunciation).

Table 13-1 introduces the different types of media resources.

Table 13-1 Media Resource Functions

Resource	Function
Voice termination	TDM legs must be terminated by hardware that performs coding/decoding and packetization of the stream. This is performed in digital signal processors (DSP) on the gateway router.
Audio conferencing	A transcoder converts an input stream from one codec into an output stream that uses a different codec.
Transcoding	A transcoder converts an input stream from one codec into an output stream that uses a different codec.
MTP	An MTP bridges the media streams and allows them to be set up and torn down independently.
Annunciator	An annunciator streams spoken messages and various call progress tones.
MoH	Music on hold provides music to callers when their call is placed on hold, transferred, parked, or added to a conference.

Not all the different media resources described in Table 13-1 are needed in every deployment. Software resources are provided by CUCM and IOS services, whereas hardware features are provided by DSPs. The DSP resources are hardware modules in the gateway router or switch. The software resources are controlled by the Cisco IP Voice Media Streaming application running on CUCM.

A *conference bridge* is a resource that joins multiple participants into a single call. It can accept a number of connections for a given conference, up to the maximum number of streams allowed for a single conference on that device. The conference bridge mixes the streams together and creates a unique output stream for each connected party. The output stream for a given party is the composite of the streams from all connected parties minus their own input stream. Some conference bridges mix only the three loudest talkers on the conference and distribute that composite stream to each participant minus their own input stream if they are one of the talkers. Software conferencing is limited to the G.711 audio codec.

Note All hardware resource limitations are well documented in the media resource chapter of the Solution Reference Network Design (SRND) guide available online at www.cisco.com/go/srnd. It is best practice to use the Cisco DSP Calculator, which you can find at www.cisco.com/go/dspcalculator. The Cisco DSP Calculator requires Cisco.com membership access.

A *transcoder* takes the stream of one source device and converts it from one compression type to another compression type. For example, it could take a stream from a G.711 codec and transcode it in real time to a G.729 stream. In addition, a transcoder provides MTP capabilities and can be used to enable supplementary services for H.323 endpoints when required.

Two streams that use the same codec using different sampling intervals can also be connected.

A single-site deployment usually has no need for transcoding devices.

A *Media Termination Point (MTP)* is an entity that accepts two full-duplex G.711 streams. It bridges the media streams and allows them to be set up and torn down independently. The streaming data received from the input stream on one connection is passed to the output stream on the other connection and vice versa.

An *annunciator* is a software function of the Cisco IP Voice Media Streaming application that provides the ability to stream spoken messages or various call-progress tones from the system to a user. It is capable of sending multiple one-way Real-Time Transport Protocol (RTP) streams to devices such as Cisco IP Phones or gateways, and it uses Skinny Client Control Protocol (SCCP) messages to establish the RTP stream. The announcements can be customized by replacing the appropriate WAV file.

Music on hold (MoH) is an integral feature of the Cisco Unified Communications system. This feature provides music to callers when their call is placed on hold, transferred, parked, or added to an ad hoc conference.

Media Resource Support

CUCM offers software-based media resources. Start the IP Voice Media Streaming application to activate the following:

- Audio conferencing
- MTP
- Annunciator
- MoH

The following media resources are available only in hardware:

- Transcoding
- Voice termination

Audio conferencing and MTP media resources can also be offered by hardware media resources. MoH is a special case. Because of the potential WAN bandwidth utilization of MoH, the multicast streams of the server are normally scoped at the headquarters. Survivable Remote Site Telephony (SRST) can stream one media resource at branch locations.

Audio Conferencing

The signaling between hardware media resources and CUCM most often uses SCCP to set up and tear down calls. All audio streams from any endpoint are always terminated by the media resources involved in the call. There is no direct IP phone-to-IP phone audio stream with media resources involved in the call flow.

The voice-termination function is needed when an incoming or outgoing TDM call is terminated on a gateway. The TDM leg is terminated by the Cisco IOS router's DSP and has to perform decoding, coding, packetization, and depacketization functions.

There are two different audio streams in Figure 13-1, one inside the public switched telephone network (PSTN) and the other one a VoIP audio stream using RTP transport.

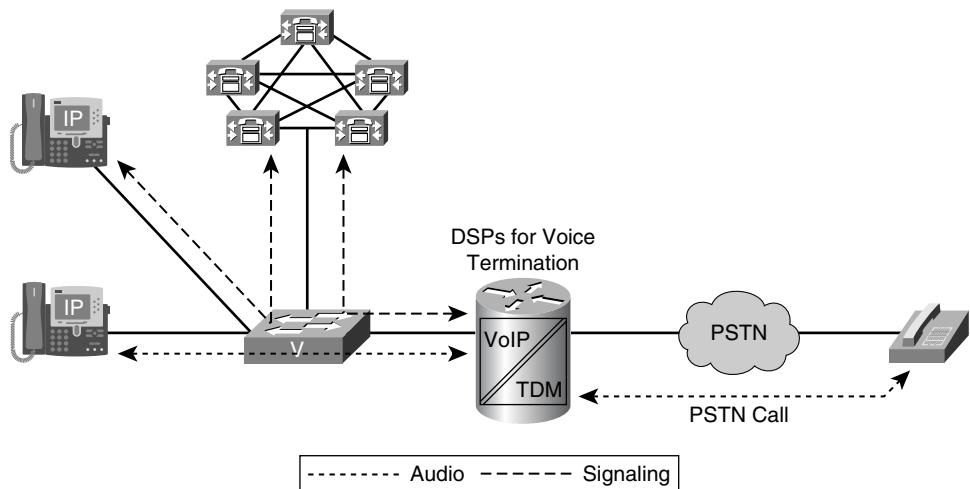


Figure 13-1 *PSTN Voice Termination*

Signaling messages are exchanged between the gateway and CUCM and between the telephony device and CUCM. The PSTN signaling is not considered in Figure 13-1.

RTP bearer traffic streams are sent from the IP phones to the conference bridge resource mixing the audio. The conference resource mixes the audio streams and sends back a unique audio stream to the IP phones. The audio stream must subtract the audio stream of the person receiving the audio stream so that no echo is heard. Some conference devices, because of processing limitations, mix only the three loudest talkers.

Signaling messages (control traffic) are exchanged among the IP phones, CUCM, and the conferencing resource (if using a hardware resource or a version of Cisco Unified MeetingPlace). Cisco Unified MeetingPlace is not covered in this book.

Note The Cisco Press book *Voice and Video Conferencing Fundamentals* is an excellent resource for a more thorough understanding of audio conferencing and videoconferencing.

Most conference bridges that are under the control of CUCM use SCCP to communicate with CUCM. Session Initiation Protocol (SIP) support is increasingly being added to all the Unified Communications components.

CUCM does not distinguish between software- and hardware-based conference bridges when it processes a conference allocation request. Allocation of conferencing resources is covered in further detail later in this chapter. The number of individual conferences and maximum number of participants per conference vary based on the resource in use. Figure 13-2 illustrates that software conferencing is integrated into CUCM.

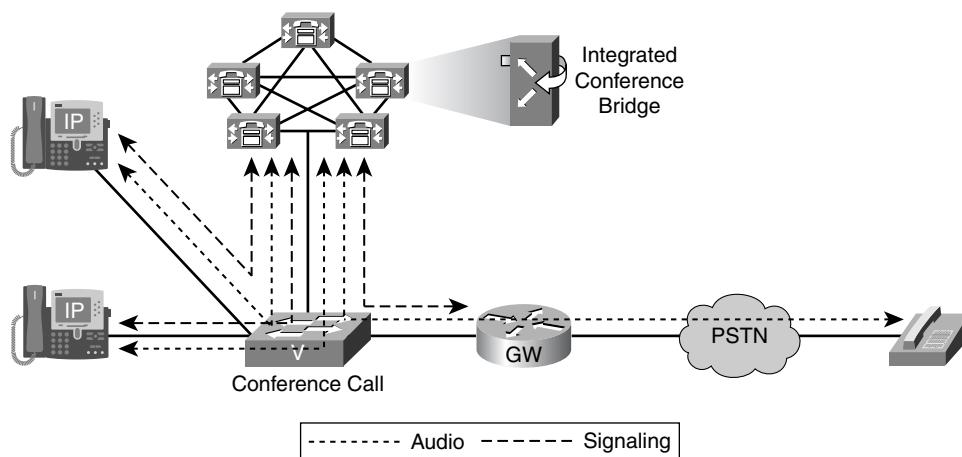


Figure 13-2 Software Conferencing

A transcoder converts an input audio stream using one audio codec into an output stream that uses a different audio codec. The transcoder in Figure 13-3 is implemented using DSP resources in the Cisco router. Transcoders are necessary when audio streams are using compressed audio codes (G.729 or Internet Low Bandwidth Codec [iLBC]), but the resource they are attempting to use accepts only G.711 calls. iLBC operates at 15.2 kbps. Most Cisco Unify voicemail deployments use the G.711 audio codec for voicemail storage to guarantee high quality.

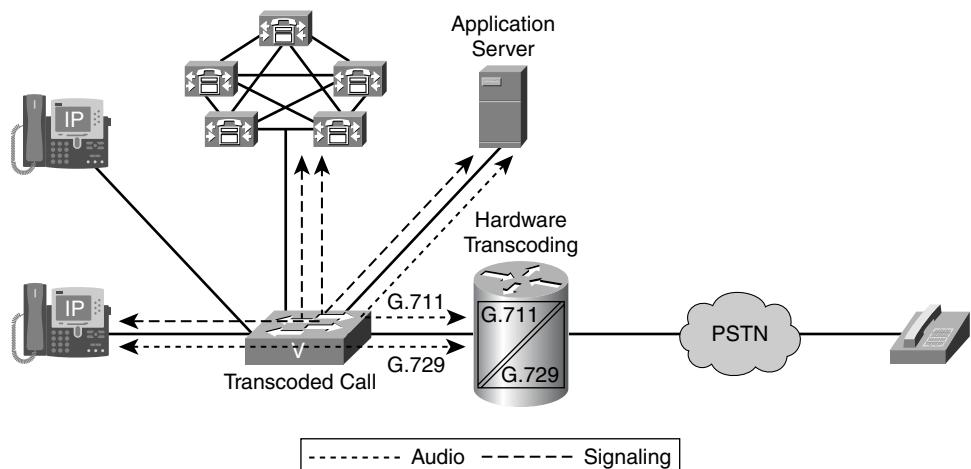


Figure 13-3 Transcoding Media Resources

Audio streams (RTP bearer channels) are set up between the telephony devices and the transcoder. Signaling messages are exchanged between the telephony devices and CUCM and between the transcoder resource and CUCM. DSP resources are required to perform transcoding. Those DSP resources are located in Cisco routers and switches.

MTP

An MTP bridges two media streams and allows them to be set up and torn down independently.

An MTP can be used as an instance of translation between incompatible audio streams, to synchronize clocking, or to enable supplementary services for devices that do not support the empty capability set (ECS) option of the H.323 version 2 protocol.

Audio streams exist between telephony devices and the MTP resource. Signaling messages are exchanged between the telephony devices and CUCM. Figure 13-4 illustrates a hardware-based MTP.

Annunciator

An annunciator is a function of the Cisco IP Voice Media Streaming application service that provides the capability to stream spoken messages or various call-progress tones from the CUCM system to a user.

The annunciator can send multiple one-way RTP streams to devices such as Cisco IP Phones or gateways, using SCCP messages to set up the RTP stream. Tones and announcements are predefined by the system. The announcements support localization and can also be customized by replacing the appropriate WAV file. The annunciator can

support G.711 a-law, G.711 mu-law, G.729, and Cisco wideband audio codecs without transcoding resources.

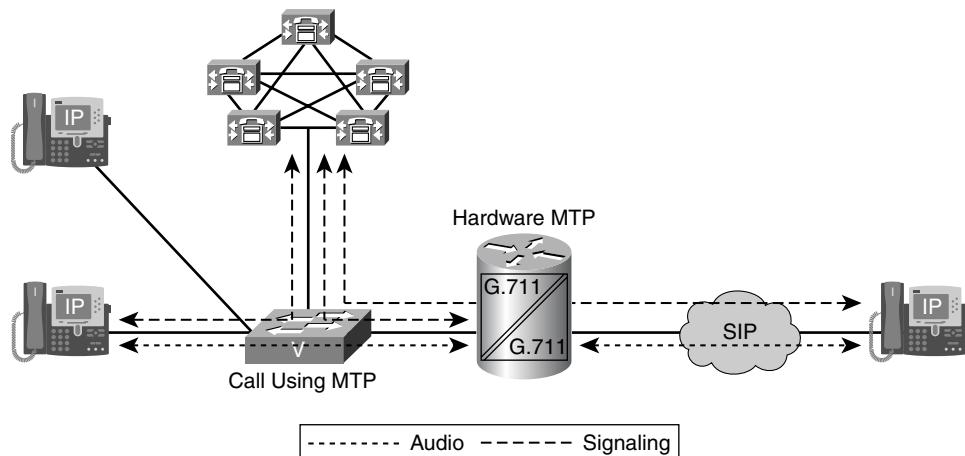


Figure 13-4 *Hardware MTP*

Signaling messages are exchanged between telephony devices and CUCM. The audio stream is one-way, from the annunciator to the telephony device. The annunciator is a software component of CUCM, as shown in Figure 13-5.

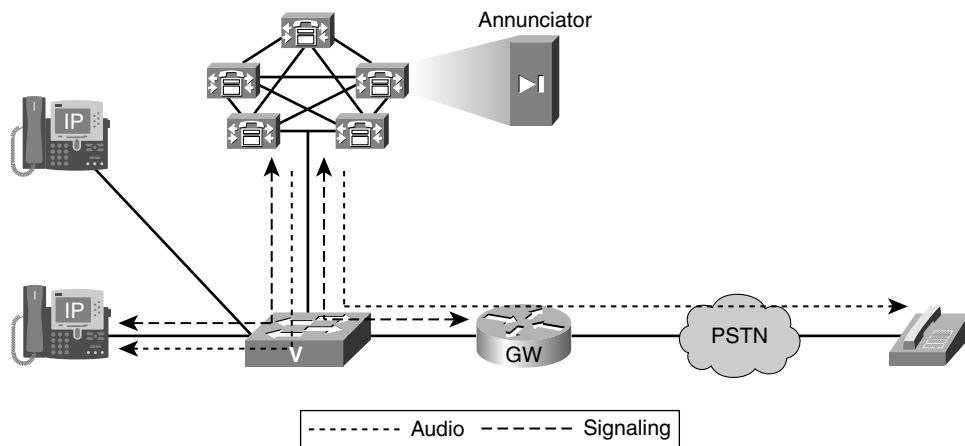


Figure 13-5 *Annunciator Services*

MoH

The MoH feature is part of the Cisco IP Voice Media Streaming (IPVMS) service running on CUCM. This feature provides music to callers when their call is placed on hold or a supplementary service is initiated. Supplementary services are not limited to but include

the following: transfer, park, and conference. When a supplementary service is initiated, the call is temporarily put on hold before the function is completed. Implementing MoH is relatively simple but requires a basic understanding of IP unicast and multicast traffic, MoH call flows, configuration options, server behavior, and requirements.

Audio streams are created between telephony devices and the MoH server. Signaling messages are exchanged between telephony devices and CUCM. Figure 13-6 illustrates the MoH component of CUCM.

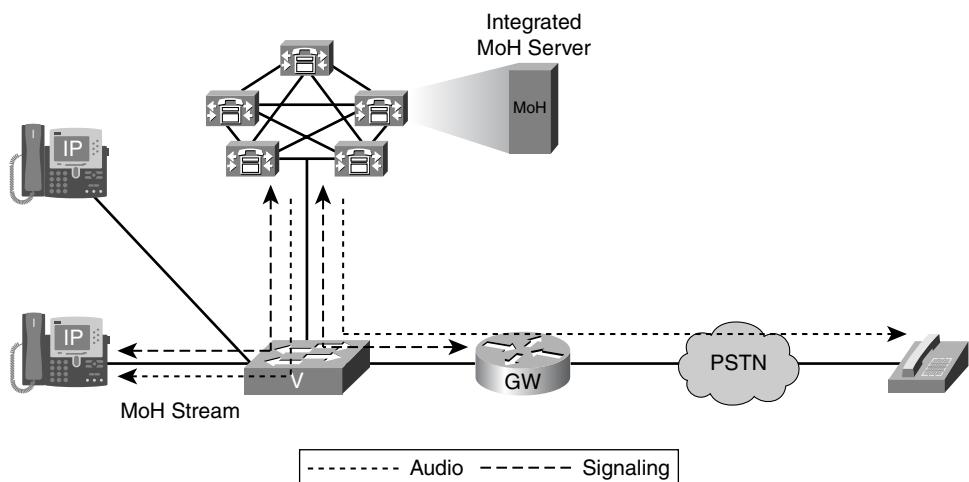


Figure 13-6 Music on Hold

Conferencing

The CUCM supports hardware and software conference bridges.

The software-based conference bridge, implemented as a CUCM service, supports only conferences, using a single audio codec (G.711 or Cisco wideband).

Some hardware conference bridges can support multiple low-bit-rate (LBR) stream types such as G.729, Global System for Mobile Communications (GSM), G.723, and iLBC. A mixed-mode conference is a conference in which multiple audio codecs are used for different audio streams. A mixed-mode conference bridge has the added burden of transcoding the RTP bearer streams. Mixed-mode conferences limit the number of conference participants and active conferences based on the capabilities of the hardware. There are multiple hardware conference bridge families that should be investigated.

Note Hardware conference capabilities are well documented in the CUCM SRND guide available at www.cisco.com/go/srnd. The DSP Calculator should also be used when designing a solution involving hardware media resources. As mentioned previously, the DSP Calculator is available at www.cisco.com/go/dspcalculator.

Software conferencing scalability is limited by the server platform CUCM is running on. Conferencing capabilities of the server are throttled by default because it is assumed that CUCM will be running call processing coresident while providing conferencing capabilities. The number of streams can be tuned up to 64 ad hoc conference participants and 128 MeetMe conference participants on a standalone server (dependent on the server hardware platform). A standalone server is dedicated to providing services to the CUCM, but it never performs call processing (call setup and teardown).

A hardware conference bridge can support multiple LBR audio stream types, including G.729, GSM, G.723, and iLBC.

All conference bridges that are under the control of CUCM currently use SCCP to communicate with CUCM.

CUCM allocates a conference bridge from a conferencing resource that is registered with the CUCM cluster. Both hardware and software conferencing resources can register with CUCM at the same time, and CUCM can allocate conference bridges from either resource. CUCM does not distinguish between these types of conference bridges when it processes conference allocation requests.

The number of individual conferences and maximum number of participants per conference vary by resource.

Cisco Conference Bridge Hardware

The following types of hardware conference bridge resources can be used on a CUCM system:

- Cisco Conference Bridge Hardware (Cisco Catalyst WS-X6608-T1 and WS-X6608-E1)
- Cisco IOS Conference Bridge (Cisco NM-HDV)
- Cisco Conference Bridge (Cisco WS-SVC-CMM and WS-SVC-CMM-ACT)
- Cisco IOS Enhanced Conference Bridge (Cisco NM-HDV2, NM-HD-1V/2V/2VE, PVDM2)
- Cisco Video Conference Bridge (CUVC-3510 or 3540)

The following sections cover the hardware resources in more detail.

Cisco Conference Bridge Hardware (Cisco Catalyst WS-X6608-T1 and WS-X6608-E1)

This hardware has eight DSPs that are physically associated to each port, and there are eight ports per card. The 6608 module is supported only in the Catalyst operating system of the 6500 series switch.

Configuration of the DSPs is at the port level, so all DSPs associated to a port perform the same function.

Conference bridges can have up to 32 participants, and each port supports 32 conference bridges.

For conferences with G.711 or G.723, there can be 32 conferences per port. If G.729 calls are used, there can be 24 conferences per port. The 6608-T1/E1 gateway module is end of sale (EoS).

Cisco IOS Conference Bridge (Cisco NM-HDV and 1700 Series Routers)

This hardware uses the PVDM-256K-type modules that are based on the C549 DSP chipset. Conferences using this hardware provide bridges that allow up to six participants in a single bridge.

The resources are configured per DSP for conference bridges.

The NM-HDV can have up to four PVDM-256K modules, whereas the Cisco 1700 series routers can have one or two PVDM-256K modules.

Each DSP provides a single conference bridge that can accept G.711 or G.729 calls.

The Cisco 1751 is limited to five conference calls per chassis, and the Cisco 1760 can support 20 conference calls per chassis.

Any PVDM2-based hardware, such as the NM-HDV2, can be used simultaneously in a single chassis for voice termination but cannot be used simultaneously for other media resource functionality. The DSPs based on PVDM-256K and PVDM2 have different DSP farm configurations, and only one can be configured in a router at a time.

Cisco Conference Bridge (Cisco WS-SVC-CMM-ACT)

This Cisco Catalyst-based hardware provides DSP resources that can provide conference bridges of up to 32 participants per bridge.

Each module contains four DSPs that are individually configurable, and each DSP can support 32 conference bridges.

The G.711 and G.729 codecs are supported on these conference bridges without extra transcoder resources. However, transcoder resources are necessary if other codecs are used.

Cisco IOS Enhanced Conference Bridge (Cisco NM-HDV2, NM-HD-1V/2V/2VE, 2800 and 2900 Series, and 3800 and 3900 Series Routers)

Based on the Texas Instruments (TI) C5510 DSP chipset, the NM-HDV2 and the router chassis use the PVDM2 (Packet Voice DSP Modules - 2nd generation) modules for providing DSPs.

DSPs on PVDM2 hardware are configured individually as voice termination, conferencing, media termination, or transcoding resources. The DSPs on a single PVDM can be used as different resource types. Allocate DSPs to voice termination first and then to other functionality as needed.

The NM-HDV2 (high-density voice) has four slots that will accept PVDM2 modules in any combination. The other network modules have fixed numbers of DSPs.

A conference based on these DSPs allows a maximum of eight participants by default. When a conference begins, all eight positions are reserved at that time. This means that unused DSP resources on the same DSP chip are not available for other conferences. The **maximum-participant** command can be used to change the maximum number of participants at the expense of the number of conferences.

The PVDM2-8 is listed as having a DSP because it has a DSP that has half the processing capacity of the PVDM2-16. If the DSP on a PVDM2-8 is configured for G.711, it can provide (0.5×8) bridges/DSP = 4 conference bridges. PVDM2 modules are available in 8, 16, 32, 48, or 64 quantities. The number of resources uses a divisor of 16. A PVDM2-64 has $64/8$, or 8 DSP resources, which will allow up to 64 conferences with 8 conference participants in each conference. The PVDM2 I/O limits the number of conference streams in this scenario because 512 (64×8) audio streams are possible with 64 conferences of 8 conference participants. A DSP farm is a configuration parameter in Cisco IOS that specifies which codecs are supported for the DSPs that are working together (farming). A DSP farm that is configured for conferencing for G.711 provides eight conferences. When configured to accept both G.711 and G.729 calls, a single DSP provides two conferences because it is also reserving its resources for performing transcoding of streams.

The I/O of an NM-HDV2 is limited to 400 streams, so ensure that the number of conference resources allocated does not cause this limit to be exceeded. If G.711 conferences are configured, no more than 6 DSPs (total of 48 conferences with 8 participants each) should be allocated per NM because 48×8 participants = 384 streams. If all conferencing is configured for both G.711 and G.729 codecs, each DSP provides only two conferences of eight participants each. In this case, it is possible to populate the network module (NM) fully and configure it with 16 DSPs (PVDM2-64) because there can only be 2 conferences with 8 participants (16) or 1 conference with 16 participants in each of the 16 DSPs ($16 \times 16 = 256$ streams).

In addition to the PVDM2 modules, Cisco has recently announced the PVDM3 module, which supports up to 256 channels and allows rich-media applications that require more processing power, such as multistream video and voice transcoding with high-bandwidth codecs.

Conferences cannot natively accept calls using the GSM codec. A transcoder must be provided separately for these calls to participate in a conference.

MeetMe conferences allow users to dial in to a conference. Ad hoc conferences allow the conference controller to add specific participants to the conference.

MeetMe conferences require that a range of directory numbers (DN) be allocated for exclusive use of the conference. When a MeetMe conference is set up, the conference controller chooses a DN and advertises it to members of the group. The users call the DN to join the conference after the conference controller has set up the bridge using the MeetMe softkey.

Ad hoc conferences comprise two types:

- **Basic:** In basic ad hoc conferencing, the originator of the conference acts as the controller of the conference and is the only participant who can add or remove other participants.
- **Advanced:** In advanced ad hoc conferencing, any participant can add or remove other participants; that capability is not limited to the originator of the conference. Advanced ad hoc conferencing also allows linking multiple ad hoc conferences. Choose **System > Service Parameters** and set the Advanced Ad Hoc Conference Enabled cluster-wide service parameter to True to gain access to advanced ad hoc conferencing. Advanced ad hoc conferencing is also referred to as conference chaining.

Conferencing Media Resource Configuration

The following steps are required to configure media resources:

Step 1. Configure software conference media resources (if desired).

- a. Enable the IP Voice Media Streaming application service.
- b. Configure the IP Voice Media Streaming application service parameters.
- c. Configure the desired software conferencing media resources.

Step 2. Implement hardware conference media resources (if desired).

- a. Configure the hardware media resources in CUCM.
- b. Configure the hardware media resources in Cisco IOS.
- c. Verify that hardware media resources are registered with CUCM.

The Cisco IP Voice Media Streaming application service is activated in Cisco Unified Serviceability at **Tools > Service Activation**. At the top of the Service Activation window, the server on which services should be activated or deactivated has to be selected. After selecting the server, select the Cisco IP Voice Media Streaming App check box (see Figure 13-7) and click **Save** to activate the service.

The Cisco IPVMS parameters are accessible through CUCM Administration by choosing **System > Service Parameters**. The following two conference bridge service parameters are illustrated in Figure 13-8:

- **Call Count:** This parameter specifies the maximum number of conference participants that the conference bridge will support. Increasing this value above the recommended default might cause performance degradation on a CUCM server that is also performing call processing (coresident). If this value needs to be tuned above the default, consider installing the Cisco IPVMS on a standalone server. Alternatively, hardware conferencing or a version of Cisco MeetingPlace can be used to offload conferencing processing from the call-processing server. The configurable range is 0 to 256, and the default is 48.

Service Activation

Save Set to Default Refresh

Status
Status : Ready

Select Server
Server* cucm Go
Check All Services

CM Services

Service Name	Activation Status
Cisco CallManager	Activated
Cisco Tftp	Activated
Cisco Messaging Interface	Activated
Cisco Unified Mobile Voice Access Service	Activated
Cisco IP Voice Media Streaming App	Activated
Cisco CTIManager	Activated
Cisco Extension Mobility	Activated
Cisco Extended Functions	Activated
Cisco Dialed Number Analyzer	Activated
Cisco DHCP Monitor Service	Activated

CTI Services

Service Name	Activation Status
Cisco CallManager Attendant Console Server	Activated
Cisco IP Manager Assistant	Activated
Cisco WebDialer Web Service	Activated

Figure 13-7 IP Voice Media Streaming Application Service Activation

Service Parameter Configuration

Save Set to Default Advanced

Annunciator (ANN) Parameters

Call Count *	48
Run Flag *	True

Conference Bridge (CFB) Parameters

Call Count *	48
Run Flag *	True

Media Termination Point (MTP) Parameters

Call Count *	48
Run Flag *	True

Figure 13-8 IP Voice Media Streaming Application Service Parameters

- **Run Flag:** This parameter determines whether the conference bridge functionality of the Cisco IPVMS is enabled. Valid values specify True (enabled) or False. The default is True. All media resources are turned on by default when the Cisco IPVMS is

activated. Each media service can be turned on or off individually through the service parameters or MoH server configuration.

Figure 13-9 shows the default configuration of a software conference resource. The only configurable items are Name, Description, Device Pool, Common Device Configuration, and Location.

The screenshot displays the 'Conference Bridge Configuration' window. At the top, there are 'Save' and 'Reset' buttons. Below them is a 'Status' section indicating 'Status: Ready'. The main configuration area is titled 'Conference Bridge Information' and contains the following details:

- Conference Bridge : CFB_2 (CFB_cucm)
- Registration Registered with Cisco Unified Communications Manager cucm
- IP Address 172.16.93.14

Below this is the 'Software Conference Bridge Info' section, which includes the following fields:

Conference Bridge Type*	Cisco Conference Bridge Software
Host Server	cucm
Conference Bridge Name*	CFB_2
Description	CFB_cucm
Device Pool*	Default
Common Device Configuration	< None >
Location*	Hub_None

Figure 13-9 IP Voice Media Streaming Application Service Parameters

Note The CUCM software conferencing media resource supports only the G.711 and Cisco wideband audio codecs. A hardware conference bridge or transcoder is necessary to allow devices that use other audio codecs to participate in a conference.

When adding a hardware conference bridge in CUCM, the type of conference bridge must match the hardware family used. The IOS Enhanced Conference Bridge used in Figure 13-9 represents an NM-HDV2 or NM-HD-1V/2V/2VE, as discussed earlier in this chapter. This particular type of conference bridge is configured by name, which must match between CUCM and the Cisco IOS router.

To add a hardware conference bridge, navigate to **Media Resources > Conference Bridge** and click the **Add New** button. The Conference Bridge Configuration window displays. Enter the appropriate settings for that particular conference bridge and click **Save**. Figure 13-10 is based on a Cisco IOS Enhanced Conference Bridge configuration. Configurable parameters vary by platform:

- **Conference Bridge Type:** Choose Cisco IOS Enhanced Conference Bridge.
- **Conference Bridge Name:** Enter a name for the conference bridge. The name must match the name of the conference media resource as configured at the Cisco IOS router.

Conference Bridge Configuration	
<input type="button" value="Save"/>	Rela
Status	
(i) Status: Ready	
Conference Bridge Information	
Conference Bridge : New	
IOS Conference Bridge Info	
Conference Bridge Type*	Cisco IOS Enhanced Conference Bridge
Conference Bridge Name*	cfb001b0cc250f8
Description	cfb001b0cc250f8
Device Pool*	Default
Common Device Configuration	< None >
Location*	Hub_None
Device Security Mode*	Non-Secure Conference Bridge

Figure 13-10 Cisco IOS Enhanced Conference Bridge Configuration

Note The name of the Cisco IOS Enhanced Conference Bridge configured in CUCM must match the name of the conference bridge configured in the Cisco IOS router. The name is case sensitive. Good naming conventions should be used to easily identify the component. Prefix CFB (conference bridge), and then use a burned-in MAC address of the router. CFB012345012345 is an example of a hardware conference bridge in a router where the MAC address of 012345012345 is burned into the Gigabit Ethernet controller.

- **Device Pool:** Choose a device pool. Best practice is to configure a separate device pool dedicated to media resources. A good naming convention recommendation is `Media_Resources_DP`.
- **Common Device Configuration:** Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes such as the MoH audio source.
- **Location:** Choose the appropriate location for this conference bridge to enforce call admission control (CAC). The location specifies the total bandwidth that is available for calls to and from this location. A location setting of `Hub_None` means that the Locations feature does not keep track of the bandwidth that this conference bridge consumes. CAC is covered in detail in the Cisco Press book *Implementing Cisco Unified Communications Manager, Part 2 (CIPT2)*.

- **Device Security Mode:** This field displays for Cisco IOS Enhanced Conference Bridge because only this audio conference bridge supports secure encrypted conferencing starting in CUCM version 6.0. If choosing Non Secure Conference Bridge, the nonsecure conference establishes a TCP port connection to CUCM on port 2000. Ensure that this setting matches the security setting on the conference bridge; otherwise, the call will fail. The Encrypted Conference Bridge setting supports the secure conference feature. Refer to the *CUCM Security Guide* for secure conference bridge configuration procedures.

Example 13-1 is a configuration of a Cisco IOS Enhanced Conference Bridge. Each command is explained following the configuration example.

Example 13-1 Cisco IOS Configuration

```

voice-card 0
  dspfarm
    dsp services dspfarm

  sccp local FastEthernet0/0.72
  sccp ccm 10.1.1.1 identifier 1 version 6.0
  sccp

  sccp ccm group 1
    associate ccm 1 priority 1
    associate profile 1 register CFB001B0CC250F8

  dspfarm profile 1 conference
    codec g711ulaw
    codec g711alaw
    codec g729ar8
    codec g729abr8
    maximum sessions 2
    associate application SCCP
    no shutdown

```

- **dspfarm (DSP farm):** To enable DSP farm service, use the **dspfarm** command in global configuration mode. The DSP farm service is disabled by default.
- **dsp services dspfarm:** To enable DSP farm services for a particular voice network module, use the **dsp services dspfarm** command.
- **sccp local:** To select the local interface that SCCP applications (transcoding and conferencing) use to register with CUCM, use the **sccp local** command in global configuration mode.

- **sccp ccm:** To add a CUCM server to the list of available servers and set various parameters, including IP address or Domain Name System (DNS) name, port number, and version number, use the **sccp ccm** command in global configuration mode.
- **sccp:** To enable the SCCP protocol and its related applications (transcoding and conferencing), use the **sccp** command in global configuration mode.
- **sccp ccm group:** To create a CUCM group and enter SCCP CUCM configuration mode, use the **sccp ccm group** command in global configuration mode.
- **associate ccm:** To associate a CUCM with a CUCM group and establish its priority within the group, use the **associate ccm** command in SCCP CUCM configuration mode.
- **associate profile:** To associate a DSP farm profile with a CUCM group, use the **associate profile** command in SCCP CUCM configuration mode.
- **dspfarm profile:** To enter DSP farm profile configuration mode and define a profile for DSP farm services, use the **dspfarm profile** command in global configuration mode.
- **codec (DSP):** To specify call density and codec complexity based on a particular codec standard, use the **codec** command in DSP interface DSP farm configuration mode.
- **associate application sccp:** To associate SCCP to the DSP farm profile, use the **associate application sccp** command in DSP farm profile configuration mode.
- **maximum sessions (DSP farm profile):** To specify the maximum number of sessions that are supported by the profile, use the **maximum sessions** command in DSP farm profile configuration mode.
- **no shutdown:** If you fail to use the **no shutdown** command, the DSP farm profile will display in the gateway but fail to operate.

To verify the Cisco IOS media resource configuration, use the **show** commands demonstrated in Example 13-2.

Example 13-2 Verifying Cisco IOS Media Resource Configuration

```
Gateway# show sccp
SCCP Admin State: UP<Anchor0>
Gateway IP Address: 10.1.1.101, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.1.1.1, Port Number: 2000<Anchor2>
    Priority: N/A, Version: 6.0, Identifier: 1
Conferencing Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.1.1.1, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 1
Reported Max Streams: 16, Reported Max OOS Streams: 0
```

```

Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
Supported Codec: g729r8, Maximum Packetization Period: 60
Supported Codec: g729br8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30
Gateway# show sccp ccm group 1
CCM Group Identifier: 1
Description: None
Binded Interface: NONE, IP Address: NONE
Associated CCM Id: 1, Priority in this CCM Group: 1
Associated Profile: 1, Registration Name: CFB001B0CC250F8
Registration Retries: 3, Registration Timeout: 10 sec
Keepalive Retries: 3, Keepalive Timeout: 30 sec
CCM Connect Retries: 3, CCM Connect Interval: 10 sec
Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
Signaling DSCP value: cs3, Audio DSCP value: ef

Gateway# show dspfarm profile 1

Dspfarm Profile Configuration
Profile ID = 1, Service = CONFERENCING, Resource ID = 1<Anchor10> <Anchor11>

Profile Description :
Profile Admin State : UP
Profile Operation State : ACTIVE
Application : SCCP Status : ASSOCIATED
Resource Provider : FLEX_DSPRM Status : UP
Number of Resource Configured : 2
Number of Resource Available : 2
Codec Configuration
Codec : g711ulaw, Maximum Packetization Period : 30 , Transcoder: Not Required
Codec : g711alaw, Maximum Packetization Period : 30 , Transcoder: Not Required
Codec : g729ar8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729abr8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729r8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729br8, Maximum Packetization Period : 60 , Transcoder: Not Required

```

Various CUCM service parameters are related to conferencing. You should consider the following conferencing options when leveraging the conferencing features of CUCM:

- **Suppress Music on Hold to Conference Bridge:** This parameter determines whether MoH plays to a conference when a conference participant places the conference on hold. Valid values specify True (the system does not play MoH to the conference when a conference participant presses the Hold button) or False. The default is True.
- **Drop Ad Hoc Conference:** This parameter determines how an ad hoc conference terminates. This is an important toll-fraud prevention setting, because inside facilitators can set up a conference call to expensive international numbers and then drop out of the call. Without the conference controller, international tariffs are billed back to the company in which the conference call was set up. Valid values are as follows:
 - **Never (default):** The conference remains active after the conference controller and all On-Net parties hang up. This default setting could result in potential toll fraud.
 - **When Conference Controller Leaves:** Terminate the conference when the conference controller hangs up.
 - **When No On-Net Parties Remain in the Conference:** Terminate the conference when there are no On-Net parties remaining in the conference. This distinction is important because the conference controller might have to drop out of the call, but other business partners on the call should continue the conference. The When Conference Controller Leaves option would hang up the call when the conference controller left the conference.
- **Advanced Ad Hoc Conference Enabled:** This parameter determines whether advanced ad hoc conference features are enabled. Advanced ad hoc conference features include the ability for conference participants other than the conference controller to add new participants to an existing ad hoc conference (conference chaining), the ability for any noncontroller conference participant to drop other participants from the conference through the ConfList and RmLstC softkeys, and whether ad hoc conferences can be linked using features such as conference, join, direct transfer, and transfer. Valid values specify True (allow advanced ad hoc conference features) or False. The default is False.
- **Nonlinear Ad Hoc Conference Linking Enabled:** This parameter determines whether more than two ad hoc conferences can be linked directly to an ad hoc conference in a nonlinear fashion. Nonlinear conference linking occurs when three or more ad hoc conferences are linked directly to one other ad hoc conference. Linear conference linking occurs when one or two ad hoc conferences are linked directly to one other ad hoc conference. For this parameter to work, the Advanced Ad Hoc Conference Enabled service parameter must be set to True. Valid values specify True (allow nonlinear conference linking so that three or more ad hoc conferences can be linked to a single other conference) or False. The default is False. The Advanced Ad Hoc Conference Enabled service parameter must be set to True for the Nonlinear Ad Hoc Conference Linking Enabled service parameter to work.

- **Maximum Ad Hoc Conference:** This parameter specifies the maximum number of participants who are allowed in a single ad hoc conference. The value of this field depends on the capabilities of the software/hardware conference bridge. The maximum number of conference bridge participants for typical conference bridges follows: Software, 64; Cisco Catalyst WS-X6608, 16; Cisco Catalyst 4000, 16; and NM-HDV, 6. Setting this value above the maximum capacity of the conference resource will result in failed entrance to a conference bridge if more ports than the specific conference bridge configuration allows are added. The range is 3 to 64. The default is 4.
- **Maximum MeetMe Conference Unicast:** This parameter specifies the maximum number of participants that are allowed in a single MeetMe conference. The value of this field depends on the capabilities of the software/hardware conference bridge. A software conference bridge is capable of conferencing up to 128 participants. When a conference is created, the system automatically reserves a minimum of three streams, so specifying a value less than 3 allows a maximum of three participants. The range is 1 to 128. The default is 4.

MeetMe Conference Configuration

To add a range of numbers to be used for MeetMe conferences in CUCM Administration, choose **Call Routing > MeetMe Number/Pattern** and click **Add New**. Configure the new pattern with the following data:

- **Directory Number or Pattern:** Enter a MeetMe number or number range.
- **Description:** Enter up to 30 alphanumeric characters for a description of the MeetMe number.
- **Partition:** To use a partition to restrict access to the MeetMe/number pattern, choose the desired partition from the drop-down list.
- **Minimum Security Level:** Choose the minimum MeetMe conference security level for this MeetMe number or pattern from the drop-down list:
 - Choose **Authenticated** to block participants with nonsecure phones from joining the conference.
 - Choose **Encrypted** to block participants with authenticated or nonsecure phones from joining the conference.
 - Choose **Non Secure** to allow all participants to join the conference.

Figure 13-11 shows a MeetMe range of 100 numbers beginning with 4500 and ending with 4599. The numbers are not in a partition, which will allow any phone to set up a MeetMe bridge by clicking the MeetMe softkey and dialing one of the numbers in the MeetMe number range. Subsequent meeting members will need to dial only the number of the bridge.

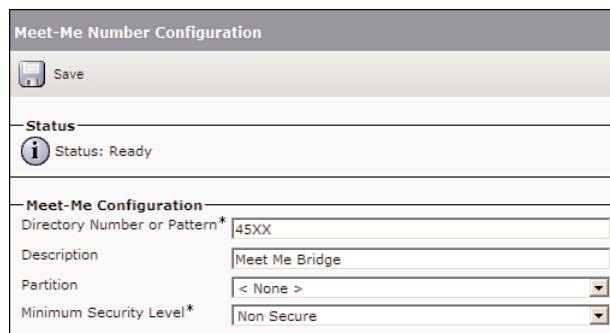


Figure 13-11 *MeetMe Conference Bridge Configuration*

Note MeetMe bridges do not offer any security, scheduling, or name-confirmation features. Security and scheduling features are offered by the Cisco MeetingPlace and Cisco MeetingPlace Express products. The conference controller could be given access to the ConfList softkey, which will allow the controller to view the conference participants by caller ID information. The conference controller can individually remove users, but the conference controller does not have access to the users' line state information. Cisco MeetingPlace and MeetingPlace Express allow the conference controller to see which conference participant has a phone on hold. This is especially useful if MoH is being injected into the conference bridge. If the bridge has not been set up by the controller, callers to the MeetMe number pattern receive a reorder tone.

Music on Hold

CUCM can be configured to provide music on hold (MoH). The MoH feature has two main requirements:

- An MoH server must provide the MoH audio stream sources.
- CUCM must be configured to use the MoH streams provided by the MoH server when a call is placed on hold.

The integrated MoH feature enables users to place On-Net and Off-Net callers on hold with music instead of the default “on hold tone.” The MoH source makes music available to any On-Net or Off-Net device placed on hold. On-Net devices include Cisco IP Phones and applications placed on hold. Off-Net users include those connected through Media Gateway Control Protocol (MGCP), SIP, and H.323 gateways. The MoH feature is also available for plain old telephone service (POTS) phones connected to the Cisco IP network through Foreign Exchange Station (FXS) ports.

It is also possible to configure multicast MoH streaming to leverage external media servers providing media streams. CUCM Express and Cisco Unified Survivable Remote

Site Telephony (SRST) gateways can be configured as media streaming servers for MoH, too. The CUCME and SRST router-based resources provide MoH by streaming one audio file stored in the router's flash memory or a fixed audio source connected through an optional ear and mouth (E&M) hardware interface. You can find detailed information about this feature in the CUCM Solution Reference Network Design (SRND) guide at Cisco.com.

The CUCM integrated MoH server supports multicast and unicast for MoH streaming. The advantage of using multicast for MoH streaming over unicast is to save bandwidth and to reduce load on the MoH server. Saving bandwidth is normally not a major issue for campus LAN environments, but reducing load on the MoH server is always a big consideration. Reducing the number of media streams is especially advantageous when the MoH server is colocated on the same server as call processing. It is advisable to scope MoH traffic to the local site so that MoH does not consume WAN bandwidth. There are various ways of implementing multicast scoping and unicast filtering on the data network.

MoH audio codecs (G.711 mu-law, G.711 a-law, Cisco wideband, and G.729) are generated by CUCM when files with a .wav extension are uploaded to the MoH server. The recommended format for audio source files includes the following specifications:

- 16-bit PCM WAV file
- Stereo or mono
- Sample rates of 48, 32, 16, or 8 kHz

If live audio (Muzak, radio broadcast) is a requirement, MoH can be generated from a fixed source. A sound card is required for a fixed audio source. The fixed audio source is connected to the audio input (line in) of the local sound card. The Cisco MoH USB audio sound card (MUSIC ON HOLD-USB-AUDIO=) must be used for connecting a fixed audio source to the MoH server. This USB sound card is compatible with all MCS platforms supporting CUCM Release 6.x.

This mechanism enables the use of radios, CD players, or any other compatible sound source. The stream from the fixed audio source is transcoded in real time to support the codec that was configured through CUCM Administration. The fixed audio source can be transcoded into G.711 (a-law or mu-law), G.729 Annex A, and wideband, and it is the only audio source that is transcoded in real time.

Before using a fixed audio source to transmit MoH, consider the legalities and the ramifications of rebroadcasting copyrighted audio materials. Consult your legal department for potential issues.

A unicast MoH stream is a point-to-point, one-way audio RTP stream between the server and one endpoint device. Unicast MoH uses a separate source stream for each connection. As more endpoint devices receive MoH, the number of MoH streams increases. If 100 devices are on hold, there will be 100 independent streams of RTP traffic generated over the network between the server and the endpoints receiving the MoH. The number

of streams can potentially have a negative effect on network throughput. Unicast MoH can be useful in networks where multicast is not enabled or where devices are not capable of multicast, thereby still allowing an administrator to take advantage of the MoH feature.

Multicast MoH streams are point-to-multipoint, one-way audio RTP stream between the MoH server and the multicast group IP address. Multicast MoH conserves system resources and bandwidth because it enables multiple users to use the same audio source stream to provide MoH. If 100 devices were simultaneously on hold, a single multicast RTP stream could be replicated over the network to all 100 resources. Bandwidth and server processor utilization would be greatly reduced. It is recommended to use a multicast IP address of 239.1.1.1 through 239.255.255.254 because these multicast addresses are implicitly scoped by the router because the IP packets are generated with a time to live (TTL) value of 2. Each data router decrements the TTL value by 1. When a TTL of 0 is reached, the packet is not forwarded by a router. A TTL of 0 has a drop operation.

The basic operation of MoH in a Cisco Unified Communications environment consists of a holding party and a held party. The holding party is the endpoint placing a call on hold, and the held party is the endpoint placed on hold, receiving MoH.

The MoH stream that an endpoint receives is determined by a combination of the user hold audio source identifier of the device placing the endpoint on hold (holding party) and the configured prioritized list of MoH resources of the endpoint placed on hold (held party). The user hold audio source configured for the holding party determines the audio file that will be streamed when the holding party puts a call on hold, and the held party's list of MoH resources determines the server from which the held party will receive the MoH stream.

Figure 13-12 illustrates an On-Net phone being placed on hold by a phone with a different MoH audio source identifier and server configuration. Phone B places Phone A on hold. Phone B will instruct CUCM to place Phone A on hold with Audio Source 2 and the MoH server relevant to Phone B's configuration.

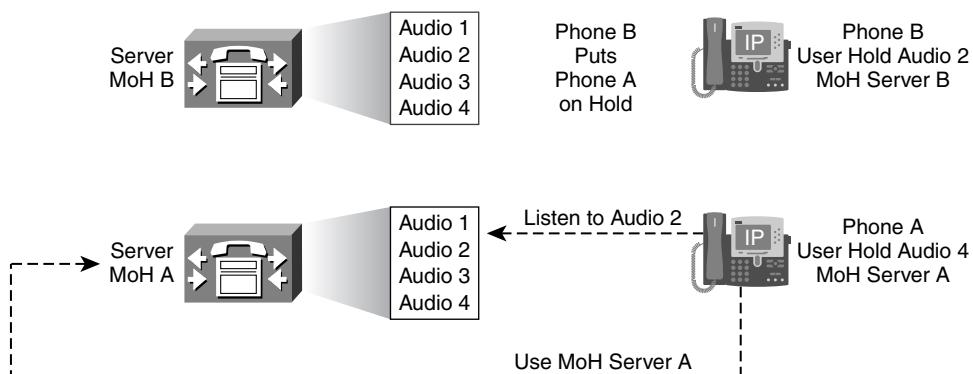


Figure 13-12 *Music on Hold: Resource Selection*

Note When multiple MoH servers are active in your network, make sure that all the configured MoH files are available on all MoH servers.

MoH Configuration

Configuration of MoH consists of four main steps. Additional configuration is required if multicast MoH is used.

Step 1. Plan MoH server capacity.

Step 2. Configure MoH audio sources:

- a. Convert MoH audio files.
- b. Configure MoH audio sources.

Step 3. Configure the MoH server.

Step 4. Configure MoH service parameters.

Step 5. (Optional) Configure multicast for MoH:

- a. Configure audio sources for multicast MoH.
- b. Configure the server for multicast MoH.

Capacity planning is crucial to ensure that the hardware can support the anticipated MoH volume of the network. The 7815 and 7825 servers allow up to 250 users to be placed on hold, and the 7835 and 7845 servers allow up to 500 users to be placed on hold (co-resident or standalone). If MoH sessions exceed the platform limitations, various issues can arise:

- Poor MoH quality
- Erratic MoH operation
- Loss of MoH functionality

The following MoH server configuration parameters affect MoH server capacity:

- **Maximum Half Duplex Streams:** This parameter determines the number of devices that can be placed on unicast MoH. This value is set to 250 by default. The Maximum Half Duplex Streams parameter should be set to the value derived from the following formula: $(\text{Server capacity}) - [(\text{Number of multicast MoH sources}) \times (\text{Number of MoH codecs enabled})]$. The value of this parameter should never be set higher than the hardware capacity of the server.
- **Maximum Multicast Connections:** This parameter determines the number of devices that can be placed on multicast MoH. The default value is set to 30, which represents a maximum of 30,000. Multicast connections are configured in thousands of held parties because multicast is scalable. The Maximum Multicast Connections parameter should be set to a number that ensures that all devices can be placed on multicast

MoH if necessary. Although the MoH server can generate only a finite number of multicast streams (204), a large number of held devices can join each multicast stream through the network multicast protocols. This parameter should be set to a number that is greater than or equal to the number of devices that might be placed on multi-cast MoH at any given time.

Typically, multicast traffic is accounted for based on the number of streams being generated; however, CUCM maintains a count of the actual number of devices placed on multicast MoH or joined to each multicast MoH stream. This method is different from the way multicast traffic is normally tracked. You can find additional information in the CUCM SRND guide (www.cisco.com/go/srnd).

CUCM ships with a default MoH audio file. To add additional MoH audio files, navigate to **Media Resources > MoH Audio File Management** from CUCM Administration (shown in Figure 13-13). Click the **Upload File** button, and browse the local directory structure for the WAV audio file.

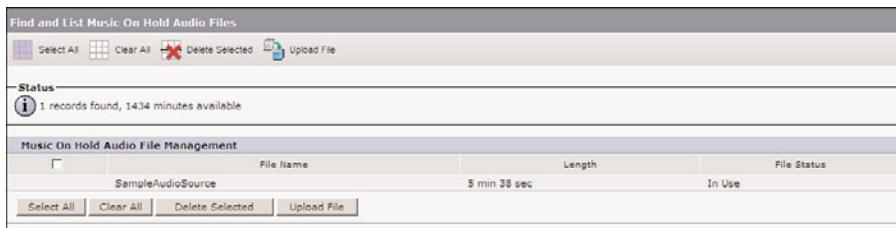


Figure 13-13 Music on Hold: Audio File Conversion

The uploaded file is automatically converted into four different audio formats. A file status of Translation Complete indicates that the audio file has been successfully converted. If any other status is displayed, or if the status remains open for a long period of time (conversion can take up to several minutes), the audio file translation has failed. The uploaded audio file might be in the wrong file format or have improper audio qualities.

Choose **Media Resources > Music On Hold Audio Source** from CUCM Administration to configure the MoH audio sources, as illustrated in Figure 13-14. The MoH audio sources are identified by an MoH audio stream number from 1 to 51. Up to 50 prerecorded sources and one live audio source are available per CUCM cluster.

In the Music On Hold Audio Source Configuration window, select the MoH audio stream number of the audio source that you want to configure. Choose the MoH audio source file. The MoH audio source name defaults to the MoH audio source filename, but it can be modified. Enable continuous playing (repeat) of the audio file if desired.

If a fixed audio source will be used, navigate to **Media Resources > Fixed MoH Audio Source** from CUCM Administration to configure a fixed MoH audio source. The source ID is 51 and cannot be modified. The name of the fixed MoH audio source has to be entered, and the fixed MoH audio source must be enabled. Figure 13-15 shows this configuration.

Music On Hold Audio Source Configuration

		<input type="button" value="Save"/> <input type="button" value="Delete"/> <input type="button" value="Add New"/> <input type="button" value="Upload File"/>
Status		
Status: Ready		
Music On Hold Server Audio Source Information		
MOH Audio Stream Number* <input type="text" value="2"/>		
MOH Audio Source File <input type="text" value="Sample AudioSource"/>		
MOH Audio Source Name* <input type="text" value="Sample AudioSource"/>		
<input checked="" type="checkbox"/> Play continuously (repeat) <input checked="" type="checkbox"/> Allow Multicasting		
MOH Audio Source File Status		
<pre> InputFileName: Sample AudioSource ErrorCode: 0 ErrorText: Translation Complete DurationSeconds: 338 DiskSpaceKB: 8092 LowDateTime: 1130860118 HighDateTime: 0 OutputFileList: Sample AudioSource.ulaw.wav Sample AudioSource.alaw.wav Sample AudioSource.g729.wav </pre>		

Figure 13-14 Music on Hold: Audio Source Configuration

Fixed MOH Audio Source Configuration

		<input type="button" value="Save"/> <input type="button" value="Delete"/>
Status		
Status: Ready		
Fixed MOH Audio Source Information		
Source ID* <input type="text" value="51"/>		
Name* <input type="text" value="cdrom"/>		
<input checked="" type="checkbox"/> Allow Multicasting <input checked="" type="checkbox"/> Enable (If checked, Name is required.)		

Figure 13-15 Music on Hold: Fixed Audio Source Configuration

Choose **Media Resources > Music On Hold Server** from CUCM Administration to configure the MoH server parameters. Figure 13-16 illustrates the default configuration of the MoH media resource. Various parameters can be modified. It is best practice to use a media resource device pool. If MoH functionality is not desired on this server, but other services of the Cisco IPVMS are, the run flag should be set to No. If a fixed audio source that is physically connected to the server is used, the name of the audio source device has to be specified.

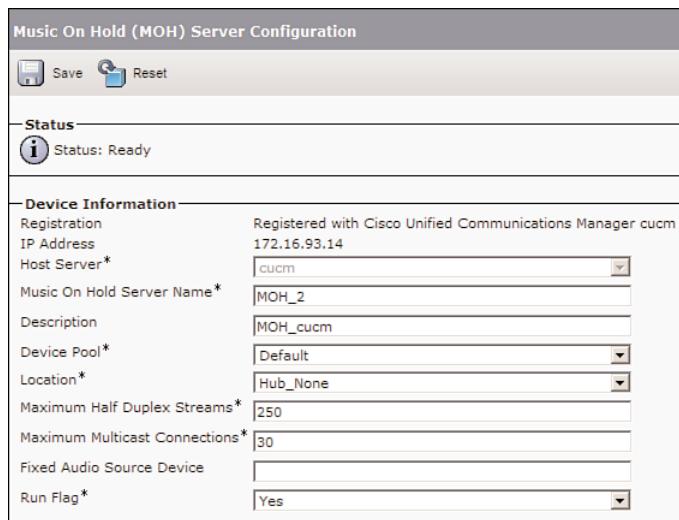


Figure 13-16 Music on Hold: Server Configuration

The following list of CUCM service parameters and the associated defaults are related to MoH:

- Suppress MoH to Conference Bridge (True)
- Default Network Hold MoH Audio Source ID (1)
- Default User Hold MoH Audio Source ID (1)
- Duplex Streaming Enabled (False)

To enable multicast MoH on an MoH server, the Multicast Audio Source Information section of the MoH Server Configuration window must be configured. Select the Enable Multicast Audio Sources on This MoH Server check box. The Base Multicast IP Address, Base Multicast Port Number, and Increment Multicast On parameters are automatically populated when you enable multicast MoH on the server. You can modify these values if desired. Figure 13-17 shows this section of the MoH Server Configuration page.

Note It is recommended to increment multicast on IP address rather than port number to avoid network saturation in firewall situations. This results in each multicast audio source having a unique IP address and helps to avoid network saturation.

All MoH audio sources that have been configured to allow multicasting are listed in the Selected Multicast Audio Sources section of the MoH Server Configuration window. Each audio source can have a different Max Hops value (default is 2). This parameter sets the TTL value in the IP header of the multicast MoH RTP packets to the specified value.

The TTL field in an IP packet indicates the maximum number of routers that an audio source is allowed to cross. If the Max Hops value is set to 1, the multicast MoH RTP packets remain in the subnet of the multicast MoH server.

Music On Hold (MOH) Server Configuration

Multicast Audio Source Information

- Enable Multicast Audio Sources on this MOH Server:
- Base Multicast IP Address: 239.1.1.1
- Base Multicast Port Number: 16384 (Even numbers only)
- Increment Multicast on: Port Number IP Address

Selected Multicast Audio Sources

There are no Music On Hold Audio Sources selected for Multicasting. Click Configure Audio Sources in the top right corner of the page to select Multicast Audio Sources.

Figure 13-17 Music on Hold: Server Configuration (Multicast Settings)

Note When you are using multicast MoH for devices that are not in the same IP subnet, multicast routing has to be enabled in the IP network.

Select the Allow Multicasting check box for each MoH audio source. This applies to MoH audio sources and to fixed MoH audio sources.

Annunciator

An annunciator is automatically created in the system when the Cisco IPVMS is activated on a server. If Cisco IPVMS is deactivated, the annunciator is also deleted. A single annunciator instance can service the entire CUCM cluster if it meets the performance requirements. Additional annunciators can be configured for the cluster if necessary.

The annunciator registers with a single CUCM at a time, as defined by its device pool. It automatically fails over to a secondary CUCM if a secondary is configured for the device pool. Any announcement that is playing at the time of an outage is not maintained.

The annunciator service is responsible for the following features:

- **Cisco Multilevel Precedence Preemption (MLPP):** This feature has streaming messages that it plays in response to the following call-failure conditions:
 - Unable to preempt because of an existing higher-precedence call.
 - A precedence (prioritization) access limitation was reached.

- The attempted precedence level was unauthorized.
- The called number is not equipped for preemption or call waiting.
- **Integration through SIP trunk:** SIP endpoints can generate and send tones in-band in the RTP stream, but SCCP cannot. An annunciator is used in conjunction with an MTP to generate or accept dual-tone multifrequency (DTMF) tones when integrating with a SIP endpoint.
- **Cisco IOS gateways and intercluster trunks:** These devices require support for call-progress tone (ringback tone).
- **System messages:** During the following call-failure conditions, the system plays a streaming message to the end user:
 - A dialed number that the system cannot recognize
 - A call that is not routed because of a service disruption
 - A number that is busy and not configured for preemption or call waiting
- **Conferencing:** During a conference call, the system plays a barge-in tone to announce that a participant has joined or left the bridge.

The annunciator is configured to support 48 simultaneous streams by default. The maximum recommended is 48 for an annunciator running on the same server with the CUCM service (call processing).

If the server has only 10-Mbps connectivity, lower the setting to 24 simultaneous streams. A standalone server without the CUCM service can support up to 255 simultaneous announcement streams, and a high-performance server with dual CPUs and a high-performance disk system can support up to 400 streams. Multiple standalone servers can be added to support the required number of streams. The maximum streams are configured in the Cisco IPVMS service parameters.

The annunciator can be configured by navigating to **Media Resources > Announcer** from CUCM Administration. Figure 13-18 shows the annunciator configuration.

Media Resource Access Control

All media resources are located in a null media resource group by default. Usage of media resources is load balanced among all existing devices. Hardware resources are preferred in the selection algorithm based on their enhanced capabilities (multiple audio codec support) and the reduction of load on the CUCM.

Media resource management controls and manages the media resources within a cluster. The Media Resource Manager (MRM) service enhances CUCM features by making it easier for CUCM to control access to transcoder, annunciator, conferencing, MTP, and MoH resources.

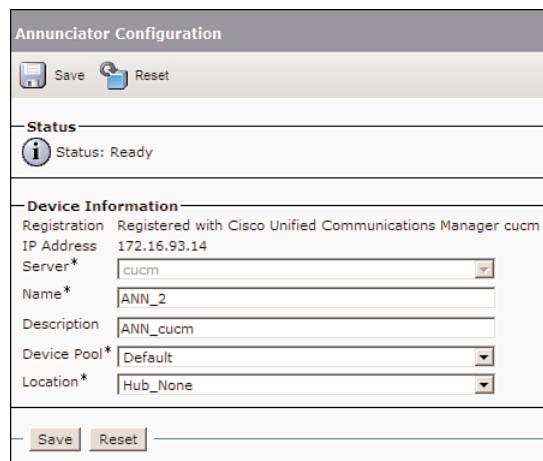


Figure 13-18 Announcer Configuration

Media resource groups (MRG) define logical groupings of media resources. MRGs create a logical collection of resources and are normally arranged to service a geographical location.

Media resource group lists (MRGL) specify a list of prioritized MRGs. An application can select required media resources from among the available resources according to the priority order that is defined in the MRGL. MRGLs are assigned to devices or device pools. Figure 13-19 illustrates the hierarchical processing order of media resources. MRGLs are similar to route lists, whereas MRGs are similar to route groups.

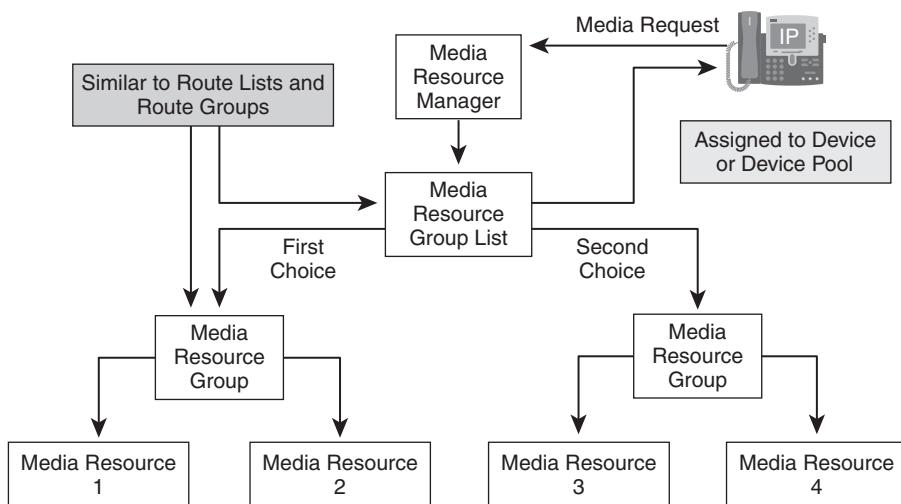


Figure 13-19 Media Resource Management

Figure 13-20 shows a media resource management scenario based on arbitrary values for learning purposes.

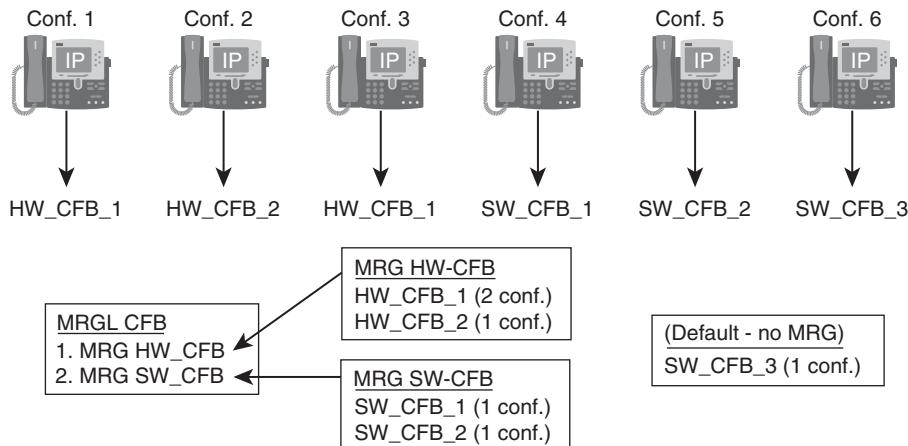


Figure 13-20 Media Resource Management Example

The five conference bridges in Figure 13-20 have the following capabilities:

- HW_CFB_1: two-conference capacity
- HW_CFB_2: one-conference capacity
- SW_CFB_1: one-conference capacity
- SW_CFB_2: one-conference capacity
- SW_CFB_3: one-conference capacity

The following media resource groups have been configured:

- MRG_HW-CFB: HW_CFB_1 and HW_CFB_2
- MRG_SW-CFB: SW_CFB_1 and SW_CFB_2
- SW_CFB_3: Not assigned to an MRG

The MRGL of MRGL_CFB has MRG_HW-CFB configured as first priority and MRG_SW-CFB listed as second priority.

Assume that six conferences are established from devices that all use the MRGL_CFB MRGL. The conference bridges will be allocated in the following way:

- The first conference uses conference bridge HW_CFB_1. The second conference uses conference bridge HW_CFB_2, because the resources within an MRG are load shared and not used in the configured order. The third conference uses HW_CFB_1 again because there are available resources available in that conference bridge resource.

- The fourth conference uses a resource in the second media resource group because the first is out of resources. The fourth conference uses SW_CFB_1, and the fifth conference uses SW_CFB_2.
- The sixth conference does not find a free resource in either MRG, but it finds SW_CFB_3 in the default list. Resources not assigned to a media resource group can be used by any device.

Three configuration steps are required to configure media resource access control:

Step 1. Configure the MRGs.

Step 2. Configure the MRGLs.

Step 3. Assign the MRGLs to phones.

To add an MRG, navigate to **Media Resources > Media Resource Group** in CUCM Administration. At the Media Resource Group Configuration window, enter a name and description for the MRG and add the desired media resources to the MRG. An MRG configuration is illustrated in Figure 13-21.

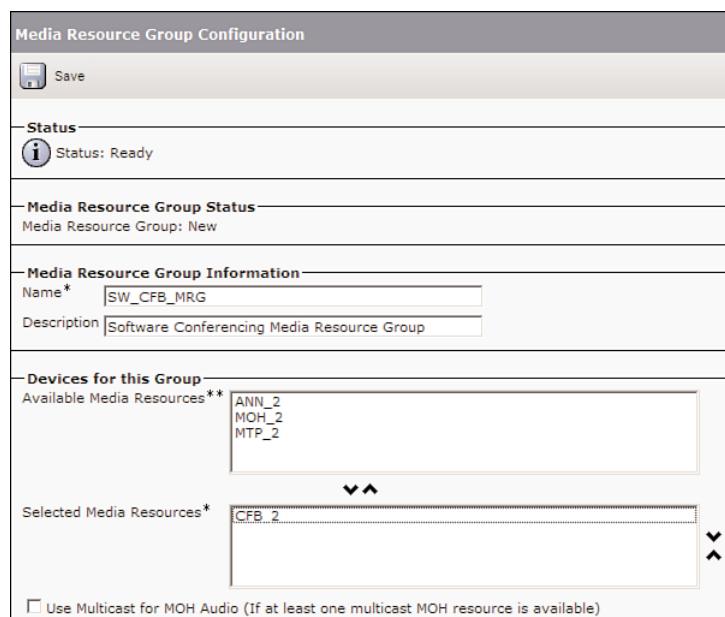


Figure 13-21 *Media Resource Group Configuration*

To add an MRGL, navigate to **Media Resources > Media Resource Group List** in CUCM Administration. At the Media Resource Group List Configuration window, enter a name for the MRGL and add the desired MRG to the MRGL.

Because the order of MRGs within an MRGL specifies the priorities of the MRG, it is important to list the MRGs in the desired order. In Figure 13-22, hardware conference bridges should be used before software conference bridges.

The screenshot shows the 'Media Resource Group List Configuration' window. At the top is a 'Save' button. Below it is a 'Status' section with an 'Info' icon and the text 'Status: Ready'. The main area is divided into sections: 'Media Resource Group List Status' (showing 'Media Resource Group List: New'), 'Media Resource Group List Information' (with a 'Name*' field containing 'Headquarters_MRGL'), and 'Media Resource Groups for this List'. The 'Available Media Resource Groups' section lists 'Sip Trunk - Meda Resources'. The 'Selected Media Resource Groups' section lists 'HW_CFB', 'SW_CFB_MRGL', and 'XCODE_MRGL'. There are up/down arrows between the two sections to move items between them.

Figure 13-22 Media Resource Group List Configuration

MRGLs can be assigned to devices (phones, trunks, or gateways) or to device pools. In Figure 13-23, an MRGL is assigned directly to an IP phone. If the device pool associated with the phone has a different MRGL, the phone configuration overrides the device pool inheritance.

The screenshot shows the 'Device Information' configuration window. It includes fields for Registration (Unknown), IP Address (Unknown), MAC Address* (012345012345), Description (SEP012345012345), Device Pool* (Default), Common Device Configuration (< None >), Phone Button Template* (Standard 7961 SIP), Softkey Template (< None >), Common Phone Profile (Standard Common Phone Profile), Calling Search Space (< None >), AAR Calling Search Space (< None >), Media Resource Group List (Headquarters_MRGL), and User Hold MOH Audio Source (< None >). The 'Media Resource Group List' field is highlighted with a red box.

Figure 13-23 Media Resource Group List Assignment

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- Media resources are required for voice termination, audio conferencing, transcoding, MTP, annunciator, and MoH.
- There are no direct endpoint-to-endpoint audio streams if a media resource is involved.
- Only some hardware-based conference bridges support mixed-mode conferences, with participants using different codecs.
- It is possible to configure external conference bridges to enhance the conferencing capabilities of CUCM.
- If the Cisco IPVMS service is running, very few additional configuration steps are required to enable conferencing.
- A maximum of 51 unique audio sources can be configured in a cluster. For a fixed audio source, a Cisco MoH USB audio sound card is required.
- The MoH stream that an endpoint receives is determined by the user hold audio source of the device placing the endpoint on hold and the configured MRGL of the endpoint placed on hold.
- The annunciator streams spoken messages and various call-progress tones to devices supporting SCCP.
- The Media Resource Manager controls the media resources within a CUCM cluster. The media resources are shared within a cluster.
- To limit media resource access, MRGs and MRGLs must be configured and assigned.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. Which of the following media resources acts as a codec translator?
 - a. Transcoder
 - b. Software conference bridge
 - c. Annunciator
 - d. Music on hold

- 2.** Which of the following media resources requires hardware (digital signal processors)?
 - a.** Conference bridge
 - b.** Music on hold
 - c.** Transcoding
 - d.** Annunciator
- 3.** Which device protocol is used to set up media resources?
 - a.** SCCP
 - b.** H.323
 - c.** SIP
 - d.** MGCP
- 4.** Which two scenarios require a Media Termination Point?
 - a.** Mixed-mode audio conference
 - b.** RFC 2833 on Type A phone
 - c.** RFC 2833 on Type B phone
 - d.** Supplementary services on H.323 Version 1 endpoint
 - e.** Supplementary services on H.323 Version 2 endpoint
- 5.** Which audio codec is supported in software conferencing?
 - a.** iLBC
 - b.** G.729
 - c.** G.722
 - d.** G.711
- 6.** What are the two media resource deployment models?
 - a.** Standalone
 - b.** Centralized
 - c.** Co-resident
 - d.** Distributed

- 7.** What are two types of valid conferences?
 - a.** Reservationless
 - b.** Ad hoc
 - c.** Scheduled
 - d.** MeetMe
 - e.** Broadcast
- 8.** Which network technology limits the processor utilization of music on hold on CUCM?
 - a.** Multicast
 - b.** Broadcast
 - c.** Unicast
 - d.** Anycast
- 9.** Which multicast IP address is used for local multicast?
 - a.** 255.255.255.255
 - b.** 239.1.1.1
 - c.** 225.1.1.1
 - d.** 235.1.1.1
- 10.** What is the maximum number of MoH streams for a 7845 server?
 - a.** 48
 - b.** 250
 - c.** 500
 - d.** 96

Chapter 14

Phone Services

Upon completing this chapter, you will be able to describe and configure Cisco Unified Communications Manager (CUCM) user features and meet these objectives:

- Describe Cisco IP Phone Services
- Describe how to provide redundant Cisco IP Phone Services
- Describe how to configure Cisco IP Phone Services
- Describe Cisco IP Phone Services subscriptions

This chapter describes the purpose and function of Cisco IP Phone Services and discusses how to implement them in Cisco Unified Communications Manager. The chapter also explains how administrators and end users can subscribe Cisco IP Phone Services to Cisco Unified IP phones.

Cisco IP Phone Services

Cisco IP Phone Services are applications that use the web client or server and XML capabilities of the Cisco Unified IP phone. The Cisco Unified IP phone firmware contains a microbrowser that enables limited web-browsing capability. By running directly on the desktop phone of users, these phone-service applications provide the potential for value-added services and productivity enhancement. (For the purposes of this chapter, the term *phone service* refers to an application that transmits and receives content to and from the Cisco Unified IP phone.)

The following phones support Cisco IP Phone Services:

- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified IP Phones 7940G, 7941G, 7942G, and 7945G
- Cisco Unified IP Phones 7960G, 7961G, 7962G, and 7965G

- Cisco Unified IP Phones 7970G, 7971G, and 7975G
- Cisco Unified IP Phones 8900 and 9900 Series

Cisco IP Phone Services can also run on the following Cisco Unified IP phones; however, these phone models support only text-based XML applications:

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phones 7912G and 7912G-A
- Cisco Unified Wireless IP Phone 7920
- Cisco Unified IP Phone 6900 Series

All of these Cisco Unified IP phones can process a limited set of XML objects that Cisco has defined for enabling the user interface between the phone and the web server that contains the running phone service. Note that these phones support phone services for both Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP).

Cisco IP Phone Services Subscriptions Overview

The administrator or end user can subscribe to Cisco IP Phone Services. After subscription, users can access these services by pressing the Services, Directories, or Messages buttons by utilizing the following mechanisms:

- The list of subscribed Cisco IP Phone Services is part of the IP phone configuration file.
- A service type is present to allow services to be provisioned to the Services, Directories, or Messages button.
- For easier access, subscribed Cisco IP Phone Services can also be bound to phone buttons.
- The administrator can also provision services with enterprise subscriptions that apply to all devices and that the user cannot override.
- Additional Cisco IP Phone Services parameters allow provisioning of applications, such as Java MIDlets, that persist in flash on the phone.
- Cisco IP Phone Services can selectively be enabled and disabled.

Cisco IP Phone Services Provisioning

Several pertinent enterprise parameters relate to Cisco IP Phone Services. In Cisco Unified Communications Manager, the new Services Provisioning enterprise parameter affects how services are provisioned with IP phones. You can configure the following options:

- **Internal:** The administrator provisions Cisco IP Phone Services, and the IP phone receives its list of configured services from its configuration file. That file is downloaded through TFTP during the phone registration cycle. The Services, Messages, and Directories URLs that might be specified with the phone URL enterprise parameters are not used. Any valid Java MIDlet services that are provisioned are installed and are available to run. With this setting, IP phones no longer need to contact the Cisco IP Phone Services list URL first to receive a list of configured services. Instead, the phones can directly access the desired service. This setting is the default.
- **External URL:** Cisco IP Phone Services are not provisioned in the configuration file that is obtained through TFTP. The phone uses only the phone services URLs that are specified in the phone URL enterprise parameter. Java MIDlets do not run because they must be provisioned internally to install and execute. This behavior is identical to the release of Cisco Unified Communications Manager prior to Cisco Unified Communications Manager version 7.0.
- **Both:** Any Cisco IP Phone Services that are provisioned in the configuration file appear first. Following are any services that are dynamically retrieved through the corresponding URL when the Services, Messages, or Directories button is pressed on the IP phone. Any Java MIDlets that are provisioned in the configuration file are installed and are available to run. The Services Provisioning enterprise parameter defines how phones should receive a list of subscribed Cisco IP Phone Services. This parameter can be configured in three hierarchical levels, in order of precedence from highest to lowest (higher precedence overrides the settings in a level of lower precedence):
 - On the Phone Configuration web page
 - On the Common Phone Profile Configuration web page
 - On the Enterprise Parameter web page

The Services Provisioning enterprise parameter can be set to one of the three values that were mentioned previously: Internal (a list of provisioned phone services is received through a configuration file), External URL (a list of provisioned phone services is specified in the phone URL enterprise parameters), or Both.

On the Phone Configuration page and the Common Phone Profile Configuration page, the Services Provisioning parameter can also be set to a value of Default. This value instructs the phone to use the setting that is defined in the configuration option of next-lower precedence. For example, if Default is used on the Common Phone Profile Configuration page, the setting that is defined on the Enterprise Parameter page is used. Such behavior is common for many settings in Cisco Unified Communications Manager.

The following list represents some of the configuration parameters that are in the Phone URL Parameters section of the Cisco Unified Communications Manager Enterprise Parameters Configuration page. These parameters relate to Cisco IP Phone Services and XML operation of IP phones:

- **URL Authentication:** (Default value is `http://<CM_IP_address>:8080/ccmcip/authenticate.jsp`.) This URL points to the authenticate.jsp service in Cisco Unified Communications Manager. This service provides an authentication proxy service between Cisco Unified IP phones and Cisco Unified Communications Manager. The URL is used to validate push requests that the phone services make directly to the phone. The service is configured automatically at installation. If no value is specified for this parameter, phone services cannot push content to the phone.
- **URL Directories:** (Default value is `http://<CM_IP_address>:8080/ccmcip/xmldirectory.jsp`.) This URL points to the xmldirectory.jsp service in Cisco Unified Communications Manager. This service generates and returns the directory menu that is presented when the user pushes the Directories (or Book icon) button on the phone. The URL is automatically configured at installation. If no value is specified for this parameter, the directory menu is not available when the user presses the Directories button.
- **URL Idle:** (Default value is <blank>.) This URL, if specified, points to a service that provides text or images to be displayed on the phone screen when the phone is idle. This parameter is closely coupled with the URL Idle Time parameter. This parameter is left blank (not configured) by default at installation.
- **URL Idle Time:** (Default value is 0.) This parameter indicates the time, in seconds, that a phone waits before initiating the URL Idle service. The parameter is set to 0 (zero) by default at installation; this setting indicates that the phone never becomes idle.
- **URL Information:** (Default value is `http://<CM_IP_address>:8080/ccmcip/GetTelecasterHelpText.jsp`.) This URL points to the GetTelecasterHelpText.jsp service in Cisco Unified Communications Manager. This service generates and returns on-screen phone help for phone keys and call statistics when the user presses the Help (i or ?) button to the right of the keypad. The URL is configured automatically at installation. If no value is specified for this parameter, no help information is displayed when the user pushes the Help button.
- **URL Services:** (Default value is `http://<CM_IP_address>:8080/ccmcip/getservicesmenu.jsp`.) This URL points to the getservicesmenu.jsp service in Cisco Unified Communications Manager. This service provides a list of user-subscribed phone services for the phone when the user presses the Services (or Globe icon) button. The service is configured automatically at installation. If no value is specified for this parameter, a list of subscribed services is not provided when the user presses the Services button.

Cisco IP Phone Services Access

Cisco IP Phone Services comprise XML applications that enable the display of interactive content, with text and graphics, on Cisco Unified IP phones.

Users have two ways to access a service from supported phone models:

- Users can press the Services button.
- Users can use a preconfigured phone button.

When a user presses the Services button, the phone either uses the configured Cisco IP Phone Services list that the phone received with its configuration file or uses its HTTP client to load a specific URL that contains a list of services to which the user has subscribed. The user then chooses a service from the listing. When the user chooses a service, the URL is requested through HTTP and a server provides the content, which then updates the phone display.

Typical services that might be supplied to a phone include weather information, stock quotes, news quotes, and first-party/third-party application integration services. Cisco IP Phone Services are deployed by using the HTTP protocol from standard web servers such as Microsoft Internet Information Services (IIS), Apache, and so on.

Users can subscribe only to services that are configured through Cisco Unified Communications Manager Administration.

After the system administrator configures the services, users can log in to the Cisco Unified IP Phone User Options and subscribe to any service on their phones. Subscriptions occur on a per-device basis.

Administrators can also subscribe to services by using Cisco Unified Communications Manager Administration or by using the Cisco Unified Communications Manager Bulk Administration Tool (BAT).

Default Cisco IP Phone Services

As illustrated in Figure 14-1, from Cisco Unified Communications Manager Administration, navigate to **Device > Device Settings > Phone Service**.

From there, you can add a new Cisco IP Phone Service or review these preconfigured Cisco IP Phone Services:

- Corporate Directory
- Intercom Calls
- Missed Calls
- Personal Directory
- Placed Calls

- Received Calls
- Voicemail

Find and List IP Phone Services			
<input type="button" value="Add New"/> <input type="button" value="Select All"/> <input type="button" value="Clear All"/> <input type="button" value="Delete Selected"/>		IP Phone Service (1 - 7 of 7)	
		Find IP Phone Service where IP Phone Service begins with	Rows per Page 50
	ID	IP Phone Service	Description
<input type="checkbox"/>	Corporate_Directory	Corporate Directory	true
<input type="checkbox"/>	Intercom_Calls	Intercom Calls	false
<input type="checkbox"/>	Missed_Calls	Missed Calls	true
<input type="checkbox"/>	Personal_Directory	Personal Directory	true
<input type="checkbox"/>	Placed_Calls	Placed Calls	true
<input type="checkbox"/>	Received_Calls	Received Calls	true
<input type="checkbox"/>	Voicemail	Voicemail	true

Figure 14-1 IP Phone Services

A common service such as the Corporate Directory service configuration includes these parameters, as illustrated in Figure 14-2:

- **Service Name:** Enter the name of the service as it will display on the menu of available services in Cisco Unified Communications Manager User Options. Enter as many as 32 characters for the service name. For Java MIDlet services, the service name must exactly match the name that is defined in the Java Application Descriptor (JAD) file.

IP Phone Services Configuration	
Service Information	
Service Name*	Corporate Directory
ASCII Service Name*	Corporate Directory
Service Description	Corporate Directory
Service URL	Application:Cisco/CorporateDirectory
Secure Service URL	
Service Category*	XML Service
Service Type*	Directories
Service Vendor	
Service Version	
<input checked="" type="checkbox"/> Enable	

Service Name, ASCII Service Name, Service Description, and Service URL or Secure-Service URL

Service Category: XML Service or Java MIDlet

Service Type: Standard IP Phone Service, Directories, or Messages

Check box to globally enable or disable the Cisco IP Phone Service.

Figure 14-2 IP Phone Service Configuration

- **ASCII Service Name:** Enter the name of the service to display if the phone cannot display Unicode.
- **Service Description:** Enter a description of the content that the service provides.
- **Service URL:** Enter the URL of the server on which the Cisco IP Phone Services application is located. Make sure that this server remains independent of the servers in the Cisco Unified Communications Manager cluster.
- **Service Category:** Select a service application type: XML or Java MIDlet.
- **Service Type:** Select whether the service will be provisioned to the Services, Directories, or Messages button.
- **Service Vendor:** For Java MIDlet services, enter the service vendor that exactly matches the vendor that is defined in the JAD file. For XML services, this field can be blank.
- **Service Version:** This field can be blank for XML and Java MIDlet services. If you enter a value for a Java MIDlet service, the value must match the version that is defined in the JAD file. Otherwise, the MIDlet will not install or execute.

Cisco IP Phone Services Redundancy

If high availability of Cisco IP Phone Services is required, you can implement the following options to provide redundancy:

- **Cisco IOS server load balancing (SLB):** HTTP requests from IP phones are directed to a virtual IP address that is configured on a Cisco IOS Server Load Balancer. The requests are then forwarded to the real IP addresses of the web servers that host the Cisco IP Phone Services. To avoid making the Cisco IOS Server Load Balancer a single point of failure, Cisco IOS redundancy options such as Hot Standby Router Protocol (HSRP) should also be implemented.
- **Using Domain Name System (DNS) as a redundancy mechanism:** The URLs for Cisco IP Phone Services that are configured in Cisco Unified Communications Manager use host names instead of IP addresses. The DNS server that is responsible for host name resolution is configured to return multiple IP addresses for a given host name. This redundancy method requires DNS support on the IP phones.

Note Another option to provide redundancy is an environment with a Network Address Translation (NAT) TCP load-sharing configuration.

Cisco IOS SLB

When implementing SLB to provide Cisco IP Phone Services redundancy, the Service URL parameter of a Cisco IP Phone Service points to a virtual IP address that is configured on the Cisco IOS Server Load Balancer, as illustrated in Figure 14-3. The Cisco IOS Server

Load Balancer then forwards HTTP requests that it receives on these virtual IP addresses to specific real IP addresses of multiple web servers, thus providing redundancy.

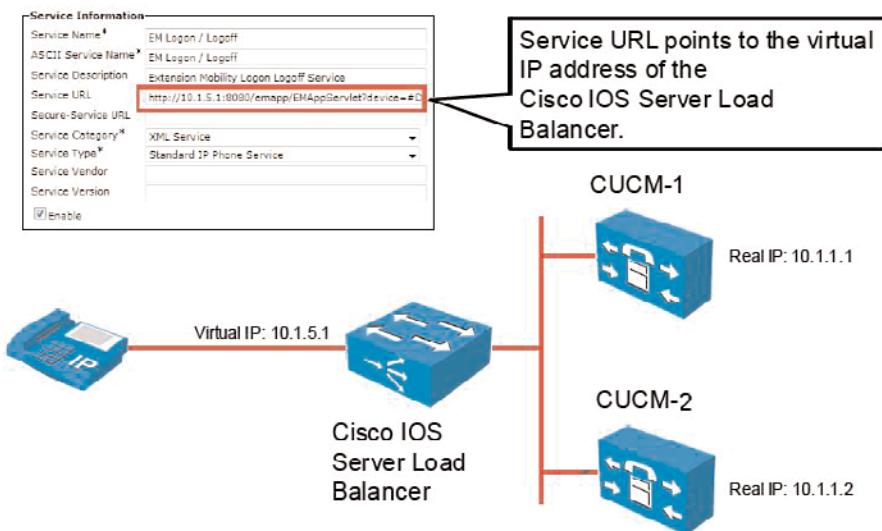


Figure 14-3 Cisco IOS SLB

Use of DNS to Provide Cisco IP Phone Services Redundancy

When you use DNS to implement Cisco IP Phone Services redundancy, the Service URL parameter of Cisco IP Phone Services points to a host name that one or more DNS servers will resolve, as illustrated in Figure 14-4. This DNS server is configured so that a single host name refers to multiple IP addresses, thus providing redundancy.

Cisco IP Phone Services Configuration

Three basic steps are required to configure Cisco IP Phone Services:

- Step 1.** Verify or, if necessary, change the enterprise parameters that are relevant to Cisco IP Phone Services.
- Step 2.** Add a new Cisco IP Phone Service.
- Step 3.** Configure the Cisco IP Phone Services parameters of the added service.

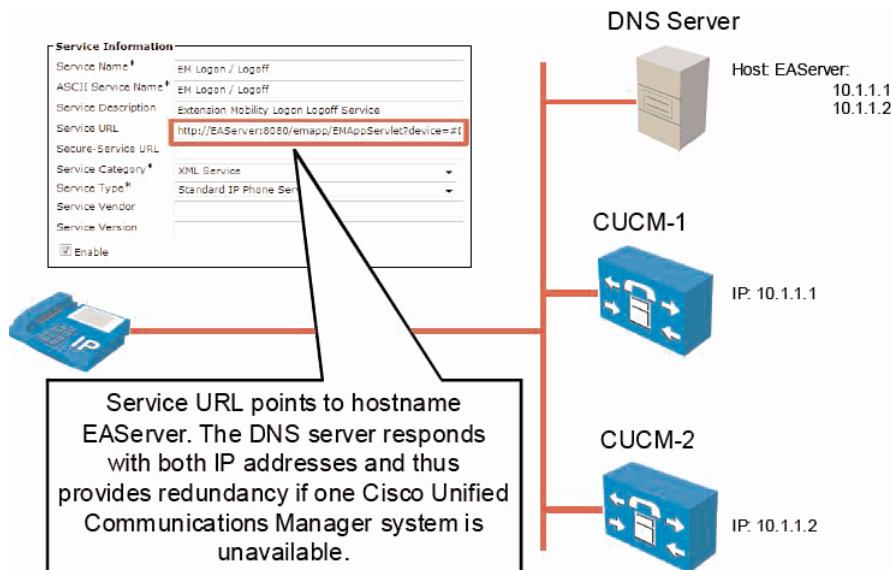


Figure 14-4 DNS IP Server Redundancy

Step 1: Verify or Change the Enterprise Parameters Relevant to Cisco IP Phone Services

Before adding a new Cisco IP Phone Service, verify and, if necessary, change the relevant enterprise parameters, as illustrated in Figure 14-5 and described in the list that follows.

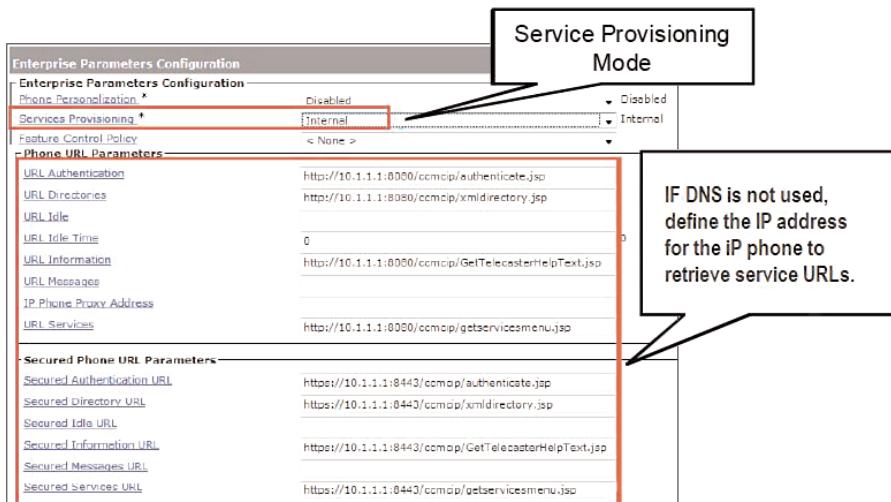


Figure 14-5 Enterprise Parameters Configuration

- **Services Provisioning:** This new device-configuration parameter controls whether the phone uses the services that are provisioned in the configuration file (Internal), the services that are received from URLs (External URLs), or both. This parameter is required for backward compatibility with third-party provisioning servers, primarily to disable the new provisioning mechanism so that the phone presents only services from the Service URL parameter.
- **URL Authentication:** This parameter specifies a URL that points to a web page in one of the Cisco CallManager Cisco IP Phone (CCMCIP) web services in the cluster. This URL provides an authentication proxy service between Cisco Unified IP phones and the Lightweight Directory Access Protocol (LDAP) directory. This URL is used to validate requests that are made directly to the phone. This URL is automatically configured at installation. If the URL is removed, the push capabilities to the Cisco Unified IP phones are disabled.
- **URL Directories:** This parameter specifies the URL that Cisco Unified IP phones use when users press the Directories button. This URL must return a CiscoIPPhoneMenu object even if no MenuItems are specified in the object. The MenuItems that are specified and the internal directories are appended to the directory list on the Cisco Unified IP phones.
- **URL Idle:** This parameter specifies the URL that a Cisco Unified IP phone uses to display information on the screen when the phone remains idle for the time that the URL Idle Time parameter specifies.
- **URL Idle Time:** This parameter specifies the time that the Cisco Unified IP phones will remain idle before displaying the URL that the URL Idle parameter specifies. If the time is set to 0 (zero), the URL that the URL Idle parameter specifies is not displayed.
- **URL Information:** This parameter specifies a URL that points to a page in the CCMCIP web service and returns the requested help text to the Cisco Unified IP phone display. This information is displayed when a user presses the i or ? button on the phone.
- **URL Messages:** This parameter specifies a URL that the Cisco Unified IP phones should call when users press the Messages button. When called, the URL must return a CiscoIPPhoneMenu object. The returned MenuItems are appended to the built-in items on Cisco Unified IP phones.
- **IP Phone Proxy Address:** This parameter specifies a proxy server name or address and port, for example, proxy.cisco.com:8080. If a proxy server is specified, the Cisco Unified IP phones use that server to request all URLs. Leave this setting blank to instruct the phones to attempt to connect directly to all URLs. If a server name is used instead of an IP address, configure phones with valid DNS servers to allow name-to-IP resolution. Confirm that the proxy server is listening at the specified destination.
- **URL Services:** This parameter specifies the URL that a Cisco Unified IP phone calls when a user presses the Services button. The initial request by the phone passes the device name as a parameter. The default page in the CCMCIP web service returns a

CiscoIPPhoneMenu object that includes a list of the services that are subscribed to the device. If no subscriptions exist, the return text indicates that no subscriptions exist for the device.

- **Secured Authentication URL:** This parameter specifies the URL that points to a web page in one of the CCMCIP web services in the cluster. This URL provides an authentication proxy service between secured Cisco Unified IP phones and the LDAP directory. This URL is used to validate requests that are made directly to the phone. This URL is configured automatically at installation. If the URL is removed, the push capabilities to the Cisco Unified IP phones are disabled.
- **Secured Idle URL:** This parameter specifies the URL that a secured Cisco Unified IP phone uses to display information on the screen when the phone remains idle for the time that the URL Idle Time parameter specifies.
- **Secured Information URL:** This parameter specifies a URL that points to a page in the CCMCIP web service and returns the requested help text to the secured Cisco Unified IP phone display. This information displays when a user presses the i or ? button on the phone.
- **Secured Messages URL:** This parameter specifies a URL that the secured Cisco IP Unified phones should call when users press the Messages button. When called, the URL must return a CiscoIPPhoneMenu object. The returned MenuItems are appended to the built-in items on secured Cisco Unified IP phones.
- **Secured Services URL:** This parameter specifies the URL that a secured Cisco Unified IP phone calls when a user presses the Services button. The initial request by the phone passes the device name as a parameter. The default page in the CCMCIP web service returns a CiscoIPPhoneMenu object that includes a list of the services that are subscribed to the device. If no subscriptions exist, the return text indicates that no subscriptions exist for the device.

Step 2: Add a New Cisco IP Phone Service

After the parameters have been set, the next step is to add the phone service. Navigate to Device > Device Settings > Phone Services and click the Add New button, as illustrated in Figure 14-6.

Step 3: Configure the Cisco IP Phone Services Parameters of the Added Service

The final step is to configure the phone service parameters. Note that these are unique from the enterprise parameters and are applicable to the individual service being configured. After you have clicked Save on the Add New Service page, the Parameter window will appear, where you can choose to add new, edit, and delete parameters, as illustrated in Figure 14-7.

Find and List IP Phone Services			
<input type="button" value="Add New"/> <input type="button" value="Select All"/> <input type="button" value="Clear All"/> <input type="button" value="Delete Selected"/>			
IP Phone Service (1 - 7 of 7)			
	Find IP Phone Service where IP Phone Service begins with	Find	Clear Filter
<input type="checkbox"/>	IP Phone Service	Description	Enterprise Subscription
<input type="checkbox"/>	Corporate Directory	Corporate Directory	true
<input type="checkbox"/>	Intercom Calls	Intercom Calls	false
<input type="checkbox"/>	Missed Calls	Missed Calls	true
<input type="checkbox"/>	Personal Directory	Personal Directory	true
<input type="checkbox"/>	Placed Calls	Placed Calls	true
<input type="checkbox"/>	Received Calls	Received Calls	true
<input type="checkbox"/>	Voicemail	Voicemail	true

Figure 14-6 Adding Cisco IP Phone Services

Choose the service category and service type.

Check **Enable** to enable the service.
Check **Enterprise Subscription** to autosubscribe this service to devices.

Service Name: A (meaningful) name for the service
 ASCII Service Name: Name for ASCII-only phone displays
 Service Description: What the service does
 Service URL: Where the service can be found
 Secure-Service URL: Used for secure URLs

Figure 14-7 IP Phone Service Configuration

Table 14-1 outlines the parameters and their descriptions.

Table 14-1 Service Parameters

Parameter	Service Description
Service Name	Enter the name of the service. If the service is not marked as an enterprise subscription, the service name will be displayed in areas in which you can subscribe to a service, for example, under Cisco Unified Communications Manager User Options. Enter as many as 32 characters for the service name. For Java MIDlet services, the service name must match the name that is defined in the JAD file.
ASCII Service Name	Enter the name of the service to display if the phone cannot display Unicode.
Service Description	Enter a description of the content that the service provides. The description can include as many as 50 characters in any language but cannot include quotation marks ("") or apostrophes (').
Service URL	<p>Enter the URL of the server on which the Cisco IP Phone Services application is located. Make sure that this server remains independent of the servers in the Cisco Unified Communications Manager cluster. Do not specify a Cisco Unified Communications Manager server or any server that is associated with Cisco Unified Communications Manager (such as a TFTP server or directory database publisher server).</p> <p>For the services to be available, the phones in the Cisco Unified Communications Manager cluster must have network connectivity to the server.</p> <p>For Java MIDlets that are signed by Cisco, enter the location where the JAD file can be downloaded, for example, a web server or the backend application server to which the Java MIDlet communicates.</p> <p>For default services that Cisco provides, the Service URL parameter is entered as Application:Cisco/name of service by default, for example, Application:Cisco/CorporateDirectory. If you modify the Service URL parameter for these default services, verify that you configured Both for the Services Provisioning setting in the Phone, Enterprise Parameter, and Common Phone Profile Configuration windows. For example, if you use a custom corporate directory, change Application:Cisco/CorporateDirectory to the URL of the external service for your custom directory and change the Services Provisioning setting to Both.</p>

Table 14-1 Service Parameters

Parameter	Service Description
Secure-Service URL	<p>Enter the secure URL of the server on which the Cisco IP Phone Services application is located. Make sure that this server remains independent of the servers in the Cisco Unified Communications Manager cluster. Do not specify a Cisco Unified Communications Manager server or any server that is associated with Cisco Unified Communications Manager (such as a TFTP server or publisher database server).</p> <p>For the services to be available, the phones in the Cisco Unified Communications Manager cluster must have network connectivity to the server.</p> <p>Note: If you do not enter a Secure-Service URL parameter, the device uses the Service URL parameter. If you enter both a Secure-Service URL parameter and a Service URL parameter, the device chooses the appropriate URL based on its capabilities.</p>
Service Category	<p>Select a service application type (XML or Java MIDlet).</p> <p>If you choose Java MIDlet, when the phone receives the updated configuration file, the phone retrieves the MIDlet application signed by Cisco (JAD and Java ARchive [JAR]) from the specified Service URL and installs the application.</p>
Service Type	<p>Choose whether the service is provisioned to the Services, Directories, or Messages button or option on the phone; that is, if the phone has these buttons or options. To determine whether a phone has these buttons or options, refer to the Cisco Unified IP Phone Administration Guide that supports the phone model.</p>
Service Vendor	<p>This field allows you to specify the vendor or manufacturer for the service. This field is optional for XML applications but is required for Java MIDlets that are signed by Cisco. For such Java MIDlets, the value that you enter in this field must match the vendor that is defined in the MIDlet JAD file.</p> <p>This field displays as blank for default services that Cisco provides.</p> <p>You can enter as many as 64 characters.</p>

Table 14-1 Service Parameters

Parameter	Service Description
Service Version	<p>Enter the version number for the application. For XML applications, this field is optional and is informational only. For Java MIDlets that are signed by Cisco, consider the following information:</p> <ul style="list-style-type: none"> • If you enter a version, the service version must match the version that is defined in the JAD file. If you enter a version that is different from the version that is installed on the phone, the phone attempts to upgrade or downgrade the MIDlet of the version. • If the field is blank, the version is retrieved from the Service URL. Leaving the field blank ensures that the phone attempts to download the JAD file every time that the phone reregisters to Cisco Unified Communications Manager, as well as every time that the Java MIDlet is launched. This action ensures that the phone always runs the most recent version of the Java MIDlet, without the Service Version field being updated manually. <p>This field displays as blank for default services that Cisco provides. You can enter numbers and periods in this field (as many as 16 ASCII characters).</p>
Enable	<p>This check box allows you to enable or disable the service without removing the configuration from Cisco Unified Communications Manager Administration (and without removing the service from the database). Deselecting the check box removes the service from the phone configuration file and the phone.</p>
Enterprise Subscription	<p>This check box allows you to automatically provision the service to all devices in the cluster that can support the service. If you select this check box, you (or an end user) cannot subscribe to the service.</p> <p>If this check box is deselected, you must manually subscribe to the service for it to be displayed on the phone (in the Phone Configuration window, in Cisco Unified Communications Manager BAT, or in the Cisco Unified Communications Manager User Options).</p> <p>Tip: This setting displays only when you configure a service for the first time. After you save the service, the check box is not displayed in the window. To identify whether the service is provisioned to all devices in the cluster that can support the service, go to the Find and List IP Phone Services window and display the services. If True is displayed in the Enterprise Subscription column, you cannot manually subscribe to the service. If False is displayed, you can manually subscribe to the service. For example, an end user can subscribe to the service through the Cisco Unified Communications Manager User Options.</p>

Table 14-1 Service Parameters

Parameter	Service Description
Parameters	<p>This pane lists the service parameters that apply to this Cisco IP Phone Service.</p> <p>Use the following buttons to configure service parameters for this pane:</p> <ul style="list-style-type: none"> • New Parameter: Click this button to display the Configure Cisco Unified IP Phone Service Parameter window, in which you can configure a new service parameter for this Cisco IP Phone Service. • Edit Parameter: Choose a service parameter that is displayed in the Parameters pane. Then click this button to display the Configure Cisco Unified IP Phone Service Parameter window, in which you can edit the selected service parameter for this Cisco IP Phone Service. • Delete Parameter: Choose a service parameter that is displayed in the Parameters pane. Then click this button to delete a service parameter for this Cisco IP Phone Service. A pop-up window asks you to confirm the deletion.

Cisco IP Phone Services Subscriptions

To use Cisco IP Phone Services, you need to subscribe the configured services to Cisco Unified IP phones. You can configure a Cisco IP Phone Services subscription through the Cisco Unified Communications Manager Administration web page, or the end user can directly configure the subscription on the Cisco Unified Communications Manager User web page.

Subscribe Cisco IP Phone Services: Administrator

To subscribe to a phone service, open the phone configuration web page for the phone that should have a service subscription. Choose **Subscribe/Unsubscribe Services** from the Related Links drop-down list and follow these steps:

- Step 1.** From the Select a Service drop-down list, as shown in Figure 14-8, choose the service that should be subscribed to the selected Cisco Unified IP phone.

Step 2. Click Next to continue.

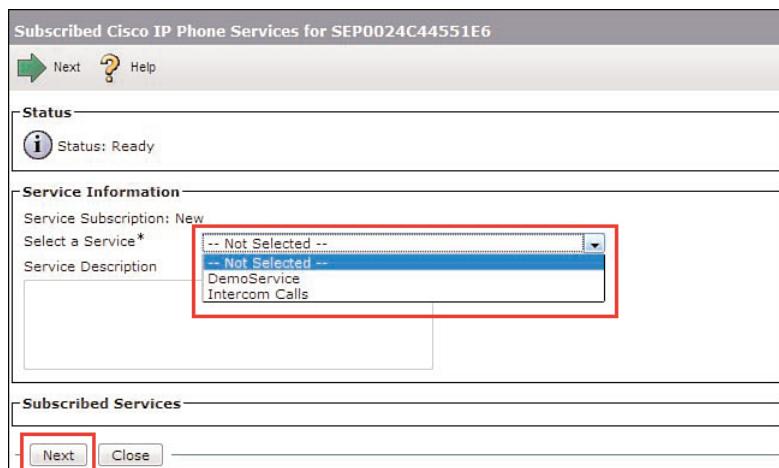


Figure 14-8 IP Phone Service Subscription

Step 3. Click **Subscribe** in the window shown in Figure 14-9 to complete the subscription process.



Figure 14-9 IP Phone Service Subscription (Continued)

Subscribe Cisco IP Phone Services: End User

End users can configure phone service subscriptions by logging in to the Cisco Unified Communications Manager User Options web page. End users should then follow this procedure:

Step 1. Open the Cisco Unified Communications Manager User Options web page at https://Server_IP/ccmuser. From the User Options menu, choose Device, and then click the Phone Services button

From the User Options menu, choose Device, and then click the Phone Services button.

- Step 2.** Click **Add New** to subscribe to a configured Cisco IP Phone Service, as shown in Figure 14-10.

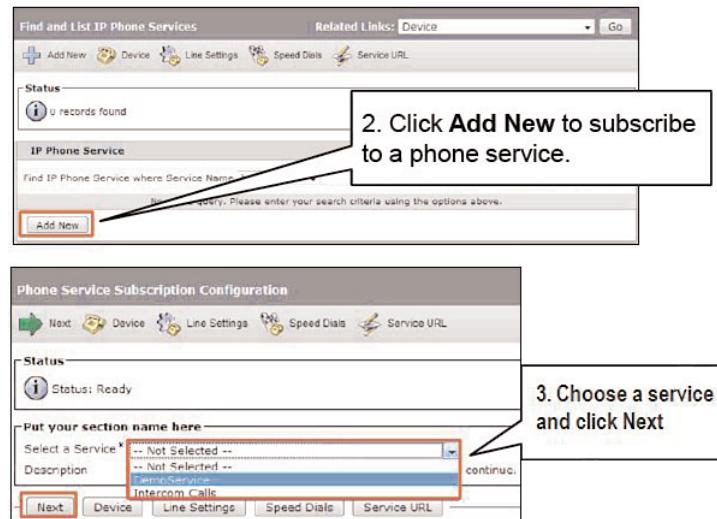


Figure 14-10 End User Phone Service Configuration

- Step 3.** From the Select a Service drop-down list, choose a Cisco IP Phone Service and click **Next**.

- Step 4.** Click **Save** to finish the subscription procedure.

After the Cisco IP Phone Services subscription has been completed, the new Cisco IP Phone Service will show up on the Cisco Unified IP phone when the user presses the Services button.

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- Cisco Unified IP phones can use Cisco IP Phone Services for a variety of functions.
- Cisco IP Phone Services redundancy can be provided through DNS or through Cisco IOS SLB.
- Cisco IP Phone Services are added and updated through the Cisco Unified Communications Manager Administration web page.
- Administrators and end users can subscribe to Cisco IP Phone Services.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

- 1.** Which is not a function of Cisco IP Phone Services?
 - a.** Displaying data (text and graphics) on the Cisco IP phone display
 - b.** Playing welcome messages
 - c.** User input
 - d.** Authentication functions
- 2.** How can redundancy be provided to Cisco IP Phone Services? (Choose two.)
 - a.** Configure backup services on a Cisco IOS gateway.
 - b.** Configure Cisco IOS server load balancing.
 - c.** Configure SRST.
 - d.** Provide redundancy by using DNS functionality.
- 3.** Which is not a valid service provisioning mode?
 - a.** Internal
 - b.** Rxternal
 - c.** Both (internal and external)
 - d.** Global
- 4.** How can configured Cisco IP Phone Services be subscribed? (Choose two.)
 - a.** By the end user, through the user web page
 - b.** Through the Active Directory server
 - c.** By the end user, through a phone softkey
 - d.** By the administrator, through the administration web page
 - e.** Cisco IP Phone Services are subscribed automatically.

This page intentionally left blank

Chapter 15

Presence-Enabled Speed Dials and Lists

Upon completing this chapter, you will be able to describe and configure Presence-enabled speed dials and lists. This ability includes being able to meet these objectives:

- Describe Cisco Unified Communications Manager (CUCM) native Presence and compare it to Cisco Unified Presence and Cisco Unified Personal Communicator
- Describe how Cisco Unified Communications Manager native presence works
- Describe how Cisco Unified Communications Manager native presence access control works

Today, users are mobile: working from homes, in the office, in airport lounges, or while traveling. To communicate efficiently with others, it is helpful to know their current availability. Can they be reached by phone, by instant messaging (IM), or by email, and are they ready to communicate now? Cisco Unified Communications Solutions offer Presence information about the reachability and status of users.

Cisco Unified Communications Manager Presence, an integrated part of Cisco Unified Communications Manager, allows IP phone users to monitor the status of directory numbers. This chapter describes how Cisco Unified Communications Manager native Presence works and how it is configured.

How Presence Works with CUCM

Cisco Unified Communications includes multiple options to integrate basic Presence information. The CUCM-included Presence information includes the following capabilities:

- **Presence-enabled speed dials:** Speed-dial buttons that indicate the status of the target of the speed dial
- **Presence-enabled call and directory lists:** Call lists and directory entries that indicate the status of each list entry
- **Presence policy:** Tools allowing access control to Presence information

When using the Cisco Unified Presence Server product, additional features are added to those provided by the native CUCM Presence feature, including the following:

- Standards-based Session Initiation Protocol (SIP)/SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) network interface
- User status information, not only device (line) status information
- IM capabilities, including integration with third-party servers such as Microsoft Exchange and IBM SameTime
- Cisco Unified Personal Communicator, which is a client tool that integrates voice, video, audio conferencing, videoconferencing, and IM communications

Note This chapter covers the CUCM Presence feature only.

Presence Support in CUCM

CUCM Presence is natively supported by CUCM, with no extra products or servers required. It allows an interested party (watcher) to monitor the real-time status of a directory number (DN) (Presence entity).

A watcher subscribes to the status information of one or more Presence entities. The status information of a Presence entity can be viewed using Presence-enabled speed dials or Presence-enabled lists—call lists such as placed, received, or missed calls and public directory lists.

The status can be one of the following:

- Unknown (shown when the watched device is unregistered)
- On-hook
- Off-hook

In Figure 15-1, John's phone has subscribed to the status of Bryan's primary DN. The CUCM Presence feature will now keep Bryan's phone updated about the status of the subscribed Presence entity.

If Bryan goes off-hook while John is browsing the call list that includes Bryan's DN, the status information for Bryan's phone changes to indicate Bryan's availability (off-hook).

If John has a Presence-enabled speed dial for Bryan's DN, the speed dial displays the current status of Bryan's DN. John's phone also subscribes to the status of the other Presence entities (users) of the call list automatically as the call list is viewed.

CUCM Presence allows DNs to be watched by Cisco IP Phones on the same cluster and by devices on remote clusters through a SIP trunk. Endpoints that can be reached

through a SIP trunk can be watched by Cisco IP Phones, and SIP devices can watch Presence status over other trunk types in addition to SIP. Cisco IP Phones running Skinny Client Control Protocol (SCCP) and Cisco IP Phones running SIP can watch Presence entities and can be watched. If Presence subscriptions are sent over a SIP trunk, CUCM handles the protocol conversion between SCCP and SIP.

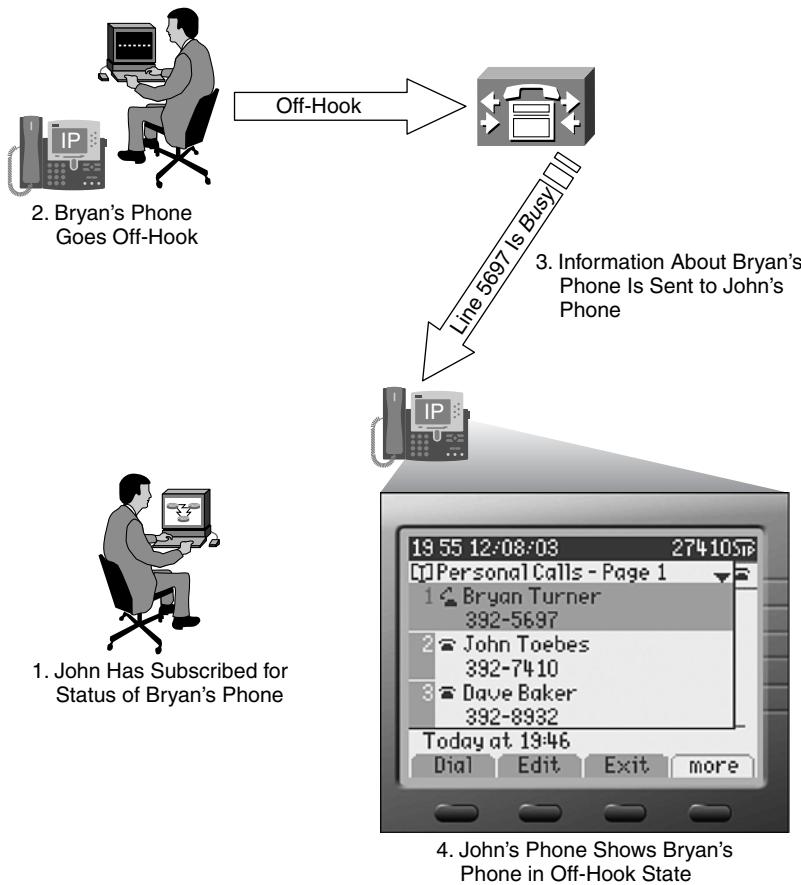


Figure 15-1 Presence Operation

Cisco IP Phones can display status information (unknown, on-hook, or off-hook) of Presence entities by using Presence-enabled speed dials or call and directory list entries, as shown in Figure 15-2.

Presence-enabled speed dials show a symbol inside the screen of the IP phone, located at the appropriate speed-dial button. Type B Cisco Unified IP Phones have an LED inside the speed-dial button and indicate the Presence entity status by an illuminated button (red indicates off-hook).

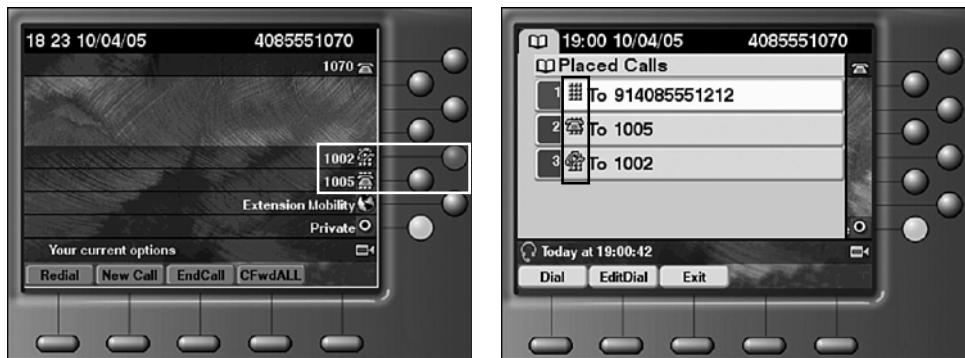


Figure 15-2 Presence Operation: Displaying Status Information

The 7914 sidecar module, which adds 14 additional buttons to a Cisco Unified IP Phone, does not support Presence when running SIP. The 7940 and 7960 IP Phones also do not support Presence running SIP. These phones support Presence when using SCCP. Type B Cisco Unified IP Phone Models 79x1, 79x2, 79x5, and 7970 support Presence-enabled call and directory lists and Presence-enabled speed dials regardless of the protocol used (SIP or SCCP).

Cisco IP Communicator also supports both Presence-enabled speed dials and Presence-enabled call and directory lists. Cisco IP Communicator 2.1 added SIP support.

Presence Configuration

The CUCM Presence configuration procedure includes the following three steps:

Step 1. Enable Presence-enabled speed dials:

- Customize phone button templates to include Presence-enabled speed-dial buttons.
- Apply phone button templates to phones.
- Configure Presence-enabled speed-dial buttons.
- Apply subscribe Calling Search Space to phones.

Step 2. Enable Presence-enabled call lists. Enable the BLF for Call Lists enterprise parameter.

Step 3. Allow Presence subscriptions through SIP trunks. Enable CUCM Presence on SIP trunks.

Presence-enabled speed dials and call lists are independent of each other. Presence subscriptions can work between vendors or CUCM clusters through SIP trunks.

Step 1: Enable Presence-Enabled Speed Dials

The first step for implementing Presence-enabled speed dials is to configure a phone button template that includes Presence-enabled speed dials. To configure a phone button template, choose **Device > Device Settings > Phone Button Template** and either add a new template or copy one of the default phone button templates and save it with a new name. Configure the phone button template with the desired number of Presence-enabled speed dials, as illustrated in Figure 15-3.

Phone Button Template Information		
Button Template Name *		
Button Information		
Button	Feature	Label
1	Line **	Line
2	Line	Line
3	Speed Dial	Speed Dial1
4	Speed Dial	Speed Dial2
5	Call Park BLF	Call Park BLF
6	Speed Dial BLF	Speed Dial BLF
7	None	
8	None	
9	None	

Figure 15-3 Speed-Dial Phone Button Template Configuration: Busy Lamp Field Speed Dial

Note In CUCM Administration, Presence-enabled speed dials are called BLF Speed Dials.

Assign the previously configured phone button template to the IP phone, as shown in Figure 15-4. Navigate to the Phone Configuration page from CUCM Administration (choose **Device > Phone > Find**) and select the appropriate template from the Phone Button Template drop-down list. Save the configuration and reset the device.

Phone Type	
Product Type:	Cisco 7961
Device Protocol:	SCCP
Device Information	
Registration	Unknown
IP Address	Unknown
MAC Address*	1234567890AB
Description	SEP1234567890AB
Device Pool*	Default
Common Device Configuration	< None >
Phone Button Template*	7961 SCCP with 2 BLF-SD
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile

Figure 15-4 Assign Phone Button Templates to Phone

After the new phone button template has been applied, the Presence-enabled speed dials display in the Association Information area of the Phone Configuration page (left side). The phone can now use buttons for Presence-enabled speed dials. To configure the Presence-enabled speed dials, click the Add a New BLF SD link, as shown in Figure 15-5.

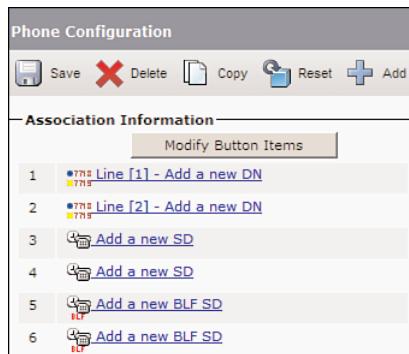


Figure 15-5 Phone Configuration: Adding Busy Lamp Field Speed Dial

Step 2: Configure the BLF Speed Dial

The Busy Lamp Field Speed Dial Configuration window will open after you click the BLF SD link. Configure the target (Presence entity to be watched) of the Presence-enabled speed-dial button and a label that will be displayed on the phone screen next to the corresponding button. Figure 15-6 shows this configuration.

Busy Lamp Field/Speed Dial Button Settings			
Destination	Directory Number	Label	Label ASCII
1	< None >	<input type="checkbox"/>	<input type="text"/>
2	< None >	<input type="checkbox"/>	<input type="text"/>

Figure 15-6 Busy Lamp Field Speed Dial Configuration

If call lists should also provide Presence information, the appropriate enterprise parameter has to be enabled, as shown in Figure 15-7. After you change this enterprise parameter, all phones that support Presence have to be reset for the change to become effective.

Step 3: Allow Presence Subscriptions Through SIP Trunks

If Presence subscriptions will be used over a SIP trunk, Presence must be enabled on the SIP trunk. Presence is enabled through the SIP trunk security profile, not directly at the SIP trunk. Configure a SIP trunk security profile by choosing System > Security Profile > SIP Trunk Security Profile. The Accept Presence Subscription and Accept Unsolicited Notification check boxes should be selected to enable SIP Presence information, as shown in Figure 15-8.

Enterprise Parameters Configuration

Parameter Name	Parameter Value	Suggested Value
Synchronization Between Auto Device Profile and Phone Configuration *	True	True
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120	120
Auto Registration Phone Protocol *	SCCP	SCCP
BLF For Call Lists *	Disabled	Disabled
Advertise G.722 Codec *	Enabled	Enabled
Phone Personalization *	0	0

Enable presence-enabled call lists

Figure 15-7 Busy Lamp Field for Call Lists

SIP Trunk Security Profile Information

Name *	Non Secure Presence Enabled SIP Trunk Profile
Description	Non Secure SIP Trunk Profile with Presence Enabled
Device Security Mode	Non Secure
Incoming Transport Type *	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins) *	600
X.509 Subject Name	
Incoming Port *	5050
<input type="checkbox"/> Enable Application Level Authorization	
<input checked="" type="checkbox"/> Accept Presence Subscription	
<input type="checkbox"/> Accept Out-of-Dialog REFER	
<input checked="" type="checkbox"/> Accept Unsolicited Notification	
<input type="checkbox"/> Accept Replaces Header	

Figure 15-8 SIP Trunk Security Profile

Apply the SIP trunk security profile to the SIP trunk, as shown in Figure 15-9.

Presence Access Control

CUCM Presence has multiple ways of limiting Presence information. Presence-enabled speed dials are configured statically by the CUCM administrator and cannot be configured or modified directly by a user. The administrator maintains control of the monitored Presence entities for each watcher. Subscribe Calling Search Spaces (CSS) also apply to Presence-enabled speed dials.

Access control for Presence-enabled call and directory lists can be provided by the following:

- Partitions and subscribe CSSs
- Presence groups

The screenshot shows the 'Trunk Configuration' dialog box. At the top left is a 'Save' button. Below it is a section titled 'Device Information' with the following fields:

- Product:** SIP Trunk
- Device Protocol:** SIP
- Device Name***: An empty text input field.
- Description**: An empty text input field.
- Device Pool***: A dropdown menu showing '< Not Selected >'.
- Common Device Configuration**: A dropdown menu showing '< None >'.
- Call Classification***: A dropdown menu showing 'Use System Default'.
- Media Resource Group List**: A dropdown menu showing '< None >'.
- Location***: A dropdown menu showing 'Hub_None'.
- AAR Group**: A dropdown menu showing '< None >'.
- Packet Capture Mode***: A dropdown menu showing 'None'.
- Packet Capture Duration**: A text input field containing '0'.

Below these fields are several checkboxes:

- Media Termination Point Required
- Retry Video Call as Audio
- Transmit UTF-8 for Calling Party Name
- Unattended Port

Figure 15-9 SIP Trunk Presence Enablement

Each of the two methods can be used independently of each other. If both are used, both have to permit a subscription for successful watching of the Presence entity's status.

A subscribe CSS is applied to a watcher. A watcher can be a SIP trunk, an IP phone, or an end user. Subscribe CSSs do not use the concept of a device and line CSS. Watching a Presence entity is always a global function of the IP phone.

Subscribe CSSs determine which Presence entities a watcher is allowed to monitor. A subscription is permitted only if the watcher has the partition of the desired Presence entity in its subscribe CSS.

A partition can be used for both calling privileges and Presence policies. If no partition is applied to the desired Presence entity, the Presence entity is available to all watchers.

Presence policies and calling privileges share a configuration element. The partitions that are applied to lines or route patterns apply to both. Therefore, implementing Presence policies impacts existing calling privileges and vice versa.

Whenever partition configuration is changed because of the implementation of one of the two features, the other one is affected. Therefore, calling privileges and Presence policies have to be designed and implemented together.

The environment in Figure 15-10 consists of three CSSs:

- CSS C-1 contains partitions P-1 and P-2.
- CSS C-2 contains partitions P-1, P-2, and P-3.
- CSS C-3 contains partition P-1 only.

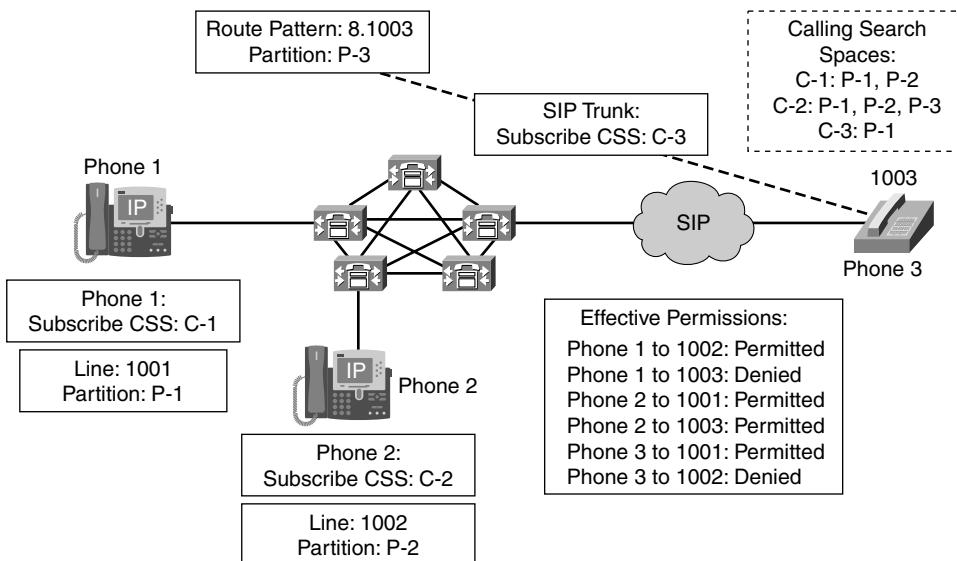


Figure 15-10 *Subscribe CSS Example*

Phone 1 has partition P-1 applied to its line, which is configured with DN 1001. CSS C-1 is assigned to Phone 1.

Phone 2 has partition P-2 applied to its line, which is configured with DN 1002. CSS C-2 is assigned to Phone 2.

A SIP phone with number 1003 can be reached through a SIP trunk. The corresponding route pattern 8.1003 is in partition P-3. CSS C-3 is assigned to the SIP trunk.

The effective permissions for Presence subscriptions are as follows:

- Phone 1 is allowed to watch the status of 1002 but not of 1003.
- Phone 2 is allowed to watch both other phones.
- Phone 3 is allowed to subscribe to Presence information of 1001 but not of 1002.

Presence policies watchers and Presence entities are put into Presence groups.

Subscriptions can be allowed or denied at an intergroup level. Within a Presence group, subscriptions are always permitted (unless denied by partitions and subscribe CSSs).

IP phones are configured with two or more Presence groups: One is applied to the device (in the role as a watcher), and each line can be configured with a Presence group in its role as a Presence entity.

Only one Presence group is configured on a SIP trunk. The SIP trunk can be used in both watcher and Presence entity roles. A Presence group cannot be applied to a route pattern.

Presence groups can also be assigned to end users. They are used when the end users are logging in to the phone using extension mobility or when the users are associated with a device.

Note Presence groups apply only to Presence-enabled call lists; they do not apply to Presence-enabled speed dials.

Figure 15-11 uses three Presence groups: G-1, G-2, and G-3. Inter-Presence group subscriptions are permitted from G-2 to G-3 and G-3 to G-1. All other inter-Presence group subscriptions are denied.

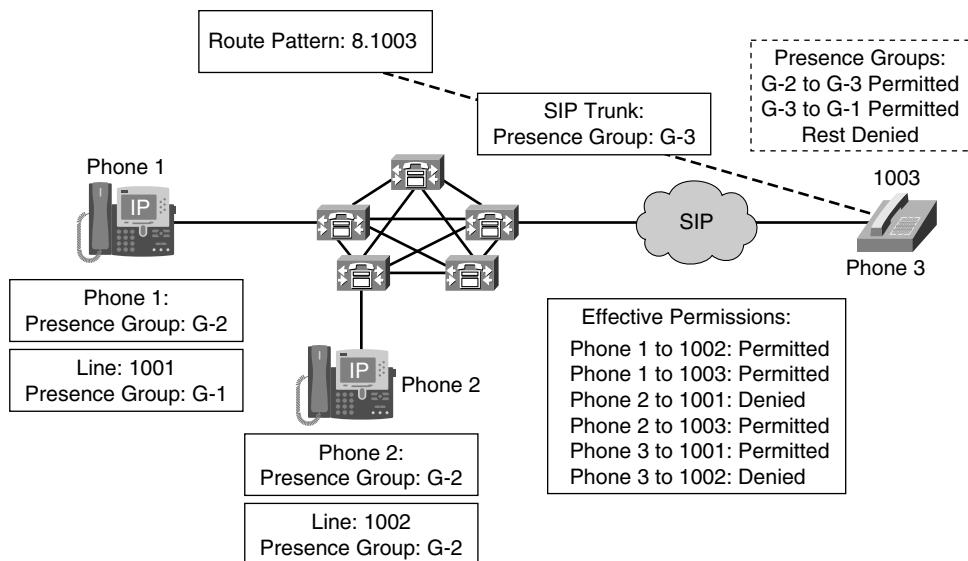


Figure 15-11 Presence Group Example

Phone 1 has Presence group G-1 applied to its line, which is configured with DN 1001. Presence group G-2 is assigned to Phone 1.

Phone 2 has Presence group G-2 applied to its line, which is configured with DN 1002. Presence group G-2 is also assigned to Phone 2.

A SIP phone with number 1003 can be reached through a SIP trunk. Presence group G-3 is assigned to the SIP trunk.

The effective permissions for Presence subscriptions are as follows:

- Phone 1 is allowed to watch the status of 1002 and 1003.
- Phone 2 is allowed to watch 1003 but not 1001.
- Phone 3 is allowed to subscribe to Presence information of 1001 but not of 1002.

Subscribe CSSs can be used with Presence groups, or either one of them can be used alone to restrict watcher access. If both are implemented, both mechanisms have to permit the subscription to allow successful watching.

Combining both Presence policy mechanisms provides two hierarchy levels, which can prove useful in larger deployments or complex scenarios.

The following example explains how subscribe CSSs and partitions and Presence groups can be effectively combined to fulfill the given requirements:

- **Requirements:** No subscriptions are allowed between different departments. Within a department, managers can be watched only by their assistants. All other subscriptions within a department should be possible.
- **Solution:** One Presence group is configured per department. Inter-Presence group subscriptions are denied by setting the default inter-Presence group policy accordingly. One partition is configured per manager. Each of these partitions is listed only in the subscribe CSS of the respective manager's assistant.

Presence groups are used for the first level of Presence policies at the department level, and subscribe CSSs and partitions are used for additional access control within a department for the assistants to watch the managers.

Presence Policy Configuration

The CUCM Presence policy configuration is done through Presence groups, but a subscribe CSS can limit the Presence entities for which the watcher can receive status information.

Subscribe CSSs are configured in the same manner as traditional CSSs. The application of the CSS is focused on restricting Presence information. The CEO of the company might not want an intern to watch his phone status. The following procedure is required to implement subscribe CSSs:

- Step 1.** Configure partitions and CSSs.
- Step 2.** Assign partitions to lines and route patterns.
- Step 3.** Assign subscribe CSSs to phones and trunks.

Presence groups represent a straightforward mechanism to limit what Presence entities a watcher can watch. If the organizational goal includes restricting Presence information within a group, subscribe CSSs must be used. The following procedure is required to implement Presence groups:

- Step 1.** Configure Presence groups.
- Step 2.** Set the default inter-Presence group policy.
- Step 3.** Assign Presence groups to lines, phones, or SIP trunks.

The first two steps of implementing subscribe CSSs involve standard partitions and CSSs that will be used for Presence information. Figures 15-12 and 15-13 display subscribe CSS applications to an IP phone and SIP trunk (respectively). The subscribe CSS at the phone level limits the Presence entities that the phone can watch. The subscribe CSS at the trunk level restricts the DNs that can be watched over the SIP trunk.

Protocol Specific Information	
Packet Capture Mode*	None
Packet Capture Duration	0
Presence Group*	Standard Presence group
Device Security Profile*	Cisco 7961 - Standard SCCP Non-Secure Profile
SUBSCRIBE Calling Search Space	< None >
<input type="checkbox"/> Unattended Port	
<input type="checkbox"/> Require DTMF Reception	
<input type="checkbox"/> RFC2833 Disabled	

Figure 15-12 *Subscribe CSS Application: Phone*

SIP Information	
Destination Address*	
<input type="checkbox"/> Destination Address is an SRV	
Destination Port*	5060
MTP Preferred Originating Codec*	711ulaw
Presence Group*	Sales_PG
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
DTMF Signaling Method*	No Preference

Figure 15-13 *Subscribe CSS Application: Trunk*

Presence groups can be configured by choosing **System > Presence Group**. The default Presence group, called the Standard Presence group, exists by default and cannot be deleted. All phones, lines, and SIP trunks by default are members of the Standard Presence group. The Standard Presence group can be modified in the way that the permissions to other groups can be set, but it cannot be deleted.

When adding a new Presence group, enter a name and description and configure the permission for subscriptions toward other Presence groups. The permission does not have to be entered toward all other Presence groups. The permission for subscriptions toward unconfigured Presence groups is determined by system default, which is configurable as a Cisco CallManager service parameter. Figure 15-14 shows the configuration of a Presence group.

Presence Group Relationship		Subscription Permission
Presence Group		
Accounting_PG		Allow Subscription
Executive_PG		Disallow Subscription
Sales_PG		Allow Subscription
Standard Presence group		Allow Subscription
NOTE: Presence Groups(s) not displayed		Use System Default
Modify Relationship to Other Presence Groups		Subscription Permission
Presence Group		Subscription Permission
Accounting_PG		Disallow Subscription
Executive_PG		
Sales_PG		
Standard Presence group		

Figure 15-14 Presence Group Configuration

Note Subscription permissions are configured in a unidirectional manner between pairs of Presence groups. It is possible to permit subscriptions from one group to another but to deny subscriptions in the opposite direction.

The Default Inter-Presence Group Subscription service parameter specifies the system default for Presence subscriptions. The system default is applied for subscriptions toward Presence groups for which no explicit permission has been set in the configuration of the Presence group from which the subscription request has been sourced.

The Default Inter-Presence Group Subscription parameter is a service parameter of the Cisco CallManager service and is therefore configured by choosing **System > Service Parameter**. The Inter-Presence Group Subscription service parameter is illustrated in Figure 15-15.

Clusterwide Parameters(System - Presence)	
Presence Subscription Throttling Threshold *	15000
Presence Subscription Resume Threshold *	80
Default Inter-Presence Group Subscription *	Disallow Subscription
BLF Status Depicts DND *	False

Figure 15-15 Inter-Presence Group Subscription Service Parameter

Figure 15-16 displays the Presence group configuration of the Cisco IP Phone.

IP phones are both watchers and Presence entities. An IP phone generates subscriptions when using Presence-enabled speed dials or Presence-enabled call lists. The DN of the IP phone can be watched by other subscribers. Presence groups must be applied to both the phone in the role as a subscriber and the DNs in the role as a Presence entity. Figure 15-17 displays the Presence group configuration performed at the DN.

CUCM sends subscribe messages on a SIP trunk when watching a Presence entity located on the other side of the SIP trunk. CUCM can also receive subscriptions over the SIP trunk when a DN on the cluster is being watched by a subscriber located on the other side of the trunk. The trunk can perform both subscriber and Presence entity roles. Only

one Presence group can be configured on a trunk, forcing the trunk to have similar restrictions in both directions of the trunk. Figure 15-18 displays the SIP trunk Presence group configuration.

The screenshot shows the 'Protocol Specific Information' section of a configuration interface. It includes fields for Packet Capture Mode (None), Packet Capture Duration (0), Presence Group (Standard Presence group), Device Security Profile (Cisco 7961 - Standard SCCP Non-Secure Profile), and SUBSCRIBE Calling Search Space (< None >). Below these are three checkboxes: Unattended Port, Require DTMF Reception, and RFC2833 Disabled.

Figure 15-16 Cisco IP Phone Presence Group

The screenshot shows the 'Directory Number Settings' section of a configuration interface. It includes fields for Voice Mail Profile (< None >), Calling Search Space (< None >), Presence Group (Standard Presence group), User Hold MOH Audio Source (< None >), Network Hold MOH Audio Source (< None >), and Auto Answer (Auto Answer Off).

Figure 15-17 Directory Number Presence Group

The screenshot shows the 'SIP Information' section of a configuration interface. It includes fields for Destination Address (*), Destination Port (5060), MTP Preferred Originating Codec (711ulaw), Presence Group (Sales_PG), SIP Trunk Security Profile (Non Secure SIP Trunk Profile), Rerouting Calling Search Space (< None >), Out-Of-Dialog Refer Calling Search Space (< None >), SUBSCRIBE Calling Search Space (< None >), SIP Profile (Standard SIP Profile), and DTMF Signaling Method (No Preference).

Figure 15-18 SIP Trunk Presence Group

Chapter Summary

The following list summarizes the key points covered in this chapter:

- CUCM Presence allows lines or endpoints reachable through SIP trunks to be monitored for their status (on-hook versus off-hook).

- Most IP phones support Presence-enabled speed dials. Type B Cisco IP Phones using SIP also support Presence-enabled call and directory lists.
- CUCM Presence configuration includes implementing Presence-enabled speed dials and enabling Presence-enabled call and directory lists.
- Presence policies can be applied to control Presence subscriptions.
- CUCM Presence policy configuration includes implementing partitions and subscribe CSSs and Presence groups.

References

For additional information, refer to these resources:

CUCM Features and Services Guide, Release 8.0(2), at
www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmfeat/fsgd.pdf.

CUCM Administration Guide, Release 8.0(2), at
www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmcfg/bccm.pdf.

Cisco Unified Communications SRND Based on CUCM 8.x, at
www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8xsrnd.pdf.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. Presence information is available over which of the following?
 - a. BLF speed dials
 - b. Speed dials
 - c. Abbreviated dialing
 - d. Fast Dial IP Phone service
2. Which component is required for Cisco Unified Personal Communicator?
 - a. Cisco Unity
 - b. Cisco Emergency Responder
 - c. Presence Server
 - d. Cisco MeetingPlace Express

- 3.** Which technology is enabled with the Cisco Presence server?
 - a.** Cisco IP Phone Messenger application
 - b.** Call History Presence
 - c.** Speed Dial Presence
 - d.** Call Directory Presence
- 4.** Which device is a watcher using Presence terminology?
 - a.** Calling party directory number
 - b.** Called party directory number
 - c.** Presence server
 - d.** Remote party's phone
- 5.** Which Presence message type is used for the watcher to check the status of a Presence entity?
 - a.** SIP subscribe
 - b.** SIP notify
 - c.** SIP refer
 - d.** SIP redirect
- 6.** What are the three possible states of a watched directory number?
 - a.** Unregistered
 - b.** On-hook
 - c.** Off-hook
 - d.** Ringing
 - e.** Ringing: Feature
 - f.** Hold
- 7.** Which of the following devices is a Presence entity?
 - a.** Calling party's phone
 - b.** Called party's phone
 - c.** Remote party directory number
 - d.** Redirected number

- 8.** Which two features restrict the watching functionality of a watcher watching a Presence entity in the same Presence group?
 - a.** Subscribe Calling Search Space
 - b.** Calling Search Space
 - c.** Partition
 - d.** Class of service
- 9.** Which three SIP features would restrict a watcher from watching a Presence group over a SIP trunk?
 - a.** Presence group
 - b.** Subscribe Calling Search Space
 - c.** Route pattern
 - d.** Translation pattern
 - e.** Inter-Presence group policy
- 10.** Presence groups apply to which of the following Presence features?
 - a.** BLF speed dials
 - b.** Call lists
 - c.** Speed dials
 - d.** Partitions

This page intentionally left blank

Chapter 16

Implementing Cisco Unified Mobility

Upon completing this chapter, you will be able to describe and configure Cisco Unified Mobility. This ability includes being able to meet these objectives:

- Describe the purpose of Cisco Unified Mobility, how it works, and when to use it
- Analyze call flows that involve Cisco Unified Mobility
- List the requirements for implementing and installing Cisco Unified Mobility
- Describe the considerations when using Cisco Unified Mobility Mobile Voice Access (MVA)
- Describe how to configure Cisco Unified Mobility

The growing use of mobile devices allows users—whether on a retail floor, at an airport, or at a Wi-Fi hotspot in a local coffee shop—to enjoy the features, efficiencies, and speed of Cisco Unified Communications. However, as more people own multiple devices ranging from office phones to home-office phones and laptop computers to mobile phones, they spend more time managing their communications across phone numbers and voice mailboxes, limiting their ability to accomplish work efficiently.

Cisco Unified Mobility allows users to be reachable at a single number, regardless of the device they use. This chapter describes the features of Cisco Unified Mobility, as well as how these features work and how to configure them.

Cisco Unified Mobility Overview

Cisco Unified Mobility consists of two main components:

- **Cisco Mobile Connect:** Allows an incoming call to the enterprise phone number of a user to be offered to the office phone of the user. The call can also be offered to as many as ten configurable remote destinations. Such remote destinations typically are

mobile or cellular telephones and home-office phones. This feature is commonly referred to as Single Number Reach in traditional telephony environments.

- **Cisco Unified Mobile Voice Access (MVA):** Provides similar features for outgoing calls. With MVA enabled, users who are outside the enterprise can make calls as if they were directly connected to Cisco Unified Communications Manager. This functionality is commonly referred to as Direct Inward System Access (DISA) in traditional telephony environments.

Both features allow active calls to be switched between the IP phone and the remote phone, as illustrated in Figure 16-1. For example, a user can initiate calls from a mobile phone while on the way to the office, and then switch the calls to an office phone after arriving at his desk.

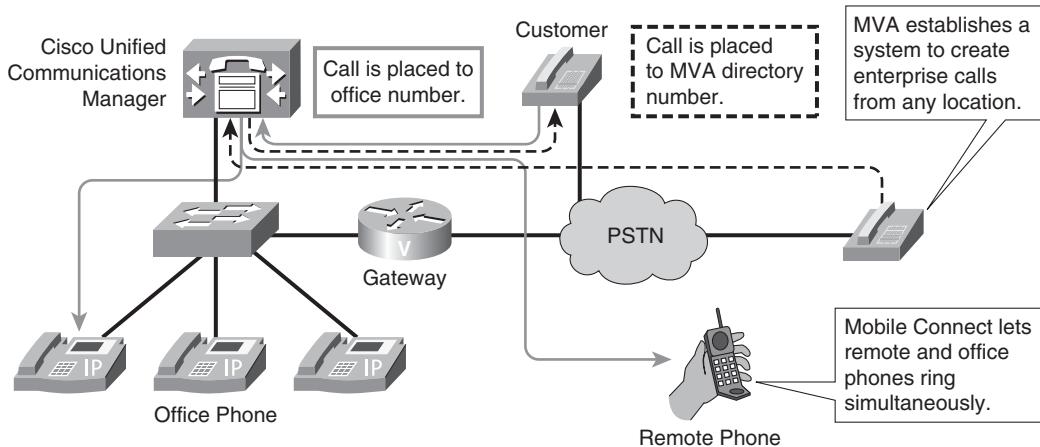


Figure 16-1 Cisco Unified Mobility Overview

Mobile Connect and MVA Characteristics

Mobile Connect enables users to receive business calls at a single phone number, regardless of the device that is used to receive the call. Mobile Connect allows users to answer incoming calls on the office phone or at a remote destination and pick up in-progress calls on the office phone or remote destination, without losing the connection. When the call is offered to the desktop and remote-destination phone or phones, the user can answer at any of those phones. After answering the call on a remote-destination phone, the user can hand off the call to the office phone. Active calls on the office phone can be handed off to a remote phone.

For example, when a user receives a call that is placed to the business number of the user, the office phone and the cell phone of the user ring. If the user is traveling to the office, the user can accept the call on the cell phone. After arriving at work, the user can pick up the in-progress call at the office IP phone by pressing a single key at the office IP phone.

The call continues without interruption on the office IP phone; the other party of the call does not notice the handover from the cell phone to the IP phone.

When MVA is used, after the call is connected, users can invoke midcall features. Users can also pick up the call on their desk phones, just like they can with received Mobile Connect calls. These actions are possible because the call is anchored at the enterprise gateway.

Cisco Unified Mobility Features

Mobile Connect and MVA enable flexible management of enterprise and remote destinations and provide several features and benefits, including the following:

- **Single enterprise number:** Regardless of the device that is used (enterprise phone, cell phone, home phone, or other), calls can be received on a single number—the number of the enterprise phone. The caller ID of the enterprise phone is also preserved on outgoing calls, regardless of the phone from which the call is initiated. Having a single enterprise number for incoming calls and always using the same enterprise number for outgoing calls also allow the use of a single voice mailbox. The enterprise voice mailbox can serve as a single, consolidated voice mailbox for all business calls. Incoming callers have a predictable means of contacting employees, and employees do not need to check multiple voicemail systems.
- **Access lists:** Cisco Unified Mobility users can configure access lists to permit or deny calling numbers to ring remote destinations. If a permit access list is used, unlisted callers are not allowed to ring remote destinations. If a deny access list is used, only unlisted callers are allowed to ring remote destinations.
- **User interfaces for enabling and disabling Cisco Unified Mobility:** Users can turn Cisco Unified Mobility on and off by using a telephone user interface (TUI) that MVA provides. A GUI for Cisco Unified Mobility user configuration is available on the Cisco Unified Communications Manager user web pages.
- **Access to enterprise features:** Cisco Unified Communications Manager features can be accessed by using dual-tone multifrequency (DTMF) feature access codes. The supported features include hold (default *81), exclusive hold (default *82), resume (default *83), transfer (default *84), and conference (default *85). The feature codes can be configured as Cisco Unified Communications Manager service parameters.
- **Smart client support:** On phones on which smart clients are installed, softkeys can be used to access features such as hold, resume, transfer, and conference. Users can also enable or disable Cisco Unified Mobility from a smart client.
- **Call logging:** Enterprise calls are logged regardless of which device (enterprise phone or remote phone) is used.

Cisco Unified Mobility Call Flows

Figure 16-2 illustrates the call flow when Mobile Connect is used. The figure shows an IP phone with extension 2001 and a mobile phone that belongs to the user of the IP phone.

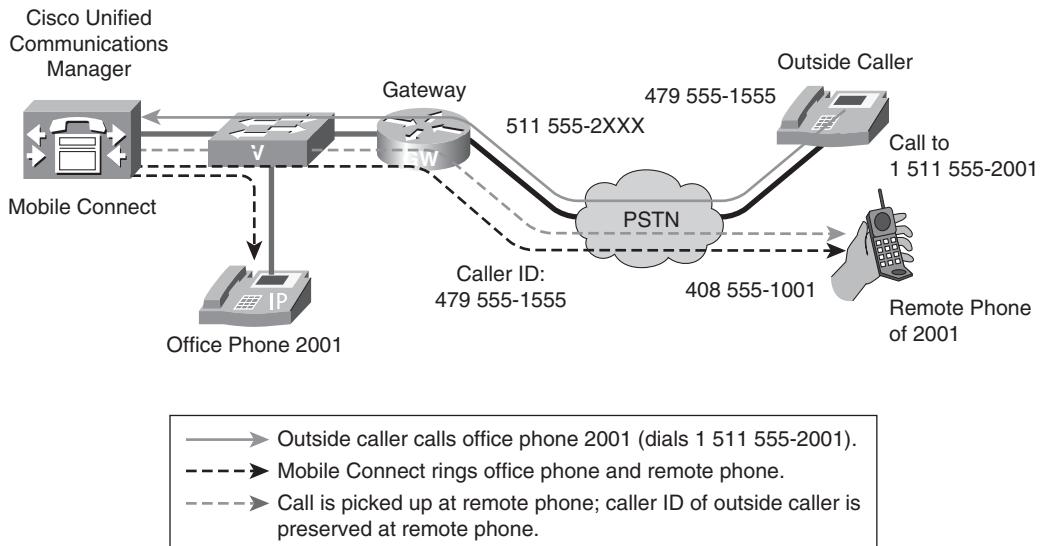


Figure 16-2 Mobility Call Flow with Mobile Connect

In this example, a public switched telephone network (PSTN) user calls the office number of the user. Because Mobile Connect is enabled, both the desktop phone 2001 and the configured remote destination (mobile phone 408 555-1001) ring simultaneously. The call is presented to the remote phone with the original caller ID (479 555-1555). As soon as the call is accepted on one of the phones, the other phone stops ringing. The user can switch the call between the office phone and the mobile phone (and vice versa) during the call, without losing the connection.

Mobile Connect Call Flow: Internal Calls Placed from Remote Phone

Mobile Connect influences the calling-number presentation. If a call is received from a recognized remote destination, the corresponding internal directory number, not the E.164 number of the remote device, is used as the calling number.

In Figure 16-3, extension 2001 has a Mobile Connect remote destination of 408 555-1001 (cell phone of the user of 2001). The user places a call from the mobile phone to an enterprise PSTN number of a colleague (by dialing 1 511 555-2002). The called colleague sees the call as coming from the internal directory number 2001 instead of the external mobile phone number.

The same applies to calls that are placed to other internal destinations, such as voicemail. If the user of extension 2001 places a call from the cell phone to Cisco Unity, Cisco Unity sees directory number 2001, not the PSTN number of the cell phone (408 555-1001),

as the source of the call. Cisco Unity can identify the user by that directory number and can provide access to the appropriate mailbox instead of playing a generic welcome greeting.

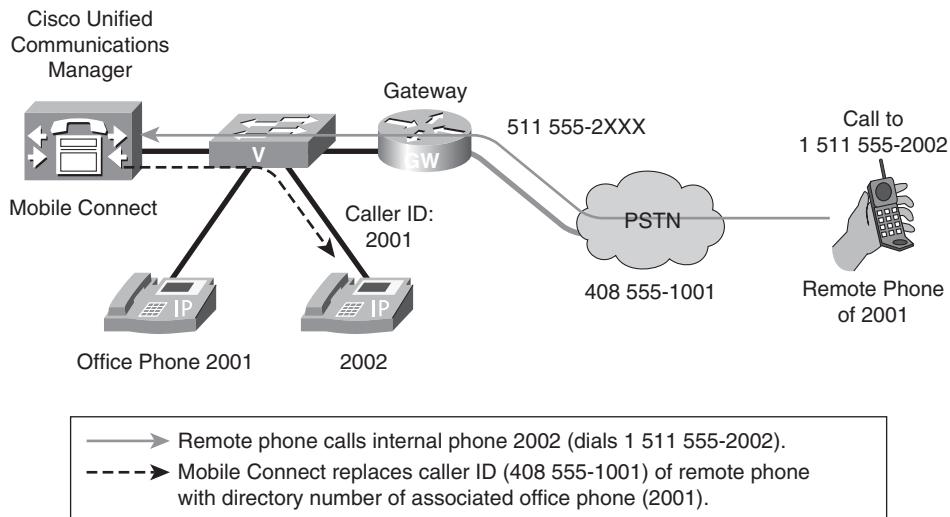


Figure 16-3 Incoming Call from Remote Phone to Internal Destination

To recognize Mobile Connect remote destinations, the Mobile Connect remote destination number must match the Automatic Number Identification (ANI) of the incoming call. Mobile Connect remote destinations typically include an access code, for example, 9 in the number 9 1 408 555-1001. The access code 9 and the long distance 1 must be prefixed to the incoming ANI 408 555-1001 to recognize the source as a Mobile Connect remote destination. Alternatively, the Cisco CallManager service Matching Caller ID with Remote Destination parameter can be set to Partial Match, and the Number of Digits for Caller ID Partial Match value can be set. This value specifies how many digits of the incoming ANI (starting with the least significant digit) must match a configured remote-destination number.

If the source of the call is not recognized as a Mobile Connect remote destination, the PSTN number of the remote destination is used for the calling number and is not changed to the internal directory number.

MVA Call Flow

When MVA is used, users can place calls from a remote destination to the outside as if they were dialing from the desktop phone. In the example shown in Figure 16-4, the user of the IP phone with directory number 2001 uses a cell phone (408 555-1001) to dial the PSTN number of the headquarters, extension 2999. The gateway is configured to start an interactive voice response (IVR) call application for calls that are placed to that number.

The call application, which is based on Voice Extensible Markup Language (VoiceXML, also known as VXML), offers a prompt and asks for the remote destination number and the PIN of the user. After login, the user can activate and deactivate MVA and can initiate a call from the enterprise network. The call is set up with the E.164 PSTN number of directory number 2001, instead of with 408 555-1001. This action allows the called party to identify the caller by the (single) office number of the user. The fact that the call is actually placed from a mobile phone instead of the office IP phone does not matter; the call appears to come from the office phone.

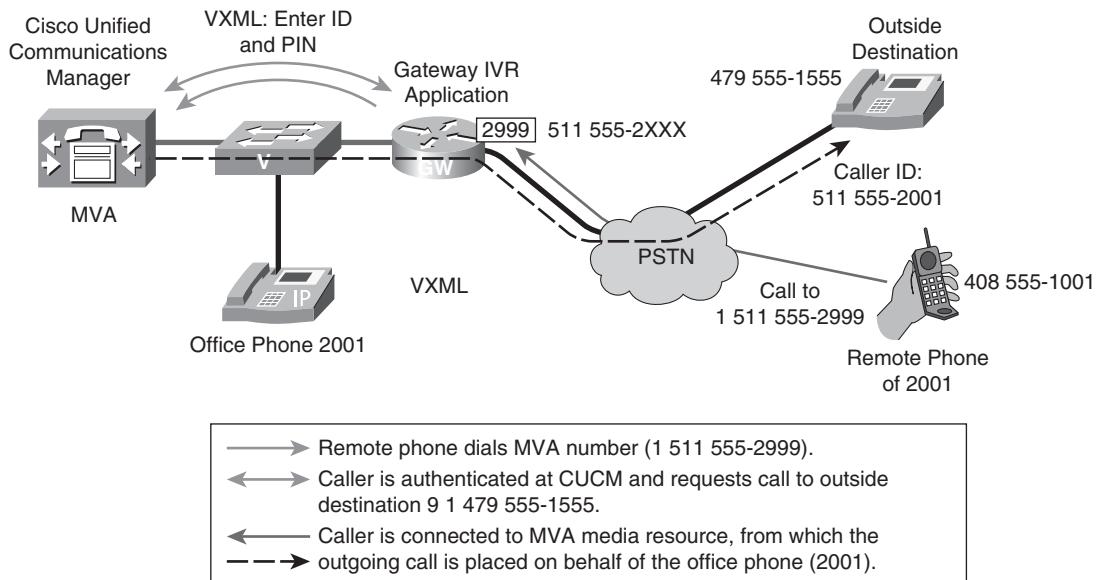


Figure 16-4 MVA Call Flow

After the user has used MVA to initiate a call from a remote destination, the user can switch the call to the office phone and back again as needed, without losing the connection.

Cisco Unified Mobility Implementation Requirements

To implement Cisco Unified Mobility features, you must start the MVA service, which interacts with the call application that runs on a Cisco IOS gateway, on at least one Cisco Unified Communications Manager system.

MVA requires an H.323 or Session Initiation Protocol (SIP) gateway to provide a VXML call application to remote callers who dial a certain number. Media Gateway Control Protocol (MGCP) is not supported because it does not support call applications.

DTMF must be sent out-of-band (OOB) for MVA to work.

The remote destination cannot be an IP phone within the enterprise. The remote destination must be an external device, typically a PSTN number. As many as ten remote destinations can be configured. Class of service (CoS) can be configured to limit access to the PSTN.

Mobility Configuration Elements

The following are configuration elements for mobility:

- **End user:** Each end user must have a configured PIN, which is used for authentication when MVA is used. Three important Cisco Unified Mobility-related settings that can be configured for the end user are as follows:
 - **Enable Mobility:** This check box must be selected to allow the user to use the Mobile Connect feature (that is, to receive enterprise calls at one or more remote destinations and to place calls from a remote phone into the enterprise).
 - **Enable Mobile Voice Access:** This check box must be selected to allow the user to place MVA calls. These calls are outgoing enterprise calls from a remote phone that should be placed on behalf of the office phone.
 - **Remote Destination Limit:** This setting is used to limit the number of remote destinations that can be configured. The maximum is 10.
- **IP phone:** The office phone of a Cisco Unified Mobility user must refer to the end-user name. This task is done by setting the owner in the Phone Configuration window to the user ID of the end user.

Note In the End User Configuration window, the end user can be associated with one or more devices, such as IP phones. Such an association allows the end user to configure the device from the Cisco Unified Communications Manager user web pages, but it is not relevant for Cisco Unified Mobility. The mapping of the IP phone to the end user must be done by setting the owner in the Phone Configuration window.

- **Remote destination profile:** This setting creates a virtual phone that is linked to the end user and that represents all remote destinations that are associated with the user. The profile includes phone device-level configuration settings, such as user and network music on hold (MoH) audio sources and Calling Search Spaces (CSS). For each office phone that an end user should be able to use for Cisco Unified Mobility, a shared line with the line or lines of the office phone or phones must be added to the remote destination profile. In addition, the remote destination profile is configured with remote destinations.
- **Remote destination:** A remote destination is associated with one or more shared lines of a remote destination profile. For each remote destination, the remote destination number, as dialed from within the enterprise, must be specified. The rerouting

CSS of the specified remote destination profile is used to look up the configured remote destination number.

Note The remote destination profile has two CSSs that are used for call routing. One standard CSS is used for outgoing calls that are initiated by using MVA and the rerouting CSS. The rerouting CSS is used to place a call to the remote destination (either when receiving a call to the number of the line that the office phone and the remote destination profile share, or when a call is handed over from the office phone to the remote destination). Therefore, the remote destination number must be reachable by the rerouting CSS. For MVA calls, the rerouting CSS is composed of the CSS that is configured at the shared line and the CSS of the remote destination profile (with priority to the CSS of the shared line).

- **Access list:** Access lists can be configured to permit or deny calls that are to be placed to a remote destination when the shared line is called. The filter is based on the calling number. An access list is configured with one or more numbers that specify the calling number that should be permitted or denied. Access lists are also configured with an owner (end-user ID) and are applied to remote destinations. An allowed, a blocked, or a no access list can be applied. If an allowed access list is applied, all calling numbers that are not listed in the access list are blocked. If a blocked access list is applied, all unlisted numbers are allowed. If no access list is applied, all calling numbers are allowed to ring the remote destination.
- **MVA media resource:** This media resource interacts with the VXML call application that runs on the Cisco IOS gateway. The resource is required for MVA only. The number at which the Cisco IOS router can reach the media resource must be specified, a partition can be applied, and one or more locales must be chosen.

Note The CSS of the gateway that runs the VXML call application must include the partition that is applied to the number of the MVA media resource.

Shared Line Between Phone and Remote Destination Profile

A remote destination profile is associated with one or more IP phones. Each phone line that an end user should be able to use with Cisco Unified Mobility must be added to the remote destination profile that is associated with the end user. The directory number for the user is thus associated with two devices: the IP phone and the remote destination profile. Such a directory number is also called a shared line. The IP phone or phones that share a line with the remote destination profile must be owned by the end user who is associated with the remote destination profile.

Remote destinations are associated with one or more shared lines that are configured at remote destinations.

As described earlier, the settings of the shared directory number (including the partition and CSS) apply to all associated devices. The remote destination profile is configured with a (standard) CSS, which is used for calls that a remote phone places when it uses MVA, and a rerouting CSS, which is applicable to calls that are placed to a remote destination.

Consider the setup in Figure 16-5. If a call is placed to directory number 2002, Line1 at Office Phone2 and all remote destinations that are associated with Line2 of the remote destination ring. For the call to the remote destination number, the rerouting CSS is used.

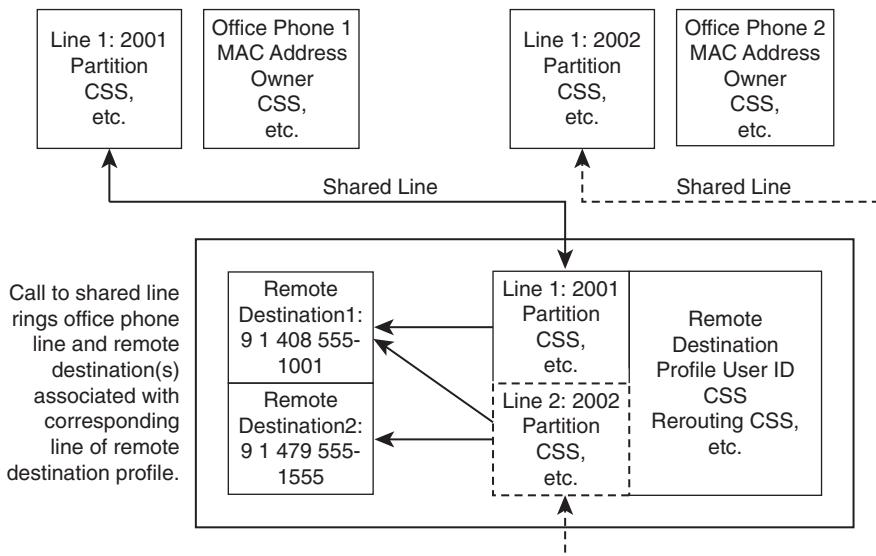


Figure 16-5 Shared Line for Remote Destination

If the remote phone with number 9 1 479 555-1555 calls in to the mobile voice application and requests an outgoing call to be placed, the CSS of Line2 and the CSS of the remote destination profile are used for the outgoing enterprise call that Remote Destination2 initiates.

Relationship of Mobility Configuration Elements

Figure 16-6 illustrates the logical structure used within the operation of mobility. To use Cisco Unified Mobility, the Cisco Unified Mobile Voice Access service must be activated if MVA is desired in addition to Mobile Connect functionality. When the Cisco Unified Mobile Voice Access service is activated, a corresponding media resource is

automatically added. The media resource must be configured with the MVA number, a partition, and locales.

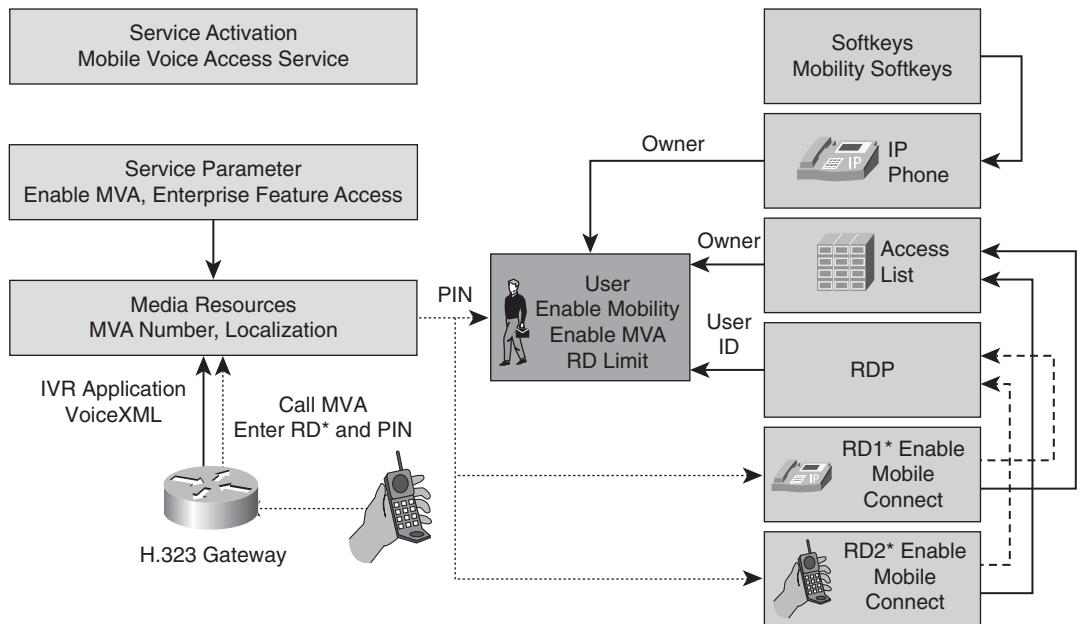


Figure 16-6 Mobility Elements

The configured number must be reachable from the Cisco IOS router that provides remote phones access to a VXML IVR call application.

Incoming MVA callers are authenticated by remote destination number. Callers are also authenticated by the PIN that is configured for the user who is associated with the remote destination profile that the corresponding remote destination number references.

When Mobile Connect is used and incoming calls are sent to a line that is shared by an IP phone and a remote destination profile (both referring to the same end-user ID), access lists that are applied to remote destinations can be used to control which callers are allowed to ring the remote destination. The access list must refer to the end user who is configured in the remote destination profile to which the remote destination has been assigned.

To allow an active call to be handed over from an IP phone to a remote destination, the IP phone must have the Mobility softkey configured for the Connected call state. If the Mobility softkey is also added to the On Hook call state, the softkey can be used to check the status of Cisco Unified Mobility (Mobile Connect on or off).

In summary, the end user is the central element that is associated with IP phones (at which the user is configured as the owner), access lists, and remote destination profiles. Remote destinations are associated with shared lines of remote destination profiles and access lists. For MVA, the appropriate service must be activated, and the automatically generated media resource is made available to a router that runs the VXML call application.

Cisco Unified Mobility Considerations

On the voice gateway, the MVA application is configured and triggered as part of a voice dial peer application. Dial peer matching takes place only if the gateway provides call control functionality. When MGCP or Skinny Client Control Protocol (SCCP) is used to control voice interfaces that receive incoming PSTN calls, the gateway no longer has complete call control.

Call control is passed over to the Cisco Unified Communications Manager. In this case, the MVA application cannot be started because no dial peer matching process takes place. To use MVA in such an environment, Cisco Unified Communications Manager must forward calls that were received from an MGCP- or SCCP-controlled interface to an H.323 gateway, to start the MVA application. From then on, the call treatment is like an H.323-only environment, except that the outbound PSTN call is established through the MGCP gateway.

MVA Call Flow with MGCP PSTN Gateway Access

In Figure 16-7, the incoming PSTN call is received on an MGCP-controlled interface. Cisco Unified Communications Manager forwards the call to an H.323 gateway. On the H.323 gateway, the MVA application is started and the caller can be authenticated and can define the final destination for the call. The caller is then connected to the MVA media resource, from which the outgoing call is placed on behalf of the caller office phone (2001). Cisco Unified Communications Manager establishes the outgoing call through the MGCP gateway.

Note The H.323 gateway functionality can be combined on the gateway that receives the PSTN call on the MGCP-controlled interface. In this case, only one gateway that provides MGCP and H.323 signaling is required.

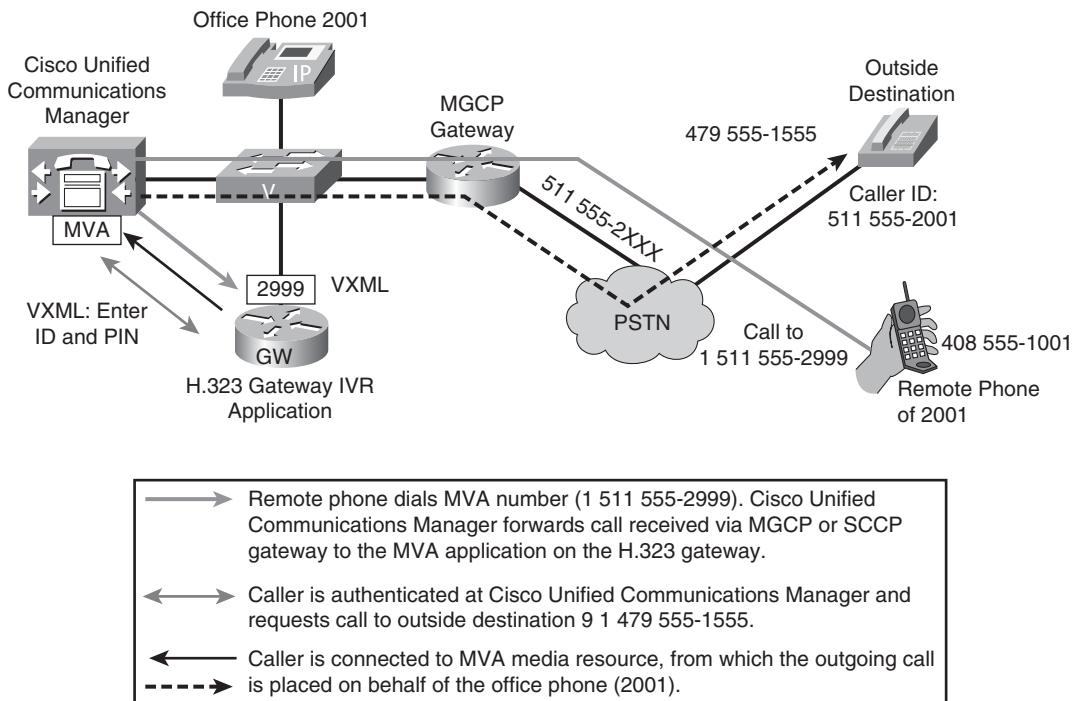


Figure 16-7 MVA and MGCP Call Flow

CSS Handling in Mobile Connect

Depending on the origin of a call that uses the Mobile Connect feature, different CSSs are used:

- For an incoming PSTN call to an office phone that is associated with a remote destination, the rerouting CSS at the remote destination needs access to the mapped remote destination number.
- For an incoming call from a remote phone (remote destination) to an internal destination, the CSS of the receiving device (trunk, gateway) needs access to the called internal number.

CSS Handling in MVA

The incoming and outgoing call legs of an MVA call are treated independently. The incoming call leg is the call leg from the gateway where the MVA call application is running to the MVA media resource in Cisco Unified Communications Manager. The CSS

that is used for this call leg depends on a Cisco CallManager service parameter. This service parameter is called Inbound CSS for Remote Destination. The parameter can be set to one of these values:

- **Trunk or Gateway Inbound CSS:** This value is the default value in Cisco Unified Communications Manager. If this option is chosen, Cisco Unified Communications Manager uses the CSS of the trunk or gateway from which the MVA call arrived. The CSS of the shared line and the CSS that is configured at the remote destination profile are not considered for the incoming call leg of an MVA call.
- **Remote Destination Profile + Line CSS:** If this option is selected, the CSS of the shared line and the CSS that is configured at the remote destination profile are combined (with priority given to the partitions of the shared-line CSS).

The outgoing call leg of an MVA call is the call leg from the MVA media resource to the PSTN destination that is called from the MVA call application. The CSS that is used for this call leg is always the combination of the CSS of the shared line and the CSS that is configured at the remote destination profile (with priority given to the partitions of the shared-line CSS).

Cisco Unified Mobility Access List Functions

In Cisco Unified Communications Manager, the end user and the administrator can control access to remote destinations based on the time of the day and the day of the week.

To support time of day-based access to remote destinations, the remote destination configuration page allows the configuration of a ring schedule. This schedule applies to the remote-destination configuration page on both the administrator and user web pages.

The remote destination can be generally enabled (enabled all the time), or explicit time ranges can be configured. The default is to enable the remote destination all the time.

When an explicit time range is configured, each day of the week can be disabled, enabled for the entire day (24 hours), or configured with a From/To time range.

Access lists can limit access through caller IDs. These lists are applied at the remote-destination configuration page:

- The Allowed Access List Access List setting is called Ring This Destination Only If Caller Is in <Access List>.
- The Blocked Access List Access List setting is called Do Not Ring This Destination If Caller Is in <Access List>.

Basically, two things must be considered when using time-of-day access control to remote destinations:

- The remote destination rings only when the call is received during the specified ring schedule. This first decision is independent of the access list configuration.
- If no access list is configured, all callers are permitted. However, this permission applies only after the first check (the call received during the specified ring schedule). If a caller is permitted according to an access list configuration but the call is received outside the configured ring schedule, the call is not extended to the remote destination.

Figure 16-8 shows how calls that are received at a shared line that is configured at a remote destination profile are processed.

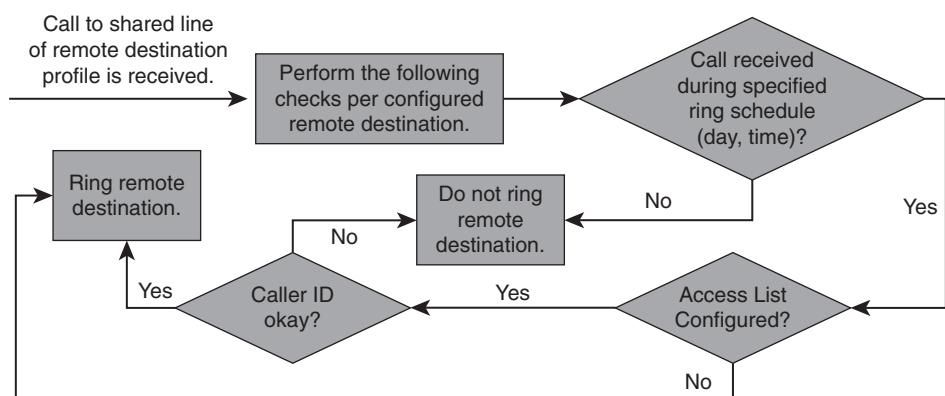


Figure 16-8 Access List Considerations

For each remote destination that is associated with the called line, the ring schedule that is configured at the remote destination is checked in the following way:

- If the call is received outside the configured ring schedule, the remote destination does not ring.
- If the call is received within the configured ring schedule, the access list configuration of the remote destination is checked. If the caller ID is permitted, the remote destination rings. If the caller ID is not permitted, the remote destination does not ring.

The caller ID is permitted in the following scenarios:

- The Always Ring the Destination parameter is selected.
- An access list is applied by using the Ring This Destination Only If Caller Is in <Access List> parameter, and the caller ID is found in the specified access list.

- An access list is applied by using the Do Not Ring This Destination If Caller Is in <Access List> parameter, and the caller ID is not found in the specified access list.

Mobility Phone Number Matching

For Mobile Connect and for MVA, the calling line ID of an incoming call is compared against configured remote destinations to identify the end user and the associated office phone. This matching process can easily fail because incoming PSTN calls typically do not contain prefixes such as access or long-distance codes. To allow successful number matching, even if not all digits of an incoming caller ID and configured remote destinations match, the following two Cisco CallManager service parameters exist:

- Matching Caller ID with Remote Destination (Partial Match or Complete Match [Default])
- Number of Digits for Caller ID Partial Match

Cisco Unified Mobility Configuration

The following list summarizes the steps for configuring Mobile Connect and MVA:

- Step 1.** Add the Mobility softkey to the IP phone softkey templates.
- Step 2.** Add and configure the end user.
- Step 3.** Configure the IP phone.
- Step 4.** Configure the remote destination profile with a shared line.
- Step 5.** Add the remote destination or destinations to a remote destination profile.
- Step 6.** Configure service parameters.
- Step 7.** Optional: Implement access lists to specify which caller ID is allowed to ring a remote destination when a call to the office phone is received:
 - a.** Configure access lists.
 - b.** Apply access lists to the remote destination.

Note In addition, the appropriate partitions and CSSs must be configured and applied. The shared-line directory number can be assigned with a partition, and standard CSSs can be configured at the shared directory number (the line CSS) and at the device level (the IP phone and remote destination profile). In addition, for Mobile Connect calls (that is, calls to a remote destination), a rerouting CSS can be configured in the remote destination profile.

Step 1: Configure Softkey Template

The first step is to configure a softkey template that includes the Mobility softkey.

In Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Softkey Template**, and in the resulting window, as shown in Figure 16-9, configure a softkey template that includes the Mobility softkey for the following call states:

- On Hook
- Connected

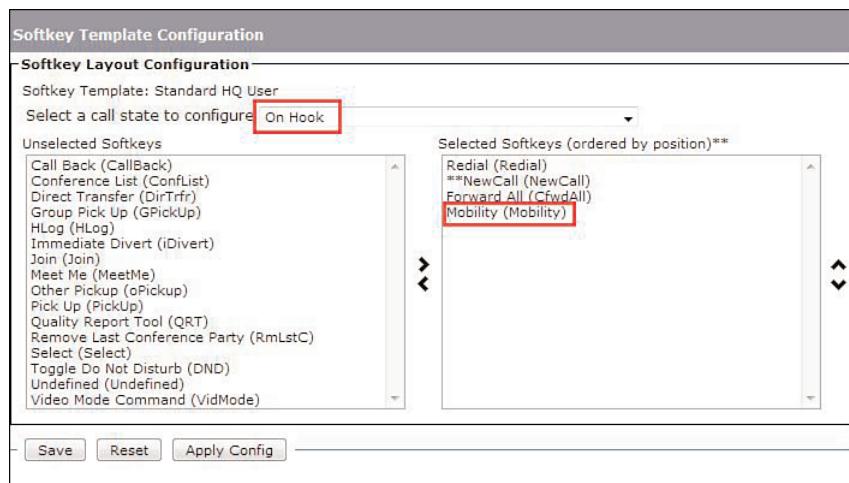


Figure 16-9 Softkey Template Configuration

Step 2: Configure End User

End-user accounts must be created and configured when Cisco Unified Mobility is used. To configure end users, choose **User Management > End User**. Configure Cisco Unified Mobility parameters in the Mobility Information section of the End User Configuration window, as shown in Figure 16-10:

- **Enable Mobility:** Select this check box to enable Mobile Connect, which allows the user to receive calls on multiple devices that are placed to a single enterprise phone number and to hand over in-progress calls between the desktop phone and a remote phone. Mobile Connect also allows users to place calls from remote phones into the enterprise, for example, to voicemail or internal directory numbers that are signaled with the internal directory number of the user.
- **Enable Mobile Voice Access:** Select this check box to allow the user to use the MVA feature to place outgoing enterprise calls from a remote phone.

The screenshot shows the 'End User Configuration' window. The 'User Information' section contains fields for User ID (mpolo), Password, Confirm Password, PIN, Confirm PIN, Last name (Polo), Middle name, and First name (Marco). There are 'Edit Credential' buttons next to the password and PIN fields. The 'Mobility Information' section includes a checked checkbox for 'Enable Mobility' (highlighted with a red box), a dropdown for 'Primary User Device' (set to '< None >'), an unchecked checkbox for 'Enable Mobile Voice Access', a field for 'Maximum Wait Time for Desk Pickup' (10000 ms), a field for 'Remote Destination Limit' (4), and a scrollable list for 'Remote Destination Profiles'.

Figure 16-10 End User Mobility Configuration

- **Maximum Wait Time for Desk Pickup:** Enter the maximum time, in milliseconds, that can pass before the user must pick up a call that is handed over from the remote phone to the office phone. The range is from 0 to 30,000 ms, with a default value of 10,000 ms.
- **Remote Destination Limit:** Enter the maximum number of remote destinations to which incoming calls that are placed to the enterprise phone number of the user can be sent. The range is from 1 to 10; the default value is 4.
- **Remote Destination Profiles:** This read-only field lists the remote destination profiles that have been created for this user.
- **Access Lists:** (Field not shown.) This read-only field displays the access lists that have been created for this user.

Step 3: Configure IP Phone

The next step is to configure the office IP phone of the user for Cisco Unified Mobility.

As shown in Figure 16-11, two parameters must be configured in the Phone Configuration window of the office IP phone of the user:

- **Softkey Template:** Apply the softkey template (which you created in Step 1) to the IP phone so that the user can access the Mobility softkey in the On Hook and Connected states.

- **Owner User ID:** Choose the end-user name that you configured in Step 2. This action enables Cisco Unified Communications Manager to locate related configuration elements, such as the remote destination profile of the end user.

Note As the line is shared with the line of the office phone, the same partition that is applied to the line of the office phone has to be set here. The screen shot does not show a partition, so in this case, the office line would also have no partition assigned.

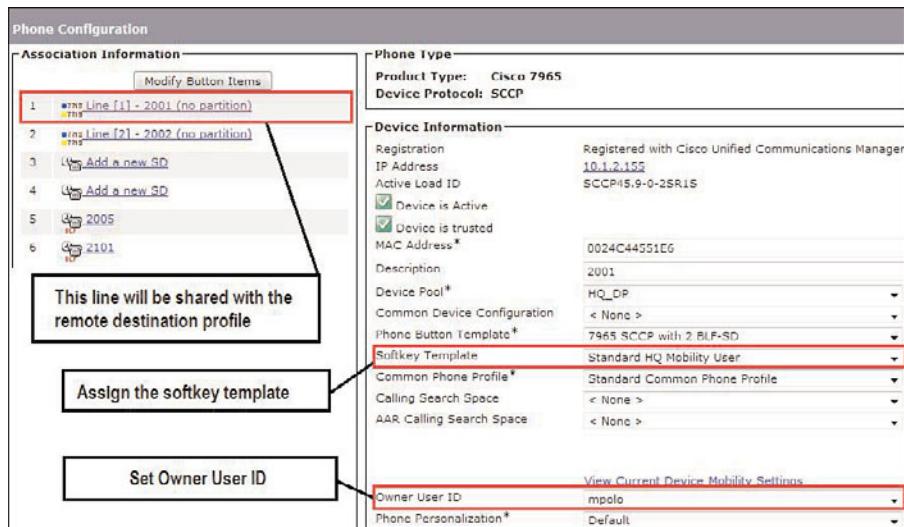


Figure 16-11 Phone Mobility Configuration

Step 4: Configure Remote Destination Profile

To configure remote destination profiles, choose Device > Device Settings > Remote Destination Profile. The remote destination profile contains the parameters that apply to all the remote destinations of the user. In the Remote Destination Profile Configuration window, as shown in Figure 16-12, enter a name, description, device pool, CSS, rerouting CSS, and network and user MoH audio sources for the remote destination profile. Also enter these mobility-specific parameters:

- **User ID:** Choose the user to whom this profile is assigned. The choice must match the ID of an end user for which the Enable Mobility check box is selected.
- **Privacy:** Choose a privacy option for this profile. Possible values are On, Off, or Default.
- **Ignore Presentation Indicators:** Select this check box to ignore the connected line ID presentation. This setting is recommended for internal calls.

- **Calling Search Space:** This CSS (combined with the line CSS) is used for outgoing enterprise calls that are placed from a remote destination by using MVA. The setting has no relevance to Mobile Connect.
- **Rerouting Calling Search Space:** Set the CSS that should be used when sending calls that are placed to the enterprise phone number of the user to the specified remote destinations. This CSS is also used when an active call is handed over from the office phone to a remote phone.

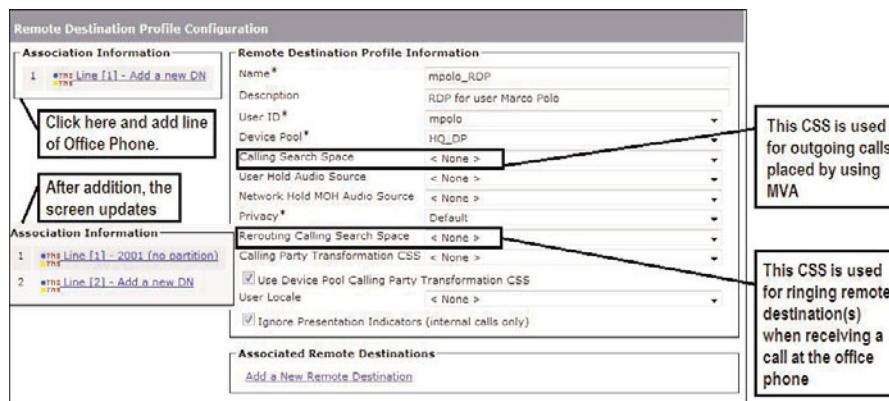


Figure 16-12 Remote Destination Profile Configuration

After a remote destination profile is created, one shared line must be configured for each directory number that is used at the office phone or phones of the user. To add a shared line, click **Add a New DN** at the appropriate phone link.

Step 5: Add Remote Destinations to Remote Destination Profile

To configure remote destinations, choose **Device > Remote Destination**. Alternatively, you can click the **Add a New Remote Destination** link in a remote destination profile. In the Remote Destination Configuration window, as shown in Figure 16-13, enter a name for the remote destination and configure the parameters that follow:

- **Destination Number:** Enter the telephone number for the remote destination. Include the area code and any additional digits that are required to dial the remote phone from within the enterprise. The maximum field length is 20 characters.

Note The destination number must not be an internal directory number; the destination number must be an external number. The number must be entered as it would be if it were being dialed from an IP phone: Use a complete E.164 number that includes the access code so that the number matches a route pattern that points to the PSTN. The rerouting CSS

that is configured in the remote destination profile will be used to look up the specified number in the call-routing table.

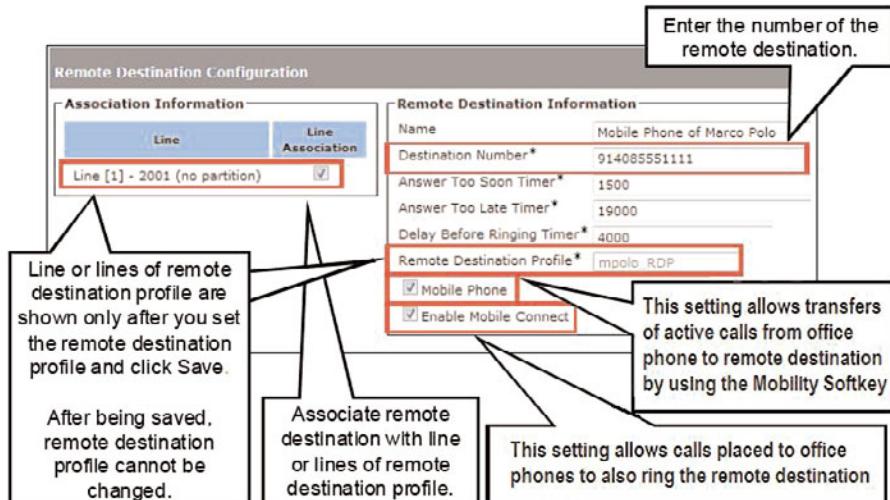


Figure 16-13 *Remote Destination Configuration*

- **Remote Destination Profile:** The remote destination profile must be chosen if you created a new remote destination after choosing Device > Remote Destination. If you open the Remote Destination Configuration window by clicking the Add a New Remote Destination link in the Remote Destination Profile window, or if you are editing an existing remote destination, the remote destination profile is already set up and cannot be changed.

Note If you want to associate a remote destination that is already associated with one remote destination profile with another remote destination profile, you must delete and re-create the remote destination.

- **Mobile Phone:** Select this check box to allow active calls to be handed over from the office phone to this remote destination when the user presses the Mobility softkey at the office phone.
- **Enable Mobile Connect:** Select this check box to allow calls to be placed to this remote destination when there is an incoming call to a shared-line directory number of an office phone.

Note End users can create their own remote destinations on the Cisco Unified Communications Manager user web pages.

Finally, the remote destination must be associated with one or more shared lines of the specified remote destination profile.

From now on, the remote destination rings if a call is placed to the appropriate shared line of an office phone. When a call is placed from a recognized remote destination to an internal destination, the calling number is modified from the remote phone number to the office phone directory number. However, in most cases, the caller ID of that incoming call is a ten-digit number. The remote destination number usually has a PSTN access code (for example, 9) and then an 11-digit number (trunk prefix 1 followed by the ten-digit number). If the incoming calling number is not prefixed with 91, internal phones see the call coming from the E.164 number of the remote phone instead of from the associated internal directory number. The next step shows how to resolve such issues.

Step 6: Configure Service Parameters

To set partial matches so that a calling number can be recognized as a remote destination, you can configure Cisco CallManager service parameters. To access Cisco Unified CallManager service parameters, choose **System > Service Parameters** and choose Cisco CallManager to display the window shown in Figure 16-14.

Configure the following parameters to allow incoming caller IDs that do not include the 91 prefix that is used in the remote destination to be recognized:

- **Matching Caller ID with Remote Destination:** Set this parameter to Partial Match (default is Complete Match).
- **Number of Digits for Caller ID Partial Match:** Set this parameter to the number of digits that must match (beginning with the least significant digit) when comparing the incoming calling number against the configured remote destination number.

Note Alternatively, choose **Call Routing > Transformation Pattern** to configure caller ID transformations. Each pattern can be assigned a partition. The Calling Party Transformation CSS, which is configured in the remote destination profile, is used to control access to the configured transformation patterns.

Step 7a: Configure Access List

To configure access lists, choose **Device > Device Settings > Access Lists** to open the Access List Configuration window, as shown in Figure 16-15. Enter a name and a description for the access list. In the Owner drop-down list, choose the user to whom the access list applies. Then select the Allowed radio button to create a list of phone numbers that

should be allowed to ring a certain remote destination when a call is placed to the office phone number of the user. To block the numbers that are listed in the access list from ringing the remote destinations to which the access list will be applied, select the Blocked radio button.

Service Parameter Configuration	
Clusterwide Parameters (System - Mobility)	
<u>Enterprise Feature Access Code for Hold</u> *	*81
<u>Enterprise Feature Access Code for Exclusive Hold</u> *	*82
<u>Enterprise Feature Access Code for Resume</u> *	*83
<u>Enterprise Feature Access Code for Transfer</u> *	*84
<u>Enterprise Feature Access Code for Conference</u> *	*85
<u>Enterprise Feature Access Code for Session Handoff</u> *	*74
<u>Smart Mobile Phone Interdigit Timer</u> *	500
<u>Non-Smart Mobile Phone Interdigit Timer</u> *	2000
<u>Send Call to Mobile Menu Timer</u> *	60
<u>SIP Dual Mode Alert Timer</u> *	1500
<u>Call Screening Timer</u> *	4000
<u>Inbound Calling Search Space for Remote Destination</u> *	Trunk or Gateway Inbound Calling Search Space
<u>Enable Enterprise Feature Access</u> *	False
<u>Dial-via-Office Forward Service Access Number</u>	
<u>Enable Mobile Voice Access</u> *	False
<u>Mobile Voice Access Number</u>	
<u>Matching Caller ID with Remote Destination</u> *	Complete Match
<u>Number of Digits for Caller ID Partial Match</u> *	10
<u>System Remote Access Blocked Numbers</u>	

Figure 16-14 Service Parameters

Access List Configuration	
Access List Information	
Name *	MarnPrivate-ACL
Description	Filter calls from 800 555 1111 and from unknown
Owner	impo
Access List Type	<input checked="" type="radio"/> Blocked
Access List Member Information	
Selected Filters	Not Available PRV10 Directory Number (8005551111)
Removed Filters	
Access List Members	
<input checked="" type="checkbox"/> ims Not Available <input checked="" type="checkbox"/> ims Private <input checked="" type="checkbox"/> ims Directory Number (8002551111) <input checked="" type="checkbox"/> ims	
<input type="button" value="Save"/> <input type="button" value="Delete"/> <input type="button" value="Copy"/> <input type="button" value="Add New"/>	

Figure 16-15 Access List Configuration

After saving the access list, the window reopens to display the Access List Member Information area. Click Add Member to add a member, and then choose an option from the Filter Mask drop-down list in the Access List Member Detail window. Choose to enter a directory number or to filter out calls that do not have caller ID (the Not Available option) or do not display their caller ID (the Private option). You can also change existing members by clicking the appropriate link.

In the Access List Member Detail window, if Filter Mask is set to Directory Number, enter a phone number or filter in the DN Mask field. You can use the following wildcards:

- **X:** Matches a single digit (must be entered as an uppercase X)
- **!:** Matches any number of digits

Step 7b: Apply Access List to Remote Destination

To apply an access list to a remote destination, open the Remote Destination Configuration window. Choose **Device > Remote Destination** or click the appropriate link in the Remote Destination Profile window. From the Remote Destination Configuration window, shown in Figure 16-16, choose the access list from the **Ring this destination only if caller is in** (allowed access list) or **Do not ring this destination if caller is in** (blocked access list) drop-down list.

The screenshot shows the 'Remote Destination Configuration' window. On the left, there's a sidebar with 'Association Information' and a 'Line' tab selected, showing 'Line [1] - 2001 (no partition)'. The main area is titled 'Remote Destination Information' and contains fields for Name (Mobile Phone of Marco Polo), Destination Number (914085551111), Answer Too Soon Timer (1500), Answer Too Late Timer (19000), Delay Before Ringing Timer (4000), and a dropdown for Remote Destination Profile (mpolo_RDP). Below these are checkboxes for 'Mobile Phone' and 'Enable Mobile Connect'. A large section titled 'When Mobile Connect is Enabled' follows, containing a 'Ring Schedule' table where every day is mapped to 'No Office Hours'. At the bottom, a section titled 'When receiving a call during the above ring schedule:' has three radio button options: 'Always ring this destination', 'Ring this destination only if caller is in ... Not Selected ...', and 'Do not ring this destination if caller is in MarcoPolo-ACL'. The third option is selected and highlighted with a red box. At the very bottom are buttons for Save, Delete, Copy, and Add New.

Figure 16-16 Access List application

Note Only an allowed (Ring this destination only if caller is in), blocked (Do not ring this destination if caller is in), or no access list (Always ring this destination) can be applied to a remote destination. Calling numbers that are not listed in an allowed access list are denied, and calling numbers that are not listed in a blocked access list are allowed.

Cisco Unified Mobility: MVA Configuration Procedure

This list summarizes the steps for configuring MVA:

Step 1. Activate Cisco Unified Mobile Voice Access service.

Step 2. Configure the service parameters:

- a. Enable MVA globally.
- b. Enable and configure enterprise feature access.

Step 3. Enable MVA per end user.

Step 4. Configure the MVA media resource.

Step 5. Configure the MVA VoiceXML application at the Cisco IOS gateway.

Step 1: Activate Cisco Unified Mobile Voice Access Service

Open the Cisco Unified Serviceability window. Choose Tools > Service Activation and select the Cisco Unified Mobile Voice Access Service check box, as shown in Figure 16-17. When the service has been activated, verify that it is started by following the Control Center—Feature Services link.

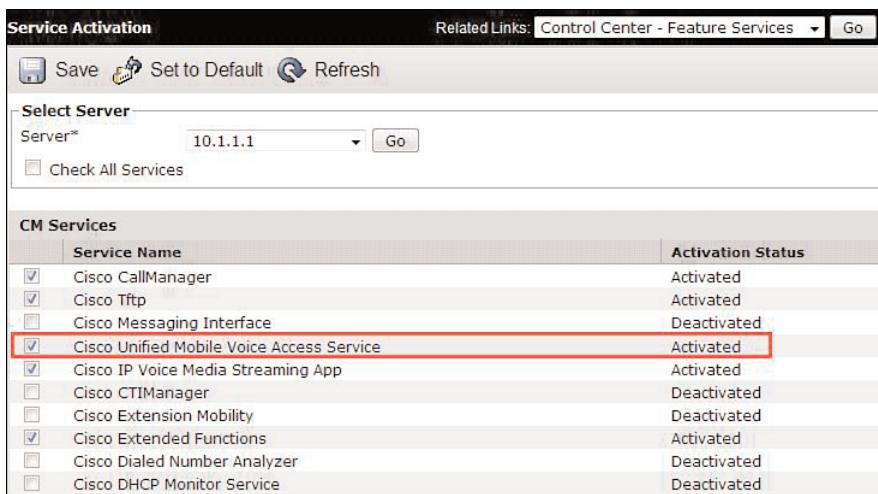


Figure 16-17 Service Activation

Step 2: Configure Service Parameters

To configure Cisco Unified Mobility service parameters, choose **System > Service Parameters** and choose a server. Then choose the Cisco CallManager service. The parameters that are shown in Figure 16-18 are cluster-wide parameters, which apply to all servers.

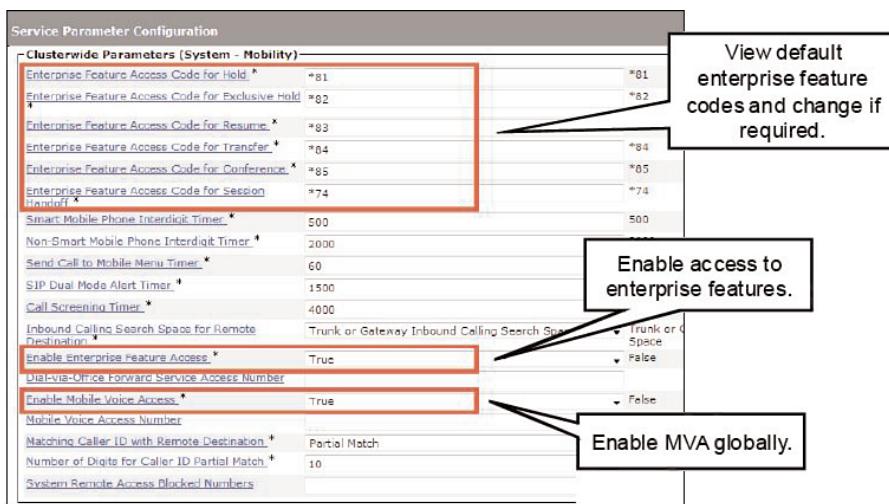


Figure 16-18 Service Parameter Configuration

You can enable access to enterprise features by setting the **Enable Enterprise Feature Access** parameter to True. In this case, the following features can be used from a remote destination phone, and the corresponding feature access codes can be modified from their default values:

- Hold: *81
- Exclusive Hold: *82
- Resume: *83
- Transfer: *84
- Conference: *85

These parameters must be unique and two or three digits or letters long. Allowed values are 0 through 9, A through D, and *.

To enable MVA, set the **Enable Mobile Voice Access** parameter to True.

Note By setting the Enable Mobile Voice Access parameter to True, you enable MVA in general only. To allow MVA to be used, you must enable it individually for each end user, in the End User Configuration window.

Step 3: Enable MVA per End User

In the End User Configuration window shown in Figure 16-19, select the Enable Mobile Voice Access check box to allow the end user to use MVA.

The screenshot shows the 'End User Configuration' window. The 'User Information' section contains fields for User ID (mpolo), Password, Confirm Password, PIN, Confirm PIN, Last name (Polo), Middle name, and First name (Marco). The 'Edit Credential' button is visible next to the password fields. The 'Mobility Information' section includes a 'Enable Mobility' checkbox (checked), a 'Primary User Device' dropdown set to 'None', an 'Enable Mobile Voice Access' checkbox (checked and highlighted with a red box), a 'Maximum Wait Time for Desk Pickup' input field (10000), a 'Remote Destination Limit' input field (4), and a 'Remote Destination Profiles' scrollable list. A 'View Details' link is at the bottom right.

Figure 16-19 End User Configuration

Step 4: Configure MVA Media Resource

The MVA media resource is automatically added when the Cisco Unified Mobile Voice Access Service is activated. The resource can be configured by choosing **Media Resources > Mobile Voice Access**, as shown in Figure 16-20.

The following configuration options exist:

- **Mobile Voice Access Directory Number:** Remote users who want to use the MVA feature must dial a certain PSTN number at an H.323 gateway that provides access by a call application to the MVA feature. The call application will route the incoming calls to the MVA media resource. The number that is used for this call leg (gateway to media resource) is the Mobile Voice Access Directory Number that is configured at the MVA media resource. The VXML call application resides in Cisco Unified Communications Manager and is accessed from the gateway by HTML. Therefore, the local VXML application code can refer to this configuration parameter, which is

stored in the Cisco Unified Communications Manager configuration database. However, the gateway must have a dial peer for this number, and that dial peer must point to the Cisco Unified Communications Manager system or systems on which the Cisco Unified Mobile Voice Access service has been activated.

- **Mobile Voice Access Partition:** Assign a partition to the Mobile Voice Access Directory Number. Make sure that the CSS of the gateway has access to this partition.
- **Selected Locales:** Choose at least one locale from the list of available locales. By default, only U.S. English is available.

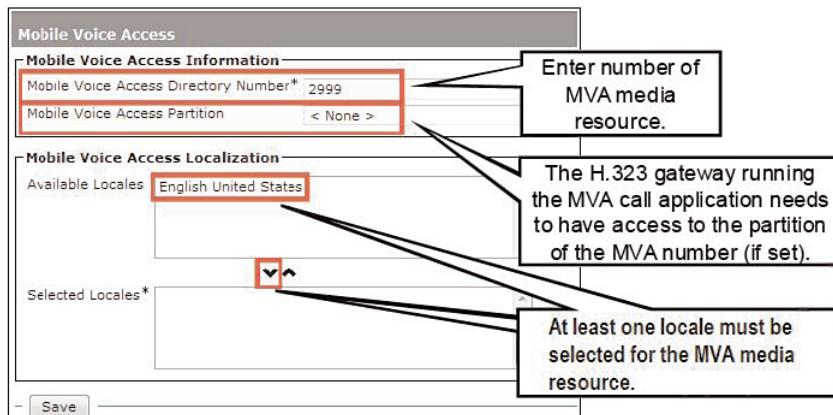


Figure 16-20 Mobile Voice Access

Step 5: Configure MVA on Cisco IOS Gateway

Example 16-1 shows the configuration of an H.323 gateway that provides access to the MVA feature.

Example 16-1 MVA Configuration on H.323 Gateway

```
Router# show run | begin application
application
service mva http://10.1.1.1:8080/ccmivr/pages/IVRMainpage.vxml
!
voice-port 0/0/0:23
translation-profile incoming pstn-in
!
voice translation-profile pstn-in
translate called 1
!
voice translation-rule 1
rule 1 /.*5552\(...$\|)/ /2\1/
!
```

```
dial-peer voice 29991 pots
service mva
incoming called-number 2999
direct-inward-dial
!
dial-peer voice 29992 voip
destination-pattern 2999
session target ipv4:10.1.1.1
dtmf-relay h245-alphanumeric
codec g711ulaw
no vad
!
dial-peer voice 1 pots
destination-pattern 9T
incoming called-number 2...
direct-inward-dial
port 0/0/0:23
!
dial-peer voice 2 voip
destination-pattern 2...
session target ipv4:10.1.1.1
incoming called-number 9T
codec g771ulaw
!
```

In the example, an incoming translation profile, which strips the called number down to four digits, is applied to the voice port. Therefore, all other dial peers that are applicable to calls from the PSTN refer to four-digit, called numbers only.

Thus, the following happens when a remote user dials the MVA number 1 511 555-2999.

- Step 1.** The call is routed to the voice port of the router, and the PSTN delivers a ten-digit national number that the translation profile then strips down to four digits.
- Step 2.** The called number 2999 matches the incoming plain old telephone system (POTS) dial peer 29991, which is configured by using the **call application mva service** command. The Mobile Voice Access service is configured with the URL of the MVA VoiceXML call application. This application is on the Cisco Unified Communications Manager server on which the Cisco Unified Mobile Voice Access service has been activated.

Note The MVA application URL can be found in the Cisco Unified Communications Manager Help pages.

When the call is passed on to the MVA media resource, the number that was configured at the MVA media resource during the previous step (in this case, also 2999) is used.

Note The number that is used to start the call application on incoming PSTN calls (1 511 555-2999) does not need to match (or partially match) the number that is used for the call leg from the H.323 gateway to the Cisco Unified Communications Manager MVA media resource. However, you should use the same number to avoid confusion.

The outgoing Voice over IP (VoIP) dial peer that is used for this call leg (dial peer 29992) must be configured for DTMF relay, and voice activity detection (VAD) must be disabled.

All other dial peers that are shown in the example apply to incoming PSTN calls to directory numbers other than 2999 (**dial-peer voice 1 pots** and **dial-peer voice 2 voip** command sections, which are located in the lower section of the example) and outgoing PSTN calls (all received VoIP calls use incoming **dial-peer 2** and outgoing **dial-peer 1**). These outgoing PSTN calls include normal calls that are placed from internal devices as well as calls that are initiated from remote phones that use MVA to place enterprise calls to the PSTN.

Chapter Summary

The following list summarizes the key points that were discussed in this chapter:

- Mobile Connect enables users to receive calls that are placed to their enterprise number at the enterprise phone and remote phones, such as cell phones. MVA extends the Mobile Connect functionality by allowing enterprise calls placed from a remote phone to connect first to the enterprise and then to break back out to the called number, using the enterprise number of the user as the calling number.
- MVA requires an H.323 gateway that provides an IVR application to MVA users.
- The Cisco Unified Mobile Voice Access service must be activated in the Cisco Unified Communications Manager cluster for MVA.
- If an MGCP gateway is used for PSTN access, an additional H.323 gateway is required for the MVA feature. Proper CSS and access list configuration is required for MVA and Mobile Connect.
- Implementation of Cisco Unified Mobility includes the configuration of access lists, remote destination profiles, and remote destinations.

References

For additional information, refer to these resources:

Cisco Systems, Inc. Cisco Unified Communications System Release 8.x SRND, at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8srnd.pdf.

CUCM Administration Guide, Release 8.0(2), at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmcfg/bccm.pdf.

Cisco Unified Communications Manager Features and Services Guide, at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmfeat/fsgd.pdf.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, “Answers to Review Questions.”

1. Cisco Unified Mobility consists of which two features? (Choose two.)
 - a. Single Number Connect
 - b. Cisco Mobile Connect
 - c. Mobile IVR
 - d. Cisco Unified Mobile Voice Access
 - e. Mobile Voice Connect
2. Which number is indicated as the calling number for a call that is placed from a remote destination to an internal directory number?
 - a. The Mobile Voice Access number
 - b. The number of the remote destination
 - c. The directory number of the office phone that the remote destination is associated with
 - d. The directory number of the called office phone, if associated with the calling remote destination
3. Which is not a requirement for Cisco Unified Mobility?
 - a. Remote destinations that have to be external numbers
 - b. H.323 or SIP gateway that provides the Mobile Voice Access IVR application
 - c. Out-of-band DTMF
 - d. Transcoder that runs at the gateway providing the Mobile Voice Access IVR application

4. What must be considered when implementing Cisco Unified Mobility in an environment with MGCP-controlled PSTN gateways?
 - a. MGCP dial peers must be configured on the PSTN gateway.
 - b. The MVA call application must be set to MGCP mode.
 - c. PSTN calls that arrive at the MGCP gateway must be sent to an H.323 gateway by Cisco Unified Communications Manager.
 - d. MGCP gateways cannot receive Cisco Unified Mobility calls.
5. Which configuration element is not used to implement Cisco Unified Mobility?
 - a. Softkey templates
 - b. User accounts
 - c. Access lists
 - d. Remote destination profiles
 - e. Remote destinations
 - f. Enterprise parameters
6. Which protocol is used for signaling with CUCM?
 - a. SIP
 - b. SCCP
 - c. H.323
 - d. MGCP
7. Mobile Voice Access exists in which two variants? (Choose two.)
 - a. Remote
 - b. Forward
 - c. Backward
 - d. Reverse
 - e. Transparent
8. What call admission control mechanism is used with video in centralized call-processing architectures?
 - a. Gatekeeper
 - b. Regions
 - c. Device pool
 - d. Locations

This page intentionally left blank

Appendix A

Answers to Review Questions

Chapter 1

- 1. C
- 2. D
- 3. C
- 4. B
- 5. C
- 6. A
- 7. C
- 8. D
- 9. D
- 10. C

Chapter 3

- 1. C
- 2. B and C
- 3. A
- 4. B
- 5. B
- 6. A
- 7. B
- 8. B
- 9. A
- 10. B

Chapter 2

- 1. C
- 2. D
- 3. A
- 4. B
- 5. B
- 6. C
- 7. C
- 8. A
- 9. C

Chapter 4

- 1. A
- 2. D
- 3. D
- 4. B
- 5. A
- 6. C
- 7. A
- 8. A
- 9. B

Chapter 5

- 1.** A, B, and C
- 2.** A
- 3.** B
- 4.** A and B
- 5.** B
- 6.** B
- 7.** A
- 8.** D
- 9.** A
- 10.** C

6. B

7. D

8. A

9. A and D

10. A

Chapter 8

- 1.** B
- 2.** C
- 3.** C
- 4.** A
- 5.** A

6. A and E

7. D

Chapter 6

- 1.** A
- 2.** D
- 3.** D
- 4.** C
- 5.** A
- 6.** A
- 7.** A
- 8.** C
- 9.** C
- 10.** B

Chapter 9

- 1.** A
- 2.** A
- 3.** B
- 4.** A
- 5.** B
- 6.** E
- 7.** C and D

Chapter 7

- 1.** A
- 2.** D
- 3.** D
- 4.** A
- 5.** A

Chapter 10

- 1.** A
- 2.** B
- 3.** A
- 4.** B and C

Chapter 11

1. A
2. B
3. C
4. A
5. B
6. D
7. C
8. C
9. B
10. C

7. B and D
8. A
9. B
10. C

Chapter 14

1. B
2. B and D
3. D
4. A and D

Chapter 12

1. A
2. C
3. A and B
4. B
5. D
6. C
7. D
8. A
9. D
10. C

Chapter 15

1. A
2. C
3. A
4. D
5. A
6. A, B, and C
7. C
8. A and C
9. A, B, and E
10. A

Chapter 13

1. A
2. C
3. A
4. B and D
5. D
6. B and D

Chapter 16

1. D and E
2. C
3. D
4. D
5. F
6. C
7. A and B
8. D

This page intentionally left blank

Index

Symbols & Numerics

! wildcard, 251-252
1:1 redundancy design model, 41
11-digit long-distance dialing, 243
802.1q trunk ports, 132-133
802.3af PoE, powering Cisco IP Phones, 126-129
8900 series Cisco IP Phones, 106-107

A

access analog trunk gateways, 186
access control
 Presence, 413-417
 UC databases, 15
access control, media resources, 379-383
access lists, configuring Cisco Unified Mobility, 437-439, 445-447
accessing Cisco IP Phone Services, 391

activating feature services, 59
adding
 IP phones to CUCM
 Auto-Register Phone Tool, 168
 auto-registration, 163-167
 BAT, 169-176
 manual method, 176-181
 subscribers to UC database, 15
analog station gateways, 186
annunciators, 353, 378-379
 CUCM support for, 356-357
application users (CUCM), 72
 managing, 76-82
 privileges, 73-75
applications layer (Cisco UC), 3-4
applying
 common phone profiles to Cisco IP Phones, 162
 line templates, 171-172
assigning
 privileges to CUCM user accounts, 73-75
 roles to CUCM user accounts, 78-82

audio conferencing, CUCM support for, 354-356

authentication

 LDAP, 94-97

 SIP IP phones, 118-119

Auto-Register Phone Tool, adding IP phones to CUCM, 168

auto-registration, adding IP phones to CUCM, 163-167

B

BAT (Bulk Administration Tool), 82-84

 adding IP phones to CUCM, 169-176

 BPS, 84

 templates, 83-84

 user accounts, managing, 84-85

best practices, LDAP synchronization, 91-92

boot sequence, Cisco IP Phones, 111-115

BPS (Bulk Provisioning Service), 84, 170

C

calculating CUCM license units, 22

call classification, 252-253

call control layer (Cisco UC), 2

call coverage, 328-330

 call forwarding, 328

 call pickup, 329-330

 shared lines, 329

call flow

 Cisco Unified Mobile Voice Access, 429-430

 Cisco Unified Mobility, 427-428

 Mobile Connect, 428-432

call forwarding, 328

 features, 343-347

call hunting, 330-334

 call flow, 335-337

 configuring, 337-343

 hunt lists, 333

 hunt pilots, 332-333

 line groups, 333-334

distribution algorithms, 334

call pickup, 329-330

call processing, 6

call routing, 230-244

 ! wildcard, 251-252

 call classification, 252-253

 destinations, 232-233

 digit analysis, 237-244

 digit forwarding, 244-248

 emergency call routing, 290-292

 intercluster call routing, 260

 route filters, 248-251

 route patterns, 233-237

 secondary dial tone, 253

 time-of-day call routing, 277-282

call survivability, 187-188

 H.323, 212

called party transformation patterns, 313

 configuring, 317

calling party transformations, configuring, 316

calling privileges, 265-267

call-processing redundancy, 39-43

CatOS, configuring single-VLAN access ports, 136-138

CDP (Cisco Discovery Protocol), 109

CER (Cisco Emergency Responder), 3

CIPC (Cisco IP Communicator), 103

- circular distribution algorithm**, 334
- Cisco Catalyst switches**, 124-138
 - Cisco IP Phones
 - 802.1q trunk port*, 132-133
 - multi-VLAN access port*, 131-132
 - providing power to*, 126-129
 - single-VLAN access port*, 130-131, 134-136
 - voice VLAN support*, 129-138
- Cisco gateways**, 186-187
- Cisco IOS SLB (Server Load Balancing)**, 393-394
- Cisco IOS Software**
 - H.323 functionality, configuring, 209-212
 - MGCP Configuration Server feature, 198-201
 - SIP, configuring, 216-217
- Cisco IP Phone Services**, 387-394
 - added service parameters, configuring, 397-402
 - configuring, 394-402
 - default services, 391-393
 - enterprise parameters, configuring, 395-397
 - provisioning, 389-390
 - redundancy, 393
 - service access, 391
 - subscriptions, 388, 402-404
- Cisco IP Phones**, 106-107. *See also* 8900 series Cisco IP Phones
 - adding to CUCM
 - Auto-Register Phone Tool*, 168
 - auto-registration*, 163-167
 - BAT*, 169-176
 - manual method*, 176-181
 - boot sequence, 111-115
- Cisco IP Phone Services**, subscribing to, 402-404
- Cisco Unified IP Phone 9900 Series**, 107-108
 - common phone profiles, applying, 162
 - CUCM groups, configuring, 149-151
 - date/time groups, configuring, 148
 - device defaults, configuring, 157
 - device pools, configuring, 144-145
 - entry-level, 105-106
 - high-end, 106
 - inserting in database, 175-176
 - locations, configuring, 153-155
 - midrange, 106
 - NTP, configuring, 146-148
 - phone button templates, configuring, 157-158
 - providing power to, 126-129
 - regions, configuring, 151-153
 - security profiles, configuring, 155
 - softkey templates, applying, 158-160
 - supplementary services, 187
 - voice VLAN support, 129-138
- Cisco Mobile Connect**, 425
- Cisco UC (Unified Communications)**, 2-6
 - Cisco Catalyst switches, 124-138
 - communications technologies, 5-6
 - databases
 - state configuration data*, 13
 - UFF*, 13-14
 - standard layers, 2-4
- Cisco Unified IP Phone 9900 Series**, 107-108
- Cisco Unified Mobile Voice Access**, 426
 - call flow, 429-430
 - configuring, 448-453

- Cisco Unified Mobility, 425-428**
 - access lists
 - configuring, 437-439, 445-447*
 - call flow, 427-428
 - configuration elements, 431-432
 - relationship between, 433-435*
 - end users, configuring, 440
 - features, 427
 - IP phones, configuring, 441
 - Mobile Connect, CSS, 436
 - number matching, 439
 - remote destination profile, 432-439
 - configuring, 442-445*
 - requirements, 430-431
 - service parameters, configuring, 445
 - softkey templates, configuring, 440
- clustering**
 - call-processing redundancy, 39-43
 - CUCM, 10-13
 - over IP WAN, 37-39
 - servers
 - feature services, 58-59*
 - network services, 58*
- CMCs (client matter codes), 282-285**
- common phone profiles, 162**
- communications technologies, Cisco UC, 5-6**
- comparing**
 - gateway signaling protocols, 190
 - SIP and SCCP phone boot sequence, 113-115
- compound DDI (digit discard instructions), 311**
- conference bridges, 352**
 - configuring, 362-370
 - hardware conference bridges, 359-362
- conferencing, rich-media conferencing, 6**
- configuration elements**
 - Cisco Unified Mobility, 431-432
 - relationship between, 433-435*
 - CUCM, relationship between, 162-163
- configuring**
 - call hunting, 337-343
 - Cisco Catalyst switches, single-VLAN access ports, 134-136
 - Cisco IP Phone Services, 394-402
 - added service parameters, 397-402*
 - enterprise parameters, 395-397*
 - Cisco IP Phones, phone button templates, 157-158
 - Cisco Unified Mobile Voice Access, 448-453
 - Cisco Unified Mobility
 - access lists, 437-439, 445-447*
 - end users, 440*
 - IP phones, 441*
 - remote destination profile, 442-445*
 - service parameters, 445*
 - softkey templates, 440*
 - CUCM, 48-57
 - DHCP, 51-53*
 - DNS, 54-57*
 - NTP, 48-51*
 - dial plans
 - CSSs, 274-277*
 - partitions, 274-277*
 - endpoints
 - CUCM groups, 149-151*
 - date/time groups, 148*

- device pool*, 144-145
- locations*, 153-155
- regions*, 151-153
- security profiles*, 155
- H.323, 206-212
- LDAP
 - authentication*, 97
 - synchronization*, 92-94
- media resources
 - conference bridges*, 362-370
 - MeetMe conferencing*, 370-371
- MGCP, fractional E1/T1,203-205
- MoH, 374-378
- path selection
 - local route groups*, 256-257
 - route groups*, 254-256
 - route lists*, 258-262
- Presence, 410-413
 - CUCM Presence policy configuration*, 417-420
- single-VLAN access ports, with CatOS, 136-138
- SIP, 212-218
 - on Cisco IOS Software*, 216-217
 - third-party SIP phones, 179-181
 - translation patterns, 304-307
- Control Center (feature services), 60
- core gateway requirements, 187-188
- CoS (class of service), 266, 285-290
- CSSs (calling search spaces), 267-273, 285-290
 - configuring, 274-277
 - in Mobile Connect, 436
- CSV files, adding IP Phones to CUCM, 172-173
- CUCM (Cisco Unified Communications Manager)
 - call hunting, 330-334
 - call flow*, 335-337
 - configuring*, 337-343
 - clustering, 10-13
 - call-processing redundancy*, 39-43
 - over IP WAN*, 37-39
 - configuration elements
 - naming*, 144
 - relationship between*, 162-163
 - configuring, 48-57
 - dial plans, path selection, 253-261
 - digit manipulation, 298-302
 - Digit Prefix feature, 309-311
 - DNS, configuring, 54-57
 - endpoints, 102-111
 - device defaults, configuring*, 157
 - device pools, configuring*, 144-145
 - groups, configuring*, 149-151
 - H.323 phones*, 115-116
 - locations, configuring*, 153-155
 - NTP, configuring*, 146-148
 - regions, configuring*, 151-153
 - registration, verifying*, 178
 - third-party IP phone support*, 116-119
 - validation routine, running on IP phones*, 174-175
 - functions, 6-7
 - global transformations, 312-320
 - hardware, 9-10
 - LDAP
 - authentication*, 94-97
 - directory integration*, 86-87
 - synchronization*, 87-94

- licensing, 16-23
 - additional licenses, obtaining, 19-21*
 - DLUs, 16-18*
 - file request process, 18*
 - license units, calculating, 22*
 - license units, reporting, 22-23*
 - media paths, 7-9
 - media resources, support for, 353-358
 - MGCP Configuration Server feature, 193-206
 - minimum hardware requirements, 11
 - multisite deployment with distributed call processing deployment model, 34-37
 - multisite WAN with centralized call processing deployment model, 31-34
 - NTP, configuring, 48-51
 - Off-Net calls, 225
 - On-Net calls, 225, 227-229
 - operating system, 12-13
 - PLAR, 292-294
 - Presence, 407-408
 - access control, 413-417*
 - configuring, 410-413*
 - support for, 408-410*
 - Presence groups, CUCM Presence policy configuration, 417-420
 - security profiles, configuring, 155
 - signaling, 7-9
 - Significant Digits feature, 312
 - single-site deployment model, 30-31
 - SIP, configuring, 212-218
 - software, 9-10
 - user accounts, 71-82
 - managing, 76-82*
 - privileges, assigning, 73-75*
 - roles, assigning, 78-82*
 - virtualization, 12
- CUP (Cisco Unified Presence), 4**
- CUPC (Cisco Unified Personal Communicator), 103**
- customer contact centers, 5**
-
- ## D
- databases (UC)**
 - access control, 15
 - IDS, 12
 - IP phones, inserting, 175-176
 - state configuration data, 13-274
 - UFF, 13-14
 - date/time groups, configuring on endpoints, 148**
 - DDI (digit discard instructions), 309**
 - default services (Cisco IP Phone Services), 391-393**
 - deleting security profiles, 155**
 - deployment models (CUCM)**
 - clustering over the IP WAN, 37-39
 - multisite deployment with distributed call processing deployment model, 34-37
 - multisite WAN with centralized call processing deployment model, 31-34
 - single-site deployment model, 30-31
 - destinations (call routing), 232-233**
 - device defaults, configuring on IP Phones, 157**
 - device detection, 802.3af PoE, 127-129**
 - device pools, configuring, 144-145**
 - DHCP (Dynamic Host Configuration Protocol), configuring on CUCM, 51-53**

- dial plans, 6, 222-224
 - call coverage, 328-330
 - call forwarding*, 328
 - call pickup*, 329-330
 - shared lines*, 329
 - call routing, 230-244
 - wildcard*, 251-252
 - call classification*, 252-253
 - destinations*, 232-233
 - digit analysis*, 237-244
 - digit forwarding*, 244-248
 - emergency call routing*, 290-292
 - route filters*, 248-251
 - route patterns*, 233-237
 - secondary dial tone*, 253
 - time-of-day call routing*, 277-282
 - calling privileges, 265-267
 - CoS, 285-290
 - CSSs, 267-273
 - configuring*, 274-277
 - E.164, 229
 - endpoint addressing, 224-225
 - On-Net, 227-229
 - partitions, 267-273
 - configuring*, 274-277
 - path selection, 253-261
 - route patterns
 - CMCs*, 282-285
 - FACs*, 282-285
 - dialing transformations, transformation masks, 307-309
 - digit analysis, 237-244
 - digit forwarding, 244-248
 - user input
 - SCCP phones*, 245
 - SIP phones*, 246-248
 - digit manipulation, 298-302
 - transformation masks, 307-309
 - translation patterns, 303-307
 - Digit Prefix feature (CUCM), 309-311
 - directory services, 6
 - distribution algorithms (line groups), 334
 - DLUs (device license units), 16-18
 - DNS, configuring on CUCM, 54-57
 - DRS (Disaster Recovery System), 7
 - DTMF (dual-tone multifrequency) relay, 187

E

 - E.164, 229
 - ELIN (emergency line identification number), 3
 - emergency dialing, 242
 - emergency call routing, 290-292
 - end users (CUCM), 72
 - managing, 76-82
 - privileges, 73-75
 - endpoint addressing, 224-225
 - endpoint identifiers, 191-192
 - endpoints, 102-111
 - adding to CUCM, manual method, 176-181
 - Cisco IP Phones, 105-111
 - 8900 series*, 106-107
 - boot sequence*, 111-115
 - Cisco Unified IP Phone 9900 Series*, 107-108
 - entry-level*, 105-106
 - H.323 phones*, 115-116
 - high-end*, 106
 - midrange*, 106
 - network features*, 109-111

CUCM groups, configuring, 149-151
date/time groups, configuring, 148
device defaults, configuring, 157
device pool, configuring, 144-145
features, 103-104
locations, configuring, 153-155
MGCP, configuring, 197-198
NTP, configuring, 146-148
regions, configuring, 151-153
registration, verifying, 178
SIP phones, SIP profiles, 161
third-party IP phones, 116-119
endpoints layer (Cisco UC), 4
enterprise parameters (CUCM servers), 60-63
entry-level Cisco IP Phones, 105-106
examples
 of intercluster call routing, 260
 of On-Net dial plans, 227-229
 of PLAR, 293
 of transformations, 320-323
 of translation patterns, 306
external phone number mask, 302-303

F

FACs (forced authorization codes), 282-285
feature services
 activating, 59
 Control Center, 60
 on CUCM servers, 58-59
features
 of call forwarding, 343-347
 of Cisco IP Phones, network features, 109-111
 of Cisco Unified Mobility, 427
 of endpoints, 103-104

file request process (CUCM licenses), 18
functions of CUCM, 6-7

G

gateways, 186-187
 core gateway requirements, 187-188
 H.323, 115
 call survivability, 212
 configuring, 206-212
 MGCP, 191-193
 configuring on CUCM, 193-206
 endpoint identifiers, 191-192
 fractional E1/T1, configuring, 203-205
 support in CUCM, 193
 signaling protocols, 188-190
 SIP, 212-218
global server settings
 enterprise parameters, 60-63
 service parameters, 64-65
global transformations, 312-320

H

H.323, 188
 call survivability, 212
 Cisco IOS functionality,
 configuring, 209-212
 gateways, 115
 IP phones, 115-116
hardware, CUCM, 9-10
 minimum requirements, 11
hardware conference bridges, 359-362
 configuring, 362-370
high-end Cisco IP Phones, 106
hunt lists, 333
hunt pilots, 332-333

I

IDS (IBM Informix Database Server), 12
 IEEE 802.3af PoE, powering Cisco IP Phones, 126-129
 infrastructure layer (Cisco UC), 2
 initial configuration of CUCM, 48-57
 DHCP, 51-53
 DNS, 54-57
 NTP, 50-51
 inline power delivery, Cisco IP Phones, 126-129
 inserting IP phones in database, 175-176
 intercluster call routing, 260
 interdigit timeout, 241
 international dialing, 243
 IP phones
 Cisco Unified Mobility, configuring, 441
 third-party IP phones, configuring, 179-181
 IP telephony, 5
 Cisco Catalyst switches, 124-138
 core gateway requirements, 187-188

J-K-L

LDAP (Lightweight Directory Access Protocol)
 authentication, 94-97
 configuring, 97
 synchronization, 87-94
 agreements, 88-89
 best practices, 91-92
 configuring, 92-94
 search base, 90-91
 voice integration, 86-87

licensing, CUCM, 16-23
 additional licenses, obtaining, 19-21
 calculating license units, 22
 DLUs, 16-18
 file request process, 18
 reporting license units, 22-23
 line groups, 333-334
 distribution algorithms, 334
 line templates, applying, 171-172
 local route groups, configuring, 256-257
 locations, configuring on endpoints, 153-155
 longest idle time distribution algorithm, 335

M

managing user accounts (CUCM), 76-82
 BAT, 82-85
 manually adding IP phones to CUCM, 176-181
 media paths, CUCM, 7-9
 media resources, 351-353
 access control, 379-383
 annunciators, 353, 378-379
 CUCM support for, 356-357
 audio conferencing, CUCM support for, 354-356
 conference bridges, 352
 configuring, 362-370
 hardware conference bridges, 359-362
 CUCM support for, 353-358
 MeetMe conferencing, configuring, 370-371

- MoH, 353, 371-378
 configuring, 374-378
 CUCM support for, 357-358
- transcoders, 353
- MeetMe conferencing, configuring, 370-371
- MGCP (Media Gateway Control Protocol), 188, 191-193
 configuring on CUCM, 193-206
 endpoint identifiers, 191-192
 fractional E1/T1, configuring, 203-205
 gateway registration, verifying, 201-203
 support in CUCM, 193
- midrange Cisco IP Phones, 106
- midspan power injection, powering Cisco IP Phones, 126
- minimum hardware requirements, CUCM, 11
- Mobile Connect
 call flow, 428-432
 CSSs, 436
- MoH (Music on Hold), 353, 371-378
 configuring, 374-378
 CUCM support for, 357-358
- MRGLs (media resource group lists), 380
- multisite WAN with centralized call processing deployment model (CUCM), 31-34
- multi-VLAN access ports, 131-132
-
- N**
-
- naming CUCM configuration elements, 144
- NENA (National Emergency Number Association), 3
- network appliances, 9
- network features of Cisco IP Phones, 109-111
- network services on CUCM servers, 58
- NTP (Network Time Protocol)
 configuring on CUCM, 48-51
 configuring on endpoints, 146-148
- number matching, Cisco Unified Mobility, 439
-
- O**
-
- obtaining additional CUCM licenses, 19-21
- Odom, Wendell, 125
- Off-Net calls, 225
- On-Net calls, 225, 227-229
- operating system, CUCM, 12-13
-
- P**
-
- partitions, 267-273
 configuring, 274-277
 Presence access control, 413-417
- path selection, 253-261
 local route groups, configuring, 256-257
 route groups, configuring, 254-256
 route lists, configuring, 258-262
- phone button templates, configuring on Cisco IP Phones, 157-158
- PLAR (private line automatic ringdown), 292-294
- PoE (Power over Ethernet), 110
 Cisco IP Phone bootup sequence, 111
 Cisco IP Phones, providing power to, 126-129

powering Cisco IP Phones, 126-129
Presence, 407-408
 access control, 413-417
 configuring, 410-413
 support in CUCM, 408-410
Presence groups, CUCM Presence policy configuration, 417-420
 privileges, assigning to users, 73-75
 provisioning Cisco IP Phone Services, 389-390

Q-R

Q.931 backhaul, 194

redundancy
 call-processing redundancy, 39-43
 Cisco IP Phone Services, 393
 CUCM supported features, 187
regions, configuring on endpoints, 151-153
relationship between Cisco Unified Mobility configuration elements, 433-435
relationship between configuration elements, 162-163
remote destination profile (Cisco Unified Mobility), 432-439
 configuring, 442-445
reporting CUCM license units, 22-23
requirements
 for Cisco Unified Mobility, 430-431
 core gateway requirements, 187-188
rich-media conferencing, 6
roles, assigning to CUCM
 user accounts, 78-82
route filters, 248-251
route groups, configuring, 254-256

route lists, configuring, 258-262
route patterns, 233-237
 CMC, 282-285
 FACs, 282-285
 and translation patterns, 304

S

SCCP (Skinny Client Control Protocol), 103, 189
 digit forwarding, 245
 IP Phone boot sequence, 113-115
search base (LDAP), 90-91
secondary dial tone, 253
security
 authentication
LDAP, 94-97
SIP IP phones, 118-119
 authorization, FACs, 282-285
 UC databases access control, 15
security profiles, configuring on endpoints, 155
servers
 feature services, 58-59
Control Center, 60
 global settings, enterprise parameters, 60-63
 network services, 58
service parameters (CUCM servers), 64-65
seven-digit dialing, 243
shared lines, 329
signaling, 6-9
signaling protocols, 188-190
 H.323
call survivability, 212
configuring, 206-212

- MGCP, 191-193
 - configuring on CUCM*, 193-206
 - endpoint identifiers*, 191-192
 - fractional E1/T1, configuring*, 203-205
 - gateway registration, verifying*, 201-203
 - support in CUCM*, 193
 - SIP, 212-218
 - Significant Digits feature (CUCM), 312
 - single-site CoS deployments, 285
 - single-site deployment model (CUCM), 30-31
 - single-VLAN access ports, 130-131
 - configuring, 134-136
 - SIP (Session Initiation Protocol), 189, 212-218
 - digit forwarding, 246-248
 - IP Phone boot sequence, 113-115
 - SIP profiles, 161
 - third-party IP phone support in CUCM, 116-119
 - authentication*, 118-119
 - third-party SIP phones, configuring, 179-181
 - softkey templates
 - applying to Cisco IP Phones, 158-160
 - Cisco Unified Mobility, configuring, 440
 - software, CUCM, 9-10
 - standard layers (Cisco UC), 2-4
 - state configuration data, 13-14
 - subscribers, adding to UC database, 15
 - subscriptions, Cisco IP Phone Services, 388, 402-404
 - supplementary services, 187
 - synchronization (LDAP), 87-94
 - agreements, 88-89
 - best practices, 91-92
 - configuring, 92-94
 - search base, 90-91
-
- ## T
- TAPS, phone insert process, 169
 - TEHO (tail-end hop off), 266
 - templates
 - BAT, 83-84
 - line templates, applying, 171-172
 - phone button templates, configuring, 157-158
 - softkey templates, applying to Cisco IP Phones, 158-160
 - ten-digit dialing, 243
 - third-party IP phones, 116-119
 - SIP phones, configuring, 179-181
 - three-digit service codes, 243
 - time-of-day call routing, 277-282
 - time-of-day routing, 266
 - top-down distribution algorithm, 334
 - transcoders, 353
 - transformation masks, 307-309
 - transformation patterns, 314
 - examples, 320-323
 - global transformations, 312-320
 - translation patterns, 303-307
 - configuring, 304-307
 - and route patterns, 304
 - Triple Combo GUI tool, 240
 - trunks
 - access analog trunk gateways, 186
 - SIP, configuring, 213-215

U

UFF (user-facing features), 10, 13-14

user accounts (CUCM), 71-82

managing, 76-82

with BAT, 82-85

privileges, assigning, 73-75

roles, assigning, 78-82

user input (digit forwarding)

SCCP phones, 245

SIP phones, 246-248

V-W-X-Y-Z

validation routine, running on IP phones in CUCM, 174-175

vanity numbers, 290-292

verifying

endpoint registration, 178

MGCP gateway registration, 201-203

video telephony, 5

virtualization, CUCM, 12

VLANs

single-VLAN access ports

configuring on Cisco Catalyst switches, 134-136

configuring with CatOS, 136-138

voice integration, LDAP, 86-87

voice VLAN support on Cisco IP Phones, 129-138