

Implementing Cisco Unified Communications Manager

Part 2 (CIPT2)

Foundation Learning Guide



Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide

Chris Olsen

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) Foundation Learning Guide CCNP Voice CIPT2 642-457

Chris Olsen

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 Number is on file.

ISBN-13: 978-1-58714-253-6

ISBN-10: 1-58714-253-8

Warning and Disclaimer

This book is designed to provide information about Cisco Unified Communications administration and to provide test preparation for the CIPT Part 2 version 8 exam (CCNP Voice CIPT2 642-457), 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 author, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

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

Trademark Acknowledgments

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

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 of the U.S., 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 Dusthimer

Manager Global Certification: Erik Ullanderson

Executive Editor: Brett Bartow

Senior Development Editor: Christopher Cleveland

Managing Editor: Sandra Schroeder

Copy Editor: Sheri Cain

Project Editor: Mandie Frank

Technical Editors: James McInvaille, Joe Parlas

Editorial Assistant: Vanessa Evans

Proofreader: Apostrophe Editing Services

Cover 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, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networks, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

About the Author

Chris Olsen, CCSI, CCVP, and CCNP, along with numerous other Cisco voice and data center specializations, Microsoft, VMware, and Novell certifications, has been an independent IT and telephony consultant, author, and technical editor for more than 15 years. He has been a technical trainer for more than 19 years and has taught more than 60 different courses for Cisco, Microsoft, VMware, and Novell. For the last 7 years, he has specialized in Cisco, and recently, Microsoft Unified Communications along with VMware virtualization and Cisco data-center technologies. He has done a wide array of IT and telephony consulting for many different companies. Chris and his wife, Antonia, live in Chicago and Mapleton, Illinois. He can be reached at chrisolsen@earthlink.net.

About the Technical Reviewers

James McInvaille, CCSI No. 21904, is a certified Cisco Systems instructor for Cisco Learning Partner Global Knowledge Network, Inc., and a contract consultant. As an instructor, he is responsible for training students worldwide and consulting in the deployment of routing, switching, and IP telephony solutions. Previously, James was a solutions engineer for EDS for the Bank of America voice-transformation project. Prior to EDS, James was a senior network engineer for iPath Technologies, based in Reston, Virginia. In this role, he provided technical training and professional services to service providers and enterprise users of Juniper Networks routing and security product line. During this time, James earned his Juniper Networks Certified Internet Professional (JNCIP #297) certification. Prior to iPath, James was the lead technical consultant (LTC) for the Carolina's region of Dimension Data, NA. As an LTC, his responsibilities included the support and guidance of five engineers and technicians involved in the consultation, implementation, delivery, and training of VoIP and IP telephony solutions, and high-level routing and switching designs. In his spare time, James and his beautiful wife, Lupe, enjoy riding their Harley-Davidsons near their home in Kershaw, South Carolina.

Joe Parlas, CCSI No. 21904, has been an instructor for more than 10 years, specifically concentrating on Cisco voice technologies. He consults for numerous Fortune 500 and Fortune 1000 companies, such as SweetHeart Cup, Inc., Black and Decker, and McCormick Spice Corporation. He has acted as a senior consultant with Symphony Health Services, Inc., in various capacities. Joseph's consulting practice is growing with the main emphasis of bridging voice technologies between Cisco and Microsoft Lync Server. Joseph holds CCNP, CCVP, CCNA, A+, and MSCE – Messaging 2003 industry certifications, and he primarily instructs for Global Knowledge Network, Inc. Joseph has lived in the San Diego area with his wife, Parvin Shaybany, for more than 4 years after relocating from the Washington D.C. area.

Dedication

This book is dedicated to my wonderful wife, Antonia, whose constant love and tireless commitment to making my life better gave me the time to write this book. I am forever grateful.

Acknowledgments

I want to thank the entire team at Global Knowledge for its excellent support and creation of a high-quality learning environment. Thanks also to the staff at Cisco Press for its excellent support and advice.

Contents at a Glance

Introduction	xxi	
Chapter 1	Identifying Issues in a Multisite Deployment	1
Chapter 2	Identifying Multisite Deployment Solutions	23
Chapter 3	Implementing Multisite Connections	57
Chapter 4	Implementing a Dial Plan for International Multisite Deployments	83
Chapter 5	Examining Remote-Site Redundancy Options	123
Chapter 6	Implementing Cisco Unified SRST and MGCP Fallback	151
Chapter 7	Implementing Cisco Unified Communications Manager Express (CUCME) in SRST Mode	181
Chapter 8	Implementing Bandwidth Management	201
Chapter 9	Implementing Call Admission Control	233
Chapter 10	Implementing Device Mobility	289
Chapter 11	Implementing Extension Mobility	317
Chapter 12	Implementing Service Advertisement Framework (SAF) and Call Control Discovery (CCD)	343
Answers Appendix	395	
Index	399	

Contents

Introduction	xxi
Chapter 1 Identifying Issues in a Multisite Deployment	1
Multisite Deployment Challenge Overview	1
Quality Challenges	2
Bandwidth Challenges	3
Availability Challenges	6
Dial Plan Challenges	7
<i>Overlapping and Nonconsecutive Numbers</i>	9
<i>Fixed Versus Variable-Length Numbering Plans</i>	10
<i>Variable-Length Numbering, E.164 Addressing, and DID</i>	10
<i>Detection of End of Dialing in Variable-Length Numbering Plans</i>	12
<i>Optimized Call Routing and PSTN Backup</i>	14
<i>Various PSTN Requirements</i>	15
<i>Issues Caused by Different PSTN Dialing</i>	16
Dial Plan Scalability Issues	17
NAT and Security Issues	17
Summary	19
References	19
Review Questions	19
Chapter 2 Identifying Multisite Deployment Solutions	23
Multisite Deployment Solution Overview	23
Quality of Service	24
<i>QoS Advantages</i>	25
Solutions to Bandwidth Limitations	26
<i>Low-Bandwidth Codecs and RTP-Header Compression</i>	27
<i>Codec Configuration in CUCM</i>	28
<i>Disabled Annunciator</i>	29
<i>Local Versus Remote Conference Bridges</i>	30
<i>Transcoders</i>	30
<i>Mixed Conference Bridge</i>	32
<i>Multicast MOH from the Branch Router Flash</i>	33
<i>Preventing Too Many Calls by CAC</i>	37
Availability	38
<i>PSTN Backup</i>	39

<i>MGCP Fallback</i>	39
<i>Fallback for IP Phones</i>	41
<i>Using CFUR to Reach Remote Site Cisco IP Phones During WAN Failure</i>	42
<i>Using CFUR to Reach Users of Unregistered Software IP Phones on Their Cell Phones</i>	43
<i>AAR and CFNB</i>	44
Mobility Solutions	44
Dial Plan Solutions	45
<i>Dial Plan Components in Multisite Deployments</i>	45
Globalized Call-Routing Overview	46
<i>Globalized Call Routing: Three Phases</i>	48
<i>Globalized Call Routing Advantages</i>	50
NAT and Security Solutions	51
<i>CUBE in Flow-Through Mode</i>	51
Summary	52
References	53
Review Questions	53

Chapter 3 Implementing Multisite Connections 57

Examining Multisite Connection Options	57
CUCM Connection Options Overview	58
Cisco IOS Gateway Protocol Functions Review	59
Cisco IOS Gateway Protocol Comparison Review	60
SIP Trunk Characteristics	60
H.323 Trunk Overview	61
MGCP Gateway Implementation Review	64
Cisco IOS Gateway MGCP Configuration Methods Review	65
Configuring Cisco IOS Gateway for MGCP: Example	66
H.323 Gateway Implementation	68
Cisco IOS H.323 Gateway Configuration	69
CUCM H.323 Gateway Configuration	71
Trunk Implementation Overview	71
Gatekeeper-Controlled ICT and H.225 Trunk Configuration	72
Trunk Types Used by Special Applications	73
Implementing SIP Trunks	74
Implementing Intercluster and H.225 Trunks	75

CUCM Gatekeeper-Controlled ICT and H.225 Trunk Configuration	77
Summary	79
References	79
Review Questions	80
Chapter 4 Implementing a Dial Plan for International Multisite Deployments	83
Multisite Dial Plan Overview	84
Dial Plan Requirements for Multisite Deployments with Distributed Call Processing	84
Dial Plan Scalability Solutions	85
Implementing Site Codes for On-Net Calls	86
Digit-Manipulation Requirements When Using Access and Site Codes	87
Access and Site Code Requirements for Centralized Call-Processing Deployments	88
Implementing PSTN Access in Cisco IOS Gateways	90
Transformation of Incoming Calls Using ISDN TON	90
Implementing Selective PSTN Breakout	93
Configuring IP Phones to Use Local PSTN Gateway	93
Implementing PSTN Backup for On-Net Intersite Calls	95
Digit-Manipulation Requirements for PSTN Backup of On-Net Intersite Calls	95
Implementing TEHO	97
TEHO Example Without Local Route Groups	98
TEHO Example with Local Route Groups	100
Implementing Globalized Call Routing	102
Globalized Call Routing: Number Formats	103
Normalization of Localized Call Ingress on Gateways	106
Normalization of Localized Call Ingress from Phones	107
Localized Call Egress at Gateways	108
Localized Call Egress at Phones	110
Globalized Call-Routing Example: Emergency Dialing	112
Considering Globalized Call-Routing Interdependencies	115
Globalized Call Routing—TEHO Advantages	116
Globalized Call Routing—TEHO Example	116
Summary	118
References	118
Review Questions	119

Chapter 5 Examining Remote-Site Redundancy Options 123

Remote-Site Redundancy Overview	123
Remote-Site Redundancy Technologies	124
MGCP Fallback Usage	126
Basic Cisco Unified SRST Usage	127
Cisco Unified SIP SRST Usage	127
CUCME in SRST Mode Usage	128
Cisco Unified SRST Operation	128
SRST Function of Switchover Signaling	129
SRST Function of the Call Flow After Switchover	130
SRST Function of Switchback	131
SRST Timing	132
MGCP Fallback Operation	133
MGCP Gateway Fallback During Switchover	133
MGCP Gateway Fallback During Switchback	134
MGCP Gateway Fallback Process	136
Cisco Unified SRST Versions and Feature Support	137
SRST 4.0 Platform Density	138
Plus (+) Prefix and E.164 Support in Cisco Unified SRST	138
Support for Multiple MOH Sources	139
Dial Plan Requirements for MGCP Fallback and SRST Scenarios	139
<i>Ensuring Connectivity for Remote Sites</i>	140
<i>Ensuring Connectivity from the Main Site Using Call Forward Unregistered</i>	141
<i>CFUR Considerations</i>	142
CFUR Interaction with Globalized Call Routing	143
CFUR Example Without Globalized Call Routing	143
CFUR Example with Globalized Call Routing	145
<i>Keeping Calling Privileges Active in SRST Mode</i>	145
<i>SRST Dial Plan Example</i>	146
Summary	147
References	147
Review Questions	147

Chapter 6 Implementing Cisco Unified SRST and MGCP Fallback 151

MGCP Fallback and SRST Configuration	151
Configuration Requirements for MGCP Fallback and Cisco Unified SRST	152

Cisco Unified SRST Configuration in CUCM	152
SRST Reference Definition	153
CUCM Device Pool	153
SRST Configuration on the Cisco IOS Gateway	154
SRST Activation Commands	154
SRST Phone Definition Commands	155
SRST Performance Commands	156
Cisco Unified SRST Configuration Example	157
MGCP-Gateway-Fallback Configuration on the Cisco IOS Gateway	158
MGCP Fallback Activation Commands	158
MGCP Fallback Configuration Example	159
Dial Plan Configuration for SRST Support in CUCM	160
SRST Dial Plan of CFUR and CSS	161
SRST Dial Plan: Max Forward UnRegistered Hops to DN	162
MGCP Fallback and SRST Dial Plan Configuration in the Cisco IOS Gateway	163
SRST Dial Plan Components for Normal Mode Analogy	163
Cisco Unified SRST Dial Plan Dial Peer Commands	164
SRST Dial Plan Commands: Open Numbering Plans	167
SRST Dial Plan Voice Translation-Profile Commands for Digit Manipulation	170
SRST Dial Plan Voice Translation-Rule Commands for Number Modification	171
SRST Dial Plan Profile Activation Commands for Number Modification	172
SRST Dial Plan Class of Restriction Commands	173
SRST Dial Plan Example	173
Summary	178
References	178
Review Questions	179
Chapter 7 Implementing Cisco Unified Communications Manager Express (CUCME) in SRST Mode	181
CUCME Overview	181
CUCME in SRST Mode	183
Standalone CUCME Versus CUCM and CUCME in SRST Mode	183
CUCME Features	185
CUCME Features	186

Other CUCME Features	186
General Configuration of CUCME	187
CUCME Basic Configuration	188
CUCME Configuration Providing Phone Loads	189
CUCME Configuration for Music On Hold	190
Additional MOH Sources	191
Configuring CUCME in SRST Mode	192
Phone-Provisioning Options	193
Advantages of CUCME SRST	194
Phone Registration Process	195
Configuring CUCME for SRST	195
CUCME for SRST Mode Configuration	197
Summary	198
Reference	198
Review Questions	198
Chapter 8 Implementing Bandwidth Management	201
Bandwidth Management Overview	201
CUCM Codec Configuration	202
Review of CUCM Codecs	203
Local Conference Bridge Implementation	205
Transcoder Implementation	208
Implementing a Transcoder at the Main Site	209
Configuration Procedure for Implementing Transcoders	211
<i>Step 1: Add a Transcoder Resource in CUCM</i>	211
<i>Step 2: Configure the Transcoder Resource in Cisco IOS Software</i>	212
Multicast MOH from Remote Site Router Flash Implementation	215
Multicast MOH from Remote Site Router Flash Region Considerations	216
Multicast MOH from Remote Site Router Flash Address and Port Considerations	216
Multicast MOH: Address and Port Increment Example	217
Implementing Multicast MOH from Remote Site Router Flash	219
Configuration Procedure for Implementing Multicast MOH from the Remote Site Router Flash	221
<i>Step 1: Enable Multicast Routing on Cisco IOS Routers</i>	222
<i>Step 2a: Configure MOH Audio Sources for Multicast MOH</i>	223
<i>Step 2b: Configure Multicast MOH in CUCM</i>	223

<i>Step 2c: Enabling Multicast MOH at the Media Resource Groups</i>	225
<i>Step 3: Enable Multicast MOH from Branch Router Flash at the Branch Router</i>	226
<i>Step 4a: Configure the Maximum Hops to Be Used for MOH RTP Packets</i>	227
<i>Step 4b: Use an IP ACL at the IP WAN Router Interface</i>	227
<i>Step 4c: Disable Multicast Routing on the IP WAN Router Interface</i>	228
Summary	229
Reference	229
Review Questions	230
Chapter 9 Implementing Call Admission Control 233	
CAC Overview	234
CAC in CUCM	234
Standard Locations	235
Locations: Hub-and-Spoke Topology	236
Locations: Full-Mesh Topology	237
Configuration Procedure for Implementing Locations-Based CAC	238
Locations Configuration Example of a Hub-and-Spoke Topology	238
<i>Step 1: Configure Locations</i>	239
<i>Step 2: Assign Locations to Devices</i>	240
RSVP-Enabled Locations	241
Three Call Legs with RSVP-Enabled Locations	241
Characteristics of Phone-to-RSVP Agent Call Legs	242
Characteristics of RSVP Agent-to-RSVP Agent Call Legs	243
RSVP Basic Operation	243
RSVP-Enabled Location Configuration	245
Configuration Procedure for Implementing RSVP-Enabled Locations-Based CAC	246
<i>Step 1: Configure RSVP Service Parameters</i>	247
<i>Step 2: Configure RSVP Agents in Cisco IOS Software</i>	250
<i>Step 3: Add RSVP Agents to CUCM</i>	252
<i>Step 4: Enable RSVP Between Location Pairs</i>	253
Automated Alternate Routing	255
AAR Characteristics	256
<i>AAR Example Without Local Route Groups and Globalized Numbers</i>	257

<i>AAR Example with Local Route Groups and Globalized Numbers</i>	258
AAR Considerations	259
AAR Configuration Procedure	260
Step 1: Configure AAR Service Parameters	261
Step 2: Configure Partitions and CSSs	261
Step 3: Configure AAR Groups	261
Step 4: Configure Phones for AAR	262
SIP Preconditions	264
CAC Without SIP Preconditions	265
CAC with SIP Preconditions	265
SIP Preconditions Operation	266
SIP Preconditions Call Flow Summary	267
Fallback from End-to-End RSVP to Local RSVP	269
SIP Preconditions Configuration Procedure	270
<i>Step 2a: Configure SIP Profile</i>	271
<i>Step 2b: Apply SIP Profile to Trunk</i>	272
H.323 Gatekeeper CAC	273
H.323 Gatekeeper Used for Call Routing for Address Resolution Only	274
Using an H.323 Gatekeeper for CAC	277
H.323 Gatekeeper Also Used for CAC	279
Provide PSTN Backup for Calls Rejected by CAC	281
Configuration Procedure for Implementing H.323 Gatekeeper-Controlled Trunks with CAC	282
Summary	283
References	283
Review Questions	284
Chapter 10 Implementing Device Mobility	289
Issues with Devices Roaming Between Sites	289
Issues with Roaming Devices	290
Device Mobility Solves Issues of Roaming Devices	291
Device Mobility Overview	292
Dynamic Device Mobility Phone Configuration Parameters	292
Device Mobility Dynamic Configuration by Location-Dependent Device Pools	294
Device Mobility Configuration Elements	295
Relationship Between Device Mobility Configuration Elements	295

Device Mobility Operation	297
Device Mobility Operation Flowchart	298
Device Mobility Considerations	300
Review of Line and Device CSSs	301
Device Mobility and CSSs	302
Examples of Different Call-Routing Paths Based on Device Mobility Groups and Tail-End Hop-Off	302
Device Mobility Interaction with Globalized Call Routing	304
Advantages of Using Local Route Groups and Globalized Call Routing	305
Example of No Globalized Call Routing with a Different Device Mobility Group	306
Example of No Globalized Call Routing with the Same Device Mobility Group	307
Globalized Call Routing Example	308
Device Mobility Configuration	309
Steps 1 and 2: Configure Physical Locations and Device Mobility Groups	309
Step 3: Configure Device Pools	310
Step 4: Configure Device Mobility Infos	311
Step 5a: Set the Device Mobility Mode CCM Service Parameter	312
Step 5b: Set the Device Mobility Mode for Individual Phones	313
Summary	314
References	314
Review Questions	315
Chapter 11 Implementing Extension Mobility	317
Issues with Users Roaming Between Sites	317
Issues with Roaming Users	318
Extension Mobility Solves Issues of Roaming Users	319
CUCM Extension Mobility Overview	319
Extension Mobility: Dynamic Phone Configuration Parameters	320
Extension Mobility with Dynamic Phone Configuration by Device Profiles	320
CUCM Extension Mobility Configuration Elements	321
Relationship Between Extension Mobility Configuration Elements	323
CUCM Extension Mobility Operation	323
Issues in Environments with Different Phone Models	326

Default Device Profile and Feature Safe	326
How Cisco Extension Mobility Handles Phone Model Differences	327
Cisco Extension Mobility and CSSs	328
Alternatives for Mismatching Phone Models and CSS Implementations	329
CUCM Extension Mobility Configuration	329
Step 1: Activate the Cisco Extension Mobility Feature Service	330
Step 2: Set Cisco Extension Mobility Service Parameters	330
Step 3: Add the Cisco Extension Mobility Phone Service	331
Step 4: Create Default Device Profiles	332
Step 5a: Create Device Profiles	333
Step 5b: Subscribe the Device Profile to the Extension Mobility Phone Service	334
Step 6: Associate Users with Device Profiles	335
Step 7a: Configure Phones for Cisco Extension Mobility	337
Step 7b: Subscribe the Phone to the Extension Mobility Phone Service	337
Summary	338
References	339
Review Questions	339

Chapter 12 Implementing Service Advertisement Framework (SAF) and Call Control Discovery (CCD) 343

SAF and CCD Overview	344
Dial Plan Scalability Issues in Large Networks	344
Scalable Dial Plan Solution for Large Networks	345
CCD Overview	345
SAF Characteristics	346
SAF Client Types	348
SAF Message Components	349
SAF Routing Characteristics	349
SAF Neighbor Relationships	350
SAF Client and SAF Forwarder Functions	351
CCD Characteristics	351
CCD Services in CUCM	353
Processing Received Routes in CUCM	354
CCD Operation	355
CCD Propagation of HQ Routes	356

CCD Propagation of BR Routes	356
CCD Call from HQ to BR	357
CCD with a Link Failure at BR	359
CCD for Call from HQ to BR During Link Failure	360
SAF and CCD Implementation	361
External SAF Client Configuration Elements	362
Internal SAF Client Configuration Elements	364
SAF Forwarder Configuration Procedure	365
External SAF Client Configuration Procedure	367
<i>Step 1: Configure SAF Security Profile</i>	367
<i>Step 2: Configure SAF Forwarder</i>	368
<i>Step 3: Configure SAF-Enabled SIP Trunk</i>	369
<i>Step 4: Configure Hosted DN Group</i>	370
<i>Step 5: Configure Hosted DN Pattern</i>	370
<i>Step 6: Configure CCD Advertising Service</i>	371
<i>Step 7: Configure CCD Requesting Service and Partition</i>	372
<i>Step 8: Configure CCD Blocked Learned Patterns</i>	373
<i>Step 9: Configure CCD Feature Parameters</i>	374
Internal SAF Client Configuration Procedure	376
<i>Step 1: Configure Trunk Profile</i>	376
<i>Step 2: Configure Directory-Number Blocks</i>	377
<i>Step 3: Configure Call-Control Profile</i>	378
<i>Step 4: Configure Advertising Service</i>	378
<i>Step 5: Configure Requesting Service</i>	379
<i>Step 6: Configure VoIP Dial Peer</i>	380
CCD Considerations	381
<i>Monitoring Learned Routes from CUCM in RTMT</i>	382
<i>Monitoring Learned Routes in CUCME</i>	382
CCD PSTN Backup CSS	383
SRST Considerations	384
<i>CCD and Static Routing Integration Considerations</i>	385
<i>Cisco IOS SAF Client Considerations When Using Globalized Call Routing</i>	386
<i>Solution for PSTN Backup Advertised in E.164 Format Without Leading +</i>	387
TEHO Considerations	388
Trunk Considerations When Using Globalized Call Routing	388

<i>CUCM Clusters and CCD Configuration Modes</i>	389
<i>Other SAF and CCD Considerations</i>	390
Summary	390
References	391
Review Questions	391

Answers Appendix 395

Index 399

Icons Used in This Book



Cisco Unified Communications Manager



Unified CM Express



Cisco Unified Border Element



Cisco Unity Server



Router



Voice-Enabled Router



SRST-Enabled Router



Gatekeeper



Voice Gateway



Switch



Conference Bridge



Transcoder



Server



Security Management



Certificate Authority



IP Communicator



Web Browser



Web Server



PC



Laptop



IP Phone



Phone



Cell Phone



Relational Database



Ethernet Connection



Serial Line Connection



Network Cloud

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 (UC), deploying the Cisco Unified Communications Manager (CUCM) product. Another goal of this book is to help you with the Cisco IP Telephony (CIPT) Part 2 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's 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 it helps you truly learn and understand the topics. The Cisco IP Telephony Part 2 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 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 via test questions at the end of each chapter

Who Should Read This Book?

This book is designed to be both a general CUCM 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 2.

Why should you want to pass the CCNP Voice Cisco IP Telephony exam? The second 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 the 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 CUCM on the job. Regardless of the strategy you use or your background, this book helps 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, “Identifying Issues in a Multisite Deployment,”** sets the stage for this book by identifying all the relevant challenges in multisite deployments requiring UC solutions.
- **Chapter 2, “Identifying Multisite Deployment Solutions,”** overviews the solutions to the challenges identified in Chapter 1 that are described in this book.
- **Chapter 3, “Implementing Multisite Connections,”** provides the steps to configure Media Gateway Control Protocol (MGCP) and H.323 gateways, and Session Initiation Protocol (SIP) and intercluster trunks to function with CUCM.
- **Chapter 4, “Implementing a Dial Plan for International Multisite Deployments,”** provides a dial plan solution and addresses toll bypass, tail-end hop-off (TEHO), and digit-manipulation techniques in a multisite CUCM deployment.
- **Chapter 5, “Examining Remote-Site Redundancy Options,”** provides the foundation for maintaining redundancy at a remote site in the event of an IP WAN failure by exploring the options for implementing Survivable Remote Site Telephony (SRST) and MGCP fallback.
- **Chapter 6, “Implementing Cisco Unified SRST and MGCP Fallback,”** presents the configurations to implement SRST and MGCP fallback, along with implementing a gateway dial plan and voice features in the SRST router.
- **Chapter 7, “Implementing Cisco Unified Communications Manager Express (CUCME) in SRST Mode,”** discusses the configuration approaches of Cisco Unified Communications Manager Express (CUCME) to support SRST fallback.
- **Chapter 8, “Implementing Bandwidth Management,”** shows you how to implement bandwidth management with call admission control (CAC) to ensure a high level of audio quality for voice calls over IP WAN links by preventing oversubscription.

- **Chapter 9, “Implementing Call Admission Control,”** describes the methods of implementing CAC in gatekeepers and CUCM and explores the benefits of Resource Reservation Protocol (RSVP) and Automated Alternate Routing (AAR) in CUCM.
- **Chapter 10, “Implementing Device Mobility,”** describes the challenges for users traveling between sites with their phones and provides the solution of mobility.
- **Chapter 11, “Implementing Extension Mobility,”** describes the concept of Extension Mobility and gives the procedure for implementing Extension Mobility for users traveling to different sites and using a phone at the different site as their own.
- **Chapter 12, “Implementing Service Advertisement Framework (SAF) and Call Control Discovery (CCD),”** describes Service Advertising Framework (SAF) and Call Control Discovery (CCD) and how to implement dynamic call-routing updates between many Cisco Unified Communications elements.
- **Answer Appendix,** allows you to check the validity of your answers at the end of each chapter as you review the questions.

This page intentionally left blank

Chapter 1

Identifying Issues in a Multisite Deployment

Upon completing this chapter, you will be able to explain issues pertaining to multisite deployment and relate those issues to multisite connection options. You will be able to meet these objectives:

- Describe issues pertaining to multisite deployments
- Describe quality issues in multisite deployments
- Describe issues with bandwidth in multisite deployments
- Describe availability issues in multisite deployments
- Describe dial plan issues in multisite deployments
- Describe Network Address Translation (NAT) and security issues in multisite deployments

Deploying Cisco Unified Communications Manager (CUCM) in a multisite environment has considerations that are more complex than merely a single site solution. Deploying Cisco Unified Communications solutions between multiple sites requires an appropriate dial plan, enough bandwidth between the sites, implementing quality of service (QoS), and a design that can survive IP WAN failures. This chapter identifies the issues that can arise in a multisite CUCM deployment.

Multisite Deployment Challenge Overview

In a multisite deployment, some of the challenges that can arise include the following:

- **Quality issues:** Real-time communications of voice and video must be prioritized over a packet-switching network. All traffic is treated equally by default in routers and switches. Voice and video are delay-sensitive packets that need to be given priority to avoid delay and jitter (variable delay), which would result in decreased voice quality.

- **Bandwidth issues:** Cisco Unified Communications (UC) can include voice and video streams, signaling traffic, management traffic, and application traffic (such as rich media conferencing). The additional bandwidth that is required when deploying a Cisco UC solution has to be calculated and provisioned for to ensure that data applications and Cisco UC applications do not overload the available bandwidth. Bandwidth reservations can be made to applications through QoS deployment.
- **Availability issues:** When deploying CUCM with centralized call processing, IP Phones register with CUCM over the IP LAN and potentially over the WAN. If gateways in remote sites are using Media Gateway Control Protocol (MGCP) as a signaling protocol, they also depend on the availability of CUCM acting as an MGCP call agent. It is important to implement fallback solutions for IP Phones and gateways in scenarios in which the connection to the CUCM servers is broken because of IP WAN failure. Fallback solutions also apply to H.323 or Session Initiation Protocol (SIP) gateways but will require the correct dial peers to support this functionality.

Note Cisco Unified Communications Manager (CUCM) used to be called Cisco CallManager (CCM).

- **Dial plan issues:** Directory numbers (DN) can overlap across multiple sites. Overlapping dial plans and nonconsecutive numbers can be solved by designing a robust multisite dial plan. Avoid overlapping numbers across sites whenever possible for an easier design.
- **NAT and security issues:** The use of private IP addresses within an enterprise IP network is common. Internet Telephony Service Providers (ITSP) require unique public IP addresses to route IP Phone calls. The private IP addresses within the enterprise have to be translated into public IP addresses. Public IP addresses make the IP Phones visible from the Internet and therefore subject to attacks.

Note The challenge of Network Address Translation (NAT) and security is not limited to multisite deployments. For example, for Cisco Attendant Console (AC), the line-state and call-forwarding status of the primary line of each user is presented with each record entry. When you use CUCM and AC across NAT interfaces, or when a firewall is between them, TCP traffic works correctly with the NAT transversal. Therefore, most of the AC functionality works. However, line-state updates from the server to the client are sent using User Datagram Protocol (UDP) packets. If a NAT device or firewall separates the client and server, the client most likely does not receive line-state updates from the server. Ensure that both client and server are on the same side of the NAT device or the firewall.

Quality Challenges

IP networks were not originally designed to carry real-time traffic; instead, they were designed for resiliency and fault tolerance. Each packet is processed separately in an IP network, sometimes causing different packets in a communications stream to take

different paths to the destination. The different paths in the network may have a different amount of packet loss, delay, and delay variation (jitter) because of bandwidth, distance, and congestion differences. The destination must be able to receive packets out of order and resequence these packets. This challenge is solved by the use of Real-Time Transport Protocol (RTP) sequence numbers, ensuring proper reassembly and play-out to the application. When possible, it is best to not rely solely on these RTP mechanisms. Proper network design, using Cisco router Cisco Express Forwarding (CEF) switch cache technology, performs per-destination load sharing by default. Per-destination load sharing is not a perfect load-balancing paradigm, but it ensures that each IP flow (voice call) takes the same path.

Bandwidth is shared by multiple users and applications, whereas the amount of bandwidth required for an individual IP flow varies significantly during short lapses of time. Most data applications are bursty by nature, whereas Cisco real-time audio communications with RTP use the same continuous-bandwidth stream. The bandwidth available for any application, including CUCM and voice-bearer traffic, is unpredictable. During peak periods, packets need to be buffered in queues waiting to be processed because of network congestion. Queuing is a term that anyone who has ever experienced air flight is familiar with. When you arrive at the airport, you must get in a line (queue) because the number of ticket agents (bandwidth) available to check you in is less than the flow of traffic arriving at the ticket counters (incoming IP traffic). If congestion occurs for too long, the queue (packet buffers) gets filled up, and passengers are annoyed. (Packets are dropped.) Higher queuing delays and packet drops are more likely on highly loaded, slow-speed links such as WAN links used between sites in a multisite environment. Quality challenges are common on these types of links, and you need to handle them by implementing QoS. Without the use of QoS, voice packets experience delay, jitter, and packet loss, impacting voice quality. It is critical to properly configure Cisco QoS mechanisms end to end throughout the network for proper audio and video performance.

During peak periods, packets cannot be sent immediately because of interface congestion. Instead, the packets are temporarily stored in a queue, waiting to be processed. The amount of time the packet waits in the queue, called the queuing delay, can vary greatly based on network conditions and traffic arrival rates. If the queue is full, newly received packets cannot be buffered anymore and get dropped (tail drop). Figure 1-1 illustrates tail drop. Packets are processed on a first in, first out (FIFO) model in the hardware queue of all router interfaces. Voice conversations are predictable and constant (sampling is every 20 milliseconds by default), but data applications are bursty and greedy. Voice, therefore, is subject to degradation of quality because of delay, jitter, and packet loss.

Bandwidth Challenges

Each site in a multisite deployment usually is interconnected by an IP WAN, or occasionally by a metropolitan-area network (MAN), such as Metro Ethernet. Bandwidth on WAN links is limited and relatively expensive. The goal is to use the available bandwidth as efficiently as possible. Unnecessary traffic should be removed from the IP WAN links through content filtering, firewalls, and access control lists (ACL). IP WAN acceleration

methods for bandwidth optimization should be considered as well. Any period of congestion could result in service degradation unless QoS is deployed throughout the network.

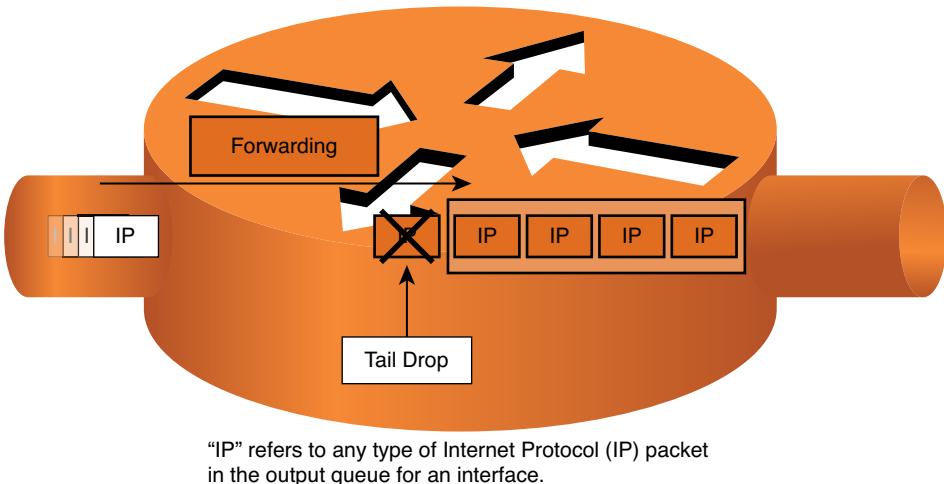


Figure 1-1 Tail Drop

Voice streams are constant and predictable for Cisco audio packets. Typically, the G.729 codec is used across the WAN to best use bandwidth. As a comparison, the G.711 audio codec requires 64 kbps, whereas packetizing the G.711 voice sample in an IP/UDP/RTP header every 20 ms requires 16 kbps plus the Layer 2 header overhead.

Voice is sampled every 20 ms, resulting in 50 packets per second (pps). The IP header is 20 bytes, whereas the UDP header is 8 bytes, and the RTP header is 12 bytes. The 40 bytes of header information must be converted to bits to figure out the packet rate of the overhead. Because a byte has 8 bits, $40 \text{ bytes} * 8 \text{ bits in a byte} = 320 \text{ bits}$. The 320 bits are sent 50 times per second based on the 20-ms rate (1 millisecond is 1/1000 of a second, and $20/1000 = .02$). So:

$$.02 * 50 = 1 \text{ second}$$

$$320 \text{ bits} * 50 = 16,000 \text{ bits/sec, or } 16 \text{ kbps}$$

Note This calculation does not take Layer 2 encapsulation into consideration. You can find more information by reading *QoS Solution Reference Network Design (SRND)* (www.cisco.com/go/srnd) or *Cisco QoS Exam Certification Guide*, Second Edition (Cisco Press, 2004). For more information on QoS, go to www.cisco.com/go/qos.

Voice packets are benign compared to the bandwidth consumed by data applications. Data applications can fill the entire maximum transmission unit (MTU) of an Ethernet frame (1518 bytes or 9216 bytes if jumbo Ethernet frames have been enabled). In

comparison to data application packets, voice packets are small (approximately 60 bytes for G.729 and 200 bytes for G.711 with the default 20-ms sampling rate).

In Figure 1-2, a conference bridge has been deployed at the main site. No conference bridge exists at the remote site. If three IP Phones at a remote site join a conference, their RTP streams are sent across the WAN to the conference bridge. The conference bridge, whether using software or hardware resources, mixes the received audio streams and sends back three unique unicast audio streams to the IP Phones over the IP WAN. The conference bridge removes the receiver's voice from his unique RTP stream so that the user does not experience echo because of the delay of traversing the WAN link and mixing RTP audio streams in the conference bridge.

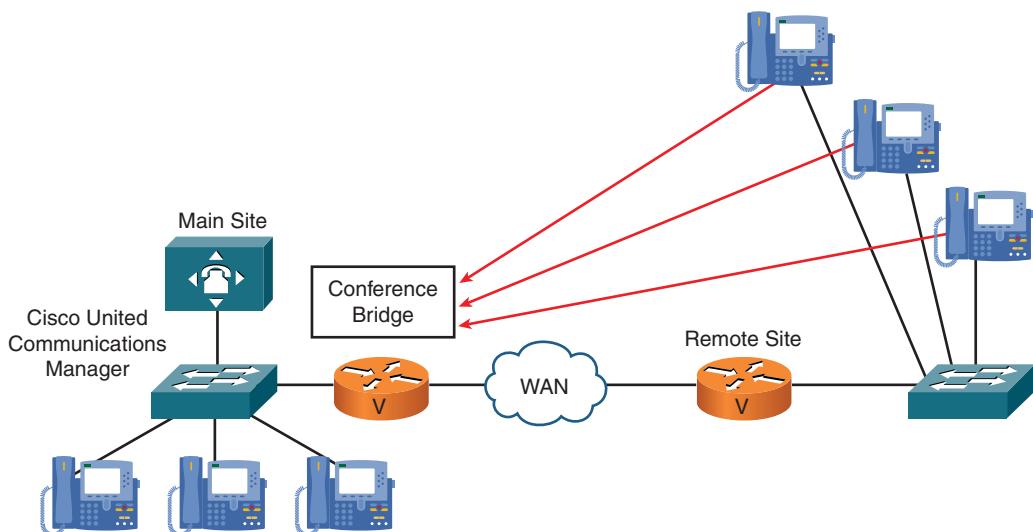


Figure 1-2 Resource Challenges

Centralized conference resources cause bandwidth, delay, and capacity challenges in the voice network. Each G.711 RTP stream requires 80 kbps (plus the Layer 2 overhead), resulting in 240 kbps of IP WAN bandwidth consumption by this voice conference. If the conference bridge were not located on the other side of the IP WAN, this traffic would not need to traverse the WAN link, resulting in less delay and bandwidth consumption. If the remote site had a CUCM region configuration that resulted in calls with the G.729 codec back to the main site, the software conferencing resources of CUCM would not be able to mix the audio conversations. Hardware conferencing or hardware transcoder media resources in a voice gateway are required to accommodate G.729 audio conferencing. Local hardware conference resources would remove this need. All centrally located media resources (Music On Hold [MOH], annunciator, conference bridges, videoconferencing, and media termination points) suffer similar bandwidth, delay, and resource exhaustion challenges.

Availability Challenges

When deploying CUCM in multisite environments, centralized CUCM-based services are accessed over the IP WAN. Affected services include the following:

- **Signaling in CUCM multisite deployments with centralized call processing:** Remote Cisco IP Phones register with a centralized CUCM server. Remote MGCP gateways are controlled by a centralized CUCM server that acts as an MGCP call agent.
- **Signaling in CUCM multisite deployments with distributed call processing:** In such environments, sites are connected via H.323 (nongatekeeper-controlled, gatekeeper-controlled, or H.225) or SIP trunks.
- **Media exchange:** RTP streams between endpoints located at different sites.
- **Other services:** These include Cisco IP Phone XML services and access to applications such as attendant console, CUCM Assistant, and others.

Figure 1-3 shows a UC network in which the main site is connected to a remote site through a centralized call-processing environment. The main site is also connected to a remote cluster through an intercluster trunk (ICT), representing a distributed call processing environment. The combination of both centralized and distributed call processing represents a hybrid call-processing model in which small sites use the CUCM resources of the main site, but large remote offices have their own CUCM cluster. The bottom left of Figure 1-3 shows a SIP trunk, which is typically implemented over a Metro Ethernet connection to an ITSP. The benefit of the SIP trunk is that the ITSP provides the gateways to the public switched telephone network (PSTN) instead of you needing to provide gateways at the main site.

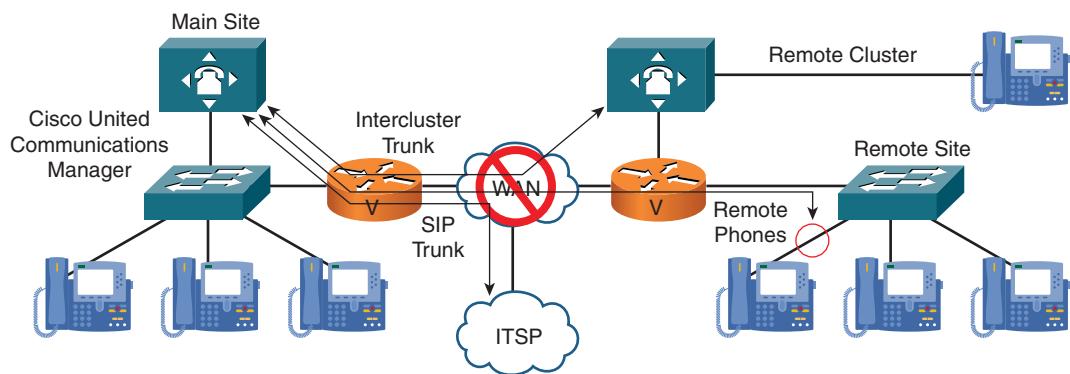


Figure 1-3 Availability Challenges

An IP WAN outage in Figure 1-3 will cause an outage of call-processing services for the remote site connected in a centralized fashion. The remote cluster will not suffer a call-processing outage, but the remote cluster will not be able to dial the main site over the IP WAN during the outage. Mission-critical voice applications (voice mail, interactive voice

response [IVR], and so on) located at the main site will be unavailable to any of the other sites during the WAN outage.

If the ITSP is using the same links that allow IP WAN connectivity, all calls to and from the PSTN will also be unavailable.

Note A deployment like the one shown in Figure 1-3 is considered a bad design because of the lack of IP WAN fault tolerance and PSTN backup.

Dial Plan Challenges

In a multisite deployment, with a single or multiple CUCM clusters, dial plan design requires the consideration of several issues that do not exist in single-site deployments:

- **Overlapping numbers:** Users located at different sites can have the same directory numbers assigned. Because directory numbers usually are unique only within a site, a multisite deployment requires a solution for overlapping numbers.
- **Nonconsecutive numbers:** Contiguous ranges of numbers are important to summarize call-routing information, analogous to contiguous IP address ranges for route summarization. Such blocks can be represented by one or a few entries in a call-routing table, such as route patterns, dial peer destination patterns, and voice translation rules, which keep the routing table short and simple. If each endpoint requires its own entry in the call-routing table, the table gets too big, lots of memory is required, and lookups take more time. Therefore, nonconsecutive numbers at any site are not optimal for efficient call routing.
- **Variable-length numbering:** Some countries, such as the U.S. and Canada, have fixed-length numbering plans for PSTN numbers. Others, such as Mexico and England, have variable-length numbering plans. A problem with variable-length numbers is that the complete length of the number dialed can be determined only by the CUCM route plan by waiting for the interdigit timeout. Waiting for the interdigit timeout, known as the T.302 timer, adds to the post-dial delay, which may annoy users.
- **Direct inward dialing (DID) ranges and E.164 addressing:** When considering integration with the PSTN, internally used directory numbers have to be related to external PSTN numbers (E.164 addressing). Depending on the numbering plan (fixed or variable) and services provided by the PSTN, the following solutions are common:
- **Each internal directory number relates to a fixed-length PSTN number:** In this case, each internal directory number has its own dedicated PSTN number. The directory number can, but does not have to, match the least-significant digits of the PSTN number. In countries with a fixed numbering plan, such as the North American Numbering Plan (NANP), this usually means that the four-digit office codes are used as internal directory numbers. If these are not unique, digits of office codes or administratively assigned site codes might be added, resulting in five or more digits being used for internal directory numbers.

Another solution is to not reuse any digits of the PSTN number, but to simply map each internally used directory number to any PSTN number assigned to the company. In this case, the internal and external numbers do not have anything in common. If the internally used directory number matches the least-significant digits of its corresponding PSTN number, significant digits can be set at the gateway or trunk. Also, general external phone number masks, transformation masks, or prefixes can be configured. This is true because all internal directory numbers are changed to fully qualified PSTN numbers in the same way. Another example is if the internal directory number is composed of parts of the PSTN number and administratively assigned digits such as site codes plus PSTN station codes, or different ranges, such as PSTN station codes 4100 to 4180 that map to directory numbers 1100 to 1180, or totally independent mappings of internal directory numbers to PSTN numbers. In that case, one or more translation rules have to be used for incoming calls, and one or more calling party transformation rules, transformation masks, external phone number masks, or prefixes have to be configured. This approach can be laborious because a one-for-one translation is required.

- **No DID support in fixed-length numbering plans:** To avoid the requirement of one PSTN number per internal directory number when using a fixed-length numbering plan, it is common to disallow DID to an extension. Instead, the PSTN trunk has a single number, and all PSTN calls routed to that number are sent to an attendant, an auto-attendant, a receptionist, or a secretary. From there, the calls are *transferred* to the appropriate internal extension.
- **Internal directory numbers are part of a variable-length number:** In countries with variable-length numbering plans, a typically shorter “subscriber” number is assigned to the PSTN trunk, but the PSTN routes all calls *starting* with this number to the trunk. The caller can add digits to identify the extension. There is no fixed number of additional digits or total digits. However, there is a maximum, usually 32 digits, which provides the freedom to select the length of directory numbers. This maximum length can be less. For example, in E.164 the maximum number is 15 digits, not including the country code. A caller simply adds the appropriate extension to the company’s (short) PSTN number when placing a call to a specific user. If only the short PSTN number without an extension is dialed, the call is routed to an attendant within the company. Residential PSTN numbers are usually longer and do not allow additional digits to be added; the feature just described is available only on trunks.
- **Type of Number (TON) in ISDN:** The calling number (Automatic Number Identification [ANI]) of calls being received from the PSTN can be represented in different ways:
 - As a seven-digit subscriber number
 - As a national ten-digit number, including the area code
 - In international format with the country code in front of the area code

To standardize the ANI for all calls, the format that is used must be known, and the number has to be transformed accordingly.

- **Optimized call routing:** Having an IP WAN between sites with PSTN access at all sites allows PSTN toll bypass by sending calls between sites over the IP WAN instead of using the PSTN. In such scenarios, the PSTN should be used as a backup path only in case of WAN failure. Another solution, which extends the idea of toll bypass and can potentially reduce toll charges, is to also use the IP WAN for PSTN calls. With tail-end hop-off (TEHO), the IP WAN is used as much as possible, and the gateway that is closest to the dialed PSTN destination is used for the PSTN breakout.

Note Any two-way phone call has two phone numbers: the calling number, or ANI, and the called number, or Dialed Number Identification Service (DNIS). Any two-way call goes from the ANI to the DNIS. Digit manipulation is the process of changing the ANI and the DNIS to any other number.

Overlapping and Nonconsecutive Numbers

In Figure 1-4, Cisco IP Phones at the main site use directory numbers 1001 to 1099, 2000 to 2157, and 2365 to 2999. At the remote site, 1001 to 1099 and 2158 to 2364 are used. These directory numbers have two issues. First, 1001 to 1099 overlap; these directory numbers exist at both sites, so they are not unique throughout the complete deployment. This causes a problem: If a user in the remote site dialed only the four digits 1001, which phone would ring? This issue of overlapping dial plans needs to be addressed by digit manipulation. In addition, the nonconsecutive use of the range 2000 to 2999 (with some duplicate numbers at the two sites) requires a significant number of additional entries in call-routing tables because the ranges can hardly be summarized by one (or a few) entries.

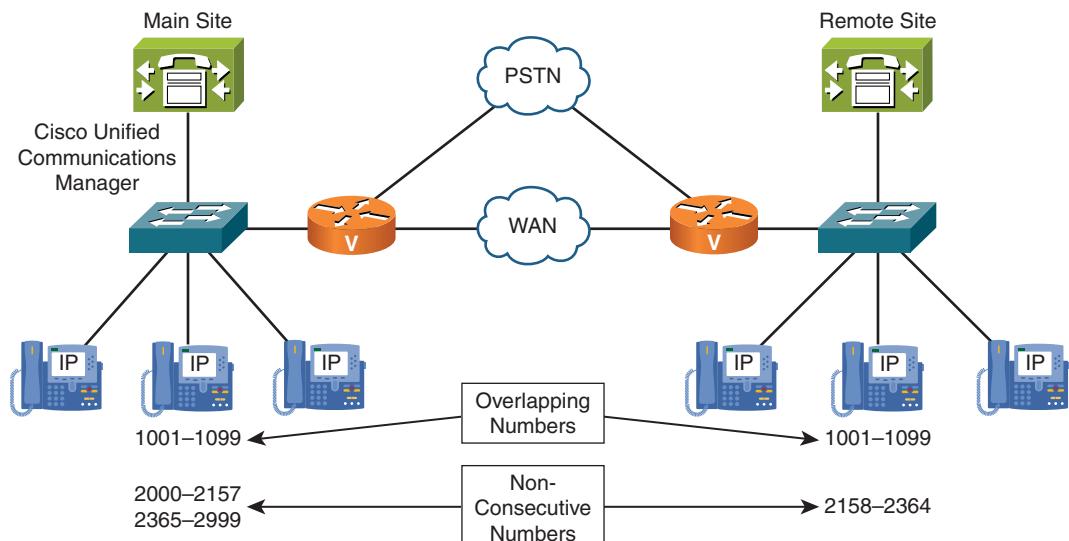


Figure 1-4 Dial Plan Challenges: Overlapping and Nonconsecutive Numbers

Note The solutions to the problems listed in this chapter are discussed in more detail in the next chapter.

Fixed Versus Variable-Length Numbering Plans

A fixed numbering plan features fixed-length area codes and local numbers. An open numbering plan features variance in length of area code or local number, or both, within the country.

Table 1-1 contrasts the NANP and a variable-length numbering plan—Germany’s numbering plan, in this example.

Examples:

- **Within the U.S.:** 9-1-408-555-1234 or 1-555-1234 (within the same area code)
- **U.S. to Germany:** 9-011-49-404-132670
- **Within Germany:** 0-0-404-132670 or 0-132670 (within the same city code)
- **Germany to the U.S.:** 0-00-1-408-555-1234 (Note: The 1 in 00-1-408 is the U.S. country code, not the trunk prefix.)

The NANP PSTN number is 408-555-1234, DID is not used, and all calls placed to the main site are handled by an attendant. There is a remote site in Germany with the E.164 PSTN number +49 404 13267. Four-digit extensions are used at the German location, and DID is allowed because digits can be added to the PSTN number. When calling the German office attendant (not knowing a specific extension), U.S. users would dial 9-011-49-404-13267. Note how the + is replaced by the international prefix 011 and the access code 9. If the phone with extension 1001 should be called directly, 9-011-49-404-13267-1001 has to be dialed.

Note In the examples shown following Table 1-1, dialing out from the U.S. illustrates the common practice of dialing 9 first as an access code to dial out. This use is common, but optional, in a dial plan. However, if the access code is used, the 9 must be stripped before reaching the PSTN, whereas the other dialed prefixes must be sent to the PSTN for proper call routing.

Variable-Length Numbering, E.164 Addressing, and DID

Figure 1-5 illustrates an example in which the main site with CUCM resides in the U.S. and a remote site without CUCM resides in Germany. The NANP PSTN number in the U.S. is 408-555-1234. Note that DID is not used, because all calls placed to the main site are handled by an attendant. A remote site in Germany has PSTN number +49 404 13267. Four-digit extensions are used at the German location, and DID is allowed because digits can be added to the PSTN number. When calling the German office attendant (not knowing a specific extension), U.S. users would dial 9-011-49-404-13267. If the phone with extension 1001 should be called directly, 9-011-49-404-13267-1001 has to be dialed.

Table 1-1 Fixed Versus Variable-Length Numbering Plans

Component	Description	Fixed Numbering Plan (NANP)	Variable-Length Numbering Plan (Germany)
Country code	A code of one to three digits is used to reach the particular telephone system for each nation or special service. Obtain the E.164 standard from http://itu.org to see all international country codes.	1	49
Area code	Used within many nations to route calls to a particular city, region, or special service. Depending on the nation or region, it may also be called a numbering plan area, subscriber trunk dialing code, national destination code, or routing code.	Three digits	Three to five digits
Subscriber number	Represents the specific telephone number to be dialed, but it does not include the country code, area code (if applicable), international prefix, or trunk prefix.	Three-digit exchange code plus a four-digit station code	Three or more digits
Trunk prefix	The initial digits to be dialed in a domestic call, before the area code and the subscriber number.	1	0
Access code	A number that is traditionally dialed first “to get out to the PSTN,” used in PBXs and VoIP systems.	9	0
International prefix	The code dialed before an international number (country code, area code if any, and then subscriber number).	011	00 or + (+ is used by cell phones)

The logic of routing calls by CUCM over the WAN or through the PSTN is appropriately transparent to the phone user.

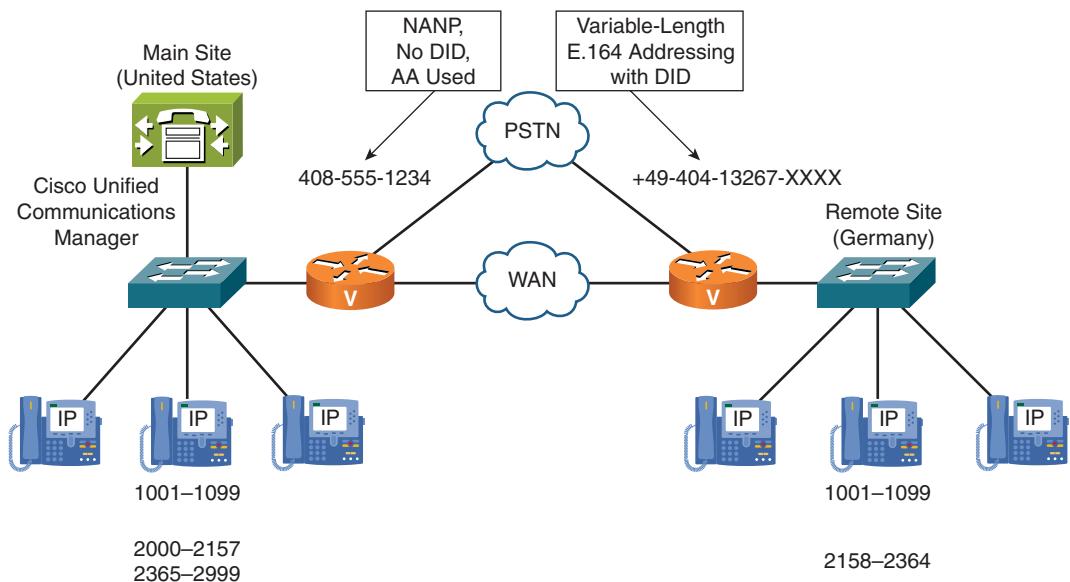


Figure 1-5 Variable-Length Numbering, E.164 Addressing, and DID

Detection of End of Dialing in Variable-Length Numbering Plans

The three ways of detecting the end of dialing in variable-length numbering plans are as follows:

- Interdigit timeout
- Use of # key
- Use of overlap sending and overlap receiving

From an implementation perspective, the simplest way to detect end of dialing is to wait for an interdigit timeout to expire. This approach, however, provides the least comfort to the end user because it adds post-dial delay. In an environment with only a few numbers of variable length (for example, NANP, where only international calls are of variable length), waiting for the interdigit timeout might be acceptable. However, even in such an environment, it might make sense to at least reduce the value of the timer, because the default value in CUCM is high (15 seconds).

Note In CUCM, the interdigit timer is set by the cluster-wide Cisco CallManager service parameter T302 timer that is found in Cisco Unified CM Administration by navigating to **System > Service Parameters** under the **Cisco CallManager Service**.

In Cisco IOS Software, the default for the interdigit timeout is 10 seconds. You can modify this value using the voice-port **timeouts interdigit** command.

Another solution for detecting end of dialing on variable-length numbers is the use of the # key. An end user can press the # key to indicate that dialing has finished. The implementation of the # key is different in CUCM versus Cisco IOS Software. In Cisco IOS gateways, the # is seen as an instruction to stop digit collection. It is not seen as part of the dialed string. Therefore, the # is not part of the configured destination pattern. In CUCM, the # is considered to be part of the dialed number and, therefore, its usage has to be explicitly permitted by the administrator by creating patterns that include the #. If a pattern includes the #, the # has to be used; if a pattern does not include the #, the pattern is not matched if the user presses the # key. Therefore, it is common in CUCM to create a variable-length pattern twice: once with the # at the end and once without the #.

An alternative way to configure such patterns is to end the pattern with `![0-9#]`. In this case, a single pattern supports both ways of dialing—with and without the #. However, be aware that the use of such patterns can introduce other issues. For example, this can be an issue when using discard digits instructions that include trailing-# (for example, PreDot-Trailing-#). This discard digit instruction will have an effect only when there is a trailing # in the dialed number. If the # was not used, the discard digit instruction is ignored and, hence, the PreDot component of the discard digit instruction is also not performed. As covered in the *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) Foundation Learning Guide*, PreDot is a form of digit manipulation in CUCM that strips off all digits before the dot.

Allowing the use of the # to indicate end of dialing provides more comfort to end users than having them wait for the interdigit timeout. However, this possibility has to be communicated to the end users, and it should be consistently implemented. As previously mentioned, it is automatically permitted in Cisco IOS Software, but not in CUCM.

The third way to indicate end of dialing is the use of overlap send and overlap receive. If overlap is supported end to end, the digits that are dialed by the end user are sent one by one over the signaling path. Then, the receiving end system can inform the calling device after it receives enough digits to route the call (number complete). Overlap send and receive is common in some European countries, such as Germany and Austria. From a dial plan implementation perspective, overlap send and receive is difficult to implement when different PSTN calling privileges are desired. In this case, you have to collect enough digits locally (for example, in CUCM or Cisco IOS Software) to be able to decide to permit or deny the call. Only then can you start passing digits on to the PSTN one by one using overlap. For the end user, however, overlap send and receive is comfortable because each call is processed as soon as enough digits have been dialed. The number of digits that are sufficient varies per dialed PSTN number. For example, one local PSTN destination might be reachable by a seven-digit number, whereas another local number might be uniquely identified only after receiving nine digits.

Optimized Call Routing and PSTN Backup

There are two ways to save costs for PSTN calls in a multisite deployment:

- **Toll bypass:** Calls between sites within an organization that use the IP WAN instead of the PSTN. The PSTN is used for intersite calls only if calls over the IP WAN are not possible—either because of a WAN failure or because the call is not admitted by call admission control (CAC).
- **Tail-end hop-off (TEHO):** Extends the concept of toll bypass by also using the IP WAN for calls to the remote destinations in the PSTN. With TEHO, the IP WAN is used as much as possible, and PSTN breakout occurs at the gateway that is located closest to the dialed PSTN destination. Local PSTN breakout is used as a backup in case of IP WAN or CAC.

Caution Some countries do not allow the use of TEHO or toll bypass because it is illegal to bypass their international tariff collections, which would deprive their operators of international inbound revenues. When implementing either, ensure that the deployment complies with legal requirements of that country.

In the example shown in Figure 1-6, a call from Chicago to San Jose would be routed as follows.

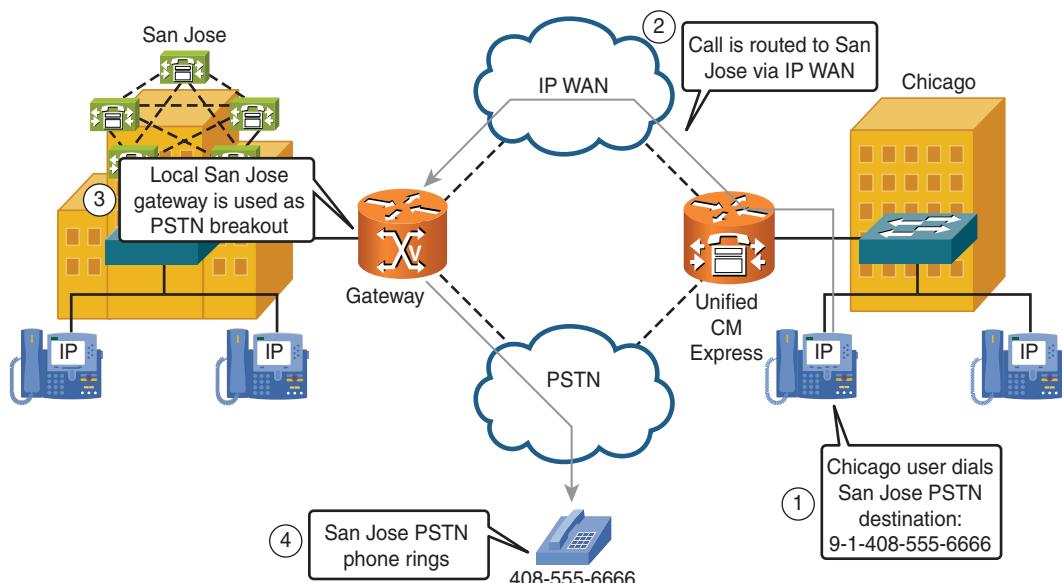


Figure 1-6 Tail-End Hop-Off (TEHO) Example

1. The Chicago CUCM Express user dials 9-1-408-555-6666, a PSTN phone located in San Jose.
2. The call is routed from Chicago CUCM Express router to the San Jose CUCM cluster over the IP WAN with either SIP or H.323.
3. The San Jose CUCM routes the call to the San Jose gateway, which breaks out to the PSTN with what now becomes a local inexpensive call to the San Jose PSTN.
4. The San Jose PSTN central office routes the call, and the phone rings.

If the WAN were unavailable for any reason before the call, the Chicago Gateway would have to be properly configured to route the call with the appropriate digit manipulation through the PSTN at a potentially higher toll cost to the San Jose PSTN phone.

Note The primary purpose of implementing TEHO is because of a reduction of operating costs from calling through the PSTN. In this TEHO example, there would be potential cost savings. However, costs savings are typically considerably higher when the remote location and destination call are international.

Various PSTN Requirements

Various countries can have various PSTN dialing requirements, which makes it difficult to implement dial plans in international deployments.

One of the issues in international deployments is various PSTN dial rules. For example, in the United States, the PSTN access code is 9, while in most countries in Europe, 0 is used as the PSTN access code. The national access code in the United States is 1, while 0 is commonly used in Europe. The international access code is 011 in the United States, while 00 is used in many European countries. Some PSTN provider networks require the use of the ISDN TON, while others do not support it. Some networks allow national or international access codes to be combined with ISDN TON. Others require you to send the actual number only (that is, without any access codes) when setting the ISDN TON.

The same principle applies to the calling-party number. As mentioned earlier, in variable-length numbering plans, the TON cannot be detected by its length. Therefore, the only way to determine whether the received call is a local, national, or international call is by relying on the availability of the TON information in the received signaling message.

Some countries that have variable-length numbering plans use overlap send and overlap receive. With overlap send, a number that is dialed by an end user is passed on to the PSTN digit by digit. Then, the PSTN indicates when it has received enough numbers to route the call. Overlap receive describes the same concept in the opposite direction: When a call is received from the PSTN in overlap mode, the dialed number is delivered digit by digit, and not en bloc. Some providers that use overlap send toward their

customers do not send the prefix that is configured for the customer trunk, but only the additional digits that are dialed by the user who initiates the call.

When dialing PSTN numbers in E.164 format (that is, numbers that start with the country code), the + sign is commonly prefixed to indicate that the number is in E.164 format. The advantage of using the + sign as a prefix for international numbers is that it is commonly known as a + sign around the world. In contrast, PSTN access codes such as 011 (used in the NANP) or 00 (often used in Europe) are known only in the respective countries.

Finally, emergency dialing can be an issue in international deployments. Because various countries have various emergency numbers and various ways to place emergency calls, users are not sure how to dial the emergency number when roaming to other countries. An international deployment should allow roaming users to use their home dialing rules when placing emergency calls. The system should then modify the called number as required at the respective site.

Issues Caused by Different PSTN Dialing

Different local PSTN dial rules can cause several issues, especially in international deployments.

The main problem that needs to be solved in international environments is how to store contacts' telephone numbers. Address book entries, speed and fast dials, call list entries, and other numbers should be in a format that allows them to be used at any site, regardless of the local dial rules that apply to the site where the user is currently located.

The same principle applies to numbers that are configured by the administrator—for example, the target PSTN number for Automated Alternate Routing (AAR) targets. Call-forwarding destinations should also be in a universal format that allows the configured number to be used at any site.

The main reason for a universal format is that a multisite deployment has several features that make it difficult to predict which gateway will be used for the call. For example, a roaming user might use Cisco Extension Mobility or Device Mobility. Both features allow an end user to use local PSTN gateways while roaming. If no universal format is used to store speed dials or address book entries, it will be difficult for the end user to place a PSTN call to a number that was stored according to the NANP dial rules while in countries that require different dial rules. Even when not roaming, the end user can use TEHO or least cost routing (LCR), so that calls break out to the PSTN at a remote gateway, not at the local gateway. If the IP WAN link to the remote gateway is down, the local gateway is usually used as a backup. How should the number that is used for call routing look in such an environment? It is clearly entered according to local dial rules by the end user, but ideally, it is changed to a universal format before call routing is performed. After the call is routed and the egress gateway is selected, the number could then be changed as required by the egress gateway.

Dial Plan Scalability Issues

In large CUCM deployments, it can be difficult to implement dial plans, especially when using features such as TEHO with local PSTN backup.

The main scalability issue of large deployments is that each call-routing domain (for example, a CUCM cluster or a CUCME router) needs to be aware of how to get to all other domains.

Such a dial plan can become large and complex, especially when multiple paths (for example, a backup path for TEHO) have to be made available. As each call-routing domain has to be aware of the complete dial plan, a static configuration does not scale. For example, any changes in the dial plan must be applied individually at each call-routing domain.

Centralized H.323 gatekeepers or SIP network services can simplify the implementation of such dial plans because there is no need to implement the complete dial plan at each call-routing domain. Instead of an any-to-any dial plan configuration, only the centralized component has to be aware of where to find which number. This approach, however, means that you rely on a centralized service. If the individual call-routing entities have no connectivity to the centralized call-routing intelligence, all calls would fail. Further, the configuration is still static. Any changes at one call-routing domain (for example, new PSTN prefixes because of changing the PSTN provider) has to also be implemented at the central call-routing component.

In addition, these centralized call-routing services do not have built-in redundancy. Redundancy can be provided, but it requires additional hardware, additional configuration, and so on. Redundancy is not an integrated part of the solution.

The ideal solution for a large deployment would allow an automatic recognition of routes. Internal and external (for PSTN backup) numbers should be advertised and learned by call-routing entities. A dynamic routing protocol for call-routing targets would address scalability issues in large deployments.

Call control discovery (CCD), which is a feature based on the Cisco Service Advertisement Framework (SAF), provides such functionality. New with CUCM v8, CCD and Cisco SAF are explained in detail in later chapters.

NAT and Security Issues

In single-site deployments, CUCM servers and IP Phones usually use private IP addresses because there is no need to communicate with the outside IP world. NAT is not configured for the phone subnets, and attacks from the outside are impossible.

In multisite deployments, however, IP Security (IPsec) virtual private network (VPN) tunnels can be used between sites. The VPN tunnels allow only intersite communication; access to the protected internal networks is not possible from the outside—only from the other site through the tunnel. Therefore, attacks from the outside are blocked at the

gateway. To configure IPsec VPNs, the VPN tunnel must be configured to terminate on the two gateways in the different sites. Sometimes this is not possible; for instance, the two sites may be under different administration, or perhaps security policies do not allow the configuration of IPsec VPNs.

In such a case, or when connecting to a public service such as an ITSP, NAT has to be configured for CUCM servers and IP Phones. Cisco calls this Hosted NAT Traversal for Session Border Controllers.

In Figure 1-7, Company A and Company B both use IP network 10.0.0.0/8 internally. To communicate over the Internet, the private addresses are translated into public IP addresses. Company A uses public IP network A, and Company B uses public IP network B. All CUCM servers and IP Phones can be reached from the Internet and communicate with each other.

As soon as CUCM servers and IP Phones can be reached with public IP addresses, they are subject to attacks from the outside world, introducing potential security issues.

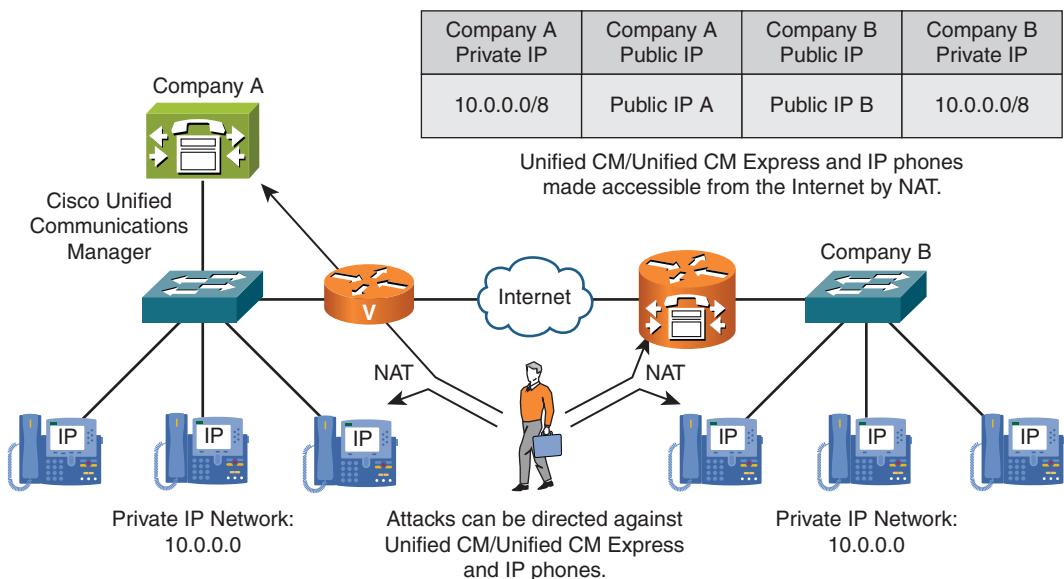


Figure 1-7 NAT Security Issues

Summary

The following key points were discussed in this chapter:

- Multisite deployment introduces issues of quality, bandwidth, availability, dial plan, and NAT and security.
- During congestion, packets have to be buffered, or they can get dropped.
- Bandwidth in the IP WAN is limited and should be used as efficiently as possible.
- A multisite deployment has several services that depend on the availability of the IP WAN.
- A multisite dial plan has to address overlapping and nonconsecutive numbers, variable-length numbering plans, DID ranges, and ISDN TON and should minimize PSTN costs.
- When CUCM servers and IP Phones need to be exposed to the outside, they can be subject to attacks from the Internet.

References

For additional information, refer to these resources:

Cisco Unified Communications Solution Reference Network Design (SRND) based on CUCM release 8.x.

CUCM Administration Guide, release 8.0.

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in Appendix A, "Answers Appendix."

1. Which of the following best describes DID?
 - a. E.164 international dialing
 - b. External dialing from an IP Phone to the PSTN
 - c. VoIP security for phone dialing
 - d. The ability of an outside user to directly dial into an internal phone

- 2.** Which of the following statements is the least accurate about IP networks?
 - a.** IP packets can be delivered in the incorrect order.
 - b.** Buffering results in variable delays.
 - c.** Tail drops result in constant delays.
 - d.** Bandwidth is shared by multiple streams.
- 3.** Which statement most accurately describes overhead for packetized voice?
 - a.** VoIP packets are large compared to data packets and are sent at a high rate.
 - b.** The Layer 3 overhead of a voice packet is insignificant and can be ignored in payload calculations.
 - c.** Voice packets have a small payload size relative to the packet headers and are sent at high packet rates.
 - d.** Packetized voice has the same overhead as circuit-switching voice technologies.
- 4.** What does the + symbol refer to in E.164?
 - a.** Country code
 - b.** Area code
 - c.** International access code
 - d.** User's phone number
- 5.** Which two of the following are dial plan issues requiring a CUCM solution in multi-site decentralized deployments?
 - a.** Overlapping directory numbers
 - b.** Overlapping E.164 numbers
 - c.** Variable-length addressing
 - d.** Centralized call processing
 - e.** Centralized phone configuration
- 6.** What is a requirement for performing NAT for Cisco IP Phones between different sites thru the Internet?
 - a.** Use DHCP instead of fixed IP addresses.
 - b.** Exchange RTP media streams with the outside world.
 - c.** Use DNS instead of hostnames in CUCM.
 - d.** Exchange signaling information with the outside world.

7. Which is the most accurate description of E.164?
 - a. An international standard for phone numbers including country codes and area codes
 - b. An international standard for local phone numbers
 - c. An international standard for dialing only local numbers to the PSTN
 - d. An international standard for phone numbers for DID
8. Which of the following is the most accurate description of TEHO?
 - a. Using the PSTN for cost reduction
 - b. Using the IP WAN link for cost reduction
 - c. Using the IP WAN link for cost reduction with remote routing over the WAN, and then transferring into a local PSTN call at the remote gateway
 - d. Using the PSTN for cost reduction with minimal IP WAN usage
9. What is the greatest benefit of toll bypass?
 - a. It increases the security of VoIP.
 - b. It creates an effective implementation of Unified Communications.
 - c. It reduces operating costs by routing internal calls over WAN links as opposed to the PSTN.
 - d. It implements NAT to allow variable-length numbering.

This page intentionally left blank

Chapter 2

Identifying Multisite Deployment Solutions

Upon completing this chapter, you will be able to describe solutions to issues that occur in CUCM multisite deployments. You will be able to meet these objectives:

- Describe solutions to multisite deployment issues
- Describe how QoS solves quality issues in multisite deployments
- Describe solutions to bandwidth limitations in multisite deployments
- Describe survivability and availability features in multisite deployments
- Describe solutions for dial plan issues in multisite deployments
- Describe how Cisco Mobility and Extension Mobility resolves issues for mobile users
- Describe how a CUBE can solve NAT and security solutions in multisite deployments

A multisite deployment introduces several issues that do not apply to single-site deployments. When implementing Cisco Unified Communications Manager (CUCM) in a multisite environment, you must address these issues. This chapter shows you how to solve issues that arise in multisite deployments.

Multisite Deployment Solution Overview

Figure 2-1 illustrates a typical multisite deployment.

This deployment incorporates the following solutions to multisite deployment issues:

- Availability issues are solved by Cisco Unified Survivable Remote Site Telephony (SRST), which may include Media Gateway Control Protocol (MGCP) fallback or H.323, both using dial peers.
- Quality and bandwidth issues are solved by quality of service (QoS), call admission control (CAC), Real-Time Transport Protocol (RTP) header compression, and local media resources.

- Dial plan solutions include access and site codes, and digit manipulation.
- Network Address Translation (NAT) and security issues are solved by the deployment of a Cisco Unified Border Element (CUBE).

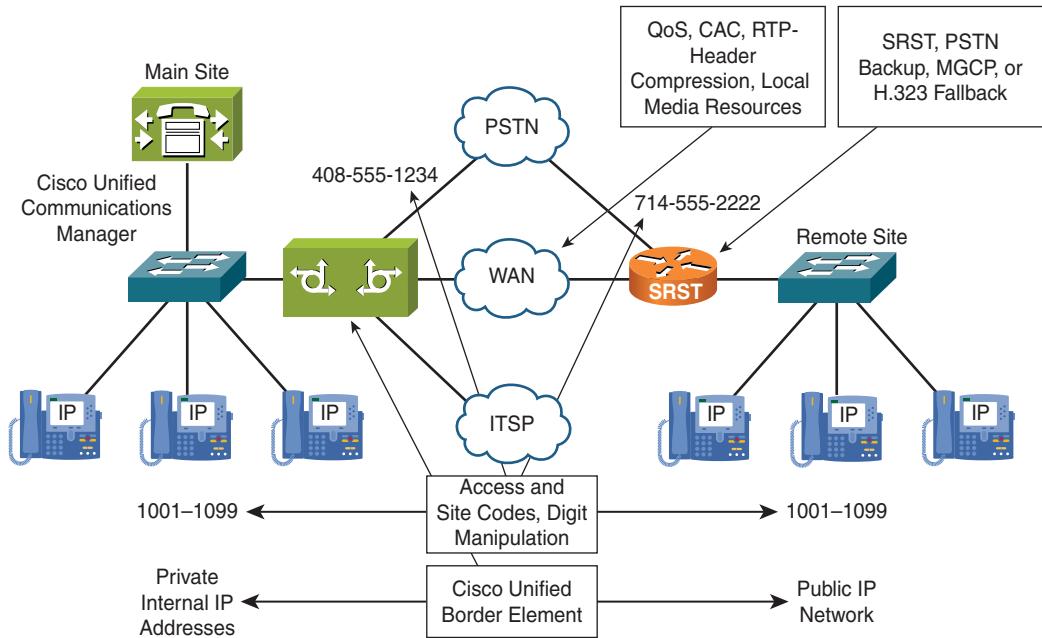


Figure 2-1 Multisite Deployment Solutions

Quality of Service

QoS refers to the capability of a network to provide better service to selected network traffic at the direct expense of other traffic. The primary goal of QoS is to provide better service—including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics—by giving priority to certain communication flows. QoS can be thought of as “managed unfairness” because whenever one type of traffic is given a higher priority, another is implicitly given a lower priority. The QoS designer must assess the level of each type of traffic and prioritize them best to suit the business needs of each organization.

Fundamentally, QoS enables you to provide better service to certain flows. This is done by either raising the priority of a flow or limiting the priority of another flow. When using congestion-management tools, you try to raise the priority of a flow by queuing and servicing queues in different ways. The queue-management tool used for congestion avoidance raises priority by dropping lower-priority flows before higher-priority flows. Policing and shaping provide priority to a flow by limiting the throughput of other flows. Link efficiency tools prevent large flows (such as file transfers) from severely degrading small flows, such as voice.

When implementing QoS, you must do the following:

- Identify traffic, such as voice, signaling, and data.
- Divide traffic into classes such as real-time traffic, mission-critical traffic, and any less-important traffic where QoS policy is implemented.
- Apply QoS policy per class, usually on a router interface, specifying how to serve each class.

QoS Advantages

QoS can improve the quality of voice calls when bandwidth utilization is high by giving priority to RTP packets. Figure 2-2 demonstrates how voice (audio) traffic is given absolute priority over all other traffic with low-latency queuing (LLQ). This reduces jitter, which is caused by variable queuing delays, and lost voice packets, which are caused by tail drops that occur when buffers are full. To avoid the complete blocking of other traffic, voice bandwidth should be limited by defining the bandwidth used by the maximum number of calls with the priority command within the LLQ configuration. The number of voice calls should also be limited by a CAC mechanism. Therefore, additional calls will not try to further saturate the WAN link, and ideally they will be configured with Automated Alternate Routing (AAR) to route the additional calls through the public switched telephone network (PSTN).

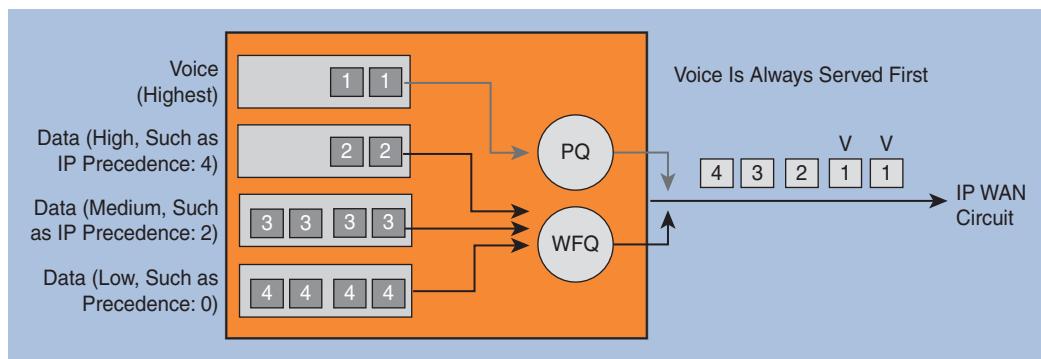


Figure 2-2 QoS Advantages

As an analogy, QoS builds a car-pool lane for prioritized drivers with LLQ. CAC is the mechanism that limits the maximum number of cars that can be in the car-pool lane at once.

Note Video frames containing visual images are also sent over RTP and should be configured with their own priority queue in LLQ. The Cisco best practice is that the priority queue should not exceed 33% of the interface bandwidth.

Finally, to ensure proper service for voice calls, you should configure QoS to guarantee a certain bandwidth for signaling traffic, such as Session Initiation Protocol (SIP) or Skinny Client Control Protocol (SCCP) with class-based weighted fair queuing (CBWFQ). Otherwise, despite that the quality of active calls might be okay, calls cannot be torn down, and new calls cannot be established in the event of WAN circuit congestion.

Note QoS is not discussed further in this book. For more information, refer to the Cisco Quality of Service or Optimizing Converged Cisco Networks courses.

Solutions to Bandwidth Limitations

Bandwidth on the IP WAN can be conserved using the following methods:

- **Using low-bandwidth codecs:** If you use low-bandwidth (compression) codecs, such as G.729, the required bandwidth for digitized voice is 8 kbps, or approximately 26 kbps in an RTP packet, compared to the 64 kbps, or approximately 87 kbps in an RTP packet, that is required by G.711. These bandwidth calculations are based on using a PPP or Frame Relay header of 6 bytes. The numbers would change if a different Layer 2 header were used.
- **Using RTP-header compression:** When you use RTP-header compression (compressed RTP [cRTP]), the IP, User Datagram Protocol (UDP), and RTP header can be compressed to 2 or 4 bytes, compared to the 40 bytes that is required by these headers if cRTP is not used. cRTP is enabled per link on both ends of a point-to-point WAN link. It should be selectively used on a slow WAN link, typically less than 768 kbps. It does not need to be enabled end-to-end across all faster WAN links.
- **Deploying local annunciators or disabling remote annunciators:** If spoken announcements are not required, the use of annunciators can be disabled for Cisco IP Phones that do not have a local annunciator. Otherwise, local annunciators could be deployed. CUCM supports annunciators running only on CUCM servers for media provided by the IP Voice Streaming Application service. Therefore, local annunciators can be implemented only if a local CUCM cluster is deployed or if clustering over the IP WAN is being used.
- **Deploying local conference bridges:** If local conference bridges are deployed, the IP WAN is not used if all conference members are at the same site as the conference bridge.

- **Deploying local Media Termination Points (MTP):** If MTPs are required, they can be locally deployed at each site to avoid the need to cross the IP WAN when using MTP services.
- **Deploying transcoders or mixed conference bridges:** If low-bandwidth codecs are not supported by all endpoints, transcoders can be used so that low-bandwidth codecs can be used across the IP WAN. Then have the voice stream transcoded from G.729 to G.711. For conferences with local members using G.711 and remote members using low-bandwidth codecs, mixed conference bridges with digital system processor (DSP) hardware in a gateway can be deployed that support conference members with different codecs.

Note CUCM can perform conference calls with a software conference bridge only with the G.711 codec.

- **Deploying local Music On Hold (MOH) servers (requires a local CUCM server) or using multicast MOH from branch router flash:** Deploying local MOH servers means that CUCM servers have to be present at each site. In centralized call-processing models in which CUCM servers are not present at remote sites, it is recommended that you use multicast MOH from branch router flash. This eliminates the need to stream MOH over the IP WAN. If this is not an option, you should use multicast MOH instead of unicast MOH to reduce the number of MOH streams that have to traverse the IP WAN. Multicast MOH requires multicast routing to be enabled in the routed IP network.
- **Limiting the number of voice calls using CAC:** Use CAC with CUCM or a gatekeeper to avoid oversubscription of WAN bandwidth from too many voice calls.

Low-Bandwidth Codecs and RTP-Header Compression

In Figure 2-3, a voice packet for a call with the G.711 codec and a 20-ms packetization period is being passed along a Frame Relay WAN link. The RTP frame has a total size of 206 bytes, composed of 6 bytes of Frame Relay header, 20 bytes of IP header, 8 bytes of UDP header, 12 bytes of RTP header, and a 160-byte payload of digitized voice. The packet rate is 50 packets per second (pps), resulting in a bandwidth need of 82.4 kbps. Note that when compressed RTP (cRTP) is used, the bandwidth is considerably reduced to 11.2 or 12 kbps.

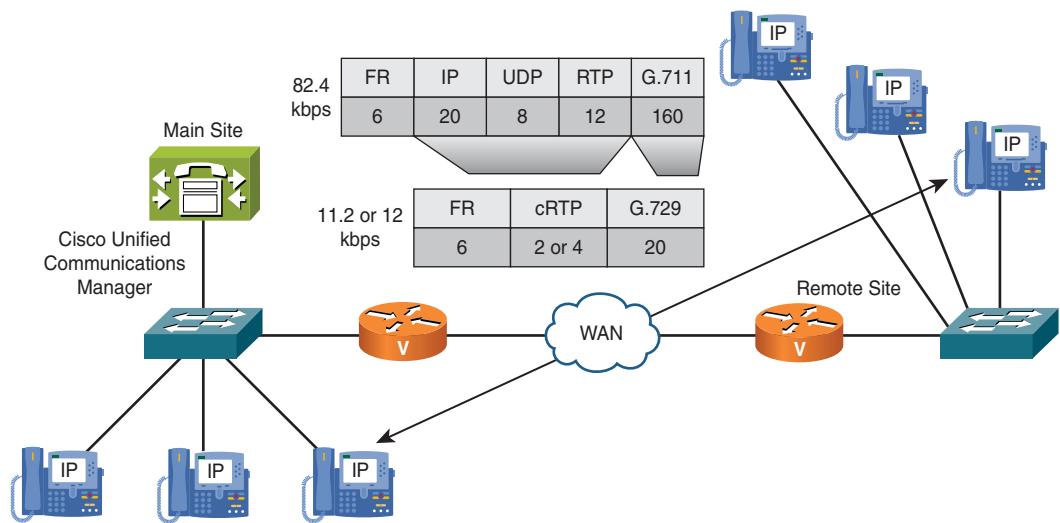


Figure 2-3 Low-Bandwidth Codecs and RTP-Header Compression

Note The traditional default codec with CUCM is G.711, with a 160-byte sample size and a 20-ms packet interval. G.722 is the newer default codec.

When you use cRTP and change the codec to G.729 with CUCM regions, the required bandwidth changes as follows: The frame now has a total size of 28 or 30 bytes per frame, composed of 6 bytes of Frame Relay header, 2 or 4 bytes of cRTP header (depending on whether the UDP checksum is preserved), and a 20-byte payload of digitized, compressed voice. The packet rate is still 50 pps (because the packetization period was not changed), resulting in bandwidth needs of 11.2 or 12 kbps.

Seven G.729 calls with cRTP enabled require less bandwidth than one G.711 call without cRTP (assuming that cRTP is used without preserving the UDP checksum).

Note While the audio codec configuration affects the end-to-end path, cRTP affects only those WAN links where cRTP is enabled. RTP header compression is configured on a per link basis on both routers in a point-to-point WAN connection.

Codec Configuration in CUCM

The codec that is used for a call is determined by the region configuration in CUCM. Each region in CUCM is configured with the codec that has the highest permitted bandwidth requirements:

- Within the configured region
- Toward a specific other region (manually configured)
- Toward all other regions (not manually configured)

Regions are assigned to device pools (one region per device pool), and a device pool is assigned to each device, such as a Cisco IP Phone. A Cisco IP Phone can be configured with a maximum of one device pool at any one time. The codec actually used depends on the capabilities of the two devices that are involved in the call. The assigned codec is the one that is supported by both devices; it does not exceed the bandwidth requirements of the codec permitted in region configuration. If devices cannot agree on a codec, a transcoder is invoked. However, if a transcoder is unavailable with different codecs configured, the audio call would fail.

Disabled Annunciator

Figure 2-4 shows how bandwidth can be conserved on the IP WAN by simply disabling annunciator RTP streams to remote phones.

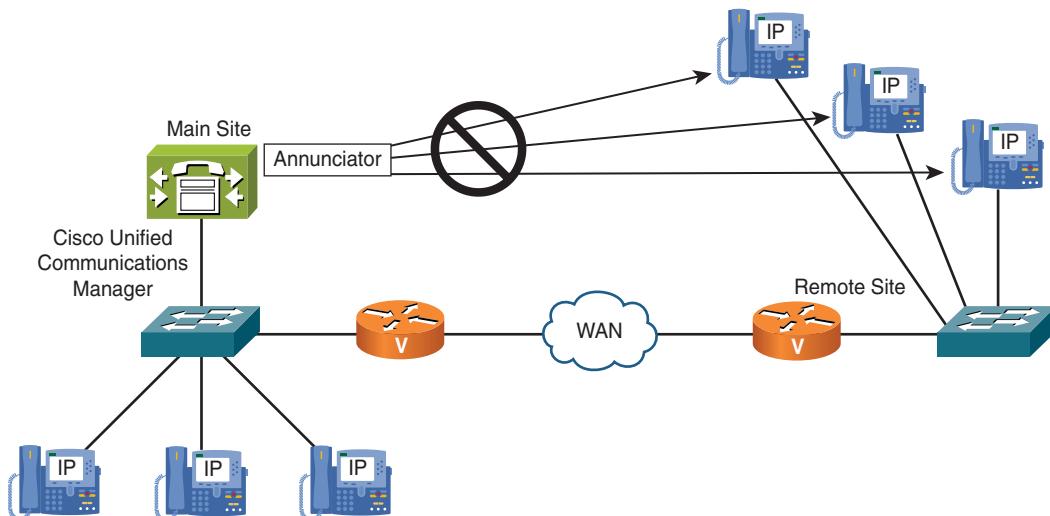


Figure 2-4 *Disabled Annunciator*

The annunciator is a CUCM feature that sends one-way audio of prerecorded messages over RTP to IP Phones. An example is the replacement to the fast busy reorder tone with the recorded message “Your call cannot be completed as dialed; please...” If announcements should not be sent over a saturated IP WAN link, Media Resource Group Lists (MRGL) can be used so that remote phones do not have access to the annunciator media resource, which can be implemented in a design like the one shown in Figure 2-4.

Note Because not every call requires annunciator messages, and because the messages usually are rather short, the bandwidth that may be preserved by disabling the annunciator is minimal.

Local Versus Remote Conference Bridges

As shown in Figure 2-5, if a local conference bridge is deployed at the remote site with the remote site gateway DSPs, it keeps voice streams off the IP WAN for conferences in which all members are physically located at the remote site. The same solution can be implemented for MTPs. MRGLs specify which conference bridge (or MTP) should be used and by which IP Phone.

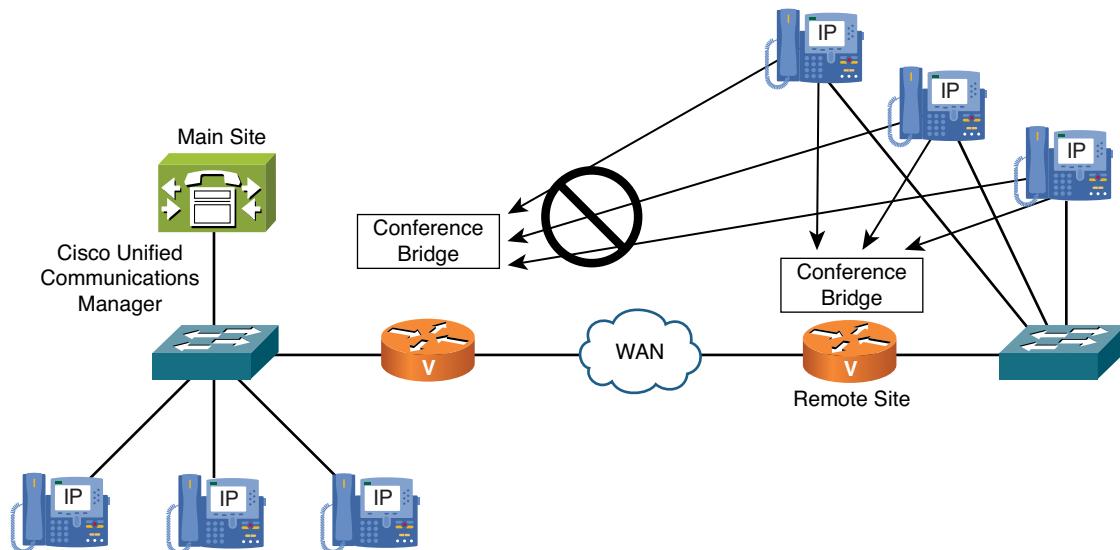


Figure 2-5 Local Versus Remote Conference Bridges

Transcoders

As shown in Figure 2-6, a voice-mail system that supports only G.711 is deployed at the main site. One CUCM server is providing a software conference bridge that also supports G.711 only. If remote Cisco IP Phones are configured to use G.729 over the IP WAN with CUCM regions to conserve WAN bandwidth, they would not be able to join conferences or access the voice-mail system. To allow these IP Phones to use G.729 and to access the G.711-only services, a hardware transcoder is deployed at the main site in the gateway using DSP resources.

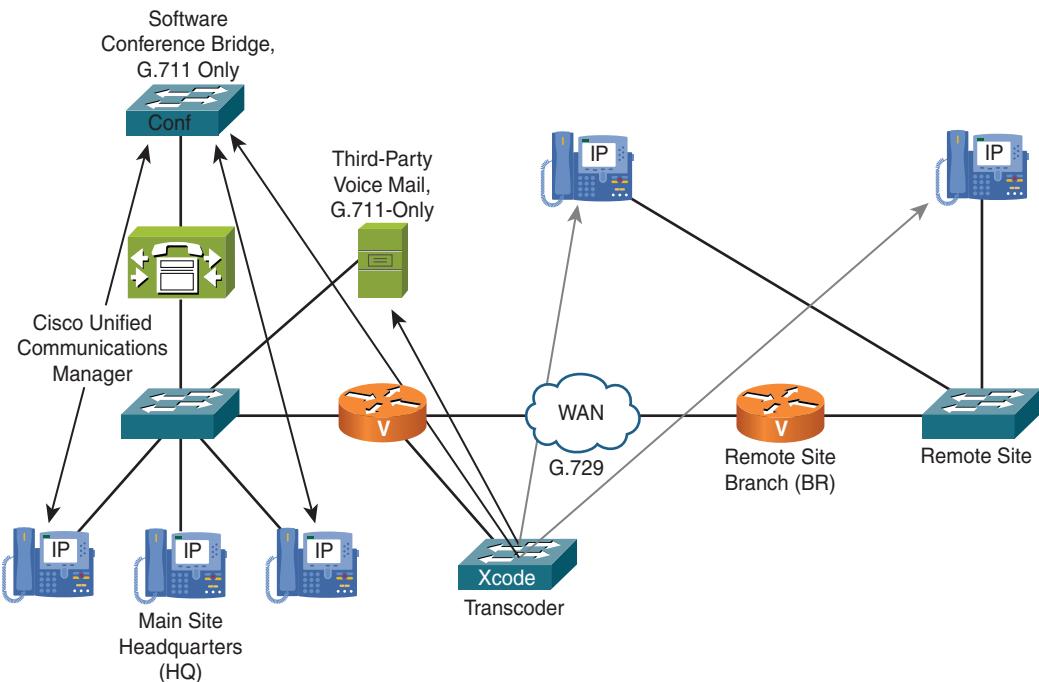


Figure 2-6 *Transcoders*

Remote Cisco IP Phones now send G.729 voice streams to the transcoder over the IP WAN, which saves bandwidth. The transcoder changes the stream to G.711 and passes it on to the conference bridge or voice-mail system, allowing the audio connection to work.

Guidelines for Transcoder Configuration

When implementing transcoders to allow G.711-only devices to communicate with remote IP Phones using G.729, consider the following guidelines:

- Step 1.** Implement the transcoding media resource. Because CUCM does not support software transcoding resources, the only option is to use a hardware-transcoding resource by first configuring the transcoder at the Cisco IOS router and then adding the transcoder to CUCM.
- Step 2.** Implement regions such that only G.729 is permitted on the IP WAN, and the transcoder can be used, if required. To do so, all IP Phones and G.711-only devices, such as third-party voice-mail systems or software conference bridges that are located in the headquarters, are placed in a region (such as headquarters). Remote IP Phones are placed in another region (such as BR). The transcoding resource is put into a third region (such as XCODER).

Step 3. Now the maximum codec for calls within and between regions must be specified:

- **Within BR—G.711:** This allows local calls between remote IP Phones to use G.711.
- **Within HQ—G.711:** This allows local calls within headquarters to use G.711. These calls are not limited to calls between IP Phones. This also includes calls to the G.711-only third-party voice-mail system or calls that use the G.711-only software conference bridge.
- **Within XCODER—G.711:** Because this region includes only the transcoder media resource, this setting is irrelevant, because there are no calls within this region.
- **Between BR and HQ—G.729:** This ensures that calls between remote IP Phones and headquarters devices, such as IP Phones, software conference bridges, and voice-mail systems, do not use the G.711 codec for calls that traverse the IP WAN.

Note Calls between IP Phones at headquarters and remote IP Phones do not require a transcoder. They simply use the best allowed codec that is supported on both ends from the CUCM region settings—ideally, G.729.

A transcoder is invoked only when the two endpoints of a call cannot find a common codec that is permitted by region configuration. This is the case in this example. The remote IP Phones (which support G.711 and G.729) are not allowed to use G.711 over the IP WAN, and the headquarters voice-mail system and software conference bridge do not support G.729. CUCM detects this problem based on its region configurations, and the capability negotiation performed during call setup signaling identifies the need for a transcoder.

- **Between BR and XCODER—G.729:** This ensures that the RTP streams between remote IP Phones and the transcoder, which are sent over the IP WAN, do not use G.711.
- **Between HQ and XCODER—G.711:** This is required for the G.711-only devices at headquarters to be allowed to send G.711 to the transcoder.

Mixed Conference Bridge

As illustrated in Figure 2-7, a hardware conference bridge is deployed at the main site gateway. The hardware conference bridge is configured to support mixed conferences, in which members use different codecs. Headquarters IP Phones that join the conference can use G.711, whereas remote IP Phones can join the conference using a low-bandwidth codec. The end result is a minimum WAN utilization with relatively high voice quality.

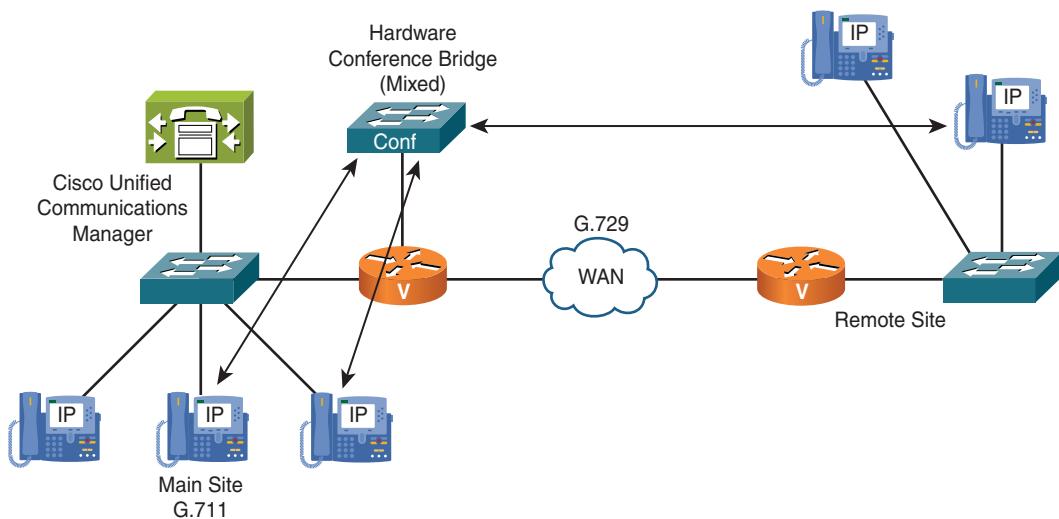


Figure 2-7 Mixed Conference Bridge

Multicast MOH from the Branch Router Flash

Multicast MOH from the branch router flash is a feature for multisite deployments that use centralized call processing.

The feature works only with multicast MOH and is based on MOH capabilities of Cisco Unified SRST. The Cisco IOS SRST gateway is configured for multicast MOH and continuously sends a MOH stream, regardless of its SRST mode (standby or fallback mode).

Neither CUCM nor the remote IP Phones are aware that the SRST gateway is involved. To them it appears as though a multicast MOH stream has been generated by the CUCM MOH server and received by the remote IP Phones.

Therefore, the remote Cisco IP Phones are configured to use the centralized CUCM MOH server as their MOH source. The CUCM MOH server is configured for multicast MOH (mandatory), and the max-hops value in the MOH server configuration is set to 1 for the affected audio sources. The max-hops parameter specifies the Time to Live (TTL) value that is used in the IP header of the RTP packets. The CUCM MOH server and the Cisco IOS SRST gateway located at the remote site have to use the same multicast address and port number for their streams. This way, MOH packets generated by the CUCM MOH server at the central site are dropped by the central-site router because the TTL has been exceeded. As a consequence, the MOH packets do not cross the IP WAN. The SRST gateway permanently generates a multicast MOH stream with an identical multicast IP address and port number so that the Cisco IP Phones simply listen to this stream as it appears to be coming from the CUCM MOH server.

Instead of setting the max-hops parameter for MOH packets to 1, you can use one of the following methods:

- Configure an access control list (ACL) on the WAN interface at the central site: This prevents packets that are destined for the multicast group address or addresses from being sent out the interface.
- Disable multicast routing on the WAN interface: Do not configure multicast routing on the WAN interface to ensure that multicast streams are not forwarded into the WAN.

Note Depending on the configuration of MOH in CUCM, a separate MOH stream for each enabled codec is sent for each multicast MOH audio source. The streams are incremented either based on IP addresses or based on port numbers (the recommendation is per IP address). Assuming that one multicast MOH audio source and G.711 a-law, G.711 mu-law, G.729, and the wideband codec are enabled, there will be four multicast streams. Make sure that all of them are included in the ACL to prevent MOH packets from being sent to the IP WAN.

When using multicast MOH from branch router flash, G.711 has to be enabled between the CUCM MOH server and the remote Cisco IP Phones. This is necessary because the branch SRST MOH feature supports only G.711. Therefore, the stream that is set up by CUCM in the signaling messages also has to be G.711. Because the packets are not sent across the WAN, configuring the high-bandwidth G.711 codec is no problem as long as it is enabled only for MOH. All other audio streams (such as calls between phones) that are sent over the WAN should use the low-bandwidth G.729 codec.

An Example of Multicast MOH from the Branch Router Flash

As illustrated in Figure 2-8, the CUCM MOH server is configured for multicast MOH with a destination Class D multicast group address of 239.1.1, a destination port 16384, and a max-hops TTL value of 1. Cisco recommends using an IP address in the range reserved for administratively controlled applications on private networks of 239.0.0.0 to 239.255.255.255.

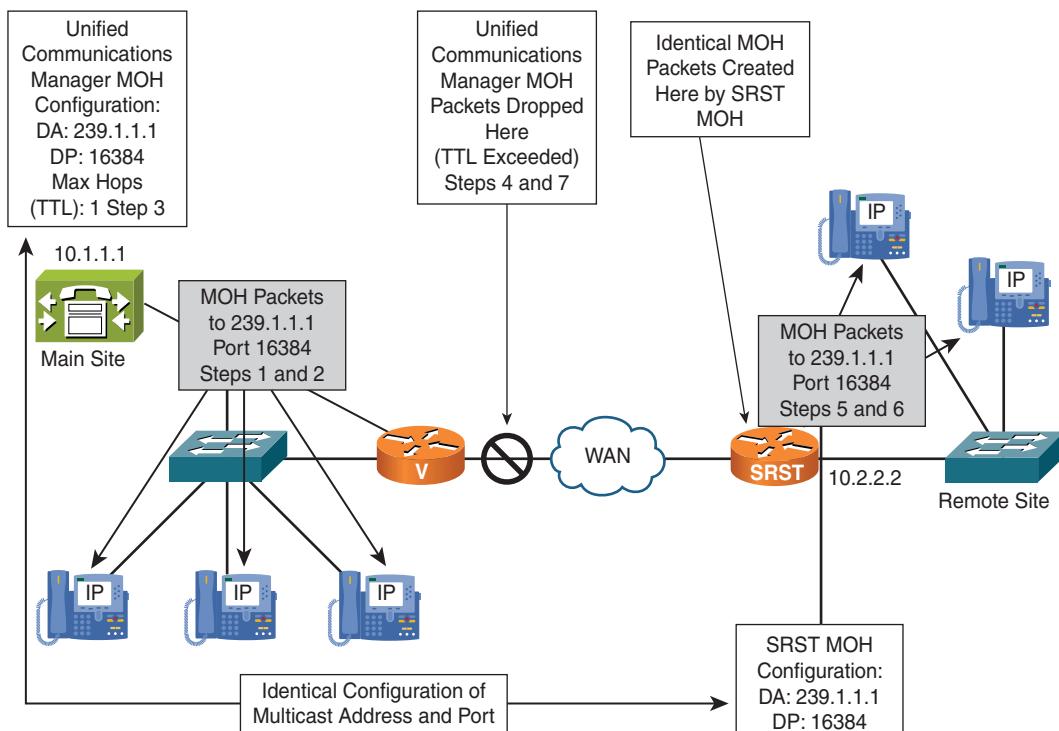


Figure 2-8 Multicast MOH from Remote Site Router Flash

The SRST gateway located at the remote site is configured with the same destination IP address and port number as the CUCM MOH server.

When a remote phone is put on hold, the following happens:

1. According to the MRGL of the remote phone, the CUCM MOH server is used as the media resource for MOH.
2. CUCM signals the IP Phone to receive MOH on IP address 239.1.1.1, port 16384.
3. The CUCM MOH server sends multicast MOH packets to IP address 239.1.1.1, port 16384, with a TTL value of 1.
4. The router located at the main site drops the multicast MOH packet sent by the CUCM MOH server because TTL has been exceeded.
5. The router at the remote site is configured as an SRST gateway. In its Cisco Unified SRST configuration, multicast MOH is enabled with destination address 239.1.1.1 and port 16384. The SRST gateway streams MOH all the time, even if it's not in fallback mode.

6. The IP Phones listen to the multicast MOH stream that was sent from the SRST gateway to IP address 239.1.1.1, port 16384, and play the received MOH stream.
7. Whether the remote gateway is in SRST mode, MOH packets never cross the IP WAN.

Note If an MOH file is used in router flash, only a single MOH file can be configured to play at a time. This is unlike CUCM, where many different MOH files can be configured.

An Example of Multicast MOH from the Branch Router Flash Cisco IOS Configuration

As shown in Figure 2-9, the name of the audio file on the branch router flash is moh-file.au, and the configured multicast address and port number are 239.1.1.1 and 16384, respectively. The optional **route** command can be used to specify a source interface address for the multicast stream. If no route option is specified, the multicast stream is sourced from the configured Cisco Unified SRST default address. This is specified by the **ip source-address** command under the Cisco Unified SRST configuration (10.2.2.2 in this example). Note that you can stream only a single audio file from flash and that you can use only a single multicast address and port number per router.

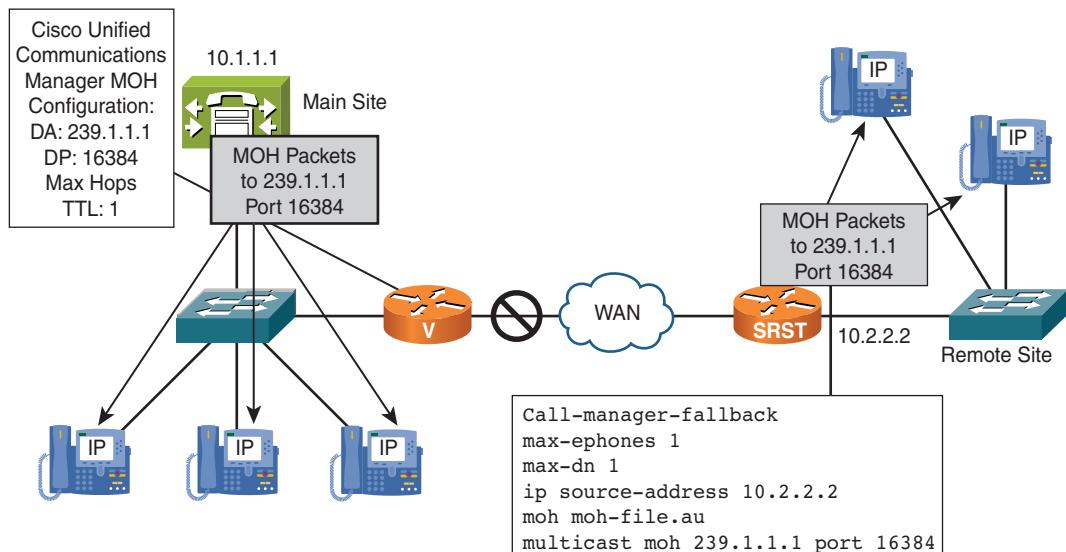


Figure 2-9 Multicast MOH from the Remote Site Router Flash Cisco IOS Configuration

A Cisco Unified SRST license is required regardless of whether the SRST functionality will actually be used. The license is required because the configuration for streaming multicast MOH from branch router flash is done in SRST configuration mode. Also, even if SRST functionality will not be used, at least one **max-ephones** for every Cisco IP

Phone supported and at least one **max-dn** for every directory number (dn) on all phones must be configured.

Alternatives to Multicast MOH from Remote Site Router Flash

Sometimes, multicast MOH from remote site router flash cannot be used. For instance, perhaps the remote site router does not support the feature or does not have a Cisco Unified SRST feature license. In that case, you can consider the following alternatives:

- **Using multicast MOH:** When you use multicast MOH over the IP WAN, the number of required MOH streams can be significantly reduced. Thus, less bandwidth is required compared to multiple unicast MOH streams. The IP network, however, has to support multicast routing for the path from the MOH server to the remote IP Phones.
- **Using G.729 for MOH to remote sites:** If multicast MOH is not an option (for instance, because multicast routing cannot be enabled in the network), you may still be able to reduce the bandwidth consumed by MOH. If you change the codec that is used for the MOH streams to G.729 and potentially enable cRTP on the IP WAN, each individual MOH stream requires less bandwidth and hence reduces the load on the WAN link. The bandwidth savings are identical to those that are achieved when using G.729 and cRTP for standard audio streams, which was discussed earlier. To use G.729 for MOH streams, the MOH server and the remote IP Phones have to be put into different regions, and the audio codec between these two regions must be limited to G.729.

Preventing Too Many Calls by CAC

CUCM allows the number of calls to be limited by these CAC mechanisms:

- **Locations:** CUCM location-based CAC is applicable to calls between two entities that are configured in CUCM. These entities can be endpoints, such as phones or devices, that connect to other call-routing domains, such as trunks or gateways. However, CAC applies to the devices that are part of the CUCM cluster, even if they represent an external call-routing domain (in case of trunks). If ingress and egress device are in different locations, the maximum bandwidth that is configured per location is checked at both ends. Calls within a location are not subject to the bandwidth limit.
- **Resource Reservation Protocol (RSVP)-enabled locations:** RSVP is a special way to configure locations. When RSVP is configured to be used between a pair of locations, the audio streams flow through two routers, also known as RSVP agents. The call leg between the two RSVP agents is subject to Cisco IOS RSVP CAC. As with standard locations, ingress and egress devices are both part of the CUCM cluster.
- **Session Initiation Protocol (SIP) Preconditions:** SIP Preconditions is a solution similar to RSVP-enabled locations, except that it is designed only for SIP trunks. With SIP Preconditions, calls through a SIP trunk flow through a local Cisco IOS router at each end of the SIP trunk, splitting the call into three call legs—just like with RSVP-enabled locations. In this case, however, the call is not within a cluster, but between clusters.

- **Gatekeepers:** Gatekeepers are an optional component used within the H.323 protocol and provide address resolution and CAC functions. H.323 gatekeepers can be configured to limit the number of calls between H.323 zones.

Availability

You can address availability issues in multisite deployments in several ways:

- **PSTN backup:** Use the PSTN as a backup for on-net intersite calls.
- **MGCP fallback:** Configure an MGCP gateway to fall back, and use the locally configured plain old telephone service (POTS), H.323, or session initiation protocol (SIP) dial peers when the connection to its call agent is lost. This effectively makes the gateway use a locally configured dial plan, which is ignored when the gateway is in MGCP mode. If H.323 is deployed, the dial peers have the same functionality in or out of SRST mode.
- **Fallback for IP Phones with SRST:** Cisco IP Phones using either SIP or SCCP must register to a call-processing device for the phones to work. IP Phones that register over the IP WAN can have a local Cisco IOS SRST gateway configured as a backup to a CUCM server in their CUCM group configuration. When the connection to the primary CUCM server is lost, they can reregister with the local SRST gateway. Alternatively, CUCM Express can be used in SRST mode, which provides more features than standard Cisco Unified SRST.
- **Call Forward Unregistered (CFUR):** This is a call-forwarding configuration of IP Phones that becomes effective when the IP Phone is not registered.

Note CFUR was introduced in CallManager version 4.2, and it appeared again in CUCM version 6 and later versions.

- **Automated Alternate Routing (AAR) and Call Forward on No Bandwidth (CFNB):** AAR allows calls to be rerouted over the PSTN when calls over the IP WAN are not admitted by CAC. CFNB is a call-forwarding configuration of IP Phones, which becomes effective when AAR is used.

Note AAR is configured for calls to and from IP Phones within the same cluster. Calls to a different cluster over a SIP or H.323 trunk do not use AAR. They are configured to fail over to the PSTN with CAC by configuring route groups and route lists with path selection within the route pattern.

- **Mobility solutions:** When users or devices roam between sites, they can lose features or have suboptimal configuration because of a change in their actual physical location. CUCM Extension Mobility and the Device Mobility feature of CUCM can solve such issues. In addition, Cisco Unified Mobility allows integration of cell

phones and home office phones by enabling reachability on any device via a single (office) number.

PSTN Backup

As shown in Figure 2-10, calls to the remote site within the same cluster are configured with AAR to use the IP WAN first, and then they use the PSTN as a backup option. The end result is reduced operating cost with toll bypass over the WAN, and successful delivery of the same calls over the PSTN but potentially at a higher operating cost if the WAN fails.

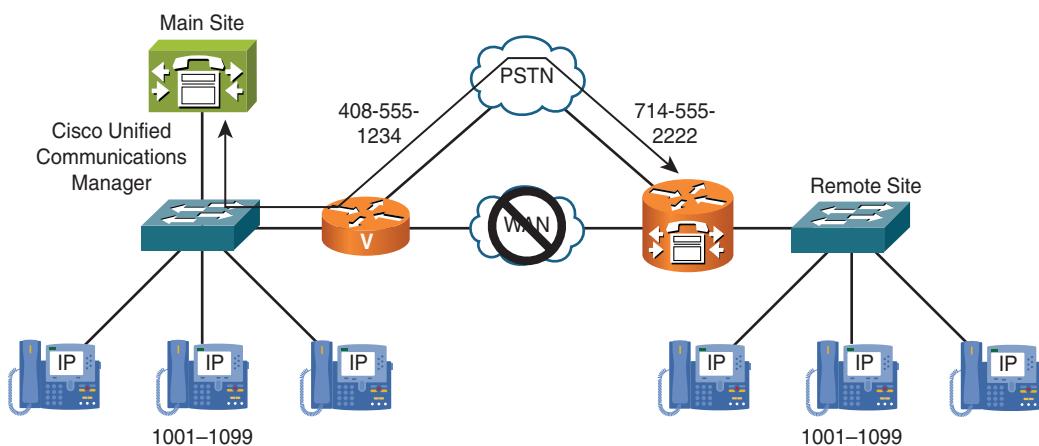


Figure 2-10 *PSTN Backup*

MGCP Fallback

MGCP gateway fallback is a feature that improves the availability of remote MGCP gateways.

A WAN link connects the MGCP gateway at a remote site to the CUCM at a main site, which is the MGCP call agent. If the WAN link fails, the fallback feature keeps the gateway working as an H.323 or SIP gateway and rehomes to the MGCP call agent when the WAN link becomes active again.

Figure 2-11 shows how MGCP fallback improves availability in a multisite environment.

The figure illustrates normal operation of MGCP fallback while the connectivity to the call agent (CUCM) is functional:

- The MGCP gateway is registered with CUCM over the IP WAN.
- CUCM is the call agent of the MGCP gateway that is controlling its interfaces. The gateway does not have (or does not use) a local dial plan because all call-routing intelligence is at the call agent. MGCP functions in a client/server model, with CUCM as the server and the gateway as the client.

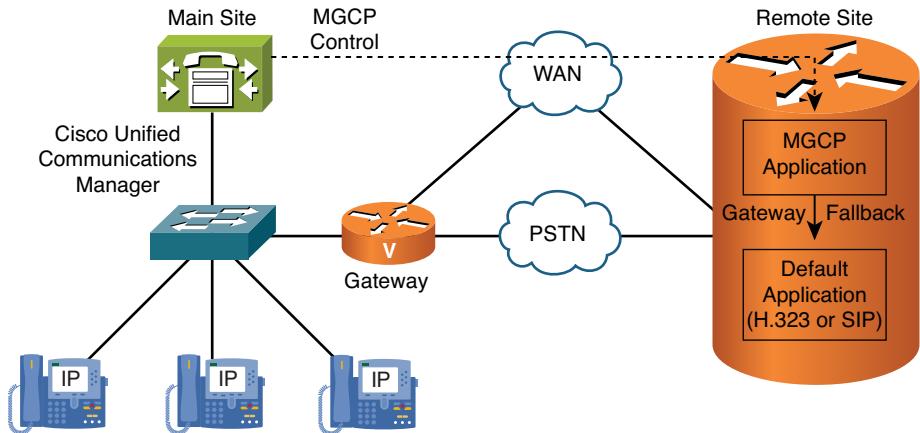


Figure 2-11 MGCP Fallback: Normal Operation

When the MGCP gateway loses the connection to its call agent, as shown in Figure 2-12, it falls back to its default call-control application (POTS, H.323, or SIP). The gateway now uses a local dial plan configuration, such as dial peers, voice translation profiles, and so on. Hence, it can operate independently of its MGCP call agent. Without MGCP fallback, the MGCP gateway would be unable to process calls when the connection to its call agent is lost.

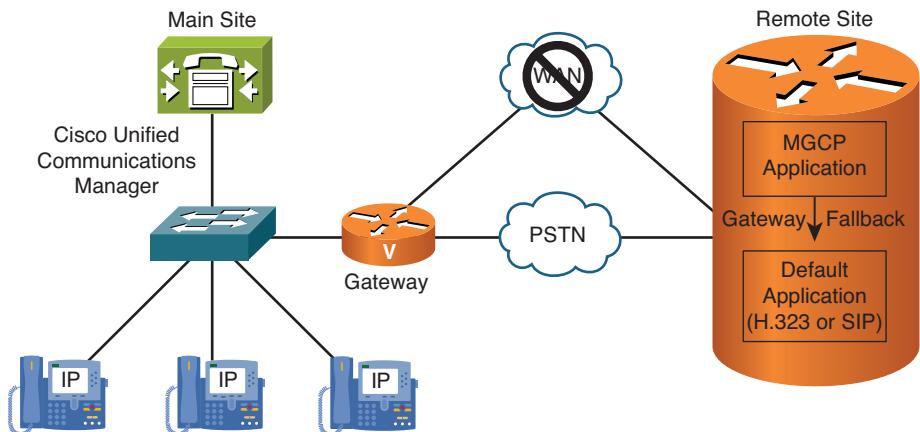


Figure 2-12 MGCP Fallback: Fallback Mode

Fallback for IP Phones

Fallback for IP Phones is provided by the SRST Cisco IOS feature and improves the availability of remote IP Phones.

A WAN link connects IP Phones at a remote site to the Cisco Communications Manager at a central site, which is the call-processing device. If the WAN link fails, Cisco Unified SRST enables the gateway to provide call-processing services for IP Phones. IP Phones register with the gateway (which is listed as a backup CUCM server in the server's group configuration of the IP Phones). The Cisco Unified SRST obtains the configuration of the IP Phones from the phones themselves and can route calls between the IP Phones or out to the PSTN.

Note When a Cisco IP Phone is in SRST mode, the configuration on the phone should never be erased, because the phone will not function until the connection to CUCM is restored.

Figure 2-13 shows how fallback for IP Phones improves availability in a multisite deployment with centralized call processing.

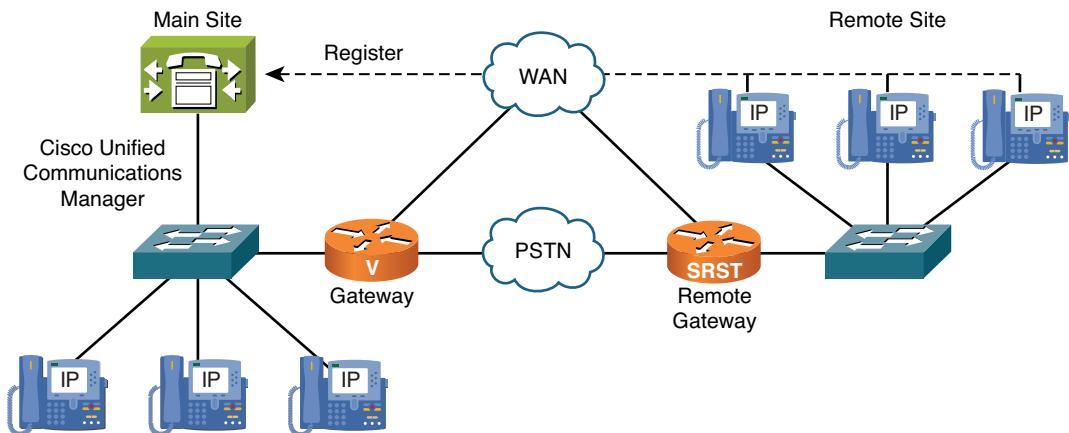


Figure 2-13 Fallback for IP Phones: Normal Operation

This figure illustrates normal operation of Cisco Unified SRST while the connectivity between IP Phones and their primary server (CUCM) is functional:

- Remote IP Phones are registered with CUCM over the IP WAN.
- CUCM handles call processing for IP Phones.

When Cisco IP Phones lose contact with CUCM, as shown in Figure 2-14, they register with the local Cisco Unified SRST router to sustain the call-processing capability necessary to place and receive calls.

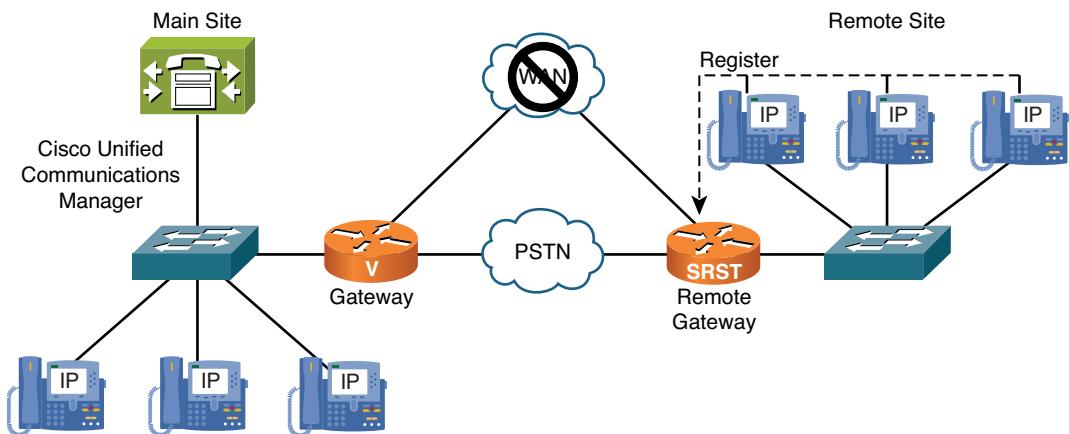


Figure 2-14 Fallback for IP Phones: Fallback Mode

When the WAN connection between a router and the CUCM fail or when connectivity with CUCM is lost for any reason, Cisco Unified IP Phones in the remote site become unusable for the duration of the failure. Cisco Unified SRST overcomes this problem and ensures that the Cisco Unified IP Phones offer continuous (although minimal) service by providing call-handling support for Cisco Unified IP Phones directly from the Cisco Unified SRST router. The system automatically detects a failure and uses Simple Network Auto Provisioning (SNAP) technology to autoconfigure the remote site router to provide call processing for Cisco Unified IP Phones that are registered with the router. When the WAN link or connection to the primary CUCM is restored, call handling reverts back to the primary CUCM.

CUCM Express in SRST mode can be used instead of standard Cisco Unified SRST functionality. In this case, IP Phones register with CUCM Express when they lose connection to their primary CUCM server. CUCM Express in SRST mode provides more features than standard Cisco Unified SRST.

Using CFUR to Reach Remote Site Cisco IP Phones During WAN Failure

As discussed, IP Phones located at remote locations can use an SRST gateway as a backup for CUCM in case of IP WAN failure. The gateway can use its local dial plan to route calls destined for the IP Phones in the main site over the PSTN. But how should intersite calls be routed from the main to the remote site while the IP WAN is down?

The problem in this case is that CUCM does not consider any other entries in its dial plan if a dialed number matches a configured but unregistered directory number. Therefore, if users at the main site dial internal extensions during the IP WAN outage, their calls fail (or go to voice mail). To allow remote IP Phones to be reached from the IP Phones at the main site, configure CFUR for the remote-site phones, as shown in Figure 2-15. CFUR should be configured with the PSTN number of the remote-site gateway so that internal calls for remote IP Phones get forwarded to the appropriate PSTN number.

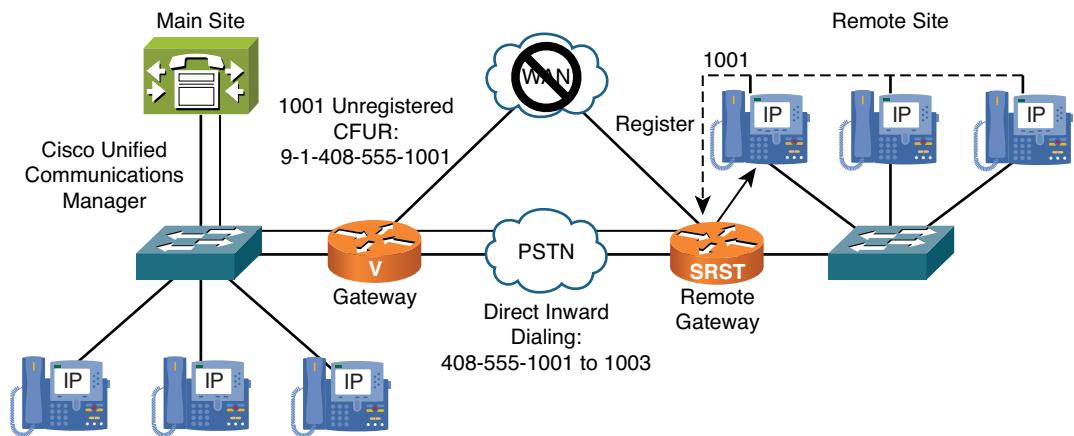


Figure 2-15 Using CFUR to Reach Remote-Site IP Phones over the PSTN During WAN Failure

Using CFUR to Reach Users of Unregistered Software IP Phones on Their Cell Phones

If a mobile user has a laptop with a softphone (for instance, Cisco IP Communicator or Cisco Unified Personal Communicator) and the user shuts down the laptop, CFUR can forward calls placed to the softphone to the user's cell phone, as illustrated in Figure 2-16. The user does not have to set up Call Forward All (CFA) manually before closing the soft-phone application. However, if the softphone is not registered, calls are forwarded to the user's cell phone. This is another application of the CFUR feature that improves availability in CUCM deployments.

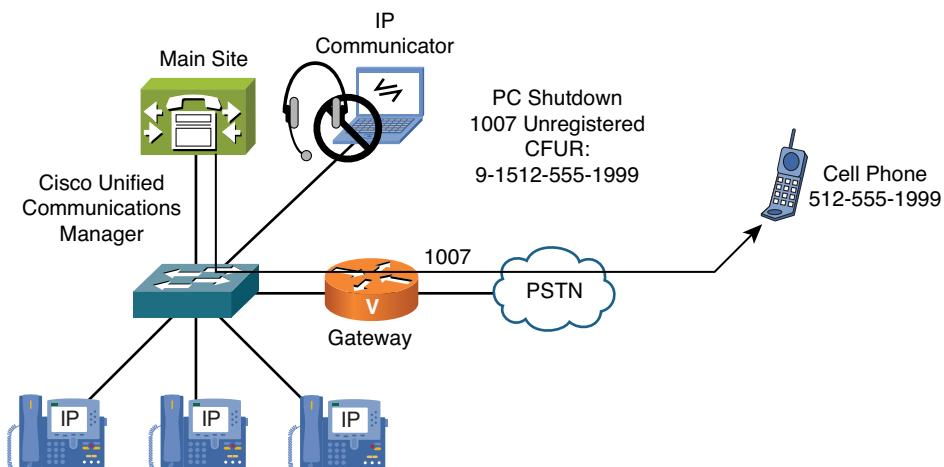


Figure 2-16 Using CFUR to Reach Users of Unregistered Software IP Phones on Their Cell Phones

Note This application is for CFUR, which is not related to SRST.

AAR and CFNB

If a call over the IP WAN to another IP Phone in the same cluster is not admitted by CAC, the call can be rerouted over the PSTN using AAR, as shown in Figure 2-17. The AAR feature includes a CFNB option that allows the alternative number to be set for each IP Phone. In the example, because the remote site does not have PSTN access, the call is not rerouted to the IP Phone over the PSTN (instead of over the IP WAN). It is alternatively rerouted to the cell phone of the affected user. AAR and CFNB improve availability in multisite environments by providing the ability to reroute on-net calls that failed CAC over the PSTN.

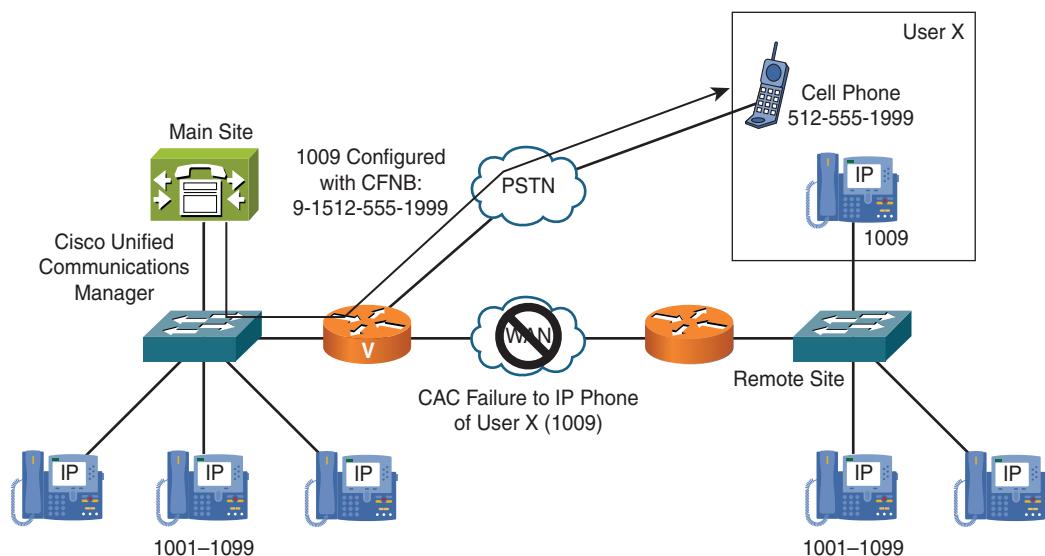


Figure 2-17 AAR and CFNB

Mobility Solutions

This section provides an overview of mobility solutions that solve issues that are the result of roaming users and devices and multiple telephones (office phone, cell phone, home phone, and so on).

When users or devices roam between sites, issues arise that can be solved by mobility solutions:

- **Device Mobility:** Solves issues caused by roaming devices, including invalid device configuration settings such as regions, locations, SRST reference, AAR groups,

Calling Search Spaces (CSS), and so on. The Device Mobility feature of CUCM allows device settings that depend on the physical location of the device to be automatically overwritten if the device appears in a different physical location.

- **CUCM Extension Mobility:** Solves issues that are the result of roaming users using shared guest IP phones located in other offices. Issues include wrong directory number, missing IP Phone service subscriptions, CSS, and so on. CUCM Extension Mobility allows users to log in to guest phones and replace the IP phone's configuration with the IP Phone configuration of the logged-in user.
- **Cisco Unified Mobility:** Solves issues of having multiple phones and consequently multiple phone numbers, such as an office phone, cell phone, home (office) phone, and so on. Cisco Unified Mobility allows users to be reached by a single number, regardless of the phone that is actually used.

Note All these mobility features are explained in detail in Chapter 10, “Implementing Device Mobility,” and Chapter 11, “Implementing Extension Mobility.”

Dial Plan Solutions

Dial plan issues in multisite deployments can be solved in the following ways:

- **Overlapping and nonconsecutive numbers:** You can implement access codes and site codes for intersite dialing. This allows call routing that is independent of directory numbers. Appropriate digit manipulation (removing site codes in Dialed Number Identification Service [DNIS] of outgoing calls) and prefixing site codes in Automatic Number Identification (ANI) of incoming calls are required.
- **Variable-length numbering plans:** Dial string length is determined by timeout. Overlap sending and receiving is enabled, allowing dialed digits to be signaled one by one instead of being sent as one whole number.
- **Direct inward dialing (DID) ranges and E.164 addressing:** Solutions for mapping of internal directory numbers to PSTN numbers include DID, use of attendants to transfer calls, and extensions added to PSTN numbers in variable-length numbering plans.
- **Different number presentation in ISDN (Type of Number [TON]):** Digit manipulation based on TON enables the standardization of numbers signaled using different TONs.
- **Toll bypass, tail-end hop-off (TEHO), and PSTN backup:** Can be implemented by appropriate call routing and path selection based on priorities.

Dial Plan Components in Multisite Deployments

Table 2-1 lists dial plan components and their configuration elements in CUCM and in Cisco IOS gateways.

Table 2-1 Fixed Versus Variable-Length Numbering Plans

Dial Plan Component	Cisco IOS Gateway	CUCM
Endpoint addressing	ephone-dn, dynamic POTS, dial peers	Directory number
Call routing and path selection	Dial peers	Route patterns, route groups, route lists, translation patterns, partitions, CSSs
Digit manipulation	Voice translation profiles prefix, digit-strip, forward-digits, num-exp	Translation patterns, route patterns, route lists, significant digits
Calling privileges	COR and COR lists	Partitions, CSSs, time schedules, time periods, FACs
Call coverage	Dial peers, call applications, ephone hunt groups	Line groups, hunt lists, hunt pilots

Note All these elements are discussed in other books, such as *Cisco Voice over IP and QoS (CVOICE)* and *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1 v8.0)*. Information on how to use these elements to implement a dial plan in multisite deployments is provided in Chapter 4, “Implementing a Dial Plan for International Multisite Deployments.”

Globalized Call-Routing Overview

Globalized call routing simplifies the implementation of international CUCM deployments.

Globalized call routing consists of the following main components:

- **Normalization:** Localized call ingress (that is, local dial rules) is normalized to a common format (E.164 with + prefix). This action would not be necessary if all endpoints and users dialed destinations only in a normalized format (like + dialing from directories). However, it is unlikely that only + dialing would be permitted. When manually typing a number, users still want to follow their local dial rules; therefore, normalization of this input is required.
- **Routing based on global numbers:** When all dialed numbers are globalized to an E.164 format, local dial rules do not apply during call routing. They were relevant only during call ingress. All call routing is based on numbers in a globalized format.
- **Localization of numbers before handing off the call:** After call routing and path selection, the local dial rules of the selected device have to be used. For example, when a user calls an international PSTN destination through a U.S. gateway, 011 has to be prefixed to the number, whereas in Europe, 00 is commonly used. Localized call egress is implemented at the gateway or trunk that routes the call out of the cluster.

In general, call routing is based on *normalized numbers*. As mentioned earlier, the most common format that is used is the globalized format, where both the called- and calling-party numbers are globalized for calls that are not exclusively internal. For such internal calls, internal directory numbers can be used as long as they are unique. If, for example, overlapping directory numbers are used, it is common to use the globalized format also for routing such intersite calls. End users do not have to dial phones at other sites by using the E.164 format, but their localized ingress (typically including site codes) will be globalized before the call is routed.

Assuming that all internal directory numbers are unique, this format is the most common:

- **Normalized called-party numbers:** E.164 global format with a + prefix is used for external destinations. Therefore, called-number normalization is achieved by globalization. Internal directory numbers are used for internal destinations. Normalization is achieved by stripping or translating the called number to internally used directory numbers.
- **Normalized calling-party numbers:** E.164 global format with a + prefix is used for all calling-party numbers, except for those formats of calls from internal to internal. Such purely internal calls use the internal directory number for the calling-party number.

If sources of calls (users at phones, incoming PSTN calls at gateways, calls received through trunks, and so on) do not use normalized format, the localized call ingress needs to be normalized before being routed. This principle applies to all received calls (coming from gateways, trunks, and phones), and it applies to both the calling- and called-party numbers.

Note Except for the mentioned internal calls (where the destination is a directory number and, in the case of an internal source, the source is a directory number), all numbers are normalized to E.164 global format. Therefore, this call-routing implementation model is referred to as *globalized call routing*.

After the call is routed and path selection (if applicable) is performed, the destination device might need to change the normalized numbers to a local format. This situation is referred to as *localized call egress*.

Localized call egress applies to these kinds of numbers:

- **Calling- and called-party numbers for calls that are routed to gateways and trunks:** If the PSTN or the telephony system on the other side of a trunk does not support globalized call routing, the called- and calling-party numbers need to be localized from a global format. An example would be to change the called-party number (in E164 format) +494012345 to 011494012345 before sending the call out to the PSTN in the United States.
- **Calling-party numbers for calls that are routed from gateways or trunks to phones:** The phone user may want to see caller IDs in a local format rather than a

global format. For example, a user at a U.S. phone might want to see PSTN callers who are located in the same area code as 7- or 10-digit numbers and not with +1 followed by 10 digits.

Localized call egress is not needed for the called-party number of calls that are routed to phones, because internal directory numbers are the standard (normalized) format for internal destinations (regardless of the source of the call). These numbers might have been dialed differently initially. In that case, however, this localized call ingress was normalized before call routing. Localized call egress is also not required for the calling-party number of internal calls (internal to internal), because typically, the standard for the calling-party number of such calls is to use internal directory numbers.

Note When internal directory numbers are not unique (for example, when there are overlapping directory numbers at various sites), the called- and calling-party numbers of internal calls can be globalized at call ingress and localized at call egress just like external calls.

Globalized Call Routing: Three Phases

Figure 2-18 provides an overview about the three phases involved in globalized call routing.

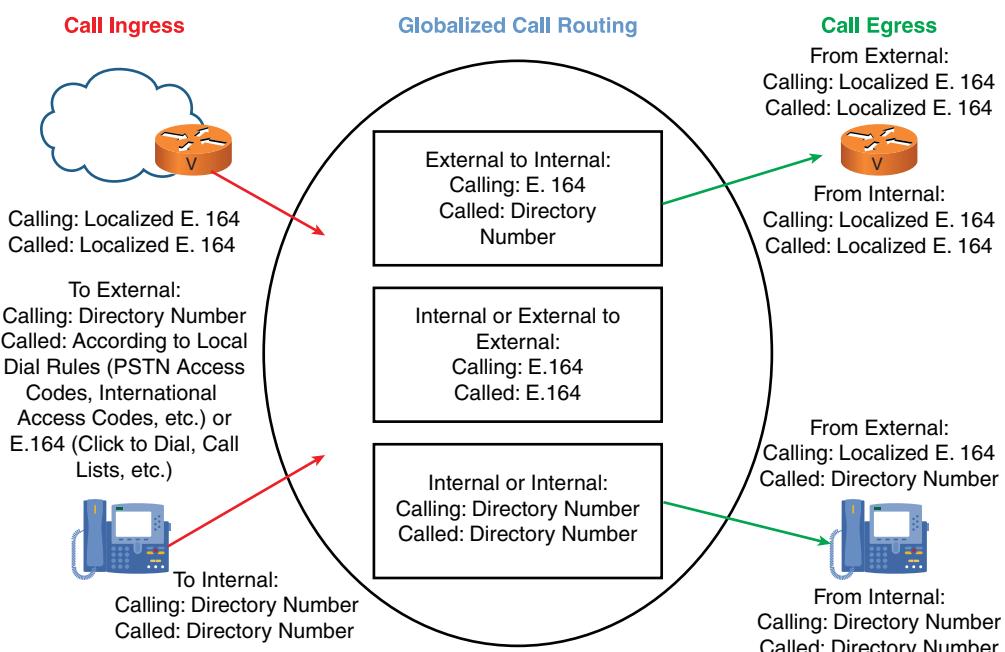


Figure 2-18 Three Phases of Global Call Routing

On the left side of the figure, call ingress is illustrated by two types of call sources:

- **External callers:** Their calls are received by CUCM through a gateway or trunk. In a PSTN gateway, calling- and called-party numbers are usually provided in a localized E.164 format.
- **Internal callers:** Their calls are received from internal phones. If a call is placed to an internal destination (for example, phone to phone), calling- and called-party numbers are typically provided as internal directory numbers. If a call is placed to an external destination (for example, phone to PSTN), the calling number is the directory number (at call ingress time), and the called number depends on the local dial rules for PSTN access. These dial rules can differ significantly per location.

The center of the figure illustrates the standards that are defined for normalized call routing. As mentioned earlier, because most calls use the global E.164 format, this process is also referred to as globalized call routing. Here are the defined standards:

- External to internal:
 - Calling-party number: E.164
 - Directory number
- External to external (if applicable):
 - Calling-party number: E.164
 - Called-party number: E.164
- Internal to internal:
 - Calling-party number: Directory number
 - Directory number
- Internal to external:
 - Calling-party number: E.164
 - Called-party number: E.164

At the right side of the figure, call egress is illustrated by two types of call targets:

- **Gateways:** When sending calls to the PSTN, the localized E.164 format is used for both the calling and the called-party number. The format of these numbers (especially of the called-party number) can significantly differ based on the location of the gateway (for example, various international access codes in the United States [011] versus the EU [00]).
- **Phones:** When a call from an internal phone is sent to another internal phone, the call should be received at the phone with both the calling and called number using internal directory numbers. Because this format is also used by globalized call routing, there is no need for localized call egress in this case. When a call from an external

caller is sent to an internal phone, most users (especially users in the United States) prefer to see the calling number in localized format. For example, a call from the local area code should be displayed with seven digits. The called number is the directory number and usually is not displayed at the phone.

It is evident from Figure 2-18 that, in several situations, the numbers that are provided at call ingress do not conform to the normalized format to be used for call routing. The same situation occurs with call egress, where the normalized format is not always used when the call is being delivered. Therefore, localized call ingress has to be *normalized* (that is, globalized), and globalized format has to be *localized* at *call egress*.

Globalized Call Routing Advantages

The following are several advantages of globalized call routing that are especially applicable to international multisite deployments:

- **Universal format to store or configure PSTN numbers:** With globalized call routing, you can configure or save all PSTN numbers in a universal format that you can use worldwide, regardless of local PSTN dial rules.
- **PSTN destinations that are configured in CUCM and are independent of the site that is used for dial-out:** Speed dials, fast dials, call forward destinations, AAR destinations, and Cisco Unified Mobility remote destinations share the same format. Because all call routing is based on this format, calls to these numbers work from anywhere within the cluster, regardless of the requirements of the local PSTN gateway.
- **Transformation of input at call ingress:** When implementing globalized call routing, you can allow end users to manually dial numbers as they normally do. If you globalize their localized input during the call, any input format can be supported, while call routing itself is based on a standardized format.
- **Localization at call egress:** The various requirements that are applicable at various egress devices can be easily managed during call egress (that is, after call routing and path selection) by using features such as global transformations that allow digit manipulation at the egress device, regardless of the matched route pattern and route list.
- **Utilization across different devices:** Address book entries can be shared by all devices that support E.164 format and the + prefix. This situation allows the utilization of centralized directories regardless of the used endpoint. For example, cell phones and CUCM can synchronize their directories from one and the same source (for example, a Lightweight Directory Access Protocol [LDAP] directory like Microsoft Active Directory).
- **Localization of calling-party numbers at phones:** Caller IDs displayed at phones can be localized so that the end users are not limited to seeing all callers in a globalized format. Again, global transformations (of the calling-party number only, in this case) can be used so that caller IDs, which might be different at each site, are displayed in the desired format. Similarly, the globalized calling-party number is also

maintained in call lists so that users can place callbacks to globalized numbers without needing to edit the number.

- **Substantial simplification of dial plans:** With local route groups and global transformations, globalized call routing drastically reduces the size and complexity of dial plans. Features such as TEHO, AAR, SRST, CFUR, Cisco Device Mobility, and Cisco Extension Mobility can be implemented much more easily in international deployments.

NAT and Security Solutions

When CUCM servers and IP Phones need to connect to the Internet, Cisco Unified Border Element can be used as an application proxy. When used in this way, Cisco Unified Border Element splits off-net calls inside the CUCM cluster and outside the cluster in the PSTN into two separate call legs. Cisco Unified Border Element also features signaling interworking from SIP to SIP, SIP to H.323, H.323 to SIP, and H.323 to H.323.

Note Cisco Unified Border Element (CUBE) used to be called Cisco IP to IP Gateway.

The CUBE can function in two modes:

- **Flow-around:** In this mode, only signaling is intercepted by CUBE. Media exchange occurs directly between endpoints (and flows around CUBE). Only signaling devices (CUCM) are hidden from the outside.
- **Flow-through:** In this mode, signaling and media streams are both intercepted by CUBE (flowing through CUBE). Both CUCM and IP Phones are hidden from the outside.

In flow-through mode, only CUBE needs to have a public IP address, so NAT and security issues for internal devices (CUCM servers and IP Phones) are solved. Because CUBE is exposed to the outside, it should be hardened against attacks.

CUBE in Flow-Through Mode

In Figure 2-19, CUCM has a private IP address of 10.1.1.1, and the Cisco IP Phone has a private IP address of 10.2.1.5 with a subnet mask of 255.0.0.0. A CUBE connects the CUCM cluster to the outside world—in this case, to an Internet telephony service provider (ITSP). The CUBE is configured in flow-through mode and uses an internal private IP address of 10.3.1 and an external public IP address of A.

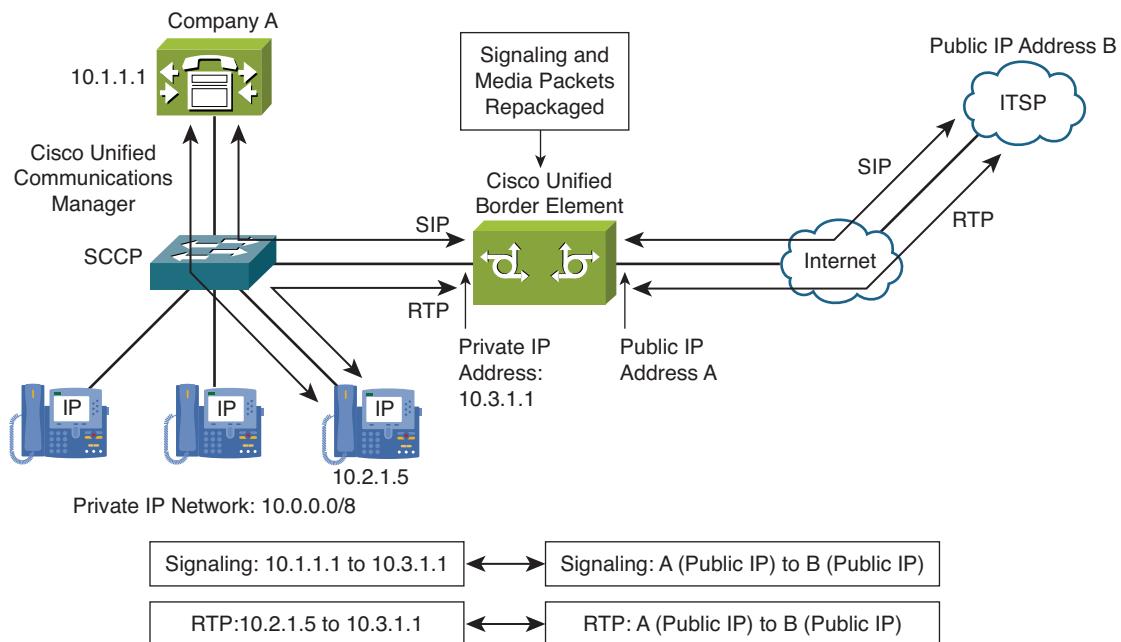


Figure 2-19 CUBE in Flow-Through Mode

When CUCM wants to signal calls to the ITSP, it does not send the packets to the IP address of the ITSP (IP address B). Instead, it sends them to the internal IP address of the CUBE(10.3.1.1) via a SIP trunk configuration. CUBE then establishes a second call leg to the ITSP using its public IP address A as the source and IP address B (ITSP) as the destination. As soon as the call is set up, the CUBE terminates RTP toward the ITSP using its public IP address and sends the received RTP packets to the internal IP Phone using its internal IP address.

This solution allows CUCM and IP Phones to communicate only with the internal, private IP address of the CUBE. The only IP address visible to the ITSP or anyone sniffing traffic on the outside is the public IP address of CUBE.

Summary

The following key points were discussed in this chapter:

- Multisite deployment solutions include QoS, efficient use of IP WAN bandwidth, backup scenarios in case of WAN failure, access and site codes, and the use of the Cisco Unified Border Element.
- QoS allows certain communication flows to be processed with higher priority than others.

- Bandwidth can be conserved by using low-bandwidth codecs, deploying mixed conference bridges or transcoders, using RTP-header compression, and deploying local media resources.
- CUCM availability features include fallback for Cisco IP Phones, CRUR, AAR, and CFNB, and mobility features such as Device Mobility, Extension Mobility, and Cisco Unified Mobility.
- Multisite dial plan solutions are built using Cisco IOS gateway and CUCM dial plan tools.
- Globalization of phone numbers into an E.164 format is the foundation of a consistent international dial plan.
- A CUBE in flow-control mode hides internal devices such as CUCM and IP Phones from the outside public Internet.

References

For additional information, refer to these resources:

Cisco Unified Communications Solution Reference Network Design (SRND), based on CUCM release 8.x.x, April 2010.

CUCM Administration Guide Release 8.0(1), February 2010.

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in Appendix A, "Answers Appendix."

1. Which of the following best describes QoS as a solution for multisite environments?
 - a. Ensuring reliable PSTN calls
 - b. Ensuring that all forms of IP traffic receive excellent performance
 - c. Ensuring excellent data performance
 - d. Ensuring that selected traffic such as RTP audio traffic receives excellent performance at the expense of lower-priority traffic
2. Which two of the following statements about bandwidth solutions in a multisite deployment are true?
 - a. RTP header compression compresses the RTP header to 1 byte.
 - b. WAN bandwidth can be conserved by using low-bandwidth codecs within a remote site.
 - c. WAN bandwidth can be conserved by deploying local media resources.
 - d. Voice payload compression is part of RTP header compression.

- e. Multicast MOH from branch router flash eliminates the need to send MOH over the WAN.
- 3. Which two of the following statements about availability are true?
 - a. CFNB is required to enable main-site phones to call remote site phones during SRST fallback.
 - b. SRST provides fallback for Cisco IP Phones in the event of a WAN failure.
 - c. MGCP fallback allows the gateway to use local dial peers when the call agent cannot be reached.
 - d. AAR is required to enable phones to reroute calls to another CUCM cluster over the PSTN when the IP WAN is down.
 - e. MGCP fallback and SRST cannot be implemented at the same device.
- 4. Which two of the following are not relevant dial plan solutions for multisite CUCM deployments?
 - a. Access and site codes
 - b. TEHO
 - c. PSTN backup
 - d. Shared lines
 - e. Overlap signaling
- 5. Which Cisco IOS feature provides a signaling and media proxy function that addresses the need for NAT?
 - a. Cisco Unified Border Element
 - b. Cisco PIX Firewall
 - c. CUCM
 - d. Cisco ASA
- 6. Which of the following most accurately describes the difference between flow-around and flow-through modes for CUBE?
 - a. Signaling is intercepted in both modes, but media is intercepted only in flow-through.
 - b. Both modes intercept media and signaling.
 - c. Both modes intercept only media.
 - d. Both modes intercept only signaling.

7. Which of the following two protocol conversions are supported by CUBE?
 - a. SCCP to SIP
 - b. H.323 to SIP
 - c. SIP to H.323
 - d. SIP to MGCP
 - e. MGCP to SCCP
8. What is the best description of MGCP fallback?
 - a. If CUCM fails, MGCP fails over to SCCP dial peers for PSTN dialing.
 - b. IF CUCM fails, MGCP fails over to MGCP dial peers for PSTN dialing.
 - c. IF CUCM fails, MGCP fails over to H.323 dial peers for PSTN dialing.
 - d. IF CUCM fails, all PSTN dialing fails.
9. What is the best benefit of multicast for MOH in a branch router?
 - a. Multiple MOH files can be used in router flash in an SRST configuration.
 - b. Router flash is not needed for MOH files, because the branch phones send multicast MOH to each other.
 - c. MOH has only one stream of RTP to all listeners with Multicast.
 - d. MOH has several streams of RTP to all listeners to ensure optimal voice quality.
10. What is the best benefit of standardizing on E.164 numbering?
 - a. E.164 only requires five digits.
 - b. E.164 provides a standard of numbering that aligns with an international dial plan.
 - c. E.164 numbering supports the + symbol, which can be dialed directly on Cisco IP Phones.
 - d. E.164 is mandatory for TEHO in CUCM v8.

This page intentionally left blank

Chapter 3

Implementing Multisite Connections

Upon completing this chapter, you will be able to configure gateways and trunks in multisite environments. You will be able to meet the following objectives:

- Identify the characteristics of the trunk and gateway types supported by CUCM
- Describe and implement MGCP gateways
- Describe and implement H.323 gateways
- Describe and configure Cisco IOS H.323 gateways
- Describe how to configure H.323 gateways in CUCM
- Understand different types of trunks supported by CUCM
- Describe and implement SIP trunks in CUCM
- Describe and implement intercluster, H.225, and gatekeeper-controlled intercluster trunks in CUCM

Cisco Unified Communications Manager (CUCM) multisite deployments can use a variety of connection options between sites. This chapter describes connection options and explains how to configure them.

Examining Multisite Connection Options

Multisite environments have several connection options. Figure 3-1 shows a CUCM cluster at the main site, with three connections to other sites.

The connections are as follows:

- Intercluster trunk (H.323) to another CUCM cluster located at a different site.
- An H.323 gateway located at a remote site.
- A Session Initiation Protocol (SIP) trunk connected to an Internet Telephony Service

Provider (ITSP) via a Cisco Unified Border Element (CUBE), which also has a SIP trunk to CUCM.

- At the remote location, a Media Gateway Control Protocol (MGCP) gateway is configured to be controlled by the remote cluster CUCM.

Figure 3-1 shows an example of different protocols in a multisite connection environment.

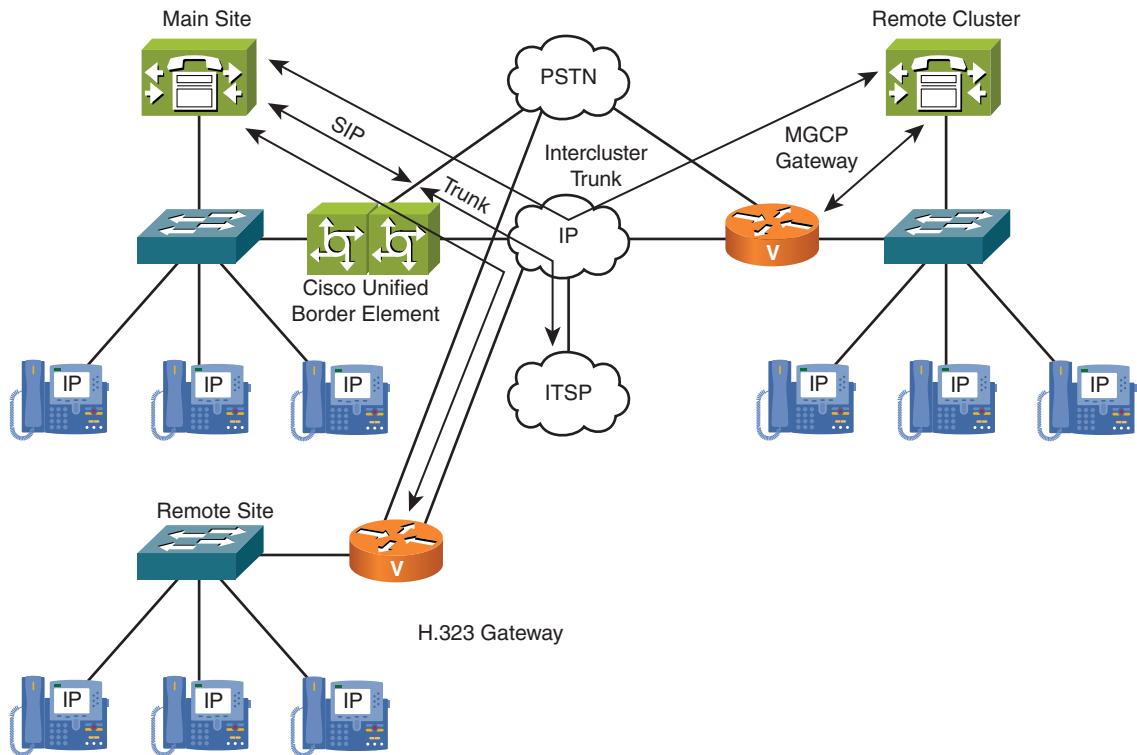


Figure 3-1 Connection Options for Multisite Deployments

CUCM Connection Options Overview

In CUCM, you can configure gateways and trunks for connections to the public switched telephone network (PSTN), an ITSP, or other VoIP domains.

Gateways are configured by the VoIP protocol that they use. CUCM supports H.323 gateways, MGCP gateways, and Skinny Client Control Protocol (SCCP) gateways. Trunks can be configured as H.323 trunks or SIP trunks. The three types of H.323 trunks are H.225 Trunk (Gatekeeper Controlled), Intercluster Trunk (Gatekeeper Controlled), and Intercluster Trunk (Nongatekeeper Controlled).

Trunks and gateways are configured when connecting to devices that allow access to multiple endpoints, such as an analog phone, Foreign Exchange Office (FXO) port, T-1 Channel Associated Signaling (CAS) line, or ISDN primary rate interface (PRI). If the destination is a single endpoint, phones are configured. Phones can be configured as SCCP, SIP, or H.323; although, H.323 phones are not as common as SCCP and SIP Phones. When CUCM routes calls to a device that uses MGCP, SCCP, or SIP, it is obvious which type of device to add because these protocols can be configured only with either a gateway or a trunk. In the case of H.323, however, an H.323 gateway and an H.323 trunk can be configured, and it is important to know whether to use the gateway or the trunk. You use only H.323 trunks when connecting to another CUCM server (either a cluster or a standalone CUCM server, in the case of CUCM Business Edition) or when using an H.323 gatekeeper. H.323 gateways are configured when connecting to any other H.323 device that is not an endpoint. Such devices can be Cisco IOS H.323 gateways or H.323 gateways of other vendors.

Cisco IOS Gateway Protocol Functions Review

Table 3-1 reviews Cisco IOS gateway (clients) protocol functions by protocol.

As shown in Table 3-1, the three main gateway signaling protocols (MGCP, H.323, and SIP) provide various features and functions when implemented with CUCM and Cisco IOS gateways.

Table 3-1 Cisco IOS Gateway Protocol Functions Review

Function	MGCP	H.323	SIP
Clients	Dumb	Intelligent	Intelligent
NFAS	Not supported	Supported	Supported
QSIG	Supported	Not supported	Not supported
Fractional T1/E1	More effort to implement	Easy to implement	Easy to implement
Signaling protocol	TCP and UDP	TCP	TCP or UDP
Code basis	ASCII	Binary (ASN.1)	ASCII
Call survivability	No	Yes	Yes
FXO caller ID	Yes*	Yes	Yes
Call applications usable	No	Yes	Yes
Function	MGCP	H.323	SIP

*Support introduced with CUCM version 8.0

Table 3-2 Cisco IOS Gateway Protocol Comparison Review

	H.323	MGCP	SIP
Pros	Dial plan directly on the gateway Translations defined per gateway Regional requirements that can be met More specific call routing Advanced fax support	Centralized dial plan configuration Centralized gateway configuration Simple gateway configuration Easy implementation Support of QSIG supplementary services	Dial plan directly on the gateway Translations defined per gateway Third-party telephony system support Third-party gateway interoperability Third-party end device support
Cons	Complex configuration on the gateway	Extra call-routing configuration for survivability	Less feature support

Cisco IOS Gateway Protocol Comparison Review

Table 3-2 reviews the advantages and disadvantages of H.323 gateways, MGCP-controlled gateways, and SIP gateways.

When compared with each other, each of the three gateway protocols has advantages and disadvantages. There is no generally “best” gateway protocol. Select the most appropriate protocol, depending on the individual needs and demands in a production-telephony environment with CUCM.

Note The *Implementing Cisco Voice Communications and QoS (CVOICE)* book provides detailed information on the functions and features of H.323, MGCP, and SIP.

SIP Trunk Characteristics

Figure 3-2 shows some examples of SIP trunks with CUCM clusters, IOS gateways, and an ITSP.

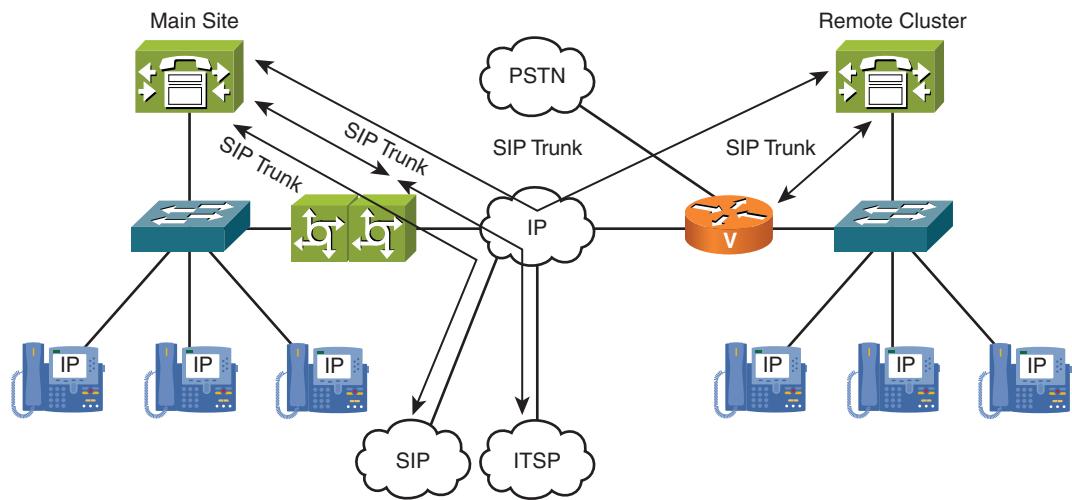


Figure 3-2 SIP Trunk Examples

SIP uses the distributed call-processing model, so a SIP gateway or proxy has its own local dial plan and performs call processing on its own. A CUCM SIP trunk can connect to Cisco IOS gateways, a CUBE, other CUCM clusters, or a SIP implementation with network servers (such as a SIP proxy).

SIP is a simple, customizable, and extensible signaling protocol with a rapidly evolving feature set.

Note When you use SIP trunks, media termination points (MTP) might be required if the endpoints cannot agree on a common method of dual-tone multifrequency (DTMF) exchange. MTPs can be software provisioned on CUCM or hardware provisioned from DSPs on gateways.

H.323 Trunk Overview

Figure 3-3 illustrates the various types of H.323 trunks.

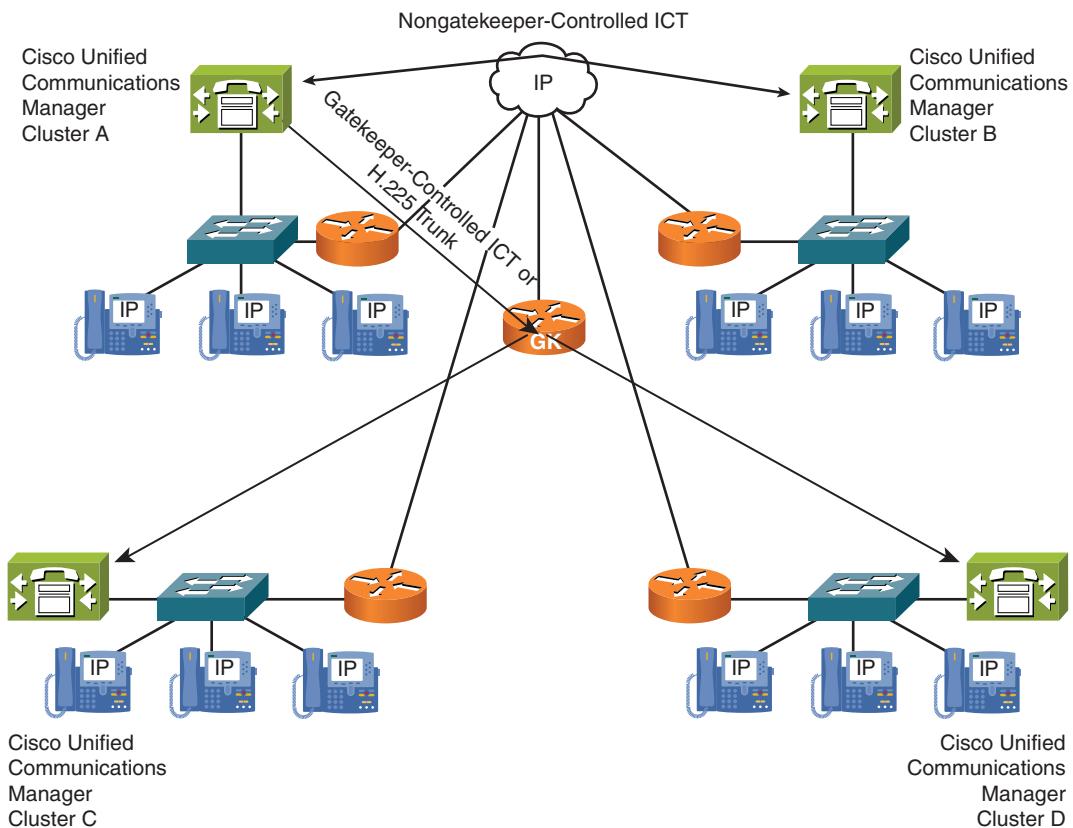


Figure 3-3 H.323 Trunk Examples

In the example, the CUCM Cluster A uses a nongatekeeper controlled ICT to CUCM Cluster B. In addition, CUCM Cluster A is configured with a gatekeeper-controlled ICT. The gatekeeper is a Cisco IOS router labeled GK in the figure. The gatekeeper-controlled ICT points to a gatekeeper, which is used for address resolution and potentially call admission control (CAC). In this example, the gatekeeper can route calls between CUCM Clusters A, C, and D.

Note Hookflash transfer with H.323 gateways is possible via a Tool Command Language (Tcl) script, which you can download from Cisco.com.

Table 3-3 compares the characteristics of the three available H.323 trunk types in CUCM.

The nongatekeeper-controlled intercluster trunk is the simplest because it does not use a gatekeeper. It requires the IP address of the remote CUCM server or servers to be specified because the dialed number is not resolved to an IP address by a gatekeeper. CAC can

be implemented by locations but not by gatekeeper CAC. Scalability is limited because no address resolution is used and all IP addresses have to be configured manually. The nongatekeeper-controlled intercluster trunk points to the CUCM server or servers of the other cluster.

Table 3-3 H.323 Trunk Comparison

	Nongatekeeper- Controlled ICT	Gatekeeper- Controlled ICT	H.225 Trunk
IP Address Resolution	IP address specified in trunk configuration	IP address resolved by H.323 RAS (gatekeeper)	
Gatekeeper Call Admission	No	Yes, by H.323 RAS (gatekeeper)	
Scalability	Limited	Scalable	
Peer	CUCM	Before Cisco CallManager 3.2	Cisco CallManager version 3.2 or later and all other H.323 devices

You may define up to three remote CUCM servers in the same destination cluster. The trunk automatically load-balances across all defined remote CUCM servers. In the remote cluster, it is important to configure a corresponding intercluster trunk (nongatekeeper-controlled) that has a CUCM group containing the same servers that were defined as remote CUCM servers in the first cluster. A similar configuration is required in each CUCM cluster that is connected by the intercluster trunks.

The gatekeeper-controlled intercluster trunk should be used instead of the nongatekeeper-controlled trunk for a larger number of clusters. The advantages of using the gatekeeper-controlled trunk are mainly the overall administration of the cluster and failover times. Nongatekeeper-controlled trunks generally require that a full mesh of trunks be configured, which can become an administrative burden as the number of clusters increases. In addition, if a subscriber server in a cluster becomes unreachable, a 5-second (the default) timeout occurs while the call is attempted. If an entire cluster is unreachable, the number of attempts before either call failure or rerouting over the PSTN depends on the number of remote servers defined for the trunk and on the number of trunks in the route list or route group. If many remote servers and many nongatekeeper-controlled trunks exist, the call delay can become excessive.

With a gatekeeper-controlled intercluster trunk, you configure only one trunk that can then communicate via the gatekeeper with all other clusters that are registered to the gatekeeper. If a cluster or subscriber becomes unreachable, the gatekeeper automatically directs the call to another subscriber in the cluster or rejects the call if no other possibilities exist. This allows the call to be rerouted over the PSTN (if required) with little incurred delay. With a single Cisco gatekeeper, it is possible to have 100 clusters that

each registers a single trunk to the gatekeeper, with all clusters being able to call each other through the gatekeeper. Of course, in an enormous enterprise environment with 100 clusters, multiple gatekeepers configured as a gatekeeper cluster would eliminate the single point of failure. With nongatekeeper-controlled intercluster trunks, this same topology would require 99 trunks to be configured in each cluster. The formula for full-mesh connections is $N(N-1)/2$. Therefore, without the gatekeeper, 100 clusters would require 4950 total trunks for complete intercluster connectivity. The gatekeeper-controlled intercluster trunk should be used to communicate only with other CUCMs because the use of this trunk with other H.323 devices might cause problems with supplementary services. In addition, a gatekeeper-controlled intercluster trunk must be used for backward compatibility with CUCM versions earlier than Release 3.2 (referred to as Cisco CallManager).

The H.225 trunk is essentially the same as the gatekeeper-controlled intercluster trunk, except that it can work with CUCM clusters (release 3.2 and later). It also can work with other H.323 devices, such as Cisco IOS gateways (including CUCM Express), conferencing systems, and clients. This capability is achieved through a discovery mechanism on a call-by-call basis. This type of trunk is the recommended H.323 trunk if all CUCM clusters are at least release 3.2.

MGCP Gateway Implementation Review

To implement an MGCP gateway in CUCM, you need to perform the following steps:

- Step 1.** Add an MGCP gateway in CUCM.
- Step 2.** Add voice modules in the gateway.
- Step 3.** Add voice interface cards (VIC) to the modules in the gateway.
- Step 4.** Add and configure MGCP endpoints in CUCM.
- Step 5.** Configure the MGCP IOS gateway.

To implement an MGCP gateway, you first need to add the gateway to CUCM. Next, add voice modules and VICs to the gateway, and finally, configure the endpoints, which are analog or digital POTS ports in the MGCP gateway.

Note More information about the MGCP and MGCP gateway characteristics are provided in *Implementing Cisco Unified Communications Voice over IP and QoS (Cvoice) Foundation Learning Guide, Fourth Edition*. MGCP gateway implementation with CUCM has been covered in detail in *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) Foundation Learning Guide, Second Edition*. This topic is only a high-level review of MGCP gateway implementation.

After adding the MGCP gateway and its endpoints and configuring the endpoints in CUCM, you need to configure the MGCP gateway itself. In its TFTP server, CUCM

stores an XML configuration file that can be downloaded by the MGCP gateway. Alternatively, you can manually configure the gateway.

Cisco IOS Gateway MGCP Configuration Methods Review

After adding the MGCP gateway in the CUCM web administration, you need to configure the Cisco IOS MGCP gateway to register it to CUCM. There are three methods for configuring a Cisco IOS Software-based gateway to register it to CUCM via MGCP:

- Cisco IOS MGCP gateway configuration with the use of a configuration server:
 - Specify the IP address of the configuration server (CUCM TFTP server).
 - If more than one CUCM TFTP server is deployed in the CUCM cluster, configure the gateway with all CUCM TFTP server IP addresses.
 - Enable the configuration server feature.
- Manual Cisco IOS MGCP gateway configuration:
 - Specify the IP address of the MGCP call agent (CUCM server).
 - If more than one CUCM server is used for call processing (that is, running the Cisco CallManager service), configure the gateway with a primary and redundant call agent by specifying the IP addresses of two CUCM call-processing servers.
 - Configure global MGCP parameters.
 - Examples of global MGCP configuration commands are **mgcp packet** and **mgcp rtp** commands.
 - If Foreign Exchange Station (FXS) or FXO interfaces are to be MGCP-controlled, enable MGCP on the corresponding plain old telephone service (POTS) dial peers by using the service **mpcpapp** command.
 - Enable MGCP.

Note *Implementing Cisco Unified Communications Voice over IP and QoS (Cvoice) Foundation Learning Guide, Fourth Edition* provides more information about manual configuration of MGCP gateways.

- Mixed use of configuration server and manual configuration:
 - Follow the same procedure as for the MGCP gateway configuration, using the configuration server.
 - Disable the configuration server, using the **ccm-manager config** command.
 - Manually remove the configuration that is received from the configuration server or add more configuration to it.

Note Be aware that as long as the configuration server is active on the Cisco IOS gateway, every time the MGCP endpoint is reset from CUCM, the Cisco IOS configuration is also rewritten. In addition, when you reload the MGCP gateway, the MGCP configuration is rewritten as long as the configuration server is enabled. Therefore, it is common practice to use only the configuration for initial configuration when manual changes are required. After you modify the downloaded configuration, you deactivate the configuration server so that the manually added changes are preserved. Also, when you reset an MGCP gateway or MGCP endpoint in CUCM, the gateway or endpoint is not automatically reset at the router. Therefore, when the configuration server feature is not enabled on the Cisco IOS gateway, properly reset the MGCP gateway or MGCP endpoint. First, reset the MGCP gateway or MGCP endpoint in CUCM. Then, enter the `no mgcp` command, followed by the `mgcp` command in configuration at the Cisco IOS gateway.

Note Fractional PRI support with MGCP is possible when you manually limit the timeslots at the MGCP gateway and busy out B channels in CUCM (using an advanced service parameter). However, this configuration is not officially supported.

Configuring Cisco IOS Gateway for MGCP: Example

Figure 3-4 shows an example topology, and Example 3-1 illustrates the commands that need to be entered into the MGCP gateway for this topology. In this example, a single E1 line is installed in the gateway and connected to the PSTN.

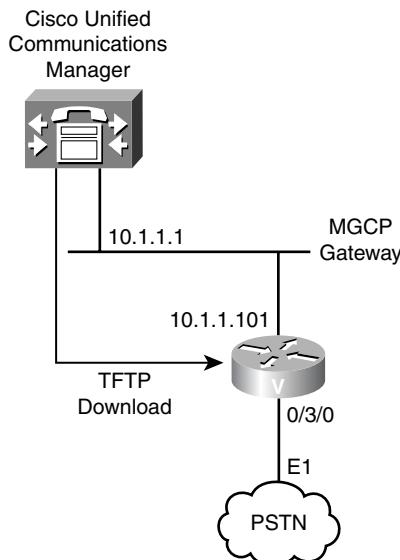


Figure 3-4 MGCP Gateway Implementation

Only the highlighted commands were manually configured. The rest of the commands were automatically added via TFTP in the cnf.xml configuration file copied from CUCM into the gateway.

Example 3-1 MGCP Gateway Configuration

```
controller E1 0/3/0
  framing hdb3
  linecode crc4
  pri-group timeslots 1-31 service mgcp
interface Serial0/3/0:15
  isdn switch-type primary-net5
  isdn incoming-voice voice
  isdn bind-13 ccm-manager
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.1.1.1
ccm-manager config

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 profile default
```

After the MGCP gateway and its endpoints have been added and configured in CUCM, the MGCP gateway itself needs to be configured. CUCM stores an XML configuration file at its TFTP server, which can be downloaded by the MGCP gateway. If this configuration server feature is used, the gateway needs to be configured with only two commands (`ccm-manager config server` IP address of Cisco TFTP and `ccm-manager config`), as shown in Example 3-1. The rest of the configuration is automatically downloaded and applied to the Cisco IOS MGCP gateway. Additional MGCP dial peers might also be automatically added to the MGCP configuration, depending on the MGCP endpoints previously configured in CUCM.

Note Be careful when using these automated MGCP commands because they automatically reserve all DSP resources for all digital channels present in the gateway. Potentially,

this may not leave available DSP resources for hardware conference bridges or transcoding. Many engineers choose not to enter these two `ccm-manager` commands and instead manually enter all commands.

H.323 Gateway Implementation

Figure 3-5 illustrates the relationship between CUCM and an H.323 gateway.

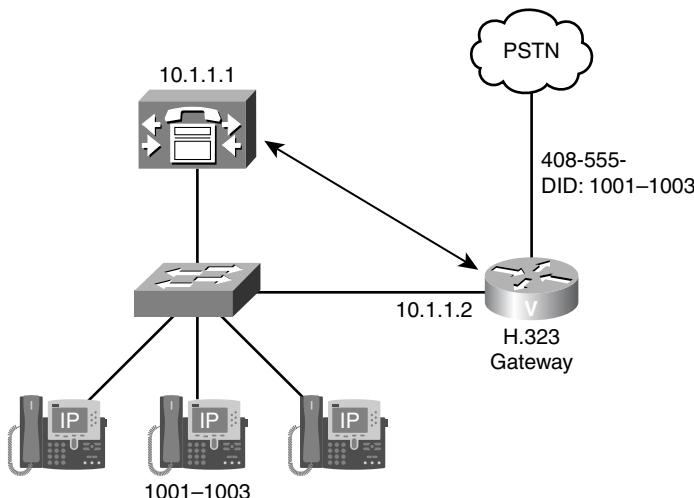


Figure 3-5 H.323 Gateway Implementation Overview

Note The number of settings available in CUCM for an H.323 gateway is substantially less than those for an MGCP gateway. This is intentional by design because MGCP is a client/server protocol and CUCM must contain all gateway settings. In contrast, H.323 is a peer-to-peer protocol, and CUCM simply needs to know how to talk to the gateway.

The Cisco IOS gateway configuration consists of these steps:

- Step 1.** Configure the H.323 gateway, specifying its H.323 ID and the IP address to use. This is done on any interface, but best practice for reliability is to use a loopback interface. Ensure that you use the same IP address you configured in CUCM for the H.323 gateway.

Note If the IP address configured in CUCM does not match the IP address used by the gateway, CUCM considers the H.323 signaling messages to be sent from an invalid (unknown) source and ignores them, unless promiscuous operation has been permitted. (This service parameter can be configured in CUCM.)

Step 2. Configure one or more VoIP dial peers pointing to CUCM.

Step 3. Configure one or more dial peers pointing to the PSTN.

Note More information about the H.323 protocol and H.323 gateway characteristics have been provided in *Implementing Cisco Unified Communications Voice over IP and QoS (Cvoice) Foundation Learning Guide*, Fourth Edition. MGCP gateway implementation with CUCM has been covered in detail in *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) Foundation Learning Guide*, Second Edition. This topic is only a high-level review of H.323 gateway implementation.

Cisco IOS H.323 Gateway Configuration

Example 3-2 shows an IOS configuration for the H.323 gateway in the network topology, which is illustrated in Figure 3-6.

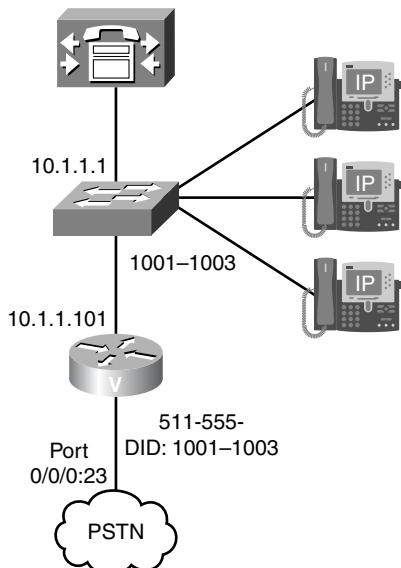


Figure 3-6 Cisco IOS H.323 Gateway Topology

Example 3-2 Cisco IOS H.323 Gateway Configuration

```
interface Loopback0
 ip address 10.1.1.101 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip bind srcaddr 10.1.1.101
!
```

```

dial-peer voice 11 voip
destination-pattern 511555....
session target ipv4:10.1.1.1
incoming called-number 9T
codec g711ulaw
!
dial-peer voice 21 pots
destination-pattern 9T
direct-inward-dial
port 0/0/0:23

```

When configuring an H.323 gateway, be sure to first enable H.323 at one IP interface. If multiple IP interfaces are present, it is recommended that you use a loopback interface. Otherwise, if the interface that has been selected for H.323 is down, the H.323 application will not work, even if other interfaces could be used to route the IP packets. In this example, H.323 has been enabled on the loopback interface using the **h323-gateway voip** interface and **h323 gateway voip bind srcaddr** IP address commands.

In contrast to MGCP gateways, in which the call agent takes care of call routing, H.323 gateways require local dial plan configuration. In the example, the H.323 gateway is configured with a VoIP dial peer that routes calls placed to the gateway's PSTN number 511555.... toward CUCM. The gateway receives these calls from the PSTN, because 511555 1001–1003 is the direct inward dialing (DID) range of the PSTN interface (port 0/0/0:23). In addition, the PSTN gateway is configured with a plain old telephone service (POTS) dial peer that routes all calls starting with 9 to the PSTN using the ISDN PRI (port 0/0/0:23).

Note that the configured digits of a destination pattern in a POTS dial peer are automatically stripped because POTS dial peers send only wildcard (variable) digits by default. Therefore, the 9 is not sent to the PSTN. In the other direction, the gateway does not perform any digit manipulation because VoIP dial peers do not strip any digits by default. CUCM receives H.323 call setup messages for calls that were received from the PSTN in full length (usually ten digits). Because the internal directory numbers are four digits, either CUCM or the H.323 gateway needs to be configured to strip the leading digits so that the remaining four digits can be used to route the call to internal directory numbers.

Note The use of 9T in dial peer 21 shown in Example 3-2 is just an example. More granular destination pattern configurations typically are used in production to allow greater call control. Additional information on how to implement digit manipulation is provided in Chapter 6, “Implementing Cisco Unified SRST and MGCP Fallback.”

CUCM H.323 Gateway Configuration

Figure 3-7 shows an example of a CUCM H.323 gateway configuration.

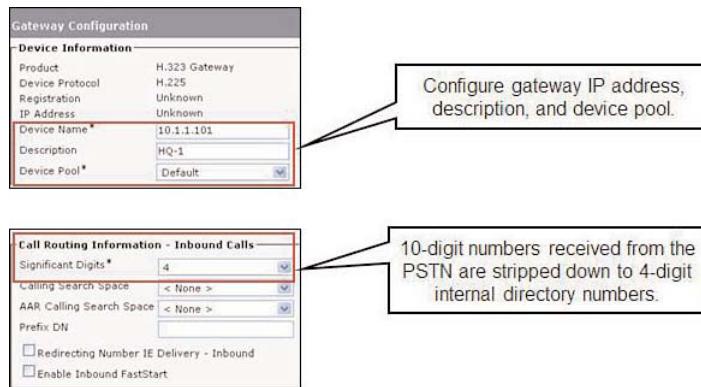


Figure 3-7 CUCM H.323 Gateway Configuration

To add an H.323 gateway to CUCM, in **Cisco Unified CM Administration**, choose **Device > Gateway** and click **Add New**. Then, from the Gateway Type drop-down list, choose **H.323** and click **Next**.

In the Gateway Configuration window, enter the IP address of the H.323 gateway in the Device Name field, select the device pool that should be used, and optionally enter a description. If CUCM should consider only some of the called digits, the significant digits parameter can be set to the number of least-significant digits that should be used to route inbound calls. In this example, in which the gateway sends full ten-digit PSTN numbers to CUCM, setting the significant digits to 4 allows the incoming calls to be routed to internal directory numbers without any additional CUCM digit manipulation configurations, such as translation patterns.

Trunk Implementation Overview

Figure 3-8 illustrates nongatekeeper-controlled ICTs between CUCM clusters.

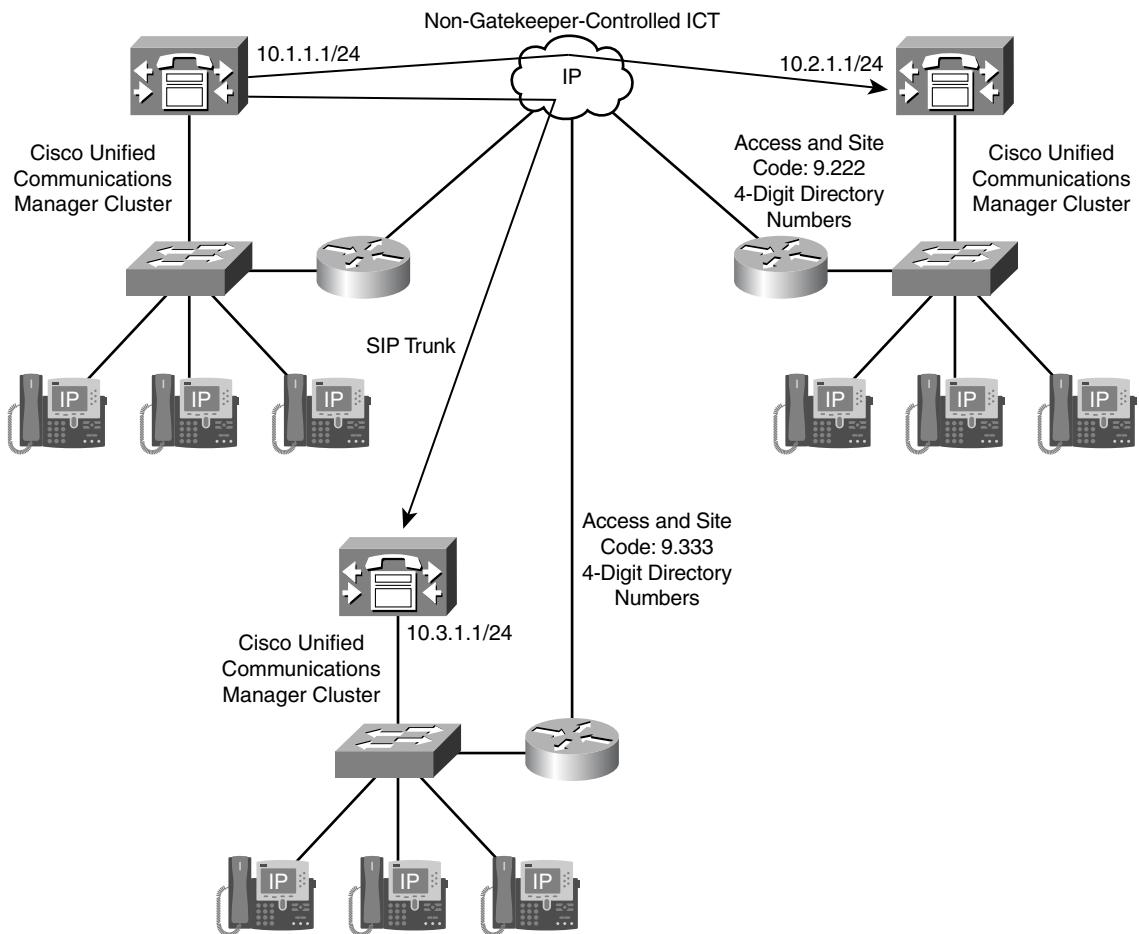


Figure 3-8 Nongatekeeper-Controlled ICT and SIP Trunk Topology

Figure 3-8 illustrates the most important configuration elements for implementing a SIP or nongatekeeper-controlled ICT in CUCM. These elements are the configuration of the trunk itself, in which you have to specify the IP address of the peer, and the route group, route list, and route pattern configuration. This implementation is like the implementation of a gateway.

Gatekeeper-Controlled ICT and H.225 Trunk Configuration

Figure 3-9 illustrates the most important configuration elements for implementing a gatekeeper-controlled intercluster trunk or H.225 trunk in CUCM.

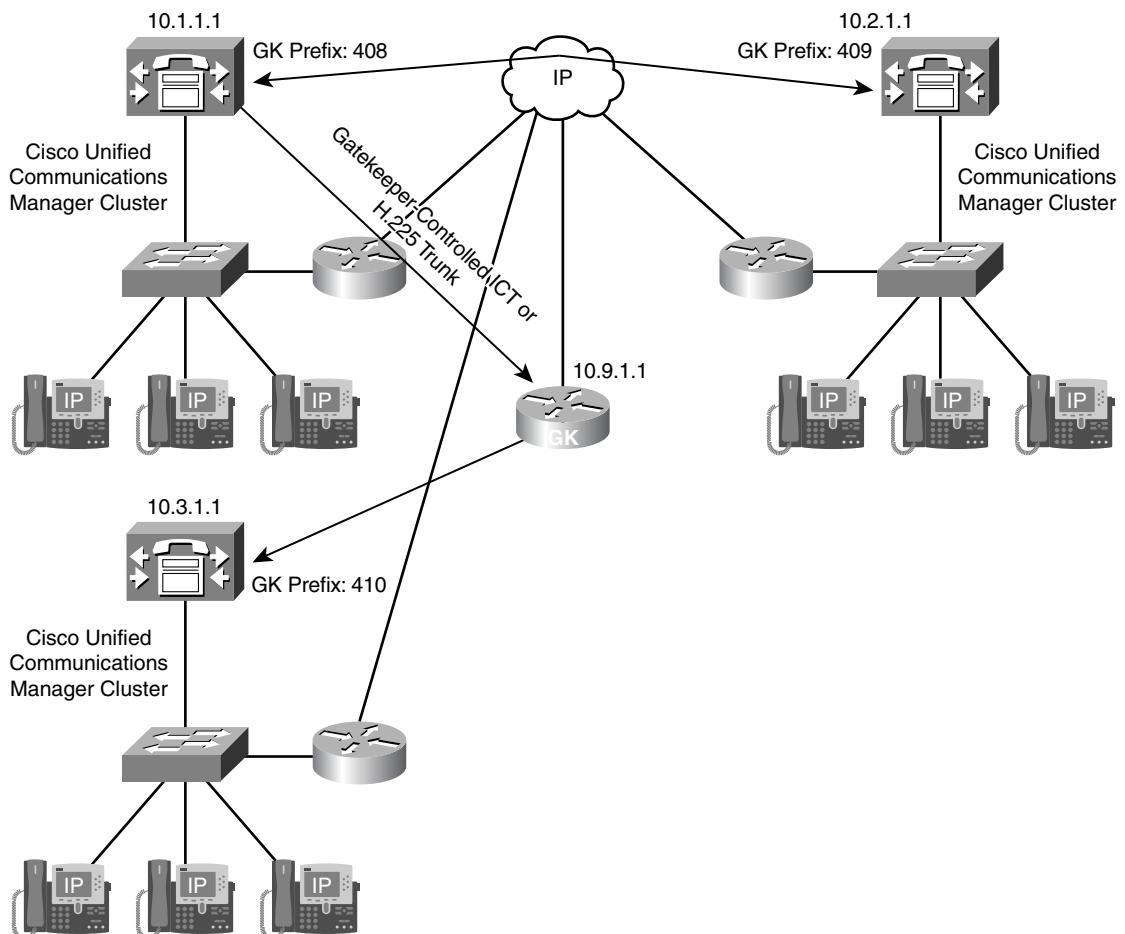


Figure 3-9 Gatekeeper-Controlled ICT and H.225 Trunk Topology

The required items are the configuration of the gatekeeper with its IP address and the gatekeeper-controlled ICT that points to the gatekeeper. CUCM also needs the route group connected to the gateway, route list, and route pattern configuration, similar to the previous example.

Trunk Types Used by Special Applications

Some applications require special trunk types to be configured.

For example, when implementing Cisco Extension Mobility Cross Clusters (EMCC), a dedicated trunk has to be configured between the CUCM clusters that allow users of the remote cluster to log in locally using Cisco EMCC. These trunks, which are exclusively configured for Cisco EMCC, must use SIP; H.323 is not supported by Cisco EMCC.

Another application that requires special trunks to be configured is Call Control Discovery (CCD). When you use CCD, internal directory numbers and the associated external PSTN numbers are advertised and learned from a Service Advertisement Framework (SAF)-enabled network. These trunks can be either SIP or H.323 and must be explicitly enabled for SAF.

Note Chapter 12, “Service Advertisement Framework (SAF) and Call Control Discovery (CCD),” provides you with more information about Cisco SAF trunks.

Implementing SIP Trunks

Figure 3-10 illustrates a CUCM SIP trunk configuration. In Cisco Unified CM Administration, choose Device > Trunk > Add New.

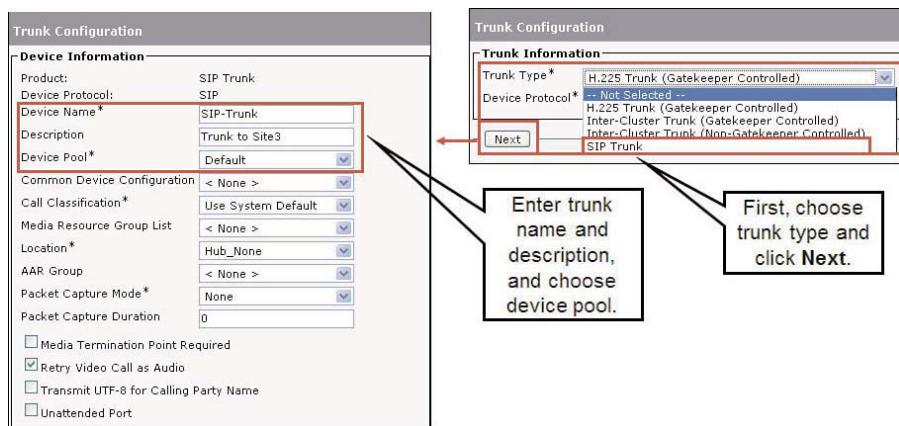


Figure 3-10 CUCM SIP Trunk Configuration

In the Trunk Configuration window, enter a name for the SIP trunk, choose the device pool that should be used, and optionally add a description.

In the SIP Information area of the Trunk Configuration window shown in Figure 3-11, enter the destination address of the device that is located on the other end of the SIP trunk. This device can be a CUBE, CUCME, or any other SIP-capable device, such as a third-party SIP proxy server.

In addition, you must choose a SIP Trunk Security Profile and a SIP Profile. Both parameters are mandatory and do not have a default value.

The SIP Trunk Security Profile is used to enable and configure security features on SIP trunks, such as Transport Layer Security (TLS) with two-way certificate exchange or SIP digest authentication. One default SIP Trunk Security Profile exists: the Non Secure SIP Trunk Profile, which has security disabled. You can configure additional SIP Trunk Security Profiles by choosing System > Security Profile > SIP Trunk Security Profile.

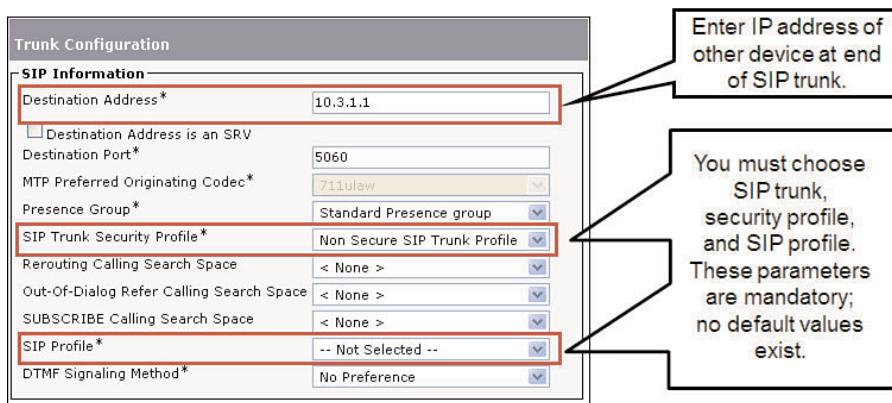


Figure 3-11 CUCM SIP Trunk Configuration, Continued

The SIP Profile is used to set timers, Real-Time Transport Protocol (RTP) port numbers, and some feature settings (such as call pickup Uniform Resource Identifiers [URI], call hold ringback, or caller ID blocking). One default SIP profile exists called the Standard SIP Profile. You can configure additional SIP profiles by choosing Device > Device Settings > SIP Profile.

Note CUCM supports SIP over TCP or UDP. Take care to ensure that this setting is identical to the device on the other end of the SIP trunk.

Implementing Intercluster and H.225 Trunks

The steps to implement nongatekeeper-controlled intercluster trunks in CUCM are as follows:

- Step 1.** In Cisco Unified CM Administration, choose Device > Trunk, and click Add New.
- Step 2.** Choose the appropriate trunk type. After you click Next, the Trunk Configuration window appears, as shown in Figure 3-12, where you can configure the nongatekeeper-controlled intercluster trunk.
- Step 3.** Enter a device name, choose the device pool that should be used, and optionally add a description.
- Step 4.** Enter the IP address(es) of the CUCM servers of the other cluster, as shown in Figure 3-13. You must enter at least one server but can add up to three CUCM servers if they are installed.

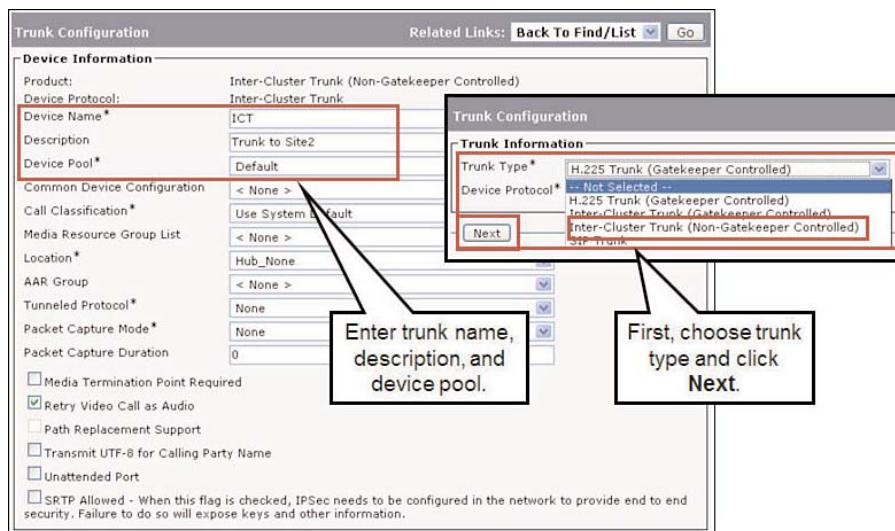


Figure 3-12 Implementing Nongatekeeper-Controlled Intercluster Trunks

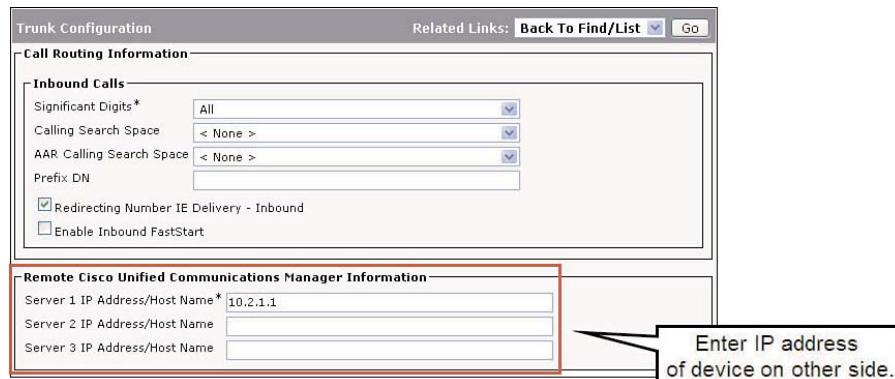


Figure 3-13 Implementing Nongatekeeper-Controlled Intercluster Trunks, Continued

Note Because the nongatekeeper-controlled intercluster trunk does not use a gatekeeper for address resolution, you must manually enter the IP address(es) of the devices on the other side.

CUCM Gatekeeper-Controlled ICT and H.225 Trunk Configuration

A gatekeeper is an optional element in a Cisco Unified Communications implementation that runs on an IOS router to provide centralized call routing, and optionally CAC, with the H.323 protocol. The only hardware of a gatekeeper is the IOS router.

The steps for how to implement gatekeeper-controlled intercluster trunks (an H.225 trunk or a gatekeeper-controlled intercluster trunk) in CUCM are as follows:

- Step 1.** In Cisco Unified CM Administration, choose Device > Gatekeeper, and click Add New. In the Gatekeeper Configuration window, as shown in Figure 3-14, enter the IP address of the H.323 gatekeeper and optionally a description. Then, make sure that the Enable Device check box is checked.

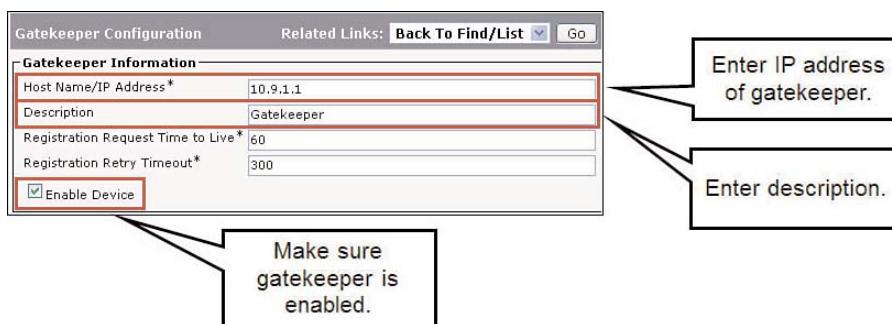


Figure 3-14 Implementing CUCM Gatekeeper-Controlled Intercluster Trunk Configuration: Step 1

- Step 2.** After you configure the gatekeeper, you can add the gatekeeper-controlled trunk, as shown in Figure 3-15. Choose Device > Trunk and click Add New. Then, choose the trunk type. As discussed earlier, there are two types of gatekeeper-controlled H.323 trunks. Gatekeeper-controlled intercluster trunks must be used when connecting to CUCM earlier than version 3.2. H.225 trunks connect to CUCM version 3.2 or higher, and other H.323 devices, such as gateways or conferencing systems.
- Step 3.** After selecting the trunk type, enter a name for the trunk, choose the device pool that should be used, and optionally enter a description.
- Step 4.** As shown in Figure 3-16, you must provide the gatekeeper information. From the drop-down list, choose the gatekeeper to which this trunk should register, and choose the terminal type. CUCM can register trunks as terminals or gateways with an H.323 gatekeeper. Usually, the terminal type is set to Gateway.
- Step 5.** In the Technology Prefix field, enter the prefix that should be registered with the gatekeeper.

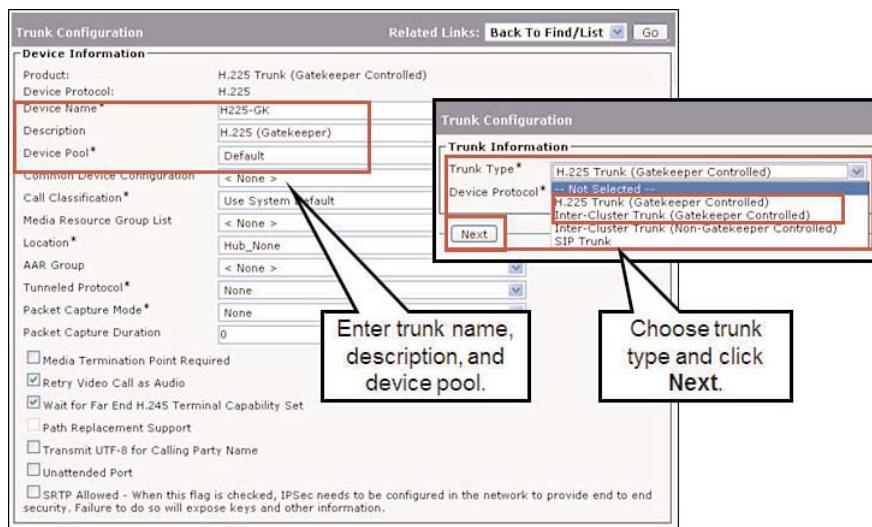


Figure 3-15 Creating a CUCM Gatekeeper-Controlled Intercluster Trunk Configuration: Steps 2 and 3

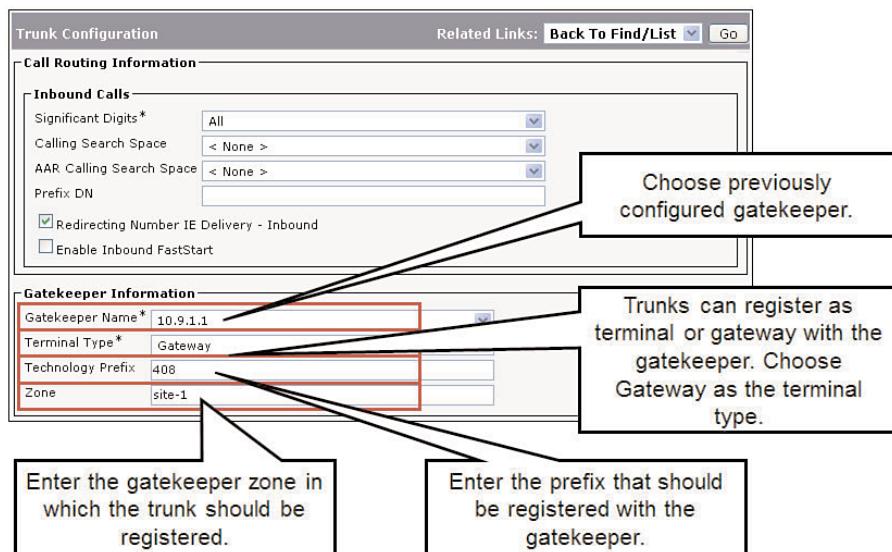


Figure 3-16 Configuring a CUCM Gatekeeper-Controlled Intercluster Trunk Configuration: Steps 4 Through 6

Note The Prefix DN you enter is the prefix that the trunk will register with the gatekeeper. It can, but does not have to, include a Technology Prefix. In Figure 3-16, a Technology

Prefix of 408 is used. Without the tech prefix set, the calls will most likely fail. More information about prefixes and technology prefixes is provided in *Implementing Cisco Unified Communications Voice over IP and QoS (Cvoice) Foundation Learning Guide*, Fourth Edition.

Step 6. Enter the gatekeeper zone in which the trunk should be registered.

Tip The H.323 zone name is case-sensitive. Make sure that it matches the zone name that was configured at the gatekeeper. In addition, if the zone name is not added and no zone security is set up, CUCM registers into the first configured zone on its assigned gatekeeper, which could cause problems.

Summary

The following key points were discussed in this chapter:

- Connection options for multisite deployments include gateways and trunks.
- When you implement MGCP gateways, most configurations are done in CUCM.
- When you implement H.323 gateways, CUCM and the gateway both have to be configured with a dial plan.
- Cisco IOS H.323 gateway configuration includes H.323 gateway and dial peer configuration tasks.
- H.323 gateway configuration in CUCM includes gateway and dial plan configuration tasks.
- Trunk support in CUCM includes SIP and three types of H.323 trunks.
- SIP trunk implementation includes trunk and dial plan configuration in CUCM.
- When configuring nongatekeeper-controlled ICTs, you must specify the IP address of the peer. Gatekeeper-controlled ICTs and H.225 trunks require you to configure an H.323 gatekeeper instead.

References

For additional information, refer to these resources:

Cisco Systems, Inc. Cisco Unified Communications System 8.x SRND, April 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8x.html.

Cisco Systems, Inc. Cisco Unified Communications Manager Administration Guide Release 8.0(1), February 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_1/ccmcfg/bccm-801cm.html.

Cisco Systems, Inc. “Cisco IOS Voice Configuration Library (with Cisco IOS Release 15.0 updates),” July 2007.

www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm.

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in the “Answers Appendix.”

1. Which of the following is not a connection option for a multisite CUCM deployment?
 - a. SIP trunk
 - b. SIP gateway
 - c. H.323 gateway
 - d. H.225 trunk
2. Which two commands are required to enable MGCP at the gateway when using the CUCM configuration server feature?
 - a. mgcp
 - b. sccp
 - c. ccm-manager config server *IP address*
 - d. ccm-manager config
 - e. ccm-manager sccp
3. What is not configured in CUCM when you configure an H.323 PSTN gateway?
 - a. The gateway in the route group
 - b. The IP address of the gateway in the route list
 - c. The route group in the route list
 - d. The route pattern pointing to the route list
4. What is not configured when you configure an H.323 PSTN gateway?
 - a. The IP address used for the H.323 interface
 - b. The VoIP dial peer pointing to CUCM
 - c. The IP address of the call agent for centralized call control of H.323
 - d. The POTS dial peer(s) pointing to the PSTN

5. Which parameter is set at the MGCP gateway configuration page in CUCM to strip the called-party number to a certain number of digits?
 - a. Called Party Transformation Mask
 - b. Significant Digits
 - c. Calling Party Transformation Mask
 - d. Number-Length
 - e. Discard Digit Instruction
6. Which two types of trunks are configured directly with the IP address of CUCM in another CUCM cluster?
 - a. SIP gateway
 - b. Nongatekeeper-controlled intercluster trunk
 - c. SIP trunk
 - d. Gatekeeper-controlled intercluster trunk
 - e. MGCP trunk
7. Where do you configure SIP timers and features for a SIP trunk?
 - a. SIP profile
 - b. SIP security profile
 - c. SIP trunk security profile
 - d. Common trunk profile
8. What do you need to specify at the gatekeeper configuration page when adding a gatekeeper to CUCM?
 - a. Hostname of the gatekeeper
 - b. H.323 ID of the gatekeeper
 - c. IP address of the gatekeeper
 - d. Zone name
 - e. Technology prefix
9. What is the best reason to implement a gatekeeper in a multisite implementation?
 - a. To allow IP Phones to register to the gatekeeper to implement centralized call routing
 - b. To prevent IP Phones from registering to the incorrect CUCM server
 - c. To implement centralized call routing with CAC
 - d. To implement centralized call routing, ensuring that CAC is not implemented

This page intentionally left blank

Chapter 4

Implementing a Dial Plan for International Multisite Deployments

Upon completing this chapter, you will be able to implement a dial plan to support inbound and outbound PSTN dialing, site-code dialing, and TEHO. You will be able to meet these objectives:

- Identify dial plan issues and possible solutions
- Describe how site codes and transformation masks solve issues caused by overlapping directory numbers
- Implement PSTN access in a multisite deployment
- Implement selective PSTN breakout
- Describe how to use the PSTN as a backup for calls to other VoIP domains
- Implement TEHO
- Describe the concept of globalized call routing and how it simplifies dial plans in international multisite deployments with centralized call processing
- Explain special considerations for implementing globalized call routing

Multisite dial plans have to address special issues, such as overlapping and nonconsecutive directory numbers, public switched telephone network (PSTN) access, PSTN backup, and tail-end hop-off (TEHO). This chapter describes how to build multisite dial plans using Cisco Unified Communications Manager (CUCM) and Cisco IOS gateways. This chapter also describes the concept of globalized call routing, which is a new way of building dial plans in international multisite deployments.

Multisite Dial Plan Overview

The following dial plan solutions exist for multisite deployments for centralized call processing:

- **Access and site codes:** By adding an access code and a site code to directory numbers of remote locations, you can do call routing based on the site code instead of directory numbers. As a result, directory numbers do not have to be globally unique, although they do need to be unique within a site. Configuration requires route patterns, translation patterns, partitions, and Calling Search Spaces (CSS). Adding access and site codes simplifies internal dialing for users in a multisite environment.
- **Implementing PSTN access:** PSTN access within a CUCM cluster is implemented using route patterns, route lists, route groups, and partitions and CSSs. When implementing TEHO, the same dial plan configuration elements are used; however, more entities have to be configured, which makes the configuration more complex. TEHO reduces the operating cost of long-distance or international dialing.
- **Implementing PSTN backup:** The IP WAN used in a multisite deployment with centralized call processing is backed up by Media Gateway Control Protocol (MGCP) fallback, Cisco Unified Survivable Remote Site Telephony (SRST), or CUCM Express in SRST mode, and Call Forward Unregistered (CFUR). PSTN backup ensures that calls will go through the PSTN in the event of a WAN link failure.

Dial Plan Requirements for Multisite Deployments with Distributed Call Processing

Dial plan requirements for multisite deployments with distributed call processing are similar to the dial plan requirements of multisite deployments with centralized call processing. In multisite environments with distributed call processing, use these dial plan solutions:

- **Access and site codes:** By adding an access code and a site code to directory numbers of remote locations, you can provide call routing based on the site code instead of the directory numbers. As a result, directory numbers do not have to be globally unique, although they must be unique within a site. Configuration elements include route patterns and translation patterns.
- **Implementing PSTN access:** You implement PSTN access within a CUCM cluster by using route patterns, route lists, route groups, partitions, and CSSs. When implementing TEHO, you use the same dial plan configuration elements; however, you have to configure more entities, which makes the configuration more complex.
- **Implementing PSTN backup:** Backup of the IP WAN is provided by route lists and route groups with on-net (prioritized) and off-net (PSTN) paths.

Dial Plan Scalability Solutions

In large Unified Communications implementations with many call agents, such as CUCM, CUCME, Cisco Unified Border Element (CUBE), Cisco Unified SRST, and Cisco IOS gateways, the implementation and maintenance of the entire integrated dial plan can be complex.

Without centralized services (such as H.323 gatekeepers or SIP network services), a full-mesh configuration is required. In other words, each call control domain has to be configured with call-routing information toward all other call-routing domains. This full mesh implementation model does not scale at all and, therefore, is suitable only for smaller deployments.

In a hub-and-spoke deployment model, call-routing information for each call-routing domain is configured only once at the centralized call-routing entity. This centralized call-routing entity can be a SIP network service or an H.323 gatekeeper. Such a solution scales better than full mesh topologies; however, it introduces a single point of failure and therefore requires redundant deployment of the centralized service. In addition, the centralized call routing still has to be manually configured with static entries. For example, if telephone-number ranges or prefixes are changed at one of the call-routing domains, these changes also have to be manually performed at the centralized call-routing service. Furthermore, PSTN backup has to be implemented independently at each call-routing domain.

With Call Control Discovery (CCD), which is a new feature introduced with CUCM version 8, each call-routing domain dynamically advertises locally known telephone numbers or number ranges. Because local numbers are typically used by internal patterns (using VoIP) and via the PSTN, each call-routing domain advertises both the internally used numbers and the corresponding external PSTN numbers. Figure 4-1 shows how CCD allows dial plans dynamically learned from call agents are compared to a static full mesh configuration.

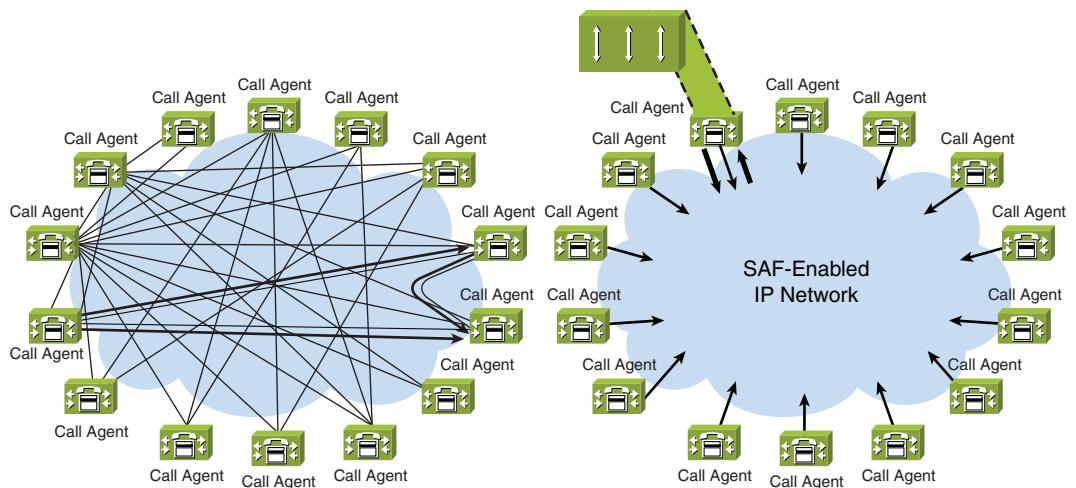


Figure 4-1 Dial Plan Scalability Comparison of Static Versus Dynamic Design

CCD solves dial plan scalability issues by allowing CUBE, Cisco Unified SRST, CUCM, CUCME, and Cisco IOS gateways to dynamically advertise and learn call-routing information in the form of internal directory numbers and PSTN numbers or prefixes. CCD uses the Cisco Service Advertisement Framework (SAF), which is based on the Cisco EIGRP dynamic routing protocol. SAF is a network-based, scalable, bandwidth-efficient, real-time approach to service advertisement and discovery.

Note CCD and SAF are described in more detail in Chapter 12, “Service Advertisement Framework (SAF) and Call Control Discovery (CCD).”

Implementing Site Codes for On-Net Calls

In Figure 4-2, two sites have overlapping and nonconsecutive directory numbers. To accommodate unique addressing of all endpoints, site-code dialing is used. Users dial an access code (8, in this example), followed by a three-digit site code. A designer can choose another site code access code as well. When calling the phone with directory number 1001 at the remote site, a user located at the main site has to dial 82221001. For calls in the other direction, remote users dial 81111001. When distributed call processing is used, each CUCM cluster is only aware of its own directory numbers in detail. For all directory numbers located at the other site, the call is routed to a CUCM server at the other site based on the dialed site code.

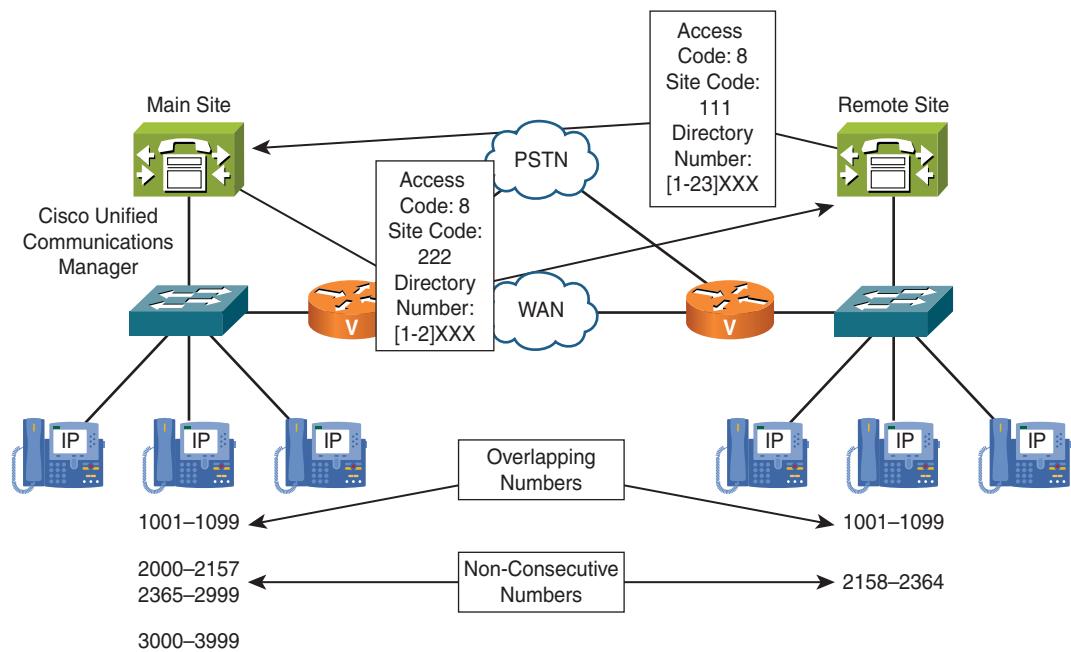


Figure 4-2 Access and Site Codes Solve Issues with Directory Numbers Used at Different Site

Digit-Manipulation Requirements When Using Access and Site Codes

When you use site codes in multisite environments with distributed call processing, as shown in Figure 4-3, the access and site code have to be stripped from the Dialed Number Identification Service (DNIS) on outgoing calls. If access and site codes are configured before the . (dot) in the route pattern, they can be easily stripped by using the discard digit instruction on the route pattern or route list. For incoming calls, you must add the access code and appropriate site code that are used to get to the caller's site. You can do this easily by using translation patterns. Note that the Automatic Number Identification (ANI) can also be properly manipulated on the outgoing CUCM servers at the main site.

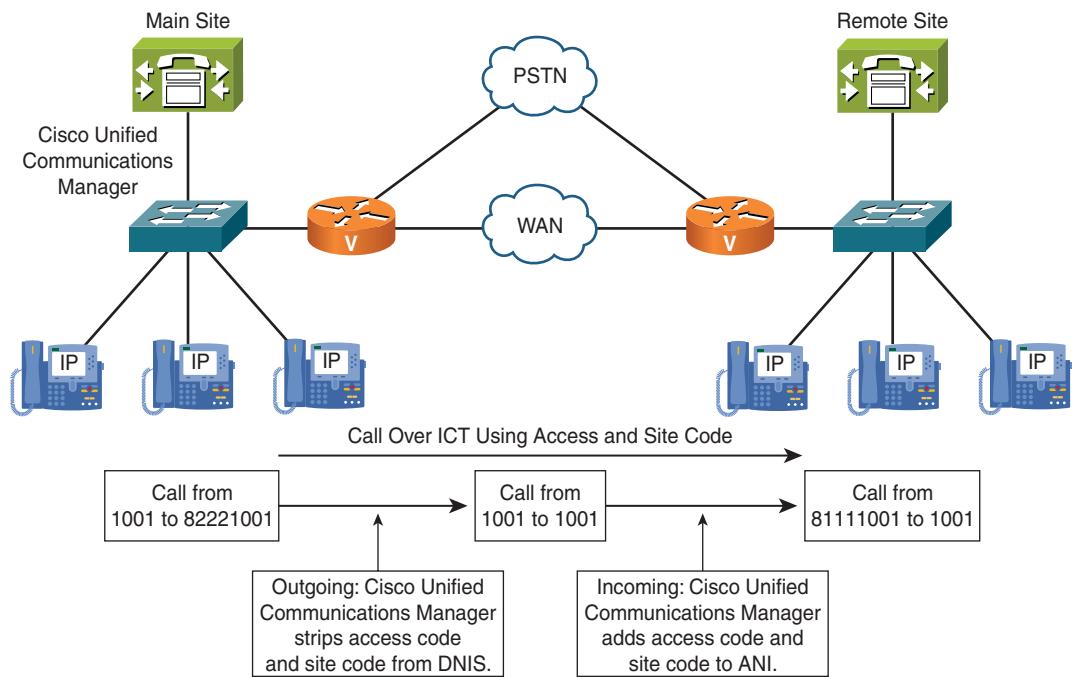


Figure 4-3 Digit-Manipulation Requirements When Using Access and Site Codes

Note If the WAN link is not functional, additional digit manipulation is required to route the call through the PSTN because the PSTN does not understand the site code.

Access and Site Code Requirements for Centralized Call-Processing Deployments

If overlapping directory numbers exist in a centralized call-processing deployment, access and site codes are implemented in a different way, as shown in Figure 4-4.

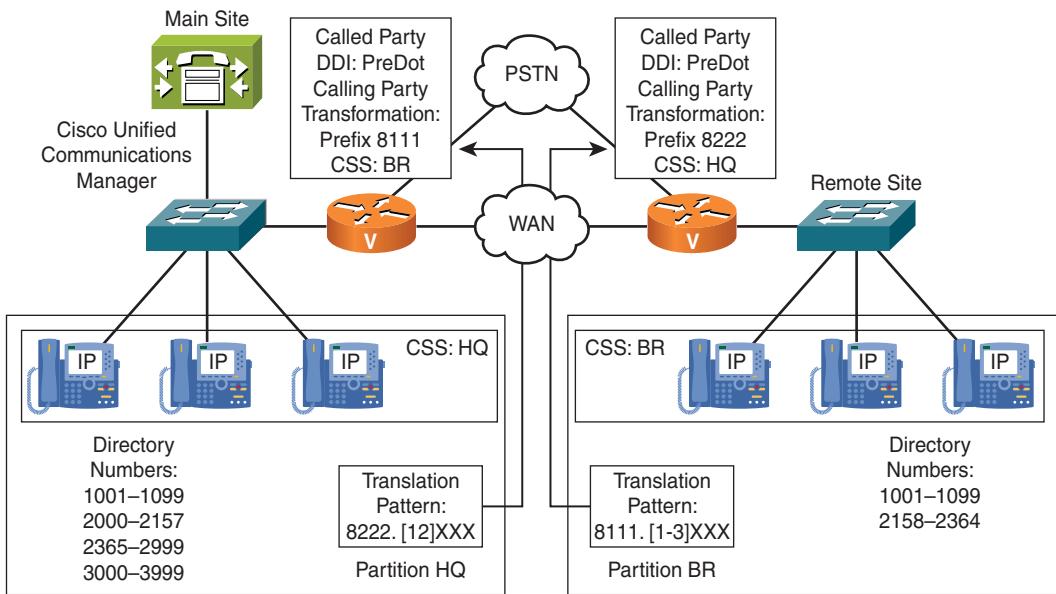


Figure 4-4 Centralized Call-Processing Deployments: Access and Site Codes

Figure 4-4 shows two sites with centralized call processing. Directory numbers in the main site (headquarters [HQ]) and the remote site (branch [BR]) partially overlap. Again, access and site codes solve the problem of overlapping directory numbers.

However, in this case, partitions and CSSs need to be deployed in a way that phones at the remote site do not see directory numbers of main-site phones and vice versa. In this case, a translation pattern is added for each site.

The translation pattern of each site includes the access and site code of the respective site. Phones at each site have a CSS assigned, which provides access to the directory numbers of the local site and the translation pattern for the other site or sites. The translation patterns are configured with a transformation mask that strips the access code and site code. Further, each translation pattern must have a CSS, which provides access to only those directory numbers that are located at the target site of the respective translation pattern. This way, all phones can dial local directory numbers and site-code translation patterns for accessing other sites. After an intersite number is dialed that consists of the access code, site code, and directory number, the directory number is extracted by the translation pattern. Then, the number is looked up again in the call-routing table using a CSS that has access only to the directory numbers of the site, which was identified by the site code.

Implementing PSTN Access in Cisco IOS Gateways

When you implement PSTN access in a multisite environment, you must perform digit manipulation, described in the following list, before the call is sent to the PSTN. Digit manipulation must be done in CUCM when you use an MGCP gateway. It can be performed either in CUCM or at the H.323 gateway when using an H.323 gateway:

- **Outgoing calls to the PSTN:**
 - **ANI or Calling Number Transformation:** If no direct inward dialing (DID) range is used at the PSTN, transform all directory numbers to a single PSTN number in the ANI. If DID is used, extend the directory numbers to a full PSTN number.
 - **DNIS or Called Number Transformation:** Strip the access code.
- **Incoming calls from the PSTN:**
 - **ANI or Calling Number Transformation:** Transform ANI into the full number (considering type of number [TON]), and add the access code so that users can easily redial the number.
 - **DNIS or Called Number Transformation:** If DID is used, strip the office code, area code, and country code (if present) to get to the directory number. If DID is not used, route the call to an attendant, such as a receptionist or an interactive voice response (IVR) application.

Figure 4-5 shows an example of digit manipulation performed for both incoming and outgoing PSTN calls.

As shown in Figure 4-5, internal numbers have to be represented as valid PSTN numbers, and PSTN numbers should be shown with access code 9 internally. Recall from Chapter 1, “Identifying Issues in a Multisite Deployment,” that the ANI is the number calling from, and the DNIS is the number calling to.

Note Adding the access code (and changing 10-digit PSTN numbers to 11-digit PSTN numbers, including the long-distance 1 digit) to the ANI of incoming calls is not required. Adding it, however, allows users to call back the number from call lists (such as received calls or missed calls) without having to edit the number by adding the required access code.

Transformation of Incoming Calls Using ISDN TON

The ISDN TON can specify the format of a number, such as how ANI or DNIS is represented for calls to and from the PSTN. To have a unique, standardized way to represent PSTN numbers in CUCM, the numbers have to be transformed based on the TON.

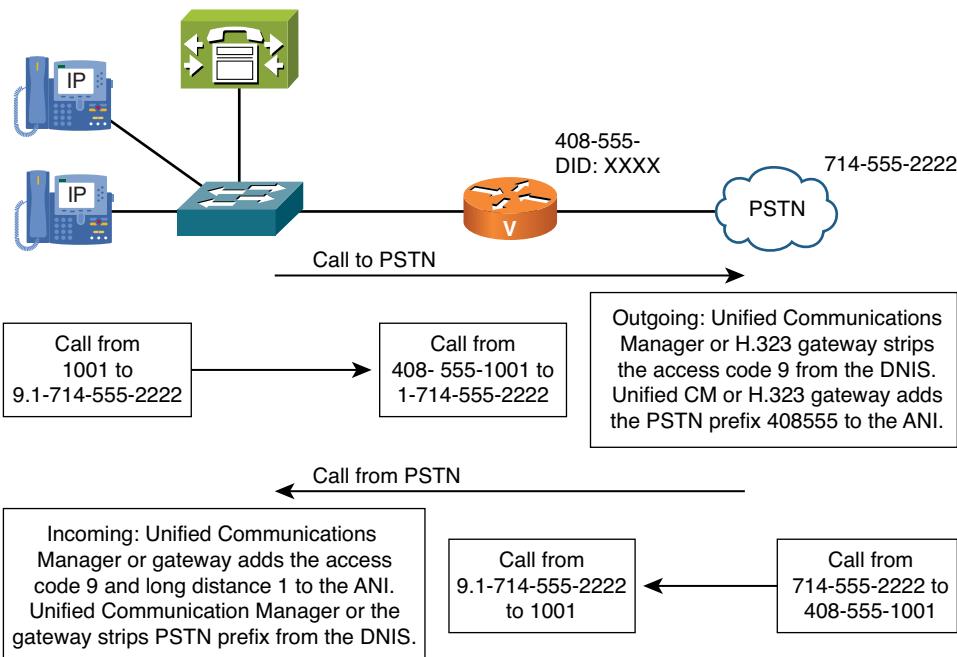


Figure 4-5 *PSTN Access Example*

U.S. TON in ISDN provides information about number format:

- **Subscriber:** Seven-digit subscriber number: three-digit exchange code, four-digit station code
- **National:** Ten-digit number: three-digit area code, seven-digit subscriber number
- **International:** Variable length (11 digits for U.S. numbers):
- **Country code:** One digit for U.S. country code; one, two, or three digits for all other countries
- **Area code:** Three digits for U.S. area code
- **Subscriber number:** Seven digits for U.S. subscriber number

For example, if the calling number of an incoming PSTN call is received with a TON subscriber, the PSTN access code can be prefixed so that the user can place a callback on his IP Phone without editing the number. If the calling number is in national format, the PSTN access code and the national access code are prefixed. If a calling number is received with an international TON, the PSTN access code and the international access code are prefixed. In countries with fixed-length numbering plans, such as the U.S. and Canada, transforming the numbers is not required because users can identify the type of calling number that is based on the length. In this case, users can manually prefix the necessary access codes.

However, in countries with variable-length numbering plans, such as Great Britain, it can be impossible to identify whether the call was received from the local area code, from

another area code of the same country, or from another country by just looking at the number itself. In such cases, the calling numbers of incoming PSTN calls have to be transformed based on the TON.

Note Figure 4-5 is based on the North American Numbering Plan (NANP), which applies to the United States, Canada, and several Caribbean nations, as described at www.nanpa.com.

Figure 4-6 shows an example of performing TON-based digit manipulation based on the incoming call's ANI.

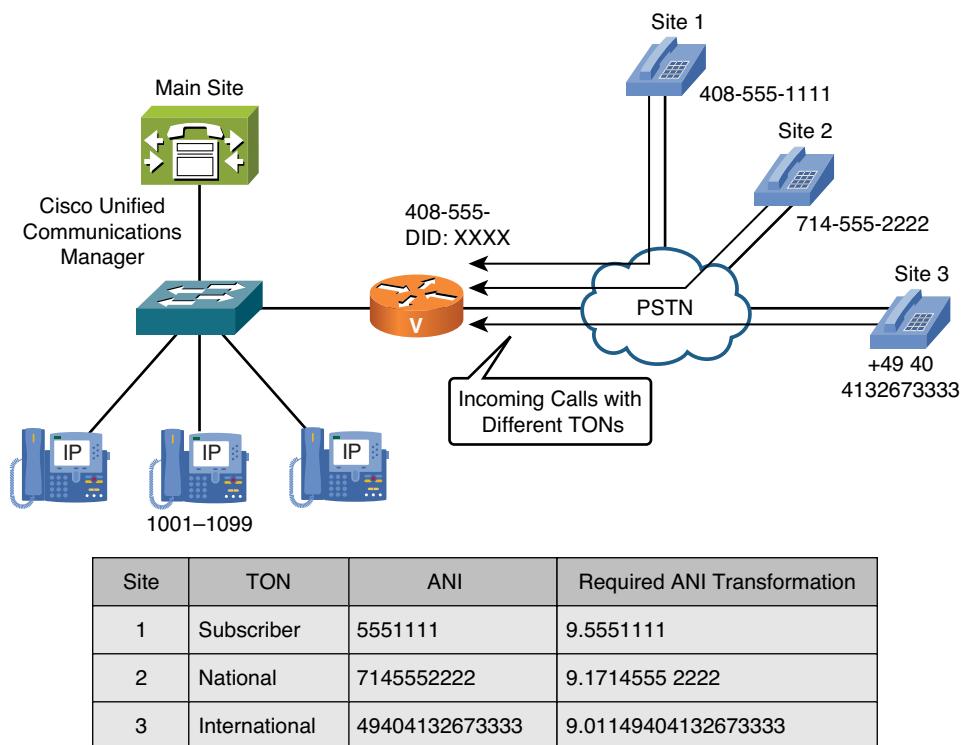


Figure 4-6 ISDN TON: ANI Transformation of an Incoming Call

In Figure 4-6, three different calls are received at the main site gateway:

- The first call is received from the same area code (site 1) with a subscriber TON and a seven-digit number. This number only needs to be prefixed with access code 9.
- The second call, received with national TON and ten digits (site 2), is modified by adding access code 9 and the long-distance 1, both of which are required for placing calls back to the source of the call.

- The third call is received from Germany (site 3), with an international TON. For this call, the access codes 9 and 011 have to be added to the received number, which begins with Germany's E.164 country code of 49. Note that 011 is the NANP international access code, which is different for calls originating outside the NANP.

The end result benefits an internal user who receives but misses any calls from these sites and wants to easily call back any of these numbers without editing it from his missed call list.

Note Figure 4-6 demonstrates the commonly used access code 9 to dial out to the PSTN. It is perfectly acceptable for an organization to choose another access code, such as 8, or no access code. The required ANI transformation digits in this example would be changed accordingly.

Implementing Selective PSTN Breakout

A centralized multisite deployment typically has multiple PSTN gateways, usually one per site. Selective PSTN breakout ensures that local gateways are used to access the PSTN.

There are two ways to select the local gateway for PSTN calls. One way is to configure a site-specific set of route patterns, partitions, CSSs, route lists, and route groups. If you apply a site-specific CSS at the end, a site-specific route group is used. This implementation model was the only one available before CUCM version 7.

With CUCM version 7 and later, the local route group feature was introduced. With local route groups, all sites that share the same PSTN dial rules can use one and the same route pattern (or set of route patterns). The route pattern (or set of route patterns) is put into a systemwide route list, which includes the local route group. At the device pool of the calling device, one of the configured route groups is configured to be the Standard Local Route Group for this caller. In this model, the route group used is determined by the device pool of the calling device, not by its CSS. The local route group feature simplifies dial plans because it eliminates the need for duplicate CSSs, partitions, route patterns, and route lists. Since local route groups have been introduced, they are the preferred method for local gateway selection because they can significantly reduce the total number of route patterns in a multisite dial plan.

Configuring IP Phones to Use Local PSTN Gateway

In a multisite deployment, there are typically multiple PSTN gateways, usually one per remote site. Figure 4-7 demonstrates that selective PSTN breakout ensures that local gateways are used to access the PSTN.

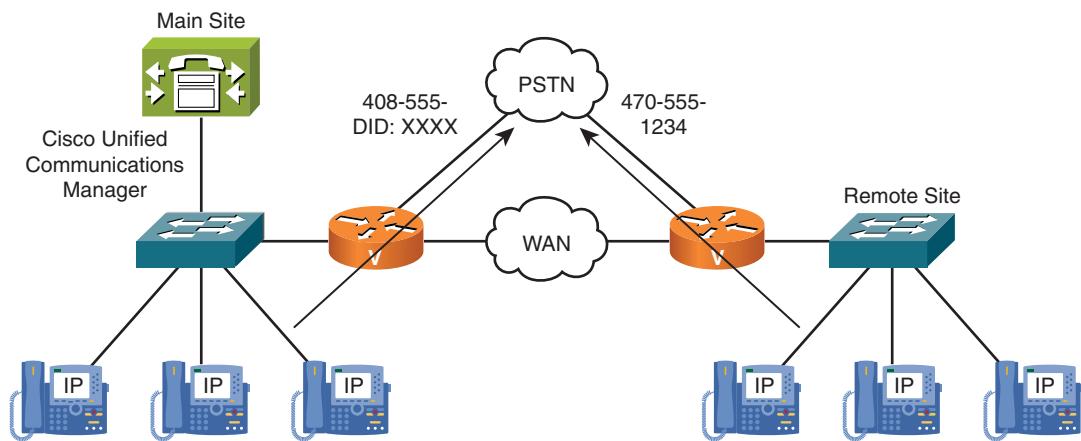


Figure 4-7 Configure IP Phones to Use a Local PSTN Gateway

From a dial plan perspective, you can create one 9@ route pattern (assuming that the NANP is used). This route pattern is in a partition that is part of a global CSS used by all phones. The route pattern refers to a systemwide route list that is configured to use the local route group. At the site-specific device pools, the standard local route group is set to the route group that includes the site-specific gateway.

In Figure 4-7, there would be a device pool for the main site and a device pool for the remote site. There would be a main site route group, including the main site gateway, and a remote site route group, including the remote site gateway. IP Phones at the main site and remote site can now be configured with the same CSS. They all will match the same route pattern and, hence, use the same route list. Based on the local route group feature, however, they will always use their local PSTN gateway for PSTN breakout because the local route group uses the device pool for each location.

Note The local route group is configured with NANP PreDot digit stripping, by default. If the H.323 gateway expects calls that are received from CUCM and that would be routed to the PSTN to include the PSTN prefix 9, appropriate digit manipulation has to be configured in CUCM. In this case, the best solution is to configure the called-party transformation patterns and apply gateway-specific called-party transformation CSS at the gateways in CUCM.

Note If greater control over restricting outbound dialing is required by implementing CSSs and partitions, more specific route patterns should be created instead of those using the generic @ wildcard.

Implementing PSTN Backup for On-Net Intersite Calls

Figure 4-8 shows a multisite decentralized deployment with two sites. Each site has its own CUCM cluster. Intersite calls use the intercluster trunk (ICT) or a SIP trunk over the IP WAN to the other cluster. If the IP WAN link fails for any reason, because both sites have access to the PSTN, the PSTN is used as a backup for intersite calls. Note that proper digit manipulation must take place if the calls are routed through the PSTN.

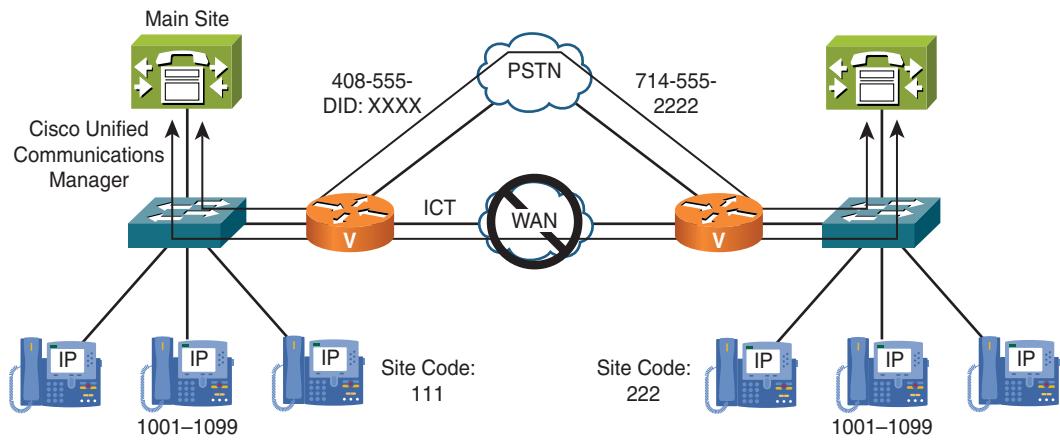


Figure 4-8 Implementing PSTN Backup for On-Net Intersite Calls

To ensure that phones at different sites always use their local gateway for PSTN backup, a route list is configured that includes the ICT as the first option and the local route group as the second option. This way, there is no need to have multiple, site-specific route lists with a different, site-specific route group as the second entry.

Digit-Manipulation Requirements for PSTN Backup of On-Net Intersite Calls

PSTN backup for on-net calls can be easily provided by route lists and route groups giving priority to the ICT over the PSTN gateway, as shown in Figure 4-9.

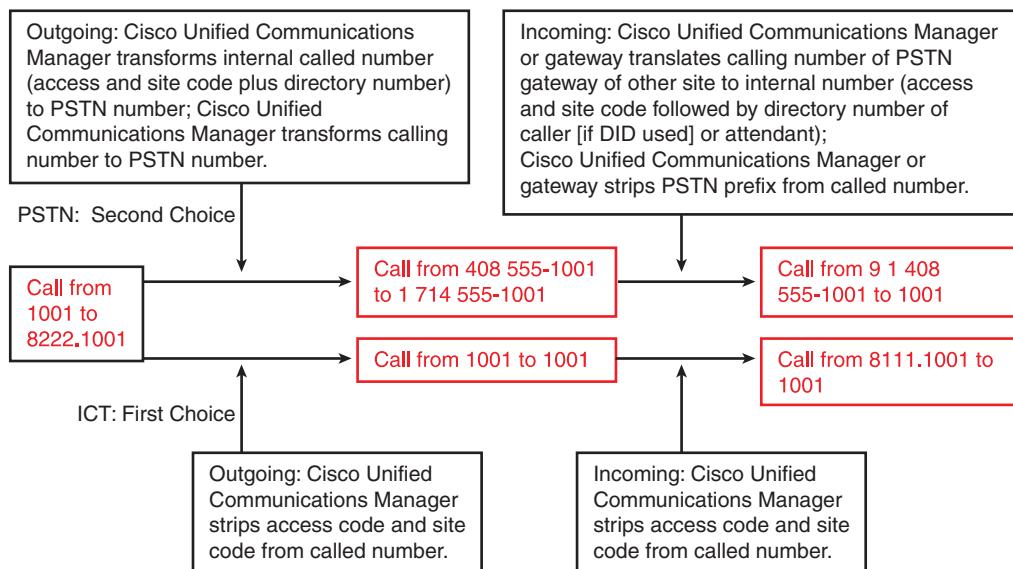


Figure 4-9 Digit-Manipulation Requirements for PSTN Backup of On-Net Intersite Calls

When using a PSTN backup for on-net calls, you must address internal versus external dialing. Although on-net calls usually use site codes and directory numbers, calls sent through the PSTN have to use E.164 numbers. Digit-manipulation requirements vary, depending on the path that is taken for the call:

- Digit-manipulation requirements when using the ICT, which is the first choice in the route list and route group:
 - At the calling site: The access and site code are removed from DNIS.
 - At the receiving site: The access and site code are added to the ANI. (This can also be done on the calling site.)
- Digit-manipulation requirements when using the PSTN (secondary choice in the route list and route group):
 - At the calling site: The internal DNIS comprising an access code, site code, and directory number is transformed into the PSTN number of the called phone. The ANI is transformed into the PSTN number of the calling phone. When different digit-manipulation configuration is required, depending on the selected path, the digit-manipulation settings are either configured at a path-specific route group or by using global transformations.

Note If DID is not supported, the site's PSTN number is used in DNIS and ANI instead of the IP Phone's PSTN number.

- At the receiving site: The PSTN ANI is recognized as a PSTN number of an on-net connected site and is transformed into the internal number: access and site code, followed by the directory number of the calling phone (if DID is used at the calling site) or of the attendant of the calling site (if DID is not used at the calling site). The DNIS is transformed into an internal directory number and is routed to the IP Phone (if DID is used at the receiving site) or to an attendant (if DID is not used at the receiving site).

Implementing TEHO

When you implement TEHO, as shown in Figure 4-10, PSTN breakout occurs at the gateway closest to the dialed PSTN destination. Basically, this action occurs because you create a route pattern for each destination area that can be reached at different costs. These route patterns refer to route lists that include a route group for the TEHO gateway first and the local route group as the second entry so that the local gateway can be used as a backup when the IP WAN cannot be used.

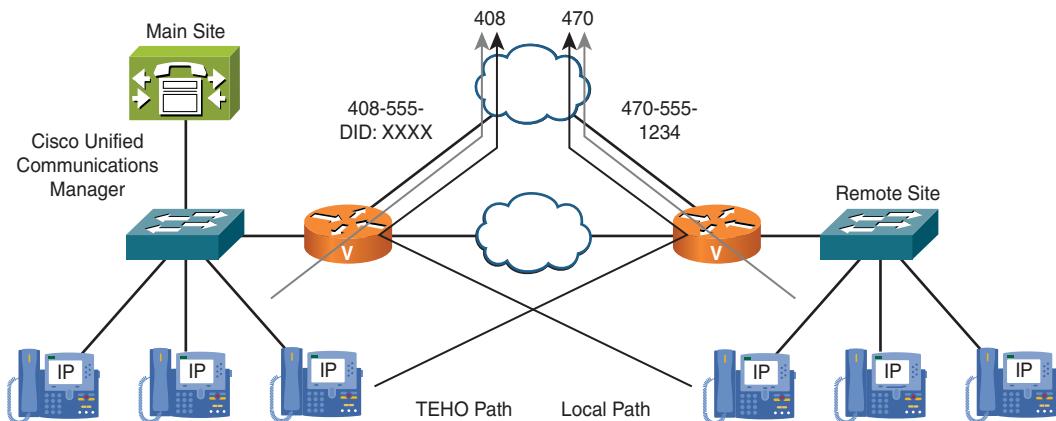


Figure 4-10 Implementing TEHO

Using TEHO might not be permitted in your country or by your provider. There can also be issues with emergency calls. Therefore, ensure that your planned deployment complies with the legal requirements of each location.

When using backup TEHO, consider the following potential issues regarding the number you want to use for the calling number of the outgoing call. Basically, there are two options:

- **Use the PSTN number of the originating site at the TEHO gateway:** When using the PSTN number of the originating device for the caller ID of a TEHO call, the called party is not aware that TEHO has been used. Standard numbering is maintained for all PSTN calls, regardless of the egress gateway; callbacks to the calling number are possible. However, sending calls to the PSTN with PSTN caller IDs of other sites

might not be permitted, or the receiving PSTN provider might remove caller IDs from the signaling messages.

Caution Sending calls out of a gateway with the calling number of another site might not be permitted in your country or by your provider. There can also be issues with emergency calls. Therefore, ensure that your planned deployment complies with legal requirements.

- Replace the PSTN number of the originating site by the PSTN number of the TEHO site: When using the calling number of the backup gateway, called parties may get confused about the number that should be used when calling back. For example, they might update their address books with the different number and inadvertently end up sending calls to the TEHO site every time they call. Furthermore, DID ranges would have to include remote phones or IVR scripts (automated attendants) to be able to route calls to phones located in any site, regardless of where the PSTN call was received.

Caution Using a remote gateway for PSTN access might not be permitted in your country or by your provider. There can also be issues with emergency calls. Therefore, ensure that your planned deployment complies with legal requirements.

In general, it is highly recommended that you use the local route group feature when implementing TEHO. To provide a local backup for TEHO calls, call processing must route all calls differently, based on the source (physical location) and on the dialed number, when the TEHO path cannot be used. When you are not using local route groups, this approach can require a huge amount of route patterns, partitions, CSS, and route lists, resulting in complex dial plans. Such dial plans are difficult to maintain and troubleshoot.

Note You also must consider call admission control (CAC) when implementing TEHO. When the primary (TEHO) path is not admitted as a result of reaching the CAC call limit, calls should be routed through the local gateway. More information about CAC is provided in Chapter 9, “Implementing Call Admission Control.”

TEHO Example Without Local Route Groups

In Figure 4-11, there are five sites in a centralized call-processing deployment. Each site uses identical call-routing policies and numbering plans, but the site-specific details of those policies prevent customers from provisioning a single set of route pattern and route list that works for all sites. This principle applies when no local route groups are used (as it was the case before CUCM version 7). Although the primary path for a given TEHO PSTN destination is always the same (the appropriate TEHO gateway), the backup path is different for each site (the local gateway of the site where the call has been placed). Without a backup path, TEHO requires only one route pattern per TEHO destination

number and refers only to the corresponding TEHO gateway from its route list and route group. However, as the IP WAN is used for TEHO calls, it is not recommended that you configure a single path only. Therefore, TEHO configurations easily end up in huge dial plans—each site requires a different route pattern and route list for each of the other sites. In addition, each site has one generic route pattern for non-TEHO PSTN destinations (using the local gateway).

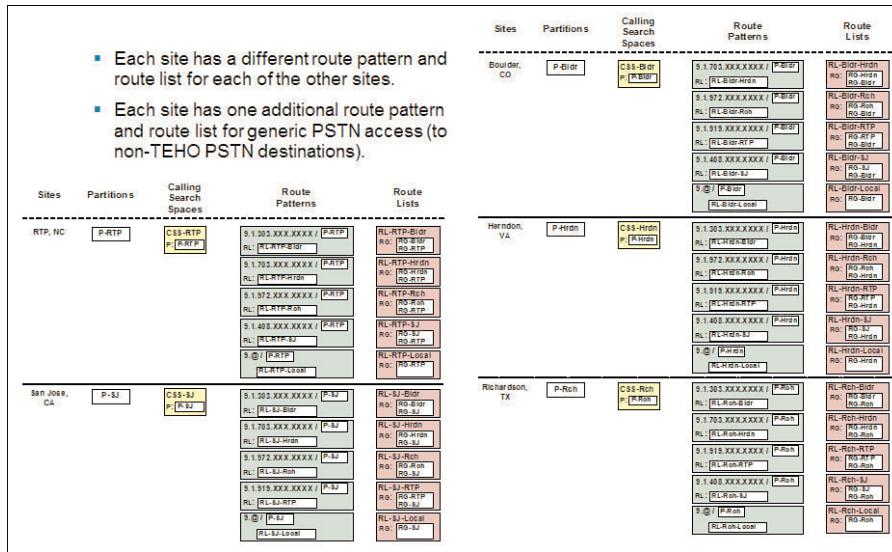


Figure 4-11 TEHO Example Without Local Route Groups

Some route patterns in the figure include the . character multiple times (for example, 9.1.703.XXX.XXXX). In this case, the . character illustrates the different components of the number patterns in order to make it easier to interpret the patterns. In reality, the . in route patterns is used only once when being referenced by a corresponding DDI (for example, the PreDot DDI).

Figure 4-12 illustrates the configuration for one site (Boulder). There is a TEHO route pattern for area code 703 (Herndon) that refers to the route list RL-Bldr-Hrdn. This route list uses the Herndon gateway first and the (local) Boulder gateway as a backup. There is also a route pattern for area code 972 (Richardson), again using a dedicated route list for calls from Boulder to Richardson (with the Richardson gateway preferred over the local Boulder gateway). There are two more such constructs for the other two sites. Finally, there is a generic PSTN route pattern (9.@@) for all other PSTN (non-TEHO) calls. The generic PSTN route pattern refers to a route list that contains only the local gateway. All five route patterns are in the Boulder partition (P-Bldr) so that they can be accessed only by Boulder phones (using the Boulder CSS CSS-Bldr).

In summary, when using CUCM v6.x or earlier, for each TEHO destination, there is a route pattern per originating site that refers to a dedicated route list using the appropriate

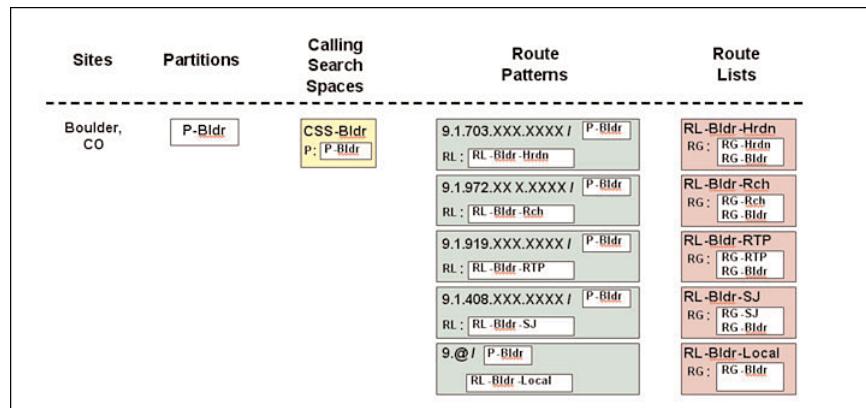


Figure 4-12 TEHO Example Without Local Route Groups, Continued

TEHO gateway before the local gateway. For n sites, there are $n * (n - 1)$ of these patterns. In addition, each site has a generic route pattern referring to a dedicated route list containing the local gateway only. This generic route pattern increases the total number of route patterns and route lists to $n * n$. In large TEHO deployments, this approach does not scale.

Some route patterns in the figure include the . character multiple times (for example, 9.1.703.XXX.XXXX). In this case, the . character illustrates the different components of the number patterns in order to make it easier to interpret the patterns. In reality, the . in route patterns is used only once when being referenced by a corresponding DDI (for example, the PreDot DDI).

TEHO Example with Local Route Groups

As shown in Figure 4-13, when implementing TEHO with local route groups, you can reduce the number of route patterns and route lists from $n * n$ to $n + 1$.

This reduction is possible because, for each TEHO destination, one route pattern is sufficient. The route pattern refers to a destination-specific route list, which lists the route group containing the TEHO gateway first, followed by the entry Default Local Route Group. Because the backup path is now determined by the device pool of the calling device instead of being explicitly listed in the route list, the route list has a generic format and can be used by all sites.

For every TEHO destination, one route pattern and one route list is required. In addition, for non-TEHO destinations, again, a single route pattern and route list can be used by all sites. This route pattern (9. @) refers to a route list, which includes the Default Local Route Group entry.

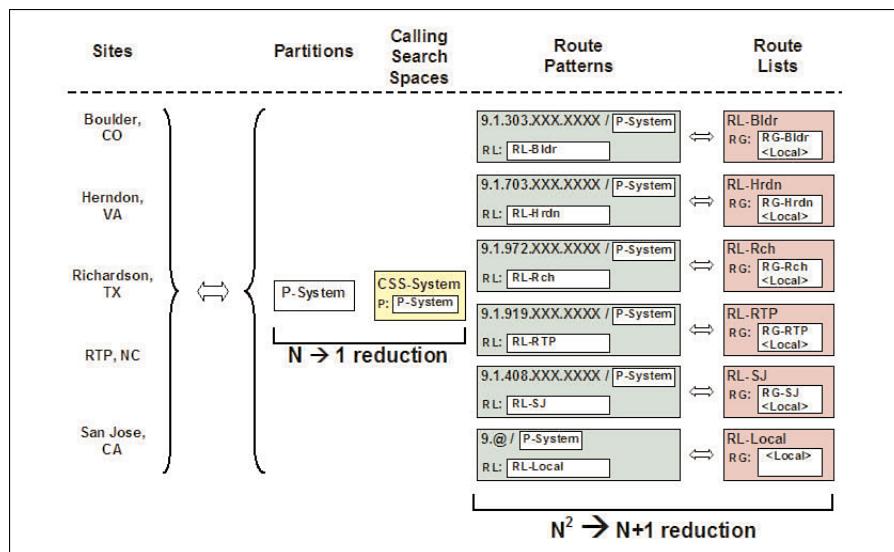


Figure 4-13 TEHO Example with Local Route Groups

Note Some route patterns in the figure include the . character multiple times (for example, 9.1.703.XXX.XXXX). In this case, the . character illustrates the different components of the number patterns in order to make it easier to interpret the patterns. In reality, the . in route patterns is used only once when being referenced by a corresponding DDI (for example, the PreDot DDI).

In Figure 4-13, with five remote sites and one local site, using local route groups simplifies the dial plan as follows:

- The number of route patterns and route lists for TEHO destinations is reduced from $n * (n - 1)$ to n . In this example, the reduction is from 20 to 5.
- The number of route patterns and route lists for non-TEHO destinations is reduced from n to 1 (5 to 1, in this example).
- Thus, the total number of route patterns and route lists is reduced from $n * n$ to $n + 1$ (25 to 6).
- The number of partitions and CSS is reduced from n to 1 (5 to 1).
- The number of gateways, route groups, and device pools remains the same: n .

Implementing Globalized Call Routing

With globalized call routing, all calls that involve external parties are based on one format with the purpose of simplifying international multisite dial plans. All numbers are normalized as follows:

- **Normalized called-party numbers:** E.164 format with the + prefix is used for external destinations. Therefore, called-number normalization is the result of globalization. Internal directory numbers are used for internal destinations. Normalization is achieved by stripping or translating the called number to internally used directory numbers.
- **Normalized calling-party numbers:** E.164 global format is used for all calling-party numbers, except calls from an internal number to another internal number. Such purely internal calls use the internal directory number for the calling party number. If sources of calls (users at phones, incoming PSTN calls at gateways, calls received through trunks, and so on) do not use the normalized format, the localized call ingress must be normalized before being routed. This requirement applies to all received calls (coming from gateways, trunks, and phones), and it applies to both the calling- and called-party numbers.

Note Except for the internal calls that were mentioned (where the destination is a directory number and, in the case of an internal source, the source is a directory number), all numbers are normalized to the E.164 global format. Therefore, call routing based on the normalized numbers is referred to as *globalized call routing*.

After the call is routed and path selection (if applicable) is performed, the egress device typically must change the normalized numbers to the local format. This situation is referred to as *localized call egress*. Localized call egress applies to these situations:

- **Calling- and called-party numbers for calls that are routed to gateways and trunks:** If the PSTN or the telephony system on the other side of a trunk does not support globalized call routing, the called- and calling-party numbers must be localized from the global format. For example, the called-party number +494012345 is changed to 011494012345 before the call is sent out to the PSTN in the United States.
- **Calling-party numbers for calls that are routed from gateways or trunks to phones:** This situation applies to the phone user who does not want to see caller IDs in a global format. For example, if a user at a U.S. phone wants to see the numbers of PSTN callers who are in the same area code, that user may want to see each number as a seven-digit number and not in the +1XXXXXXXXXX format.

Localized call egress is not needed for the called-party number of calls that are routed to phones, because internal directory numbers are the standard (normalized) format for internal destinations (regardless of the source of the call). These numbers might have been dialed differently initially; however, in that case, this localized call ingress was normalized before call routing. Localized call egress is also not required for the calling-party

number of internal calls (internal to internal) because, again, the standard for the calling-party number of such calls is to use internal directory numbers.

Globalized call routing simplifies international dial plans because the core call-routing decision is always based on the same format, regardless of how the number was initially dialed and how the number looks at the egress device.

Globalized Call Routing: Number Formats

Figure 4-14 describes the number formats that are used by globalized call routing and explains some commonly used expressions.

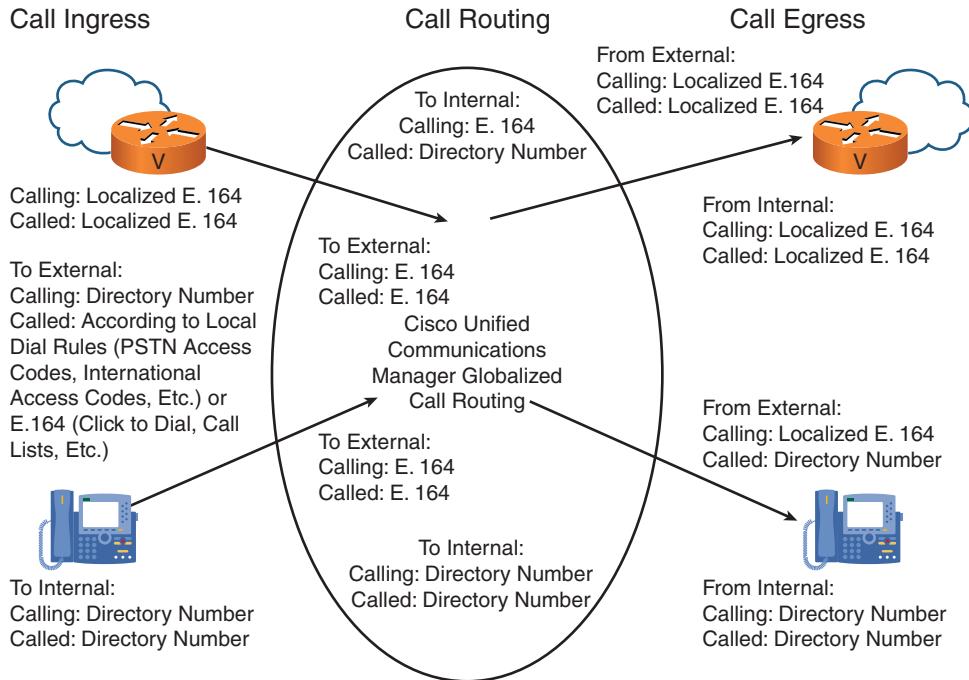


Figure 4-14 Globalized Call Routing Number Formats

Table 4-1 explains some commonly used expressions to describe globalized call routing, as illustrated in Figure 4-14.

Table 4-1 Globalized Call Routing Terminology

Term	Description
Number normalization	The process of changing numbers to a well-defined, standardized (normalized) format. In this case, all external phone numbers are changed to global E.164 format.
Number globalization	The process of changing numbers to global E.164 format. Example: Because the normalized format is E.164, you normalize a called number (for example, 4085551234) by globalizing the number—that is, by changing the number to global format (for example, +14085551234).
Number localization	The process of changing from normalized format (in this case, global format) to local format. Usually, the local format is the shortest possible format that does not conceal relevant information. An example of local format is 555-1234 instead of +1 408 555-1234, or 972 333-4444 instead of +1 972 333-4444 (assuming that the device where localization occurs is located in the +1408 area).
Incoming PSTN call	Call from PSTN to internal phone. Like all calls, such a call consists of two call legs (incoming and outgoing). <i>See also</i> call ingress and call egress in this table. On an incoming PSTN call, the incoming call leg (call ingress) is PSTN gateway to CUCM; the outgoing call leg (call egress) is CUCM to internal phone.
Outgoing PSTN call	Call from internal phone to PSTN. Like all calls, such a call consists of two call legs (incoming and outgoing). On an outgoing PSTN call, the incoming call leg (call ingress) is internal phone to CUCM; the outgoing call leg (call egress) is CUCM to PSTN gateway.
Call ingress	Incoming call leg—call received by CUCM
Call egress	Outgoing call leg—call routed to destination by CUCM
Localized E.164 (number)	PSTN number in partial (subscriber, national, international) E.164 format.
E.164 (number)	PSTN number in complete E.164 format with + prefix.

On the left side of Figure 4-14, call ingress is illustrated by these two types of call sources:

- **External callers:** Their calls are received by CUCM through a gateway or trunk. In the case of a PSTN gateway, calling- and called-party numbers are usually provided in localized E.164 format.

- **Internal callers:** Their calls are received from internal phones. In the case of calls to internal destinations (for example, phone to phone), calling- and called-party numbers are typically provided as internal directory numbers. In the case of calls to external destinations (for example, phone to PSTN), the calling number is the directory number (at call ingress time), and the called number depends on the local dial rules for PSTN access. These dial rules can differ significantly for each location.

The center of Figure 4-14 illustrates the standards defined for normalized call routing. As previously mentioned, because most calls use global E.164 format, this type of call routing is also referred to as globalized call routing. Here are the defined standards:

- **External to internal:**
 - **Calling-party number:** E.164
 - **Called-party number:** Directory number
- **External to external (if applicable):**
 - **Calling-party number:** E.164
 - **Called-party number:** E.164
- **Internal to internal:**
 - **Calling-party number:** Directory number
 - **Called-party number:** Directory number
- **Internal to external:**
 - **Calling-party number:** E.164
 - **Called-party number:** E.164

At the right side of Figure 4-14, call egress is illustrated by two types of call targets:

- **Gateways:** When sending calls to the PSTN, localized E.164 format is used for both the calling- and called-party numbers. The format of these numbers (especially of the called-party number) can significantly differ based on the location of the gateway. For example, the international access code in the United States is 011, and in most European countries, it is 00.
- **Phones:** When a call from an internal phone is sent to another internal phone, the call should be received at the phone with both the calling and called number using internal directory numbers. Because this format is the same format that is used by globalized call routing, there is no need for localized call egress in this case. When a call from an external caller is sent to an internal phone, most users (especially users in the United States) prefer to see the calling number in localized format. (For example, national and local calls should be displayed with 10 digits.) The called number is the directory number.

It should be evident from Figure 4-14 that there are several situations where the numbers provided at call ingress do not conform to the normalized format to be used for call routing. These situations also apply to call egress, where the normalized format is not always used when the call is delivered. Therefore, localized call ingress has to be normalized (that is, globalized), and the globalized format has to be localized at call egress.

Normalization of Localized Call Ingress on Gateways

Figure 4-15 illustrates how localized call ingress on gateways gets normalized.

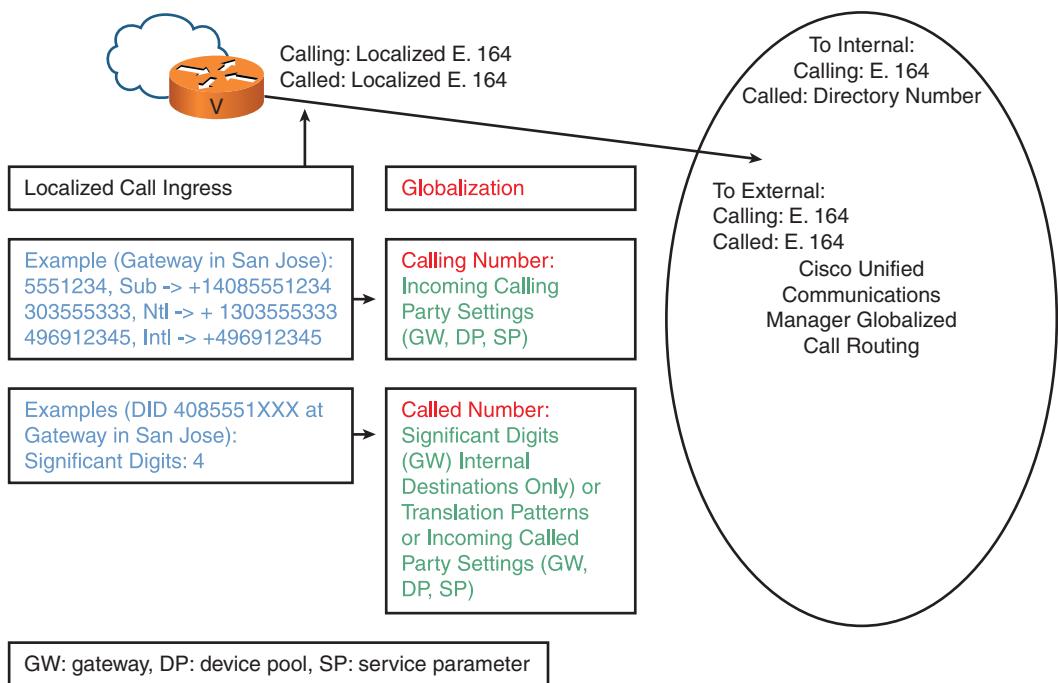


Figure 4-15 Normalization of Localized Call Ingress on Gateways

Here are the requirements for normalizing localized call ingress on gateways:

- Changing the calling number from localized E.164 format to global E.164 format
- Changing the called number from localized E.164 format to directory numbers for calls to internal destinations
- Changing the called number from localized E.164 format to global E.164 format for calls to external destinations (if applicable)

As shown in Figure 4-15, the calling number can be normalized by incoming calling-party settings. They are configured at the gateway or at the device pool, or they can be configured as CUCM service parameters. Figure 4-15 provides an example for a gateway in San Jose:

- Prefix for incoming called-party numbers with number type subscriber: +1408
- Prefix for incoming called-party numbers with number type national: +1
- Prefix for incoming called-party numbers with number type international: +

The called number can be normalized by significant digits that are configured at the gateway (applicable only if no calls to other external destinations are permitted and a fixed-length number plan is used), or by translation patterns, or by incoming called-party settings (if available at the ingress device). In Figure 4-15, the gateway is configured with four significant digits.

Normalization of Localized Call Ingress from Phones

Figure 4-16 illustrates how localized call ingress on phones gets normalized.

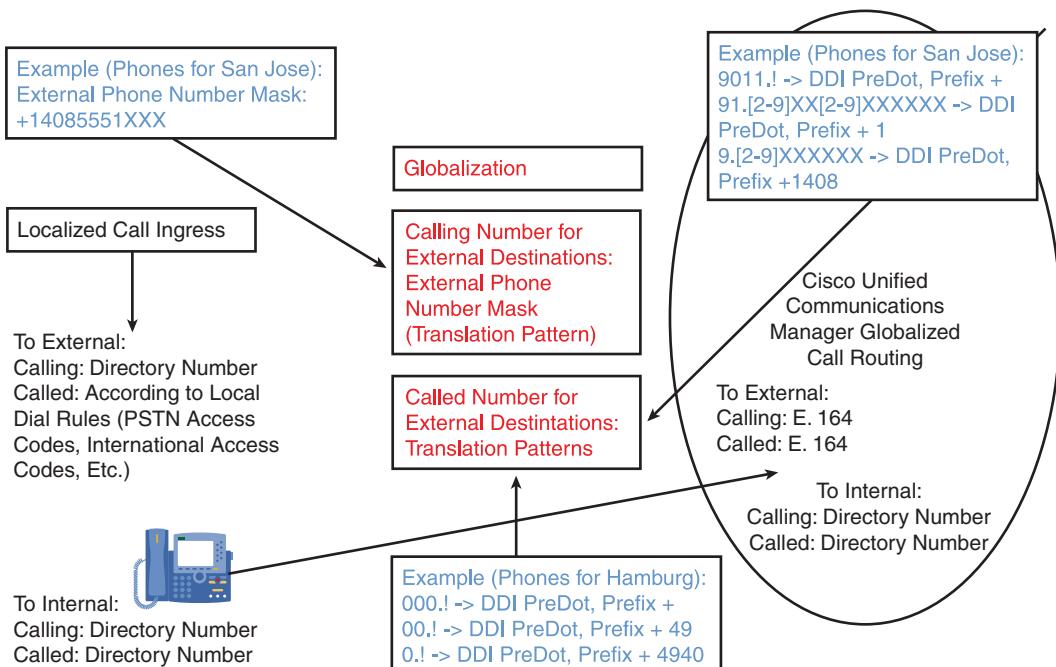


Figure 4-16 Normalization of Localized Call Ingress from Phones

The requirements for normalizing localized call ingress on phones are as follows:

- **For calls to external destinations:** Changing the calling number from an internal directory number to E.164 format. Changing the called number to E.164 format if any other format was used (according to local dial rules).
- **For calls to internal destinations:** No normalization is required.

As shown in Figure 4-16, you can normalize the calling-party number for calls to external destinations by configuring an external phone number mask (in E.164 format) at the phone. You can normalize the called-party number by using translation patterns where you would also apply the external phone-number mask to the calling-party number. In Figure 4-16, examples for phones that are located in Hamburg, Germany, and San Jose, California, are given.

Localized Call Egress at Gateways

Figure 4-17 illustrates how you can implement localized call egress at gateways.

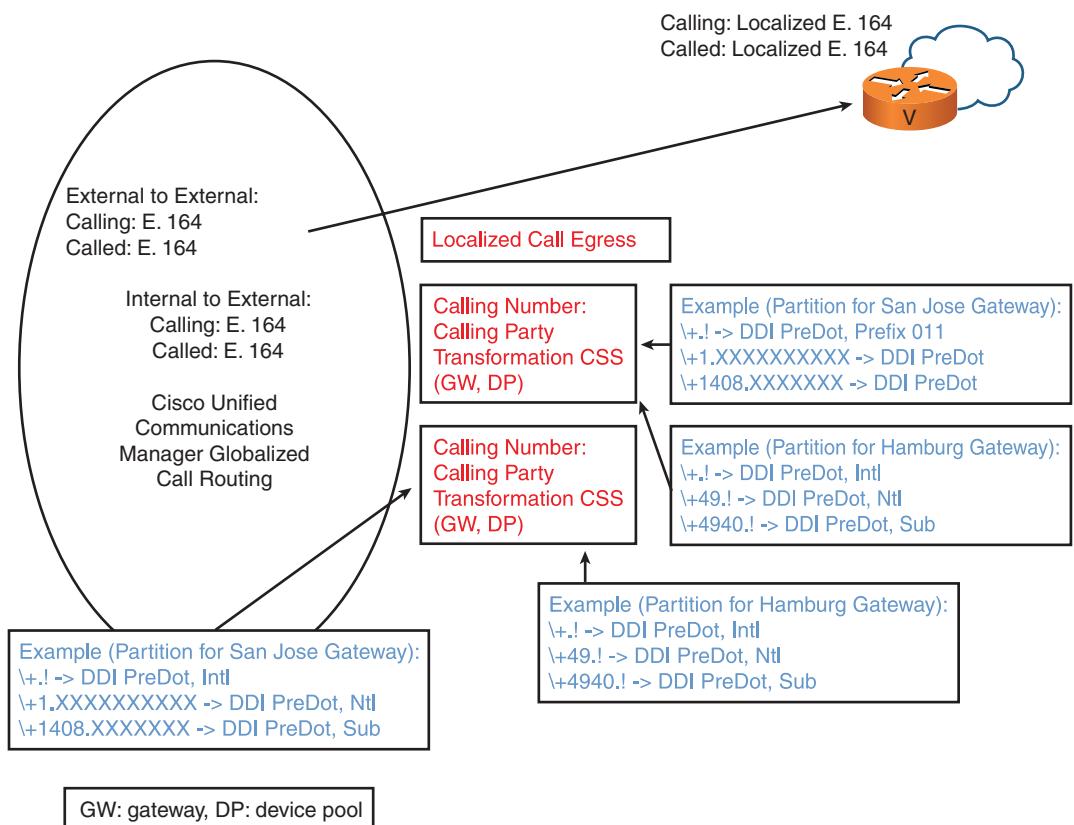


Figure 4-17 Localized Call Egress at Gateways

The only requirement is to change the calling and called number from global E.164 format to localized E.164 format. You can change the format by configuring called- and calling-party transformation patterns, putting them into partitions, and assigning the appropriate called- and calling-party transformation CSS to gateways. You can configure called- and calling-party transformation CSS at the device (gateway or trunk) and at the device pool.

Table 4-2 shows the configuration of the called-party transformation patterns that are applicable to the San Jose gateway (based on partition and called-party transformation CSS).

Table 4-2 *Called Party Transformation Patterns for the San Jose Gateway*

Transformation Pattern	Performed Transformation
\+!	DDI PreDot, Prefix 011
\+.1XXXXXXXXXX	DDI PreDot
\+1408.XXXXXXXX	DDI PreDot

Note In Figure 4-17, the San Jose gateway does not use number types. Therefore, 011 must be prefixed on international calls, and the 1 of national calls is conserved. For local calls, only the last seven digits are used.

Table 4-3 shows how you configure the called-party transformation patterns that are applicable to a gateway in Hamburg, Germany (based on partition and called-party transformation CSS).

Table 4-3 *Called-Party Transformation Patterns for the Hamburg, Germany, Gateway*

Transformation Pattern	Performed Transformation
\+!	DDI PreDot; number type: international
\+49!	DDI PreDot; number type: national
\+4940.!	DDI PreDot; number type: subscriber

Note In this example, the Hamburg gateway uses number types instead of international (00) or national (0) access codes (in contrast to the San Jose gateway, which does not use number types).

Table 4-4 shows how you configure calling-party transformation patterns that are applicable to the San Jose gateway (based on partition and calling-party transformation CSS).

Note In the example, subscriber, national, and international number types are used at the San Jose gateway for the calling-party number. If no number types were used, because of the fixed-length numbering plan, the number type could also be determined by its length

(seven-digit numbers when the source of the call is local, ten-digit numbers when the source of the call is national, or more than ten digits when the source of the call is international). In reality, however, countries that use the NANP typically use ten-digit caller IDs for both national and local callers.

Having nonlocal calling-party numbers implies the use of TEHO or PSTN backup over the IP WAN. This scenario is not permitted in some countries or by some PSTN providers.

Some providers verify that the calling-party number on PSTN calls they receive matches the locally configured PSTN number. If a different PSTN number is set for the caller ID, either the call is rejected or the calling-party number is removed or replaced by the locally assigned PSTN number.

Table 4-4 Calling-Party Transformation Patterns for the San Jose Gateway

Transformation Pattern	Performed Transformation
\+!	DDI PreDot; number type: international
\+1.XXXXXXXXXXX	DDI PreDot; number type: national
\+1408.XXXXXXX	DDI PreDot; number type: subscriber

Table 4-5 shows how you configure calling-party transformation patterns that are applicable to a gateway in Hamburg, Germany (based on partition and calling-party transformation CSS).

Table 4-5 Calling-Party Transformation Patterns for the Hamburg, Germany, Gateway

Transformation Pattern	Performed Transformation
\+!	DDI PreDot; number type: international
\+49!	DDI PreDot; number type: national
\+4940!	DDI PreDot; number type: subscriber

Localized Call Egress at Phones

Figure 4-18 illustrates how you can implement localized call egress at phones.

The only requirement is that you change the calling number from global E.164 format to localized E.164 format. You can change the format by configuring calling-party transformation patterns, putting them into partitions, and assigning the appropriate calling-party transformation CSS to IP Phones. As previously mentioned, you can configure calling-party transformation CSS at the phone and at the device pool.

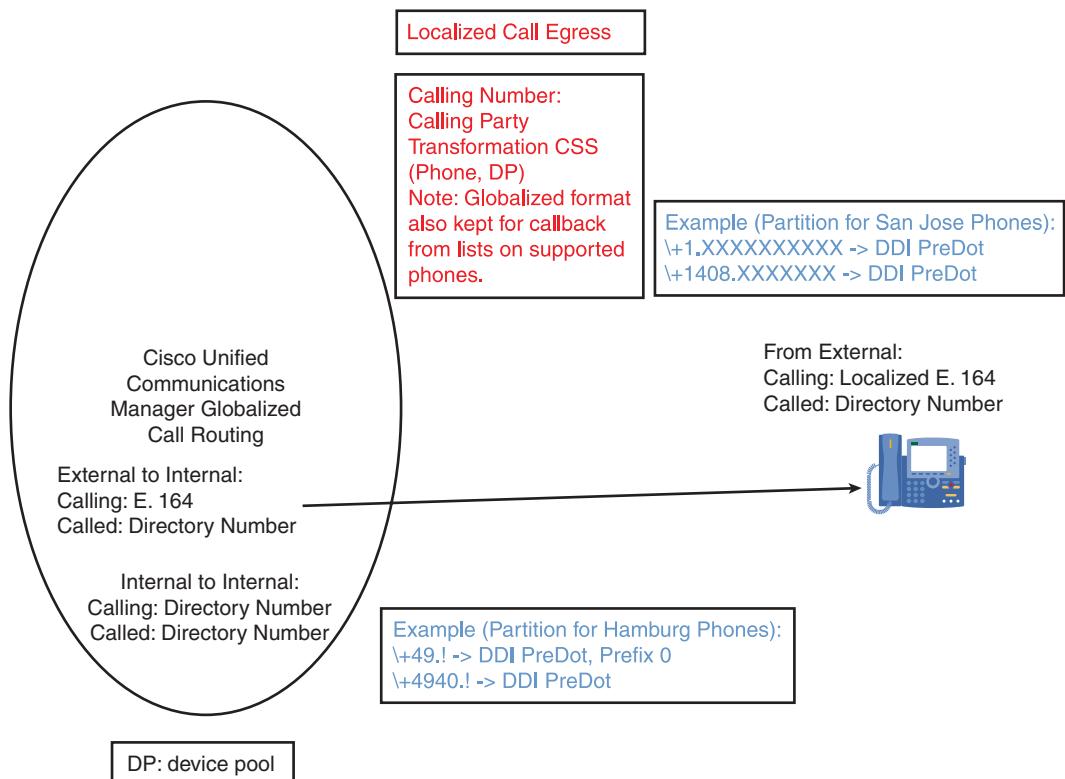


Figure 4-18 Localized Call Egress for t Phones

Table 4-6 shows how you configure the calling-party transformation patterns that are applicable to a phone that is located in San Jose (based on partition and calling-party transformation CSS), as illustrated in Figure 4-18.

In this example, international calls are shown in standard normalized format (E.164 format with + prefix), because there is no \\+! calling-party transformation pattern. National calls are shown with ten-digit caller IDs, and local calls are shown with seven-digit caller IDs.

Table 4-6 Calling-Party Transformation Patterns for San Jose Phones

Transformation Pattern	Performed Transformation
\\+1,XXXXXXXXXX	DDI PreDot
\\+1408.XXXXXXXX	DDI PreDot

Table 4-7 Calling-Party Transformation Patterns for Hamburg, Germany Phones

Transformation Pattern	Performed Transformation
\+49.!	DDI PreDot, Prefix 0
\+4940.!	DDI PreDot

Table 4-7 shows how you configure the calling-party transformation patterns that are applicable to a phone located in Hamburg, Germany (based on partition and calling-party transformation CSS), as illustrated in Figure 4-18.

Note Because there is no \+! calling-party transformation pattern, international calls are preserved in normalized format (E.164 with + prefix). As opposed to the San Jose example, phones located in Hamburg do prefix the national access code (using 0, which is equivalent to the long-distance 1 in the NANP). The reason is that, in Germany, variable-length PSTN numbering plans are used and, therefore, national and local numbers cannot be distinguished based on their length (like in the United States, with seven- and ten-digit numbers). When the national access code 0 is prefixed to numbers that are used by national callers, a user can identify national calls by their leading 0.

Note When users call back PSTN callers, the globalized number is used for the outgoing call. Therefore, there is no need to edit the localized number from a call list and add PSTN access codes and national or international access codes.

Globalized Call-Routing Example: Emergency Dialing

In a multisite deployment with centralized call processing, it might be desirable to simplify emergency dialing by introducing a globalized emergency number (or one globalized emergency number for each emergency service).

Having a globalized emergency number allows roaming users who might not be aware of the local emergency dial rules to use a corporate emergency number that is accessible from all sites.

In addition, however, localized emergency dialing should still be supported, so a user can dial either the locally relevant emergency number or the corporate emergency number.

Here is how to implement such a solution:

- You introduce one or more corporate emergency numbers.
- In addition, you allow localized emergency dialing. It can be limited to local emergency dialing rules per site (for example, an Austrian emergency number can be

dialed only from phones that are located in Austria), or you can globally enable all possible local emergency numbers. Having all possible local emergency numbers that are globally enabled allows a roaming user to use the emergency number that is local to the site where the user is located or the emergency number that the user knows from the home location of the user (for example, a UK user dials 999 while roaming in Austria), or the corporate emergency number.

- If a user dials a localized emergency number, that number is first normalized (that is, translated) to the corporate emergency number. A route pattern exists only for this corporate emergency number, and you configure the corresponding route list to use the local route group.
- At the gateway that processes the call, you localize the corporate emergency number (the globalized emergency number) by using called-party number transformations at the gateway. This localization ensures that, regardless of which emergency number was dialed, the gateway that sends out the emergency call uses the correct number as expected at this site.

Note In deployments with more complex emergency calls, like in the United States with E911, such a solution is not applicable because there are other requirements for emergency calls. In such a scenario, the emergency call is routed via a dedicated appliance (Cisco Emergency Responder) that is reached via a computer telephony integration (CTI) route point.

In Figure 4-19, a corporate emergency number of 888 has been established. In addition, Australian, European Union, and UK emergency numbers are supported at all sites of the enterprise. The appropriate numbers (000, 112, and 999) are translated (normalized) to the corporate (global) emergency number 888. A route pattern 888 exists, which refers to a route list that has been configured to use the local route group. You consider two sites in this example: one in the E.U. and one in the United Kingdom. Each site has its own PSTN gateway (GW in the figure); phones at each site are configured with a site-specific device pool. The device pool of each site has its local route group that is set to a site-specific route group.

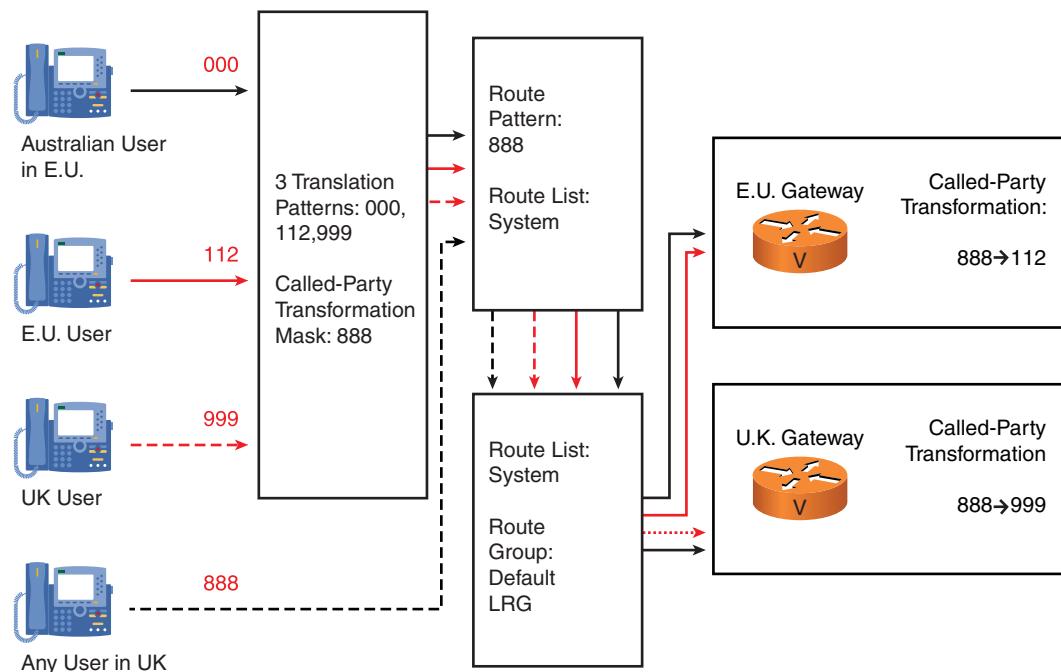


Figure 4-19 Globalized Emergency Dialing Call-Routing Example

The following scenarios examine four emergency calls:

- **A UK user dials 999 (UK emergency number):** The dialed UK emergency number 999 is translated to the corporate emergency number 888. After translation, the 888 route pattern is matched. The route list of the route pattern refers to the local route group. Because the emergency call was placed from a UK phone, the local route group in the device pool of the phone refers to the UK gateway. At that gateway, a global transformation of the called number (from 888 to 999) is configured. Therefore, the call exits the UK gateway with a destination number of 999, which is the appropriate emergency number to be used in the United Kingdom.
- **Any user who is located in the United Kingdom dials 888 (corporate emergency number):** Because no local emergency number was dialed except the corporate emergency number 888, no translation is required. The call immediately matches route pattern 888. The route list of the route pattern refers to the local route group. Because the emergency call was placed from a UK phone, the local route group in the device pool of the phone refers to the UK gateway. At that gateway, a global transformation of the called number (from 888 to 999) is configured. Therefore, the call exits the UK gateway with a destination number of 999, which is the appropriate emergency number to be used in the United Kingdom.
- **An E.U. user dials 112 (E.U. emergency number):** The dialed E.U. emergency number 112 is translated to the corporate emergency number 888. After translation, the

888 route pattern is matched. The route list of the route pattern refers to the local route group. Because the emergency call was placed from an E.U. phone, the local route group in the device pool of the phone refers to the E.U. gateway. At that gateway, a global transformation of the called number (from 888 to 112) is configured. Therefore, the call exits the E.U. gateway with a destination number of 112, which is the appropriate emergency number to be used in the E.U.

- **An Australian user, currently located at an E.U. site, dials 000 (Australian emergency number):** The dialed Australian emergency number 000 is translated to the corporate emergency number 888. After translation, the 888 route pattern is matched. The route list of the route pattern refers to the local route group. Because the emergency call was placed from an E.U. phone, the local route group in the device pool of the phone refers to the E.U. gateway. At that gateway, a global transformation of the called number (from 888 to 112) is configured. Therefore, the call exits the E.U. gateway with a destination number of 112, which is the emergency number in the European Union.

Note The Australian user can use an E.U. phone (with an E.U. extension), use his own device with Device Mobility enabled, or use an E.U. phone with his own extension (by using Cisco Extension Mobility). In all three scenarios, the emergency call would work fine, as described earlier. The reason is that the device pool of the phone will be the E.U. device pool in all three scenarios (with Device Mobility enabled, the home device pool would be replaced by the roaming device pool), and hence the local route group is always the EU-GW.

The only problem would be if the Australian user were using his own device with Device Mobility disabled. In this case, the local route group would refer to the Australian gateway, and the call would be sent through the Australian gateway instead of the local E.U. gateway. The localized egress number would be appropriate for an Australian gateway (transformed to 000), so the user would get connected to an Australian emergency service.

Considering Globalized Call-Routing Interdependencies

Globalized call routing simplifies the implementation of several dial plan features in an international deployment. The affected dial plan features include TEHO, Automated Alternate Routing (AAR), Cisco Unified SRST and CFUR, Cisco Device Mobility, and Cisco Extension Mobility.

If TEHO is configured, the appropriate TEHO gateway is used for the PSTN call. The TEHO route list can include the Default Local Route Group setting as a backup path. In this case, if the primary (TEHO) path is not available, the gateway that is referenced by the local route group of the applicable device pool will be used for the backup path. If the device pool selection is not static, but Cisco Unified Device Mobility is used, the gateway of the roaming site will be used as a backup for the TEHO path.

The same situation applies to Cisco Extension Mobility. When a user roams to another site and logs in to a local phone, PSTN calls use the local gateway (if TEHO is not configured) or the local gateway is used as a backup (if TEHO is configured). The local gateway selection is not based on the Cisco Extension Mobility user profile, but on the device pool of the phone where the user logs in. The line CSS, however, is associated with the user profile, and therefore the user can dial PSTN numbers the same way that he does at home. The localized input is then globalized. After call routing and path selection occur, the globalized number is localized again based on the requirements of the selected egress device. The localized input format that the user used can be completely different from the localized format that is used at call egress.

Globalized Call Routing—TEHO Advantages

As previously discussed, when you are using local route groups, there is no need to have duplicated TEHO route patterns for each originating site. Instead, the local PSTN gateway is selected by the local route group feature when the TEHO path cannot be used.

When combining globalized call routing with local route groups, you do not have to consider the various possible input formats for the TEHO call-routing decision. No matter how the user dialed the number, it is changed to globalized format before it is routed. Because the called number is then localized after call routing and path selection, you can localize the called- and calling-party number differently at the primary gateway (TEHO gateway) and the backup gateway (local gateway). However, the global transformations that you configure for each egress gateway all refer to a single format—a globalized format regardless of how the user dialed the destination. This globalized format that is combined with local route groups for local backup gateway selection makes implementing TEHO much simpler. Without globalized call routing, you would have to perform localization at the egress gateway differently for each originating site.

Globalized Call Routing—TEHO Example

Figure 4-20 shows an example of TEHO when globalized call routing is used.

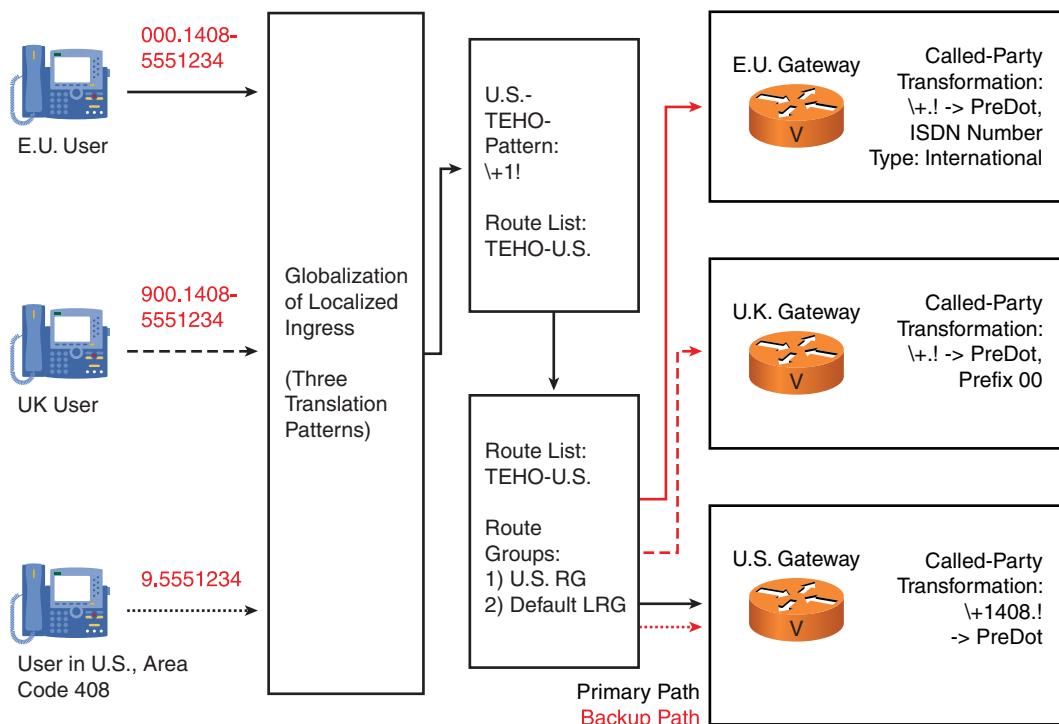


Figure 4-20 Globalized Call Routing TEHO Example

At the call ingress side, there are three PSTN dial rules: E.U., UK, and United States. The same rules apply to the egress gateways: The E.U., UK, and U.S. gateways all require different digit manipulation when you are sending calls to the PSTN.

As long as users are allowed to roam between sites and TEHO with local backup in place, users can dial each PSTN destination differently at each site. In addition, if the TEHO path is not available, the local gateway (which again can be any of the three) is used for backup. With globalized call routing, you do not have to consider all the possible combinations of ingress and egress, but you must consider call ingress and call egress independent of each other.

All that you need to configure is translation patterns for each of the PSTN dial rules (E.U., UK, and United States). Then, you create TEHO route patterns that refer to the TEHO gateway as the first choice, and to the local gateway as the backup, using the local route group feature. At the egress gateways, you configure the called- and calling-party transformations, where you do not match on all possible input formats again, but on a globalized format only.

As an example, suppose that a user travels to the San Jose location and makes a call to 555-1234 by dialing the 9 access code first. The primary path will be the U.S. gateway,

which sends the user's call to the San Jose local exchange carrier (LEC). The 9 access code is stripped off, 1408 is added, and the number 14085551234 is presented to the LEC.

Summary

This chapter covered the following key points:

- Multisite dial plans should support selective PSTN breakout with backup gateways, PSTN backup for on-net calls, TEHO, and intersite calls using access codes and site codes.
- If you add an access code and site code to directory numbers at each site, directory numbers do not have to be globally unique anymore.
- When you route calls to the PSTN, calling directory numbers have to be transformed into PSTN numbers. Also, access codes used on dialed patterns have to be removed to ensure that ANI and DNIS are in accordance with PSTN numbering schemes.
- Selective PSTN breakout means that different gateways are used for PSTN access, depending on the caller's physical location.
- When using the PSTN as a backup for intersite calls, internal directory numbers and internally dialed patterns have to be transformed to ensure that ANI and DNIS are in accordance with PSTN numbering schemes.
- When TEHO is implemented, calls to the PSTN are routed differently based on the caller's physical location and the PSTN number that was dialed. This ensures that the call uses the IP WAN as much as possible and breaks out to the PSTN at the gateway that is closest to the dialed PSTN destination.
- Globalized call routing is a dial plan concept in which the call routing is based on E.164 numbers with a + prefix.
- Globalized call routing reduces the complexity of dial plans substantially and makes it easier to implement features such as Device Mobility, Extension Mobility, AAR and CFUR, or TEHO in international deployments.

References

For additional information, refer to these resources:

Cisco Systems, Inc. Cisco Unified Communications System 8.x SRND, April 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8x.html.

Cisco Systems, Inc. *Cisco Unified Communications Manager Administration Guide Release 8.0(1)*, February 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_1/ccmcfg/bccm-801-cm.html.

Cisco Systems, Inc. *Cisco IOS Voice Configuration Library* (with Cisco IOS Release 15.0 updates), July 2007. www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

Review Questions

Use these questions to review what you've learned in this chapter. The answers are found in the "Answers Appendix"

1. Which of the following statements about implementing PSTN backup for the IP WAN is true?
 - a. In distributed deployments, PSTN backup for intersite calls requires CFUR.
 - b. Route groups including the on-net and off-net path are required for PSTN backup in a centralized deployment.
 - c. PSTN backup requires a PSTN gateway at each site.
 - d. CFUR allows remote-site phones to use the PSTN for calls to the main site.
2. When implementing TEHO for national calls and using the local PSTN gateway as a backup, how many route patterns are required for a cluster with three sites located in different area codes?
 - a. Three, when not using the local route group feature
 - b. Six, when using the local route group feature
 - c. Nine, when not using the local route group feature
 - d. Four, when using the local route group feature
3. Which two are not valid type of number (TON) codes for incoming ISDN PSTN calls?
 - a. International
 - b. National
 - c. Subscriber
 - d. Directory number
 - e. Operator number

4. Which two statements about PSTN gateway selection are true?
 - a. Using TEHO minimizes PSTN costs.
 - b. Using local PSTN gateways minimizes PSTN costs.
 - c. When you use TEHO, you must pay special attention to the configuration of the calling number.
 - d. Using remote PSTN gateways for backup is never recommended.
 - e. It is recommended that you use remote PSTN gateways as a backup when the IP WAN is overloaded.
5. You should perform digit manipulation at the _____ when digit-manipulation requirements vary based on the gateway used for the call.
 - a. Gateway
 - b. Route list as it relates to the route group
 - c. Route pattern
 - d. Trunk
 - e. Translation pattern
6. Which of these is used to globalize the calling party number of inbound PSTN calls?
 - a. Globalization type
 - b. Called number
 - c. Inbound gateway identifier
 - d. Number type
7. The implementation of globalized call routing does not simplify the deployment of which two of these features?
 - a. TEHO
 - b. Device Mobility
 - c. AAR
 - d. MOH
 - e. Cisco Extension Mobility
 - f. SRST
 - g. Local conference bridges
8. The PSTN egress gateway can be selected in which two of these ways?
 - a. By the partition of the calling device
 - b. Based on the CSS of the gateway

- c. By the local route group feature
 - d. Based on the matched route pattern when route patterns exist once per site
 - e. By the standard local route group that is configured at the gateway device pool
- 9. Where can digit manipulation be performed when digit manipulation requirements vary for the on- and off-net paths?
 - a. Per route group of the route list
 - b. Route pattern
 - c. Directory number
 - d. Translation pattern

This page intentionally left blank

Chapter 5

Examining Remote-Site Redundancy Options

This chapter provides an overview of the different options with remote-site redundancy in CUCM multisite installations. These different mechanisms are illustrated to help you understand how the technologies interact to deliver reliable communication services. This includes Media Gateway Control Protocol (MGCP) and Cisco Unified Survivable Remote Site Telephony (SRST).

Upon completing this chapter, you will be able to describe the mechanisms for providing call survivability and device failover at remote sites, including the functions, operation, and limitations of each mechanism. You will be able to meet these objectives:

- Describe remote-site redundancy options and compare their characteristics
- Describe how Cisco Unified SRST works
- Describe how MGCP fallback works
- Describe SRST versions, their protocol support and features, and the required Cisco IOS Software release
- Describe dial plan requirements for MGCP fallback and SRST with the option of using CUCM Express

Remote-Site Redundancy Overview

Two different technologies are used to provide remote-site redundancy for small and medium remote sites in a Cisco Unified Communications Manager (CUCM) environment. Survivable Remote Site Telephony (SRST) and Media Gateway Control Protocol (MGCP) gateway fallback are the key components of delivering fail-safe communication services, as shown in Figure 5-1.

CUCM supports Cisco Unified IP Phones at remote sites that are attached to Cisco multiservice routers across the WAN. Before Cisco Unified SRST, when the WAN connection between a router and the CUCM failed, or when connectivity with the CUCM was lost

for any reason, Cisco Unified IP Phones on the network became unusable for the duration of the failure. The reason is that Cisco IP Phones demand Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP) connectivity to a call-processing agent such as CUCM, and in the absence of signaling connectivity, the phones become fully unusable.

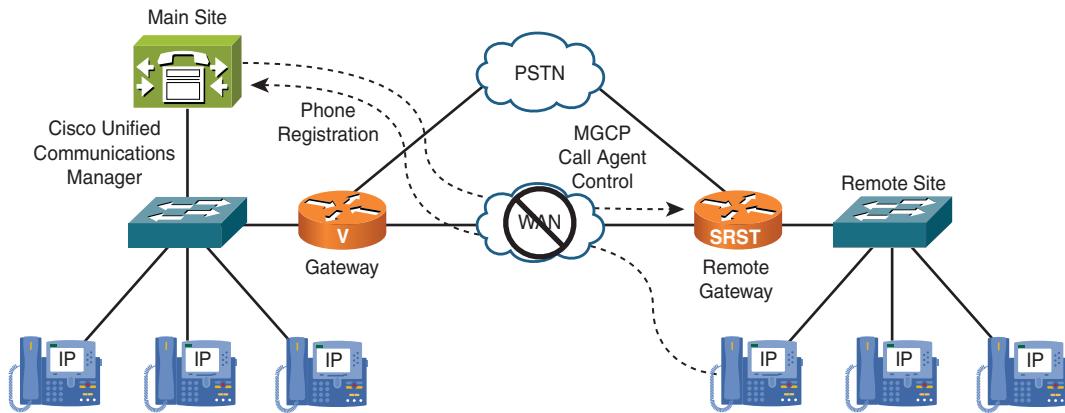


Figure 5-1 SRST and MGCP Fallback

Cisco Unified SRST overcomes this problem and ensures that Cisco Unified IP Phones offer continuous, although reduced, service by providing call-handling support for Cisco Unified IP Phones directly from the Cisco Unified SRST router. The system automatically detects a failure and uses Simple Network-Enabled Auto-Provision (SNAP) technology to autoconfigure the branch office router to provide call processing for Cisco Unified IP Phones that are registered with the router. When the WAN link or connection to the primary CUCM subscriber is restored, call handling reverts to the primary CUCM.

MGCP gateway fallback is a mechanism that allows a Cisco IOS router to continue providing voice gateway functions, even when the MGCP call agent is not in control of the media gateway. These voice gateway functions are implemented through a fallback mechanism that activates the so-called default technology application. The gateway then works in the same way as a standalone H.323 or SIP gateway by using its configured dial peers.

Remote-Site Redundancy Technologies

Table 5-1 lists the capabilities of different remote-site redundancy technologies.

To use SRST as your fallback mode on an MGCP gateway, SRST and MGCP fallback have to be configured on the same gateway.

Table 5-1 *Remote-Site Redundancy Technologies*

		MGCP Fallback	Cisco Unified SRST		
		Cisco Unified SIP SRST	Cisco Unified SIP SRST		Cisco Unified Communications Manager Express in SRST Mode
Provides redundancy for	gateways	MGCP controlled SCCP phones	SIP phones	SCCP phones	
Delivered service	Fallback to Cisco IOS default technology	Basic telephony service	Basic SIP proxy service	CUCM Express	
ISDN call preservation	No	Yes (no MGCP)	Yes (no MGCP)	Yes (no MGCP)	
Analog/CAS call preservation	Yes	Yes	Yes	Yes	
Maximum number of phones	N/A	1500	1500	450	

Note MGCP and SRST have had the capability to be configured on the same gateway since Cisco IOS Software Release 12.2(11)T.

Cisco Unified SIP SRST provides a basic set of features to SIP-based IP Phones. This set of Cisco Unified SRST basic features is also known as *Cisco Unified SIP SRST*. Cisco Unified SIP SRST must be enabled and configured separately on Cisco IOS routers.

Cisco Unified SIP SRST versions 3.3 and earlier provide a SIP Redirect Server function; in subsequent versions, this function acts as a back-to-back user agent (B2BUA).

CUCM Express in Cisco Unified SRST mode provides more features to a smaller maximum number of IP Phones by falling back to CUCM Express mode. The main feature enhancements include Presence, Cisco Extension Mobility, and support of local voice-mail integrations.

VoIP call preservation sustains connectivity for topologies in which signaling is managed by an entity (such as CUCM). For example, if an existing call is setup between two Cisco IP Phones with CUCM performing signaling, and CUCM goes down during the call, then the audio will stay connected since skinny has call preservation.

Call preservation is also useful when a gateway and the other endpoint (typically a Cisco Unified IP Phone) are colocated at the same site and the call agent is remote. In such a

scenario, the call agent (the gateway with the remote endpoint) is more likely to experience connectivity failures.

CUCM Express version 8.0 supports a maximum of 450 IP Phones (Cisco IOS 3945E router), whereas Cisco Unified SRST version 8.0 supports up to 1500 IP Phones on the same platform. Refer to Cisco Unified Communications Manager Express 8.0, www.cisco.com/en/US/docs/voice_ip_comm/cucme/requirements/guide/cme80spc.htm, for more details.

SIP is an Internet standard discussed in many Request for Comments (RFC). If you want to supplement your knowledge of SIP, here is a good RFC to start with: www.ietf.org/rfc/rfc3261.txt.

Note Before CUCM version 6, CUCM Express and SRST contained similar functionality but existed as separate technologies. SRST always requires Cisco CallManager (CCM) or CUCM, whereas CUCM Express can exist as a separate entity. However, with CUCM version 6, CUCM Express in SRST mode can add functionality to SRST when configured to provide survivability with CUCM. However, only SRST or CUCM Express can be configured at any one time on an IOS router.

MGCP Fallback Usage

A public switched telephone network (PSTN) gateway can use MGCP gateway fallback configured as an individual feature if H.323 or SIP is configured as a backup service. SRST and MGCP fallback must be configured on the same gateway with Cisco IOS Software Release 12.2(11)T or later if this single gateway will provide SRST fallback service to phones and MGCP gateway fallback.

Although MGCP gateway fallback is most often used with SRST to provide gateway functions to IP Phones in SRST mode, it can also be used as a standalone feature. For example, when a call using a T-1 channel-associated signaling (CAS) interface controlled by MGCP exists during a CUCM failure, connectivity to the PSTN or another private branch exchange (PBX) can be preserved by MGCP gateway fallback. An MGCP fallback standalone configuration can also be used to allow analog interfaces that are controlled by SCCP to stay in service even when the WAN connection to the CUCM is down.

MGCP gateway fallback preserves active calls from remote-site IP Phones to the PSTN when analog or CAS protocols are used. For ISDN protocols, call preservation is impossible because Layer 3 of the ISDN stack is disconnected from the MGCP call agent and is restarted on the local Cisco IOS gateway. This means that for active ISDN calls, all call-state information is lost in cases of switchover to fallback operation.

Basic Cisco Unified SRST Usage

Cisco Unified SRST provides CUCM with fallback support for Cisco Unified IP Phones that are attached to a Cisco router on a local network.

Cisco Unified SRST enables routers to provide basic call-handling support for Cisco Unified IP Phones when they lose connection to remote primary, secondary, and tertiary CUCM servers or when the WAN connection is down.

Cisco Unified SIP SRST Usage

Cisco Unified SIP SRST provides backup to an external SIP proxy server by providing basic registrar and redirect server services earlier than Cisco Unified SIP SRST version 3.4 or B2BUA for Cisco Unified SIP SRST version 3.4 and higher services.

A SIP phone uses these services when it is unable to communicate with its primary SIP proxy or CUCM in the event of a WAN connection outage.

Cisco Unified SIP SRST can support SIP phones with standard RFC 3261 feature support locally and across SIP WAN networks. With Cisco Unified SIP SRST, SIP phones can place calls across SIP networks in the same way that SCCP phones do.

Cisco Unified SIP SRST supports the following call combinations: SIP phone to SIP phone, SIP phone to PSTN or router voice port, SIP phone to SCCP phone, and SIP phone to WAN VoIP using SIP.

SIP proxy, registrar, and B2BUA servers are key components of a SIP VoIP network. These servers usually are located in the core of a VoIP network. If SIP phones located at remote sites at the edge of the VoIP network lose connectivity to the network core (because of a WAN outage), they may be unable to make or receive calls. Cisco Unified SIP SRST functionality on a SIP PSTN gateway provides service reliability for SIP-based IP Phones in the event of a WAN outage. Cisco Unified SIP SRST enables the SIP IP Phones to continue making and receiving calls to and from the PSTN. They also can continue making and receiving calls to and from other SIP IP Phones by using the dial peers configured on the router.

When the IP WAN is up, the SIP phone registers with the SIP proxy server and establishes a connection to the B2BUA SIP registrar (B2BUA router). But, any calls from the SIP phone go to the SIP proxy server through the WAN and out to the PSTN.

When the IP WAN fails or the SIP proxy server goes down, the call from the SIP phone cannot get to the SIP proxy server. Instead, it goes through the B2BUA router out to the PSTN.

Note The B2BUA acts as a user agent to both ends of a SIP call. The B2BUA is responsible for handling all SIP signaling between both ends of the call, from call establishment to termination. Each call is tracked from beginning to end, allowing the operators of the

B2BUA to offer value-added features to the call. To SIP clients, the B2BUA acts as a user agent server on one side and as a user agent client on the other (back-to-back) side. The basic implementation of a B2BUA is defined in RFC 3261, as mentioned earlier in this chapter.

Cisco Unified SRST does not support enhanced features, such as Presence or Cisco Extension Mobility. Message Waiting Indicator (MWI) is also not supported in fall-back mode.

CUCME in SRST Mode Usage

CUCME in SRST mode enables routers to provide basic call-handling support for Cisco Unified IP Phones if they lose connection to remote primary, secondary, and tertiary CUCM installations or if the WAN connection is down.

When Cisco Unified SRST functionality is provided by CUCM Express, you can use automatic provisioning of phones like you do with standard Cisco Unified SRST.

However, because of the wide feature support of CUCM Express, more features can be used compared to the standard Cisco Unified SRST.

Examples of features that are provided only by CUCM Express in SRST mode are Call Park, Presence, Cisco Extension Mobility, and access to Cisco Unity Voice Messaging services using SCCP.

These features, however, cannot be configured automatically when a phone falls back to SRST mode. If a certain feature is applicable to all phones or directory numbers (DN), the configuration can be applied by a corresponding template. If features have to be enabled on a per-phone (or per-DN) basis, they have to be statically configured.

Phones that do not require unique feature configuration can be configured automatically so that only those phones that require individual configuration have to be statically configured in CUCM Express.

Cisco Unified SRST Operation

Figure 5-2 illustrates the function of Cisco Unified SRST.

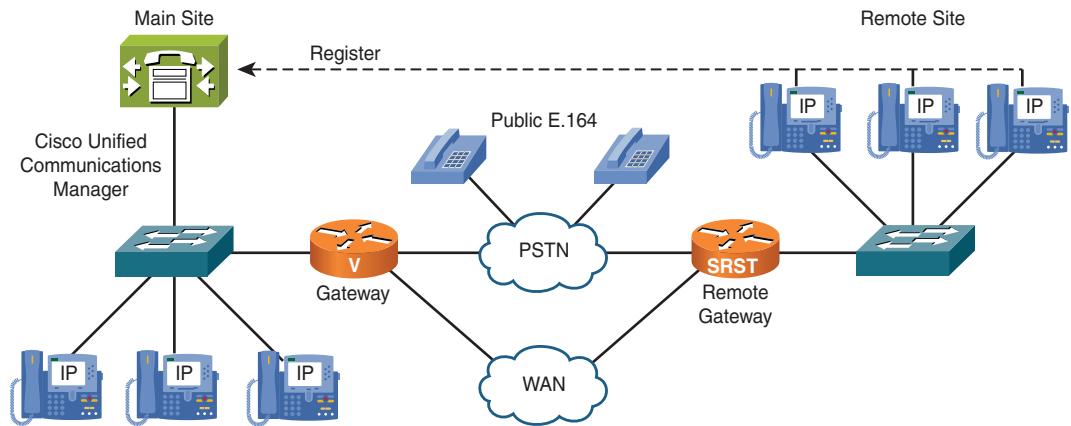


Figure 5-2 SRST Function in a Normal Situation

CUCM supports Cisco Unified IP Phones at remote sites attached to Cisco multiservice routers across the WAN. The remote-site IP Phones register with CUCM. Keepalive messages are exchanged between IP Phones and the central CUCM server across the WAN. CUCM at the main site handles the call processing for the branch IP Phones. Note that Cisco IP Phones cannot register SCCP or SIP through the PSTN to CUCM even if the PSTN is functional because SCCP and SIP must run over an IP network.

SRST Function of Switchover Signaling

When Cisco Unified IP Phones lose contact with CUCM, as shown in Figure 5-3, because of any kind of IP WAN failure, they register with the local Cisco Unified SRST router to sustain the call-processing capability that is necessary to place and receive calls.

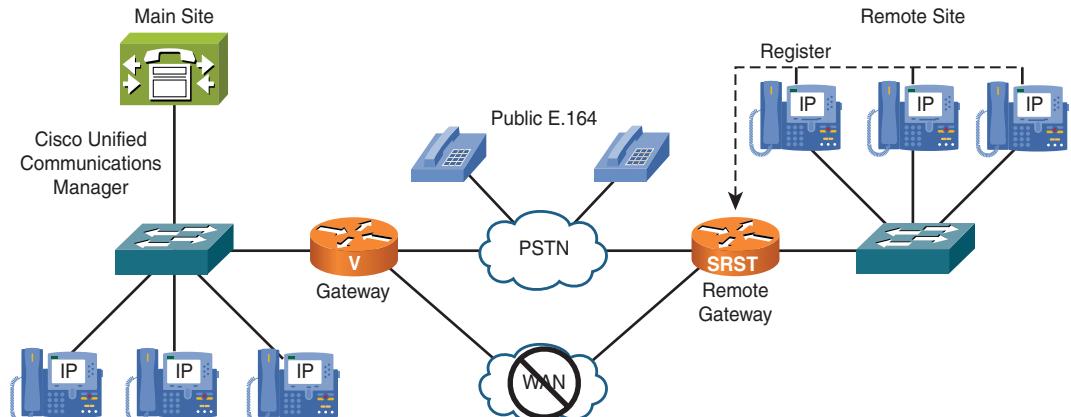


Figure 5-3 Cisco Unified SRST Function of Switchover Signaling

Cisco Unified SRST configuration provides the IP Phones with the alternative call control destination of the Cisco Unified SRST gateway.

When the WAN link fails, the IP Phones lose contact with the central CUCM but then register with the local Cisco Unified SRST gateway.

The Cisco Unified SRST gateway detects newly registered IP Phones, queries these IP Phones for their configuration, and then autoconfigures itself. The Cisco Unified SRST gateway uses SNAP technology to autoconfigure the branch office router to provide call processing for Cisco Unified IP Phones that are registered with the router.

Caution In the event of a WAN failure, when the branch IP Phones register to the SRST gateway, do not erase the settings on the phone. The phone settings, such as phone numbers, were added to the phone from CUCM when the WAN was functional, and the phone then takes its settings and uses them to register to the SRST router. If the phone has no settings, it cannot register to SRST, and the phone will not be functional.

SRST Function of the Call Flow After Switchover

Cisco Unified SRST ensures that Cisco Unified IP Phones offer continuous service by providing call-handling support directly from the Cisco Unified SRST router using a basic set of call-handling features, as shown in Figure 5-4.

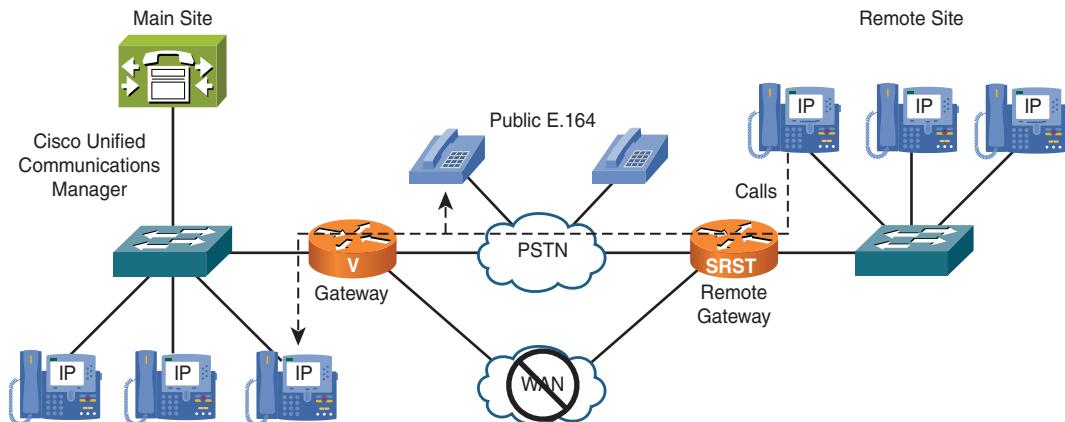


Figure 5-4 SRST Function of the Call Flow After Switchover

The Cisco Unified SRST gateway uses the local PSTN breakout with configured dial peers. Cisco Unified SRST features such as call preservation, autoprovisioning, and failover are supported.

During a WAN connection failure, when Cisco Unified SRST is enabled, Cisco Unified IP Phones display a message informing users that the phone is operating in CUCM fallback mode. This message can be adjusted.

While in CUCM fallback mode, Cisco Unified IP Phones continue sending keepalive messages in an attempt to reestablish a connection with the CUCM server at the main site.

SRST Function of Switchback

Figure 5-5 shows Cisco Unified IP Phones attempting to reestablish a connection over the WAN link with CUCM at the main site periodically when they are registered with a Cisco Unified SRST gateway.

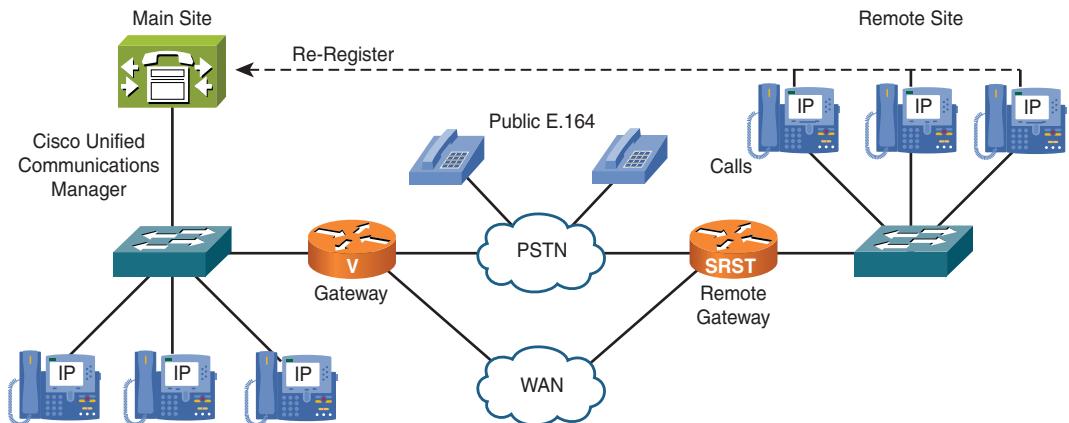


Figure 5-5 SRST Function of Switchback

Cisco IP Phones, by default, wait up to 120 seconds before attempting to reestablish a connection to a remote CUCM.

When the WAN link or connection to the primary CUCM is restored, the Cisco Unified IP Phones reregister with their primary CUCM. Three switchback methods are available on the Cisco IOS router: immediate switchback, graceful switchback (after all outgoing calls on the gateway are completed), or switchback after a configured delay. When switchback is completed, call handling reverts to the primary CUCM, and SRST returns to standby mode. The phones then return to their full functionality provided by CUCM.

SRST Timing

Typically, a phone takes three times the keepalive period to discover that its connection to CUCM has failed. The default keepalive period is 30 seconds, as shown in Figure 5-6.

If the IP Phone has an active standby connection established with a Cisco Unified SRST router, the fallback process takes 10 to 20 seconds after the connection with CUCM is lost. An active standby connection to a Cisco Unified SRST router exists only if the phone has a single CUCM in its Cisco Unified CM group. Otherwise, the phone activates a standby connection to its secondary CUCM.

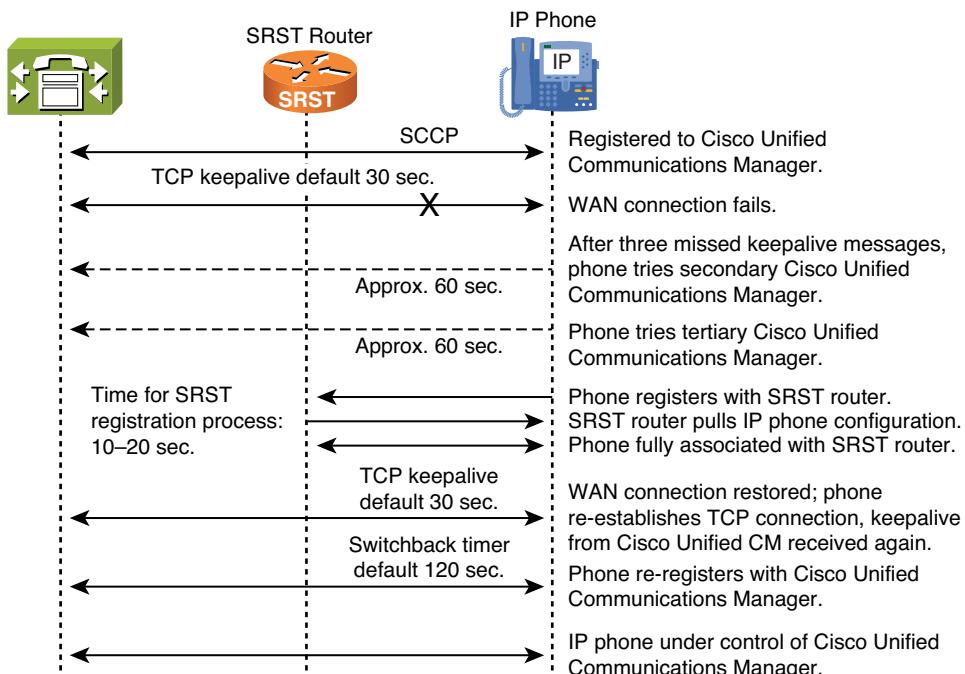


Figure 5-6 Cisco Unified SRST Timing

Note The time it takes for an IP Phone to fall back to the SRST router can vary, depending on the phone type. Phones such as the Cisco Unified IP Phone models 7902G, 7905G, and 7912G can take approximately 2.5 minutes to fall back to SRST mode.

If a Cisco Unified IP Phone has multiple CUCM systems in its Cisco Unified CM group, the phone progresses through its list before attempting to connect with its local Cisco Unified SRST router. Therefore, the time that passes before the Cisco Unified IP Phone eventually establishes a connection with the Cisco Unified SRST router increases with each attempt to connect to a CUCM. Assuming that each attempt to connect to a CUCM

takes about 1 minute, the Cisco Unified IP Phone in question could remain offline for 3 minutes or more following a WAN link failure. You can decrease this time by setting the keepalive timer to a smaller value. You can configure the keepalive timer using the CUCM service parameter Station Keepalive Interval.

While in SRST mode, Cisco Unified IP Phones periodically attempt to reestablish a connection with CUCM at the main site. The default time that Cisco Unified IP Phones wait before attempting to reestablish a connection to CUCM is 120 seconds.

Note If you want a Cisco IP Phone to come out of SRST fallback mode faster, you can manually reboot the Cisco IP Phone by pressing Settings and then **#**, or by going into the router mode CallManager-Fallback and entering Reset All.

MGCP Fallback Operation

MGCP gateway fallback, as shown in Figure 5-7, is a feature that improves the reliability of MGCP remote site networks. A WAN link connects the MGCP gateway at a remote site to the Cisco Communications Manager at a main site, which is the MGCP call agent. If the WAN link fails, the fallback feature keeps the gateway working as an H.323 or SIP gateway and rehomes to the MGCP call agent when the WAN link is active again. MGCP gateway fallback works in conjunction with the SRST feature.

Cisco IOS gateways can maintain links to up to two backup CUCM servers in addition to a primary CUCM. This redundancy enables a voice gateway to switch over to a backup server if the gateway loses communication with the primary server. The secondary backup server takes control of the devices that are registered with the primary CUCM. The tertiary backup takes control of the registered devices if both the primary and secondary backup CUCM systems fail. The gateway preserves existing connections during a switchover to a backup CUCM server.

When the primary CUCM server becomes available again, control reverts to that server. Reverting to the primary server can occur in several ways: immediately, after a configurable amount of time, or only when all connected sessions are released.

MGCP Gateway Fallback During Switchover

The MGCP gateway performs a switchover to its default technology of H.323 or SIP, as shown in Figure 5-8, when the keepalives between CUCM and the Cisco MGCP gateway are missing.

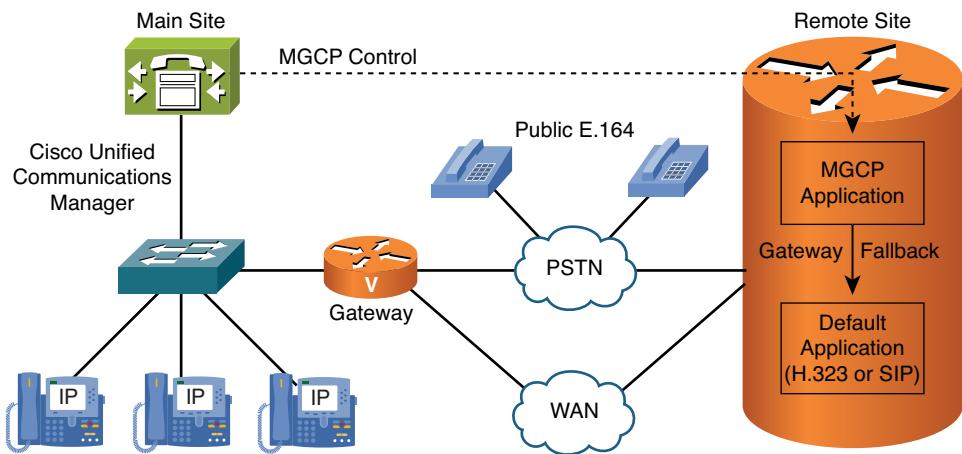


Figure 5-7 MGCP Gateway Fallback in a Normal Situation

The MGCP gateway fallback feature provides the following functionality:

- **MGCP gateway fallback support:** All active MGCP analog, E1 CAS, and T1 CAS calls are maintained during the fallback transition. Callers are unaware of the fallback transition, and the active MGCP calls are cleared only when the callers hang up. Active MGCP PRI backhaul calls are released during fallback. Any transient MGCP calls that are not in the connected state are cleared at the onset of the fallback transition and must be attempted again later.
- **Basic connection services in fallback mode:** Basic connection services are provided for IP telephony traffic that passes through the gateway. When the local MGCP gateway transitions into fallback mode, the default H.323 or SIP session application assumes responsibility for handling new calls. Only basic two-party voice calls are supported during the fallback period. When a user completes (hangs up) an active MGCP call, the MGCP application handles the on-hook event and clears all call resources.

MGCP Gateway Fallback During Switchback

The MGCP-gateway-fallback feature provides the rehome functionality to switch back to MGCP mode. As shown in Figure 5-9, the switchback or rehome mechanism is triggered by the reestablishment of the TCP connection between CUCM and the Cisco MGCP gateway.

Rehome function in gateway-fallback mode detects the restoration of a WAN TCP connection to any CUCM server. When the fallback mode is in effect, the affected MGCP gateway repeatedly tries to open a TCP connection to a CUCM server that is included in the prioritized list of call agents. This process continues until a CUCM server in the prioritized list responds. The TCP open request from the MGCP gateway is honored, and the gateway reverts to MGCP mode. The gateway sends a RestartInProgress (RSIP) message to begin registration with the responding CUCM.

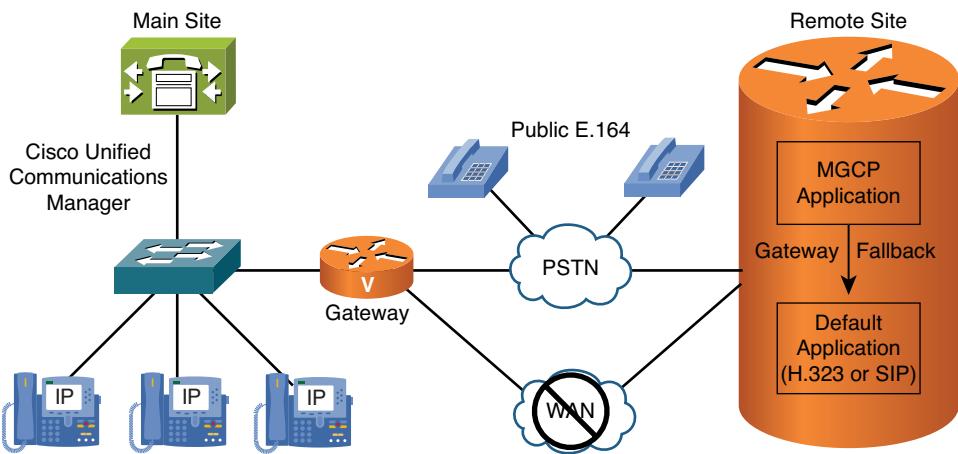


Figure 5-8 MGCP Gateway Fallback During Switchover

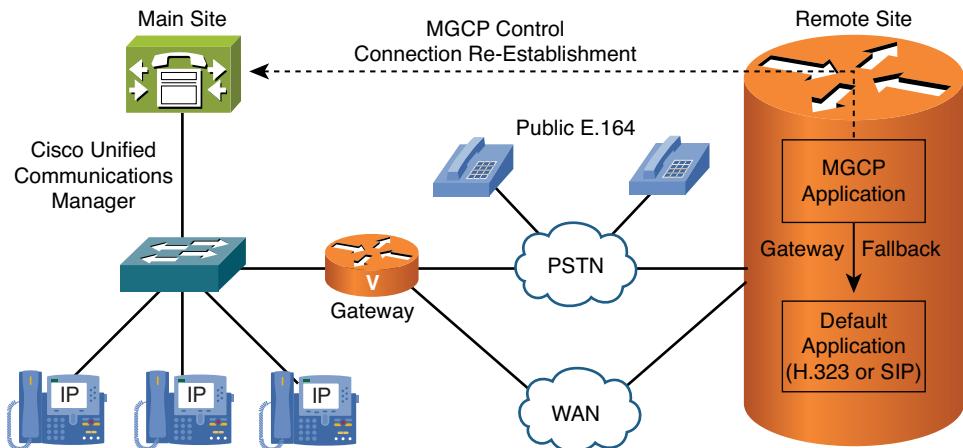


Figure 5-9 MGCP Gateway Fallback During Switchback

All currently active calls that are initiated and set up during the fallback period are maintained by the default H.323 session application, except ISDN T1 and E1 PRI calls. Transient calls are released. After rehome occurs, the new CUCM assumes responsibility for controlling new IP telephony activity.

MGCP Gateway Fallback Process

The MGCP gateway maintains a remote connection to a centralized CUCM cluster, as shown in Figure 5-10, by sending MGCP keepalive messages to the CUCM server at 15-second intervals.

If the active CUCM server fails to acknowledge receipt of the keepalive message within 30 seconds, the gateway attempts to switch over to the next available CUCM server.

If none of the CUCM servers responds, the gateway switches into fallback mode and reverts to the default H.323 or SIP session application for basic call control.

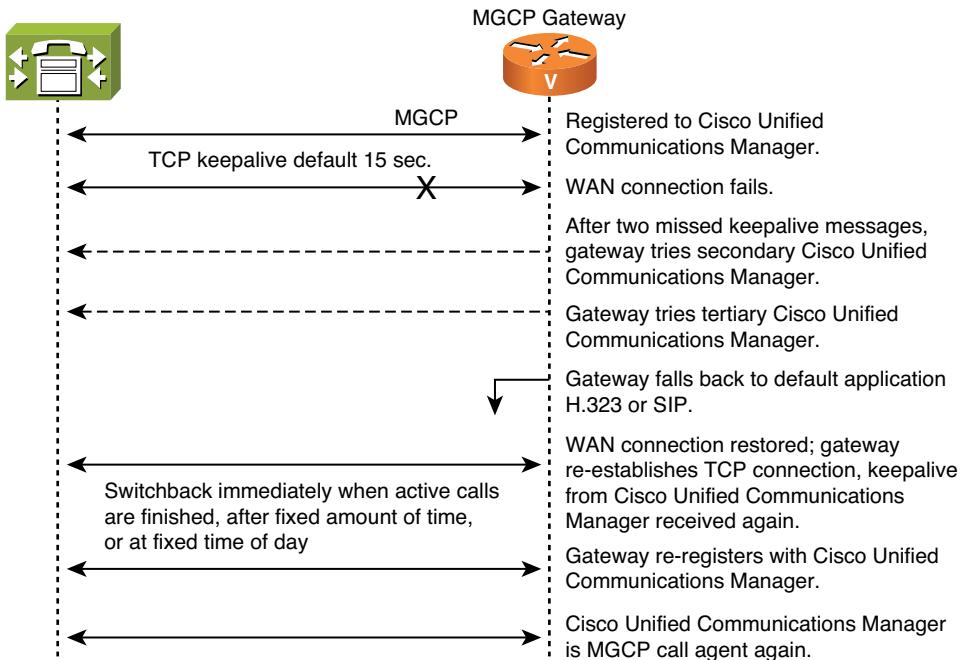


Figure 5-10 MGCP Gateway Fallback Process

Note H.323 is a standardized communication protocol that enables dissimilar devices to communicate with each other through the use of a common set of codecs, call setup and negotiating procedures, and basic data-transport methods.

The gateway processes calls on its own using H.323 until one of the CUCM connections is restored. The same occurs if SIP is used instead of H.323 on the gateway.

Cisco Unified SRST Versions and Feature Support

Table 5-2 describes Cisco Unified SRST versions, their protocol support and features, and the required Cisco IOS Software release.

Table 5-2 Cisco Unified SRST Versions

Feature	CUCM Express in SRST Mode	Cisco Unified SRST 8.0	Cisco Unified SRST 7.2	Cisco Unified SRST 4.3
Minimum Cisco IOS Software Release	12.3(11)XJ for version 8.0	15.0(1)XA	12.4(22)YB 15.0(1)M on ISR G2	12.4(11)XZ
Presence	✓			
Extension Mobility	✓			
Eight active calls per line	✓ (new in 8.0)	✓	✓	✓
Support for E.164 numbers with + prefix	✓ (new in 8.0)	✓	✓	
Five additional MOH* streams (SCCP only)	✓ (new in 8.0)	✓		

MOH = Music On Hold

The version of the Cisco Unified SRST application depends on which release of the Cisco IOS Software is running on the router. Each Cisco IOS Software release implements a

particular SRST version. You upgrade to a newer version of SRST through a Cisco IOS update into router flash. Recent Cisco IOS Software releases often have higher memory requirements than older ones, so make sure that you look into this before upgrading.

For detailed information about Cisco Unified SRST versions and their hardware and feature support, refer to the *Cisco Unified Survivable Remote Site Telephony Version 8.0* data sheet at www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps2169/data_sheet_c78-570481.html.

SRST 4.0 Platform Density

The maximum number of IP Phones and directory numbers supported by the Cisco Unified SRST 8.0 feature depends on which Cisco IOS router platform is used, as shown in Table 5-3.

Table 5-3 SRST 8.0 Platform Density

Platform	Maximum Number of IP Phones
800 Series	4
1861	15
2801–2851	25–100
2901–2951	35–250
3825, 3845	350, 730
3925–3945E	730–1500

Table 5-3 shows the maximum number of phones and DNs on phones that a Cisco Unified SRST router can accommodate. For more details, such as minimum memory requirements, see Cisco Unified SRST 8.0 Supported Firmware, Platforms, Memory, and Voice Products at www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs80spc.html.

Note These maximum numbers of IP Phones are for common SRST configurations only. Routers with large numbers of IP Phones and complex configurations may not work on all platforms and can require additional memory or a higher performance platform.

Plus (+) Prefix and E.164 Support in Cisco Unified SRST

Cisco Unified SRST version 8.0 introduces support for DNs in E.164 format with a plus (+) prefix. SIP and SCCP IP phones can fallback to SRST and register with a DN in E.164 format with a + prefix. Assigning DNs in E.164 format ensures globally unique numbers; the + sign is prefixed in order to indicate that the number is in E.164 format.

Note The E.164 standard describes telephone numbers in international format. E.164 numbers are globally unique numbers within the PSTN and start with a plus + and then the country code.

Cisco Unified SRST and CUCM Express in SRST mode allow internal callers to use internal extensions for calling IP Phones that have numbers in E.164 format. A new dial plan pattern command has been introduced with Cisco Unified SRST v8.x to achieve the demotion of the E.164 number to the internally used shorter numbers. Although the standard dial plan pattern command expands to a longer PSTN format, for any DNs that are applied to phone lines, the new dial plan pattern command has the opposite function. In this case it allows internal callers to dial shorter, internally used extensions, which are expanded to the applied DNs in E.164 format. Outside callers dial the IP Phone directory numbers as configured—with a + prefix and the complete E.164 number. At the IP Phones, the calling-party number that is shown on the phone display can be transformed independently from the number that will be used for callback. This transformation is possible because of a newly introduced translation type in the voice translation profile, which is a translation rule of the callback number.

Support for Multiple MOH Sources

Cisco Unified SRST v8.x also introduces support for multiple Music On Hold (MOH) sources.

Before Cisco Unified SRST v8.x, only a single MOH file was supported by Cisco Unified SRST, CUCM Express in SRST mode, and CUCM Express in standalone mode. Cisco Unified SRST v8.x allows you to configure up to five additional MOH sources by configuring MOH groups. Only SCCP IP Phones support these newly introduced MOH groups. You can configure each MOH group with an individual MOH file that is located in the flash memory of the router, and you can enable multicast MOH for each MOH group. Each MOH group is configured with the DN ranges that should use the corresponding MOH group when callers are put on hold, as described in Chapter 7, “Implementing Cisco Unified Communications Manager Express (CUCME) in SRST Mode.”

The traditional MOH configuration for Cisco Unified SRST and CUCM Express is still supported. It is used by all phones that do not have a MOH group assigned. All these phones are SIP and SCCP phones whose DNs have not been specified in any MOH group. MOH files can be cached in router RAM. This process reduces the amount of read operations in flash, but it requires enough available RAM at the router. You can limit RAM usage for MOH file caching by using smaller MOH files.

Dial Plan Requirements for MGCP Fallback and SRST Scenarios

Figure 5-11 illustrates the requirements of standalone dial plans to work with MGCP fallback and SRST.

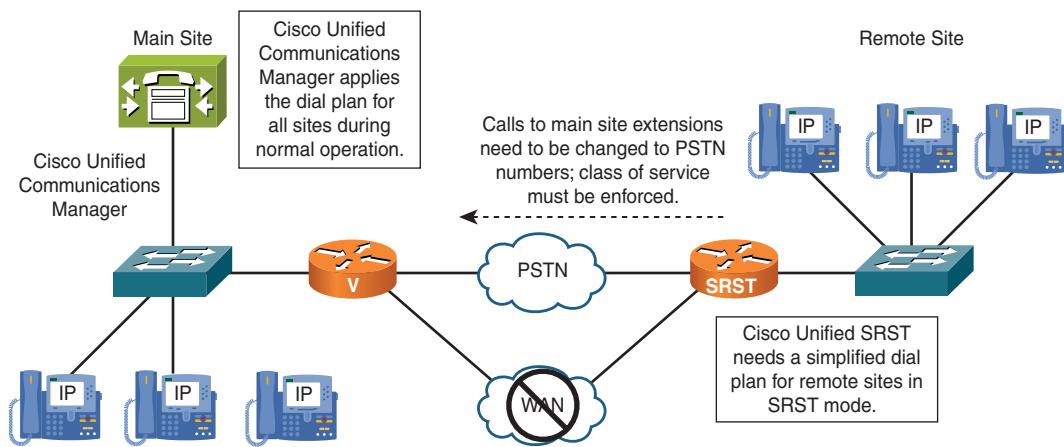


Figure 5-11 SRST Dial Plan Requirements for Calls from the Remote Site

SRST failover leaves the remote site independent from the complex dial plan implemented in CUCM at the main site. The SRST router needs to have a dial plan implemented to allow all remote-site phones, all main-site phones, and all PSTN destinations to be reached with the same numbers as in standard mode.

During fallback, users should be able to dial main-site directory numbers as usual. Because these calls have to be routed over the PSTN during fallback, main-site extensions have to be translated to E.164 PSTN numbers at the PSTN gateway.

Most enterprises limit the range of destinations that can be reached from specific extensions by applying class of service (CoS) to the extensions. This limitation should still be valid during times in SRST mode by applying IOS class of restriction (COR), as described in the next chapter.

Ensuring Connectivity for Remote Sites

When SRST is active, you must take several measures to ensure connectivity from remote sites to PSTN destinations, between different sites, and inside the site itself.

To guarantee PSTN connectivity, dial peers with destination patterns corresponding to the PSTN access code have to be implemented. In H.323 or SIP gateways, these dial peers must be present for normal operation. When MGCP gateways are used, dial peers are activated by the MGCP-gateway-fallback mechanism. Interdigit timeout adopts open numbering plans that do not have a fixed number of digits.

Voice translation profiles that are applied to dial peers, the voice interface, or the voice port modify the calling party ID to enable callback from call lists.

For intrasite and intersite connectivity, voice translation profiles are configured to expand called numbers to PSTN format during fallback.

The Cisco IOS command **dialplan-pattern** in CallManager-Fallback configuration mode performs digit manipulation on the incoming called numbers to match the remote-site extensions. It ensures that internal extensions can be dialed even though the lines are configured with the site code and extension. The Line Text Label settings defined in CUCM are not applied to the SRST phones, so the complete DN applied to the line is visible to the user.

Ensuring Connectivity from the Main Site Using Call Forward Unregistered

During fallback, mainsite users should still be able to call remote-site users by using their extension numbers, as shown in Figure 5-12.

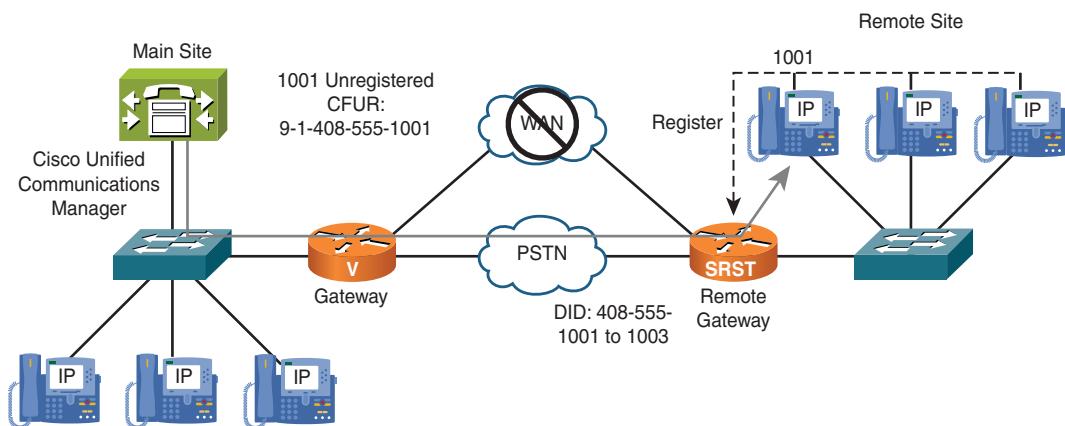


Figure 5-12 Ensure Connectivity from the Main Site Using Call Forward Unregistered

CUCM considers the remotesite phones unregistered and cannot route calls to the affected IP Phone DNs. Therefore, if mainsite users dial internal extensions during the IP WAN outage, the calls fail or go to voice mail.

To allow remote IP Phones to be reached from mainsite IP Phones, Call Forward Unregistered (CFUR) can be configured for the remotesite phones. CFUR should be configured with the PSTN number of the remotesite gateway so that internal calls for remote IP Phones get forwarded to the appropriate PSTN number.

Note In older versions of CUCM that did not support CFUR, it was not possible to allow a main-site phone registered to CUCM to call a remot-site phone in SRST mode over the PSTN during a WAN failure. This was because CUCM did not have a mechanism to route calls to unregistered DNs through the PSTN.

CFUR Considerations

CFUR was first implemented in CCM Release 4.2.

As mentioned earlier, the CFUR feature allows calls placed to a temporarily unregistered IP Phone to be rerouted to a configurable number. The configuration of CFUR has two main elements:

- **Destination selection:** When the DN is unregistered, calls can be rerouted to voice mail or to the DN that was used to reach the IP Phone through the PSTN.
- **Calling Search Space (CSS):** CUCM attempts to route the call to the configured destination number using the CFUR CSS of the directory number that was called. The CFUR CSS is configured on the target IP Phone and is used by all devices calling the unregistered IP Phone. This means that all calling devices use the same combination of route pattern, route list, route group, and gateway to place the call. In addition, all CFUR calls to a given unregistered device are routed through the same unique gateway, regardless of the location of the calling IP Phone. It is recommended that you select a centralized gateway as the egress point to the PSTN for CFUR calls and configure the CFUR CSS to route calls to the CFUR destination through this centralized gateway.

If an IP Phone is unregistered while the gateway that is associated with the direct inward dialing (DID) number of that phone is still under the control of CUCM, CFUR functionality can result in telephony routing loops. For example, if an IP Phone is simply disconnected from the network, the initial call to the phone would prompt the system to attempt a CFUR call to the DID of the phone through the PSTN. The resulting incoming PSTN call would in turn trigger another CFUR attempt to reach the directory number of the same phone, triggering yet another CFUR call from the central PSTN gateway through the PSTN. This cycle potentially could repeat itself until system resources are exhausted.

The CUCM service parameter **Max Forward UnRegistered Hops to DN** in the Clusterwide Parameters (Feature—Forward) section in CUCM Administration controls the maximum number of CFUR calls that are allowed for a directory number at one time. The default value of 0 means that the counter is disabled. If any DNs are configured to reroute CFUR calls through the PSTN, loop prevention is required. Configuring this service parameter to a value of 1 would stop CFUR attempts as soon as a single call was placed through the CFUR mechanism. This setting would also allow only one call to be forwarded to voice mail, if CFUR is so configured. Configuring this service parameter to a value of 2 would allow up to two simultaneous callers to reach the voice mail of a DN whose CFUR setting is configured for voice mail. It would also limit potential loops to two for DNs whose CFUR configuration sends calls through the PSTN.

Note CUCM Extension Mobility DNs should not be configured to send CFUR calls to the PSTN DID that is associated with the DN. The DNs of CUCM Extension Mobility

profiles in the logged-out state are deemed to be unregistered. Therefore, any calls to the PSTN DID number of a logged-out DN would trigger a routing loop. To ensure that calls made to CUCM Extension Mobility DNs in the logged-out state are sent to voice mail, their corresponding CFUR parameters must be configured to send calls to voice mail.

CFUR Interaction with Globalized Call Routing

CFUR can benefit as follows from globalized call routing when a CUCM cluster serves multiple countries if a globalized number is used as a CFUR destination number:

- CFUR calls are placed to global number.
- Single route pattern (\+!) sufficient for all CFUR calls.
- Same route pattern can be used for Automated Alternate Routing (AAR) and PSTN access.
- Route pattern refers to single route list.
- Route list includes only Standard Local Route Group.
- CFUR CSS can be the same for all phones.

If globalized numbers are used as CFUR destinations, calls to unregistered phones (for example, phones that lost IP connectivity to CUCM and are in SRST mode) are using the only configured off-net route pattern \+! for CFUR. All calling devices will use the same route pattern, route list, and route group to place the call. This route pattern is a general off-net route pattern and is used for PSTN calls, AAR calls, and CFUR calls. The CFUR CSS can be the same for all phones, and the local gateway will be used for the CFUR call because local route groups are configured.

Without using local route groups, the CFUR CSS determines the gateway that is used for the CFUR call. The CFUR CSS of the phone that is unregistered is used—not the one of the phone that tries to reach the unregistered phone. This means that all callers use the same CFUR CSS when calling an unregistered phone (the CFUR CSS configured at the destination phone). Consequently, if callers are located at different sites, they will all use the same gateway for the CFUR call. Usually, the main site gateway is used for that purpose, which means that the CFUR CSS (applied to all phones) provides access to PSTN route patterns that use the main site gateway (via the referenced route list and route group). With local route groups, each caller can use its local gateway for CFUR calls; there is no need to use the IP WAN toward the main site and then break out to the PSTN with the CFUR call at the main site gateway. Depending on the deployment, this can be a huge improvement for reaching sites that lost IP connectivity to CUCM.

CFUR Example Without Globalized Call Routing

Figure 5-13 illustrates the call flow with CFUR without local route groups.

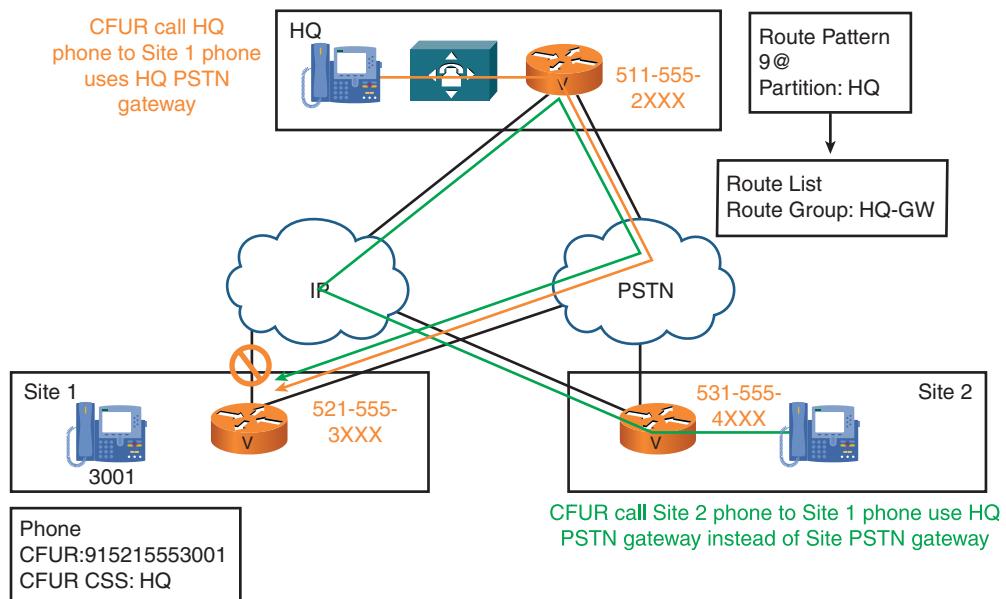


Figure 5-13 CFUR Example Without Globalized Call Routing

Three sites are in the figure: HQ, Site 1, and Site 2. The remote sites are backed up by SRST gateways. If IP connectivity between Site 1 and the HQ fails, Site 1 phones will failover to SRST mode. They can still call the HQ and Site 2 via the PSTN. When an HQ phone attempts to call a phone at Site 1 that is unregistered in CUCM, the call is placed to the CFUR destination configured at the Site 1 phone (915215553001 in this example). The CFUR CSS of the Site 1 phone ensures that route pattern 9.@ is used, which refers to how the HQ gateway is accessed. Therefore, the call is redirected to the PSTN number of the called phone and sent to the HQ gateway.

When a user at Site 2 attempts to call a phone at Site 1, the same thing happens. The CFUR destination 915215553001 is called using the CFUR CSS configured at the Site 1 phone and therefore matches the 9.@ route pattern that refers to the HQ gateway and not to a 9.@ route pattern referring to a Site 2 gateway. Therefore, the call uses the IP WAN to get from Site 2 to the HQ and, from there, it breaks out to the PSTN toward Site 1. If more sites existed, they would all use the HQ gateway for CFUR calls to Site 1. This can lead to suboptimal routing. In addition, different route patterns may be needed, depending on the destination of the CFUR call. In an international deployment, the CFUR destination number may be a mix of national and international numbers. Each destination number has to be specified in a way that it can be routed by the CFUR CSS. There is no common format for all CFUR destinations, in that some may be specified in national format and others in international format.

CFUR Example with Globalized Call Routing

Figure 5-14 shows the same scenario, but with globalized call routing.

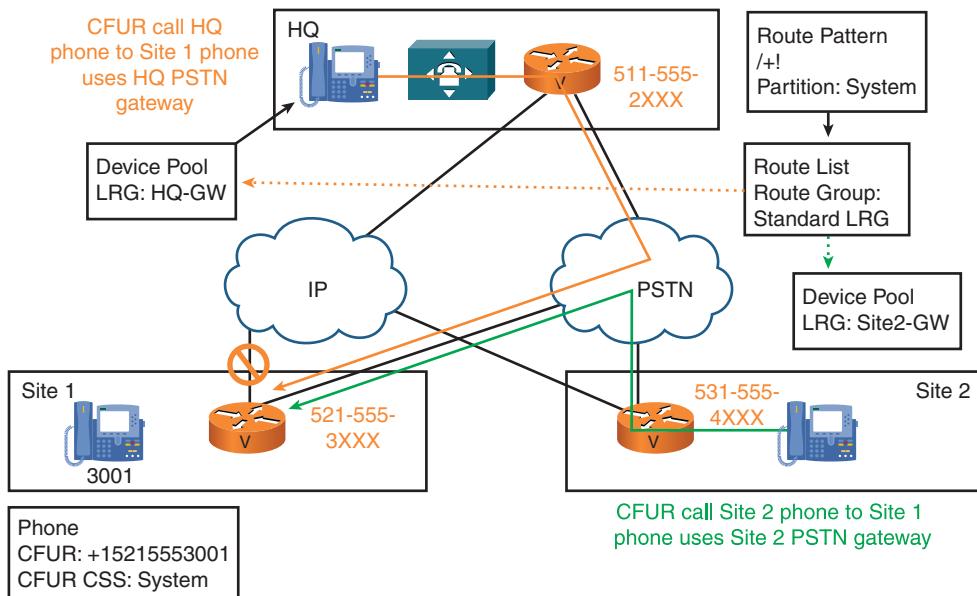


Figure 5-14 CFUR Example With Globalized Call Routing

There is only a single \+! route pattern; the referenced route list has local route groups enabled. All phones use the same CFUR CSS, which provides access to the partition of the global route pattern. The egress gateway is selected by the local route group feature. Localization of the called number occurs at the egress gateway by global transformations. If a called is placed to an unregistered phone of Site 1, the CFUR destination +15215553001 is called using the single off-net route pattern, which is configured to use the local route group (in the referenced route list). Consequently, like any other PSTN call, CFUR calls use the local gateway instead of the HQ gateway, regardless of the caller's location. There is no need for all callers to use the same gateway for CFUR calls. In addition, all CFUR destination numbers are specified in a global format (E.164 with + prefix).

Keeping Calling Privileges Active in SRST Mode

Under normal conditions in multisite deployments with centralized call processing, calling privileges are implemented using partitions and CSSs within CUCM.

However, when IP WAN connectivity is lost between a branch site and the central site, Cisco Unified SRST takes control of the branch IP Phones, and the entire configuration that is related to partitions and CSSs is unavailable until IP WAN connectivity is restored.

Therefore, it is desirable to implement CoSs within the branch router when running in SRST mode.

For this application, you must define CoSs in Cisco IOS routers using the COR functionality. You can adapt the COR functionality to replicate the CUCM concepts of partitions and CSSs by following these guidelines:

- Named tags have to be defined for each type of call that you want to distinguish.
- Outgoing COR lists containing a single tag each have to be assigned to the outgoing dial peers that should not be available to all users. These outgoing COR lists are equivalent to partitions in CUCM.
- Incoming COR lists containing one or more tags have to be assigned to the directory numbers that belong to the various CoSs. Incoming COR lists are equivalent to CSSs in CUCM.

SRST Dial Plan Example

Call-routing components on Cisco IOS routers and CUCM are necessary before a dial plan will work in SRST mode, as shown in Figure 5-15.

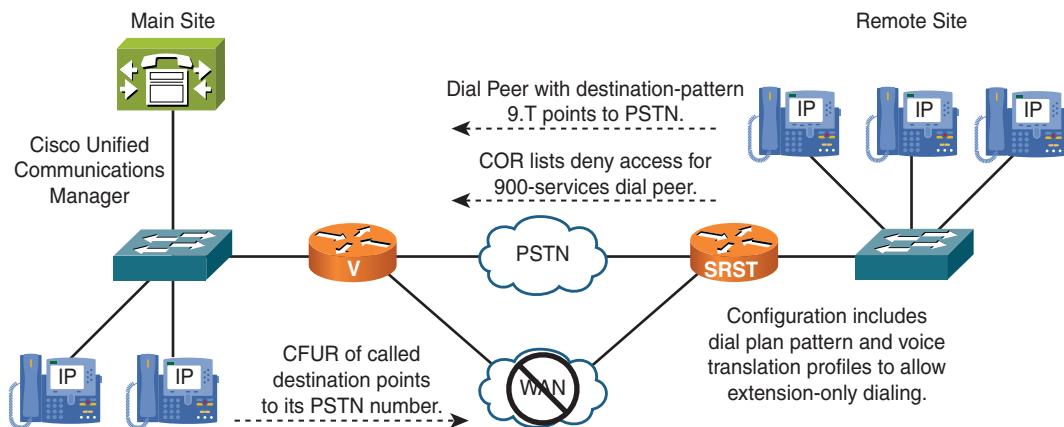


Figure 5-15 Cisco Unified SRST Dial Plan Requirement Example

CFUR must be defined on the CUCM side. Configuring the Cisco IOS router is more complex when you use dial peers, COR, dial plan pattern, and voice translation profiles to define the simplified SRST dial plan. Note how this example lets you dial 9 to get out to all numbers on the PSTN from the remote sites but limits 900 calls with COR to align with the same restrictions set in CUCM.

Summary

The following key points were discussed in this chapter:

- MGCP fallback works in conjunction with SRST to provide telephony service to remote IP Phones during WAN failure.
- Making the Cisco IP Phone CUCM list shorter results in faster SRST switchover.
- The Cisco Unified SRST version is linked with the Cisco IOS Software release.
- The MGCP gateway fallback default application is H.323 or SIP.
- When SRST is active, several measures must be taken to ensure connectivity from remote sites to PSTN destinations, between different sites, and inside the site itself.

References

For additional information, refer to these resources:

Cisco Systems, Inc. Cisco Unified Communications System 8.x SRND, April 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8x.html.

Cisco Systems, Inc. *Cisco Unified Communications Manager Administration Guide Release 8.0(1)*, February 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_1/ccmcfg/bccm-801cm.html.

Cisco Systems, Inc. Cisco Unified Survivable Remote Site Telephony Version 8.0, November 2009.
www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps2169/data_sheet_c78-570481.html.

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in the Answers Appendix.

1. Which of the following CUCM and IOS gateway features provides failover for MGCP controlled gateways?
 - a. MGCP SRST
 - b. SRST fallback
 - c. MGCP fallback
 - d. MGCP in SRST mode
 - e. MGCP failover

2. Which two show the correct numbers of supported phones in Cisco Unified SRST 8.0 for the given platform?
 - a. 800: 24
 - b. 2801–2851: 25-100
 - c. 2901–2951: 400-800
 - d. 3825, 3845: 350,730
3. What can you use to configure the dial plan at the remote-site gateway so that branch users can still reach the headquarters when dialing internal directory numbers during fallback?
 - a. This is not possible. Users have to dial headquarters users by their E.164 PSTN number while in fallback mode.
 - b. Translation profiles modifying the calling number.
 - c. The **dialplan-pattern** command.
 - d. Translation profiles modifying the called number.
 - e. Although this is possible, it should be avoided, because it may confuse users.
4. Which two signaling protocols can be used on a remote gateway with MGCP fallback when in fallback mode?
 - a. MGCP
 - b. SCCP
 - c. SIP
 - d. H.323
 - e. Megaco
 - f. RTP
5. What IOS commands are used on a remote gateway configured with MGCP fallback to give PSTN access for IP Phones during fallback mode?
 - a. This feature is unavailable. Remote phones can only dial each other.
 - b. H.323 or SIP dial peers.
 - c. Static routes.
 - d. Dynamic dial peers.
 - e. MGCP dial peers.

6. What protocol is used between the remote-office Cisco IP Phones and CUCM during fallback to send keepalives to CUCM for SRST?
 - a. MGCP
 - b. SCCP
 - c. H.323
 - d. OSPF hello packets
 - e. EIGRP keepalives
7. What method maintains SIP connectivity from remote-office Cisco IP Phones to CUCM during a complete WAN failure?
 - a. This is not possible. Remote-office Cisco IP Phones will fail over to the SRST remote-office router.
 - b. SIP can be routed through the PSTN with POTS dial peers.
 - c. SIP can be routed through the PSTN if the local exchange carrier enables SIP through the PSTN connection.
 - d. SIP can be routed through the PSTN with POTS dial peers combined with the local exchange carrier, enabling SIP through the PSTN connection.
8. What are two requirements to have multiple MOH sources in SRST?
 - a. This is not possible.
 - b. SRST v8.x must be implemented.
 - c. Configure MOH groups.
 - d. Only use SIP phones.

This page intentionally left blank

Chapter 6

Implementing Cisco Unified SRST and MGCP Fallback

This chapter describes how to configure Cisco Unified Survivable Remote Site Telephony (SRST) on Cisco IOS routers to provide redundancy to Cisco Skinny Client Control Protocol (SCCP) phones. It also describes how to configure the Media Gateway Control Protocol (MGCP) gateway fallback feature. In addition, this chapter illustrates how to configure features such as Music On Hold (MOH) and voice-mail integration for Cisco Unified SRST.

Upon completing this chapter, you will be able to configure SRST to provide call survivability and MOH for SCCP phones and MGCP fallback for gateway survivability. You will be able to meet these objectives:

- Describe the configuration requirements of CUCM and the SRST gateway
- Configure CUCM to enable SRST for remote phones
- Configure a Cisco IOS router for SRST
- Configure a Cisco IOS router to support MGCP fallback
- Configure CUCM to route calls to unregistered devices via the PSTN
- Configure a Cisco IOS router with a dial plan for SRST operation
- List features that are supported by Cisco Unified SRST and describe how to implement MOH and class of restriction

MGCP Fallback and SRST Configuration

Figure 6-1 shows the topology relating to configuring Cisco Unified SRST and MGCP gateway fallback on Cisco IOS routers.

The MGCP-gateway-fallback feature is activated and configured on the Cisco IOS router. Note that Cisco Unified SRST must be configured within CUCM and within the Cisco IOS router.

Configuration Requirements for MGCP Fallback and Cisco Unified SRST

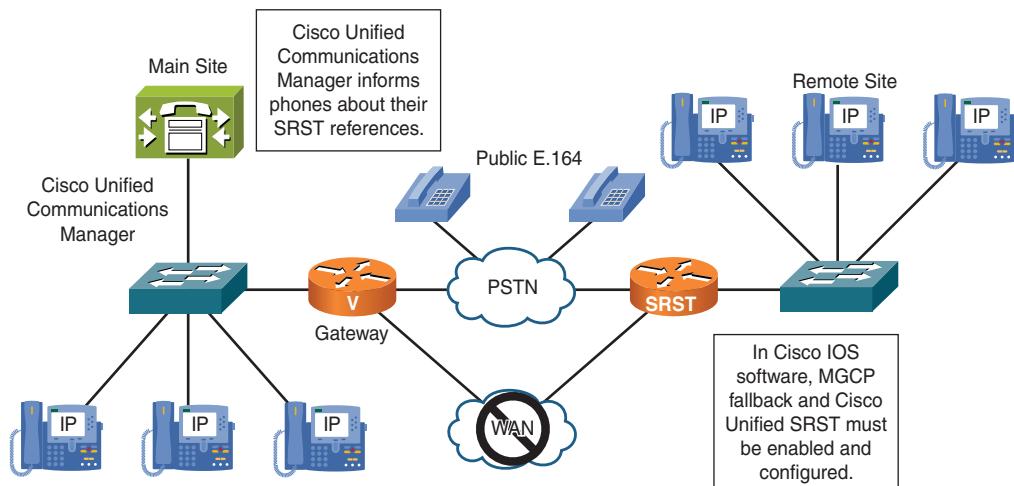


Figure 6-1 MGCP Fallback and SRST Configuration

When configuring MGCP fallback and Cisco Unified SRST, you must follow these steps at different locations:

- Define the SRST references for phones in CUCM Administration.
- Configure the Call Forward Unregistered (CFUR) feature, and set the CFUR destination of lines on remote-site phones to the correct public switched telephone network (PSTN) number in CUCM Administration to enable reachable remote sites in SRST mode.
- Enable and configure the MGCP fallback and Cisco Unified SRST features on the IOS gateways.
- Implement a simplified SRST dial plan on the remote-site gateways to ensure connectivity for remote-site phones in SRST mode.

Cisco Unified SRST Configuration in CUCM

The SRST feature in Cisco Unified Communications Manager (CUCM) provides IP Phones with the information needed to find the relative gateway to register with when they lose contact with CUCM servers.

An SRST reference must first be defined. This reference contains information about IP addresses and ports of SRST gateways for SCCP and Session Initiation Protocol (SIP)

Phones. Because the SRST functions are different for SIP and SCCP, the addresses and ports are also different.

Secondly, provide a group of phones with this information by assigning the SRST reference to a proper device pool, which is then assigned to the phones.

SRST Reference Definition

An SRST reference, as shown in Figure 6-2, comprises the gateway, which can provide limited CUCM functionality when all other CUCM servers for IP Phones are unreachable. From **Cisco Unified CM Administration**, choose **System > SRST > Add New**.

SRST Reference Information	
Name*	<input type="text" value="SRST-Remote1"/>
Port*	2000
IP Address*	<input type="text" value="172.42.2.1"/>
SIP Network/IP Address	<input type="text"/>
SIP Port*	5060
SRST Certificate Provider Port*	2445
<input type="checkbox"/> Is SRST Secure?	

Figure 6-2 SRST Reference Definition in CUCM

SRST references determine which gateways IP Phones will search when they attempt to complete a call if the CUCM is unavailable.

Administrators must configure CUCM with a unique SRST reference name that specifies the IP address of the Cisco Unified SRST gateway. The default TCP port number 2000 normally is used.

The SIP network and IP address apply to SIP SRST. If SIP SRST is used, the IP address and port that are used by the SIP protocol of the Cisco Unified SRST gateway have to be specified; the default port number is 5060. The configured address and port will be used by SIP phones to register with the SIP SRST gateway.

For Cisco Unified SRST gateways that support SCCP phones with default port number 2000 with secure SRST disabled, it is not necessary to add an SRST reference if the IP address of the Cisco Unified SRST gateway is the default gateway of the IP Phone. In this case, you can use the option **Use Default Gateway** at the device pool of the affected IP Phones.

CUCM Device Pool

The SRST reference, as shown in Figure 6-3, is assigned to IP Phones using device pools. From **Cisco Unified CM Administration**, choose **System > Device Pool > Add New**.

Administrators select the configured SRST reference from the drop-down menu in the device pool configuration.

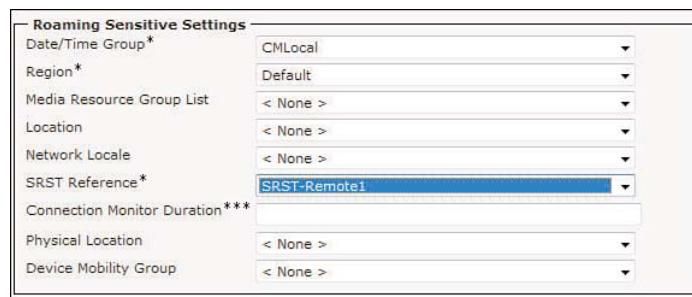


Figure 6-3 Device Pool in CUCM

Note If devices are associated with this SRST reference, a message appears that says that devices must be reset for the update to take effect.

SRST Configuration on the Cisco IOS Gateway

To configure Cisco Unified SRST on a Cisco IOS router to support the Cisco IP Phone functions, follow these steps:

- Step 1.** Enter call-manager-fallback configuration mode to activate SRST.
- Step 2.** Define the IP address and port to which the SRST service binds.
- Step 3.** Define the maximum number of directory numbers (DN) to support.
- Step 4.** Define the maximum number of IP Phones to support.
- Step 5.** Define the maximum number of numbers allowed per phone type.
- Step 6.** (Optionally) Define the phone keepalive interval.

Tip When Cisco Unified SRST is enabled, Cisco IP Phones in call-manager-fallback configuration mode do not have to be reconfigured because phones retain the same configuration that was used with CUCM.

SRST Activation Commands

Example 6-1 shows the commands for the first two SRST configuration steps.

Example 6-1 SRST Activation Commands

```
RemoteSite# configure terminal
RemoteSite(config)# call-manager-fallback
RemoteSite(config-cm-fallback)# ip source-address ip-address [port port]
[any-match | strict-match]
```

The Cisco IOS command **call-manager-fallback** enables SRST on the IOS router and enters the call-manager-fallback configuration mode.

The Cisco IOS command **ip source-address** enables the router to receive messages from the Cisco IP Phones through the specified IP addresses and provides for strict IP address verification. The default port number is 2000. This IP address will be supplied later as an SRST reference IP address in CUCM Administration.

The **ip source-address** command is mandatory. The fallback subsystem does not start if the IP address of the Ethernet port to which the IP Phones are connected (typically the Ethernet interface of the local SRST gateway) is not provided. If the port number is not provided, the default value (2000) is used.

The **any-match** keyword instructs the router to permit Cisco IP Phone registration even when the IP server address used by the phone does not match the IP source address. This option lets you register Cisco IP Phones on different subnets or those with different default DHCP routers or different TFTP server addresses.

The **strict-match** keyword instructs the router to reject Cisco IP Phone registration attempts if the IP server address used by the phone does not exactly match the source address. By dividing the Cisco IP Phones into groups on different subnets and giving each group different DHCP default router or TFTP server addresses, this option restricts the number of Cisco IP Phones allowed to register.

SRST Phone Definition Commands

The commands shown in Example 6-2, **max-dn** and **max-ephones**, are mandatory because the default values for both are defined as 0.

Example 6-2 SRST Phone Definition Commands

```
RemoteSite# configure terminal
RemoteSite(config)# call-manager-fallback
RemoteSite(config-cm-fallback)# max-dn max-directory-numbers [dual-line]
  [preference preference-order]
RemoteSite(config-cm-fallback) #max-ephones max-phones
```

The Cisco IOS command **max-dn** sets the maximum number of DNs or virtual voice ports that can be supported by the router and activates dual-line mode. The maximum number is platform-dependent. The default is 0. Select a number greater than 0 for both settings, which aligns with your licensing.

The **dual-line** keyword is optional. It allows IP Phones in SRST mode to have a virtual voice port with two channels.

Note The **dual-line** keyword facilitates call waiting, call transfer, and conference functions by allowing two calls to occur on one line simultaneously. In dual-line mode, all IP Phones on the Cisco Unified SRST router support two channels per virtual voice port.

The optional parameter **preference** sets the global preference for creating the VoIP dial peers for all DNs that are associated with the primary number. The range is from 0 to 10. The default is 0, which is the highest preference.

Note The router must be rebooted to reduce the limit on the DNs or virtual voice ports after the maximum allowable number is configured.

To configure the maximum number of Cisco IP Phones that an SRST router can support, use the **max-ephones** command in call-manager-fallback configuration mode. The default is 0, and the maximum configurable number is platform-dependent. The only way to increase the maximum number of Cisco IP Phones supported is to upgrade to a higher hardware platform.

Note The **max-dn** and the **max-ephones** commands must be configured during the initial Cisco Unified SRST router configuration to a non-zero value before any IP Phone actually registers with the Cisco Unified SRST router. However, you can change these settings later.

Note The router must be rebooted to reduce the limit on Cisco IP Phones after the maximum allowable number is configured.

SRST Performance Commands

To optimize performance of the system, best practice dictates that you use the **limit-dn** and **keepalive** commands, as shown in Example 6-3.

Example 6-3 SRST Performance Commands

```
RemoteSite# configure terminal
RemoteSite(config)# call-manager-fallback
RemoteSite(config-cm-fallback)#limit-dn {7910 | 7935 | 7940 | 7960} max-lines
RemoteSite(config-cm-fallback)# keepalive seconds
```

The optional Cisco IOS command **limit-dn** limits the DN lines on Cisco IP Phones during SRST mode, depending on the Cisco IP Phone model.

The setting for the maximum number of directory lines is from 1 to 6. The default is 6. If any active phone has the last line number greater than this limit, warning information is displayed for phone reset.

The optional Cisco IOS command `keepalive` sets the time interval, in seconds, between keepalive messages that are sent to the router by Cisco IP Phones. The range is 10 to 65,535. The default is 30.

The keepalive interval is the period of time between keepalive messages that are sent by a network device. A keepalive message is a message that is sent by one network device to inform another network device that the virtual circuit between the two is still active.

Note If the default time interval between messages of 30 seconds will be used, this command does not have to be entered in the configuration. Like many settings in the IOS, if the default setting is entered into the configuration, it does not show up with `show running-config`.

Cisco Unified SRST Configuration Example

Figure 6-4 shows a multisite topology that supports SCCP-controlled IP Phones at the remote SRST site. The configuration is shown in Example 6-4.

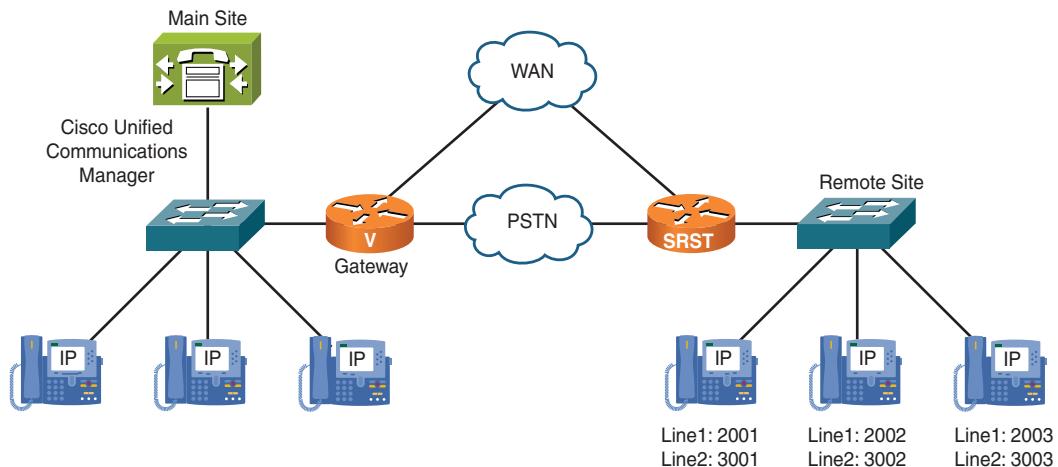


Figure 6-4 Multisite Topology Supporting SCCP-Controlled IP Phones at the Remote SRST Site

The SRST router is installed at a small-branch office site with three IP Phones, each having two lines (six lines total). The IP address 172.47.2.1 is also configured on the loopback interface. Example 6-4 shows a sample configuration for the Cisco Unified SRST router to operate in this environment.

Example 6-4 Cisco Unified SRST Configuration Example

```

RemoteSite# configure terminal
RemoteSite(config)# call-manager-fallback
RemoteSite(config-cm-fallback)# ip source-address 172.47.2.1 port 2000
RemoteSite(config-cm-fallback)# max-ephones 3 dual-line
RemoteSite(config-cm-fallback)# max-dn 6
RemoteSite(config-cm-fallback)# limit-dn 7960 2
RemoteSite(config-cm-fallback)# keepalive 20
RemoteSite(config-cm-fallback)# end
RemoteSite#

```

Note More commands might be necessary, depending on the complexity of the deployment.

MGCP-Gateway-Fallback Configuration on the Cisco IOS Gateway

To configure the MGCP gateway fallback on a Cisco IOS router to support the MGCP fallback function, follow these steps:

Step 1. Activate MGCP gateway fallback.

Step 2. Define the service to fall back to.

To enable outbound calls while in SRST mode on an MGCP gateway, you must configure two fallback commands on the MGCP gateway. These two commands allow SRST to assume control over the voice port and over call processing on the MGCP gateway. With Cisco IOS Software releases before 12.3(14)T, configuring MGCP gateway fallback involves the `ccm-manager fallback-mgcp` and `call application alternate` commands. With Cisco IOS Software releases after 12.3(14)T, configuring MGCP gateway fallback uses the `ccm-manager fallback-mgcp` and `service` commands.

Note Both commands have to be configured. Configurations will not work reliably if only the `ccm-manager fallback-mgcp` command is configured.

To use SRST on an MGCP gateway, you must configure SRST and MGCP gateway fallback on the same gateway.

MGCP Fallback Activation Commands

The Cisco IOS command `ccm-manager fallback-mgcp`, shown in Example 6-5, enables the gateway fallback feature and allows an MGCP voice gateway to provide call-processing services through SRST or other configured applications when CUCM is unavailable.

Example 6-5 MGCP Fallback Activation Commands

```
RemoteSite# configure terminal
RemoteSite(config)# ccm-manager fallback-mgcp
RemoteSite(config)# call application alternate Default
RemoteSite(config-app-global)# service alternate Default
```

The **call application alternate Default** command specifies that the default voice application takes over if the MGCP call agent is unavailable. This allows a fallback to H.323 or SIP, which means that local dial peers are considered for call routing.

The **service alternate Default** command is entered in the global-configuration submode of the application-configuration submode. To navigate to this location, follow these steps:

- Step 1.** To enter application configuration mode to configure applications, use the **application** command in global configuration mode.
- Step 2.** To enter application-configuration global mode, use the **global** command in application configuration mode.

Enter either of the two commands, depending on the Cisco IOS Software release. The newer configuration method is the **service** command.

As discussed in the preceding chapter, analog calls are preserved in the event of MGCP fallback. To provide call preservation during switchback, call preservation for H.323 has to be enabled using the commands shown in Example 6-6.

Example 6-6 H.323 Call Preservation Activation Commands

```
RemoteSite# configure terminal
RemoteSite(config)# voice service voip
RemoteSite(conf-voi-serv)# h323
RemoteSite(conf-serv-h323)# call preserve
```

MGCP Fallback Configuration Example

Figure 6-5 shows an MGCP-controlled remote-site gateway with an MGCP-gateway-fallback configuration for an SRST-enabled Cisco IOS router, as shown in Example 6-7.

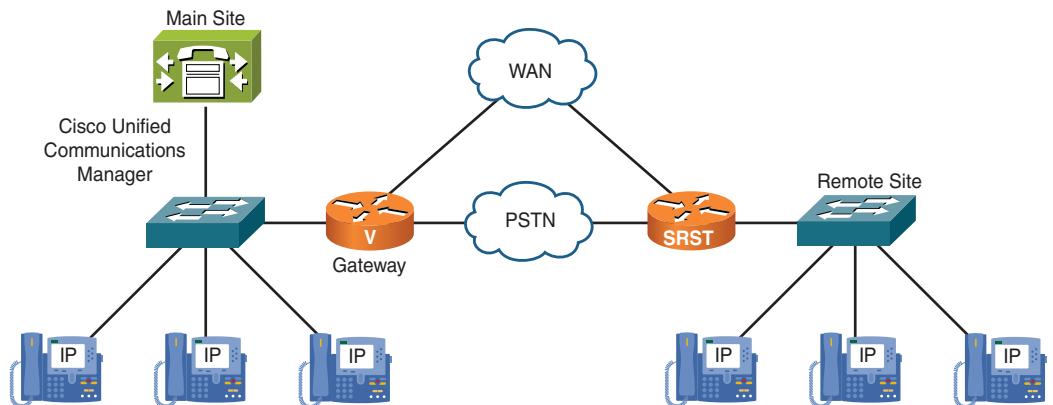


Figure 6-5 MGCP Fallback Example

Example 6-7 MGCP Fallback Configuration Example

```
RemoteSite# configure terminal
RemoteSite(config)# ccm-manager fallback-mgcp
RemoteSite(config)# application
RemoteSite(config-app)# global
RemoteSite(config-app-global)# service alternate Default
RemoteSite(config-app-global)# end
RemoteSite#
```

Note More commands might be necessary, depending on the complexity of the deployment.

Dial Plan Configuration for SRST Support in CUCM

This section describes the configuration to adjust the CUCM dial plan to work with Cisco Unified SRST.

The CUCM dial plan has to be adjusted to ensure the reachability of remote-site phones by their extensions even if the remote site runs in SRST mode. The parameter that enables this adjustment is the CFUR destination setting, which has to be defined on every line of an SRST enabled remote-site phone. This parameter was introduced in CUCM Release 4.2.

The CFUR feature forwards calls to unregistered (disconnected or logged out) DNs for the defined destination. The destination might be the PSTN number of a phone at a remote site or the voice mail for a user in a CUCM Extension Mobility setting.

To ensure that the feature works even if a major WAN breakdown disconnects all the remote sites, only voice gateways located at the main site should be used. This can be ensured by selecting the correct Calling Search Space (CSS) for the CFUR destination.

CFUR causes routing loops whenever there is a single disconnected SRST phone in which the remote location is not in SRST mode. Internal calls to that DN are forwarded to the CFUR (PSTN) destination and are received by the remote-site gateway in normal mode. This gateway handles the call as usual, sending the signaling to its CUCM subscriber. CUCM then again forwards the call to the PSTN, causing an inevitable routing loop.

To limit the impact of these routing loops, Cisco introduced a CUCM service parameter called Max Forward UnRegistered Hops to DN. When activated, this counter limits the calls that are forwarded to one CFUR destination.

SRST Dial Plan of CFUR and CSS

The CFUR feature is a way to reroute calls placed to a temporarily unregistered destination phone. The configuration of CFUR consists of the two main elements of destination selection and CSS, as shown in Figure 6-6. From Cisco Unified CM Administration, choose Call Routing > Directory Number.

Call Forward and Call Pickup Settings		Voice Mail	Destination	Calling Search Space
Calling Search Space Activation Policy				Use System Default
Forward All	<input type="checkbox"/> or			< None >
Secondary Calling Search Space for Forward All				< None >
Forward Busy Internal	<input type="checkbox"/> or			< None >
Forward Busy External	<input type="checkbox"/> or			< None >
Forward No Answer Internal	<input type="checkbox"/> or			< None >
Forward No Answer External	<input type="checkbox"/> or			< None >
Forward No Coverage Internal	<input type="checkbox"/> or			< None >
Forward No Coverage External	<input type="checkbox"/> or			< None >
Forward on CTI Failure	<input type="checkbox"/> or			< None >
Forward Unregistered Internal	<input type="checkbox"/> or	914815550001		CFUR-to-PSTN
Forward Unregistered External	<input checked="" type="checkbox"/> or			< None >
No Answer Ring Duration (seconds)				
Call Pickup Group		< None >		

Figure 6-6 SRST Dial Plan Configuration of CFUR and CSS

When the DN is unregistered, calls can be rerouted to the voice mail that is associated with the extension or to a DN that is used to reach the phone through the PSTN. The latter approach is preferable when a phone is located within a site whose WAN link is down. If the site is equipped with SRST, the phone (and its co-located PSTN gateway) reregisters with the co-located SRST router. The phone then can receive calls placed to its PSTN direct inward dialing (DID) number.

In this case, the appropriate CFUR destination is the corresponding PSTN DID number of the original destination DN. Configure this PSTN DID in the destination field, along

with applicable access codes and prefixes. For this example, the number would be 9-1-481-555-0001.

CUCM attempts to route the call to the configured destination number using the CFUR CSS of the called DN. The CFUR CSS is configured on the target phone and is used by all devices that are calling the unregistered phone.

This means that all calling devices use the same combination of route pattern, route list, route group, and gateway to place the call, and that all CFUR calls to a given unregistered device are routed through the same unique gateway, regardless of where the calling phone is located. It is recommended that you select a centralized gateway as the egress point to the PSTN for CFUR calls. You also should configure the CFUR CSS to route calls that are intended for the CFUR destination to this centralized gateway.

A better solution is to use the local route group feature. When you use this feature, the route list does not refer to a specific route group, but Standard Local Route Group is added to the route list instead. The route group that is to be used for the calls is then determined by the local route group that is configured at the device pool of the calling device. In this case, phones at different sites can refer to different route groups via their device pool configuration.

If different sites require different dialing patterns (for example, an international deployment where each country has different PSTN access codes and international access codes), it is recommended that you specify the PSTN number to be used for CFUR in E.164 format with a + prefix. The CFUR CSS should match a \+! route pattern and refer to a route list, which is configured to use the Standard Local Route Group of the calling device. At the egress gateway, after path selection has been performed using the local route group, the called number can be modified by global transformations (via a called-party transformation CSS configured at the egress gateway), based on the individual requirements of the selected egress gateway.

SRST Dial Plan: Max Forward UnRegistered Hops to DN

The CUCM service parameter Max Forward UnRegistered Hops to DN reduces the impact caused by CFUR routing loops, as shown in Figure 6-7. From Cisco Unified CM Administration, choose **System > Service Parameter > Cisco CallManager**.

This parameter specifies the maximum number of forward unregistered hops that are allowed for a DN at one time. It limits the number of times the call can be forwarded because of the unregistered DN when a forwarding loop occurs. Use this count to stop forward loops for external calls that have been forwarded by CFUR, such as intercluster IP Phone calls and IP Phone-to-PSTN phone calls that are forwarded to each other. CUCM terminates the call when the value that is specified in this parameter is exceeded. The default 0 disables the counter but not the CFUR feature. The allowed range is from 0 to 60.

Clusterwide Parameters (Feature - Forward)	
<u>Forward Maximum Hop Count</u> *	12
<u>Forward No Answer Timer</u> *	12
<u>Max Forward Hops to DN</u> *	12
<u>Retain Forward Information</u> *	False
<u>Forward By Reroute Enabled</u> *	False
<u>Transform Forward by Reroute Destination</u> *	True
<u>Always Forward Switch Voice Mail Calls</u> *	True
<u>Forward By Reroute T1 Timer</u> *	10
<u>Include Original Called Info for Q.SIG Call Diversions</u> *	Only after the first diversion
<u>Max Forward UnRegistered Hops to DN</u> *	0
<u>CFA CSS Activation Policy</u> *	With Configured CSS
There are hidden parameters in this group. Click on Advanced button to see hidden parameters.	

Figure 6-7 SRST Dial Plan Configuration of Max Forward UnRegistered Hops to DN

MGCP Fallback and SRST Dial Plan Configuration in the Cisco IOS Gateway

A dial plan in SRST mode, at a minimum, enables the remote-site users to place and receive calls from the PSTN.

At least one dial peer needs to be configured to enable calls to and from the PSTN. The destination pattern of that dial peer has to correspond to the PSTN access code (for example, 9T). The more elegant way is to configure several dedicated dial peers with destination patterns that match the number patterns in a closed numbering plan, such as 91. (91 followed by ten dots).

In countries that have variable dial plans, the only destination pattern that is needed for dialing 9 first for PSTN access is 9T. Because of the variable length of dialed numbers, the router waits for the interdigit timeout (T302) or for a hash (#) sign to indicate the end of the dial string. Cisco Unified SRST version 4.1 and CUCME Release 4.1 do not support the overlap sending feature to the PSTN. The receiving of ISDN overlap dialing from PSTN is supported but has to be enabled on the ISDN interfaces. To shorten the wait time for users after they complete the dial string, it is possible to reduce the inter-digit timeout from the IOS SRST default of 10 seconds.

Dial plan pattern configuration is a powerful tool for the modification of incoming called numbers to match remote-site extensions. Dial plan pattern is designed to function for Cisco IP Phones but not locally attached analog FXS devices.

SRST Dial Plan Components for Normal Mode Analogy

A good SRST dial plan is as close as possible between the dialing functionality in normal mode and in SRST mode. The telephony service should have the same dialing look and feel for the user, regardless of the mode the system is in. For example, it would be an

unacceptable failover design if the remote user required an awareness of WAN link connectivity when he dials his headquarters.

The numbers in the call lists (such as missed calls) must have the correct format (PSTN access code plus PSTN phone number) to enable users to use the list entries for dialing. The calling party ID of incoming calls from the PSTN needs to be modified by voice translation profiles and voice translation rules.

Abbreviated dialing between sites of the site code plus the extension number is possible in SRST mode. Voice translation profiles have to be used to expand the called numbers to PSTN format for intersite dialing.

If the calling privileges (which normally are controlled by the CUCM) have to be preserved in SRST mode, class of restriction (COR) configuration must be used.

The handling of variable-length numbers in CUCM should also be preserved in SRST mode. This includes the tuning of the interdigit timeout, the possibility to use the # key to terminate dialing, and the implementation of overlap sending.

Cisco Unified SRST Dial Plan Dial Peer Commands

The **dial-peer** command is the main component for configuring dial plans on Cisco IOS routers, as shown in Example 6-8.

Example 6-8 Dial Peer Commands for an SRST Dial Plan

```
RemoteSite# configure terminal
RemoteSite(config)# dial-peer voice tag pots
RemoteSite(config-dial-peer)# destination-pattern [+string[T]
RemoteSite(config-dial-peer)# port slot-number/port
```

You define a particular dial peer, specify the voice encapsulation method, and enter dial peer configuration mode using the **dial-peer voice** command in global configuration mode. The following list defines the keywords and parameters used in the configuration shown in Example 6-8:

- The parameter tag specifies digits that define a particular dial peer. The range is from 1 to 2147483647.
- The keyword **pots** indicates that this is a plain old telephone service (POTS) peer. The option **voip** also exists, indicating that this is a VoIP peer, but is not mentioned in Example 6-8 because POTS dial peers are predominately used for SRST. POTS dial peers contain a port, whereas VoIP dial peers contain a configured IP address.
- You specify either the prefix or the full E.164 telephone number to be used for a dial peer using the **destination-pattern** command in dial peer configuration mode.
- The optional character **+** indicates that an E.164 standard number follows.

- The parameter *string* defines a series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters:

```
*  
#  
,.  
+  
^  
$  
\  
?  
[]  
()
```

- The optional control character T indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.
- To associate a dial peer with a specific voice port, use the **port** command in dial peer configuration mode.
- The parameter *slot-number* defines the number of the slot in the router in which the voice interface card (VIC) is installed. Valid entries depend on the number of slots that the router platform has.
- The parameter *port* defines the voice port number. Valid entries are 0 and 1.

Note Details about the meanings of these special characters and about Cisco IOS dial peer configuration in general are provided in the *Implementing Cisco Unified Communications Voice over IP and QoS (Cvoice) Foundation Learning Guide*, Fourth Edition.

Table 6-1 lists an example of common classes of PSTN calls in the North American Numbering Plan (NANP) and lists the pattern that is used for each class. An access code of 9 is often used to indicate a PSTN call. The exception is 911, which should be configured with and without the access code 9. The example patterns outlined in Table 6-1, if enabled in the CUCM dial plan, must also be reachable in SRST mode.

An access code of 9 typically indicates a PSTN call; however, other access codes, such as 8, are also permissible.

The patterns in the table are the minimum number of patterns that need to be reachable in SRST mode.

Table 6-1 SRST Dial Plan Dial Peer Commands

Call Type	Pattern
Emergency	911
Services	[2-8]11
Local	[2-9]xx-xxxx
Long-distance or national	1[2-9]xx [2-9]xx-xxxx
International	011+country code+number
Toll-free	1[800,866,877,888]xxx-xxxx
Premium	1 900 xxx-xxxx 1 976 xxx-xxxx

Example 6-9 provides a sample configuration of dial peers only, demonstrating outbound dialing to the PSTN in an SRST router. This example is in the NANP, which also shows local ten-digit dialing in area code 919. The configuration as written can be directly pasted into a router.

Example 6-9 Dial Peer Example for an SRST Dial Plan

```
!
dial-peer voice 1 pots
  description PSTN-emergency dial 9 first
  destination-pattern 9911
  port 0/1/0:23
  forward-digits 3
!
dial-peer voice 2 pots
  description PSTN-emergency
  destination-pattern 911
  port 0/1/0:23
  forward-digits all
!
dial-peer voice 3 pots
  description PSTN-Local Services
  destination-pattern 9[2-8]11
  port 0/1/0:23
  forward-digits 3
!
dial-peer voice 4 pots
  description PSTN-Local 7 digit dialing
  destination-pattern 9[2-9].....
  port 0/1/0:23
  forward-digits 7
```

```

!
dial-peer voice 5 pots
  description PSTN-10 Digit Local Dialing for Area Code 919
  destination-pattern 9919[2-9].....
  port 0/1/0:23
  forward-digits 10
!
dial-peer voice 6 pots
  description PSTN-Long Distance Dialing
  destination-pattern 91[2-9]..[2-9].....
  port 0/1/0:23
  forward-digits 11
!
dial-peer voice 7 pots
  description PSTN-International Dialing
  destination-pattern 9011T
  port 0/1/0:23
  prefix 011

```

Note This example does not contain any class of restriction (COR), which currently allows all SRST registered phones to dial all numbers, including long-distance, 900, and international, without any constraint. COR is discussed later in this chapter. In addition, dial peers 3 and 4 do not require the **forward-digits** command, and the **forward-digits** commands are added only for clarity.

SRST Dial Plan Commands: Open Numbering Plans

Example 6-10 defines the configuration commands for open numbering plans in an SRST dial plan. Overlap receiving is configured on the ISDN PRI.

Example 6-10 SRST Dial Plan Commands for an SRST Dial Plan

```

RemoteSite# configure terminal
RemoteSite(config)# interface serial0/1/0:23
RemoteSite(config-if)# isdn overlap-receiving [T302 ms]
RemoteSite(config-if)# exit
RemoteSite(config)# call-manager-fallback
RemoteSite(config-cm-fallback)# timeouts interdigit sec
RemoteSite(config-cm-fallback)# dialplan-pattern tag pattern
  extension-length length [extension-pattern extension-pattern] [no-reg]

```

The following list defines the commands, keywords, and parameters used in the configuration shown in Example 6-10:

- To activate overlap receiving on ISDN interfaces, you use the **isdn overlap-receiving** command in interface configuration mode. This command is applicable on BRI interfaces or on the ISDN interface of E1/T1 controllers in PRI mode.
- The optional parameter **T302** defines how many milliseconds the T302 timer should wait before expiring. Valid values for the *ms* argument range from 500 to 20000. The default value is 10000 (10 seconds).

Caution Modifying the T302 parameter, when connected to public networks, might disable the function. The T302 describes the interdigit timeout for all phones in the CUCM cluster.

- Configure the timeout value to wait between dialed digits for all Cisco IP Phones that are attached to a router using the **timeouts interdigit** command in call-manager-fallback configuration mode.
- The parameter *sec* defines the interdigit timeout duration, in seconds, for all Cisco IP Phones. Valid entries are integers from 2 to 120.
- Create a global prefix that can be used to expand the extension numbers of inbound and outbound calls into fully qualified E.164 numbers using the **dialplan-pattern** command in call-manager-fallback configuration mode.
- The parameter *tag* is the unique identifier that is used before the telephone number. The tag number is from 1 to 5.
- The parameter *pattern* is the dial plan pattern, such as the area code, the prefix, and the first one or two digits of the extension number, plus wildcard markers or dots (.) for the remainder of the extension-number digits.
- The keyword **extension-length** sets the number of extension digits that will appear as a caller ID followed by the parameter *length*, which is the number of extension digits. The extension length must match the setting for IP Phones in CUCM mode. The range is from 1 to 32.
- The optional keyword **extension-pattern** sets the leading digit pattern of an extension number when the pattern is different from the leading digits defined in the pattern variable of the E.164 telephone number. An example is when site codes are used. The parameter *extension-pattern* that follows defines the leading digit pattern of the extension number. It is composed of one or more digits and wildcard markers or dots (.). For example, 5.. would include extensions 500 to 599, and 5... would include extensions 5000 to 5999. The extension pattern configuration should match the mapping of internal to external numbers in CUCM.

- The optional keyword **no-reg** prevents the E.164 numbers in the dial peer from registering with the gatekeeper.

Example 6-11 demonstrates the use of the **dialplan-pattern** command, which shows how to create a dial plan pattern for DNs 500 to 599 that is mapped to a DID range of 408-555-5000 to 5099. If the router receives an inbound call to 408-555-5044, the dial plan pattern command is matched, and the extension of the called E.164 number, 408-555-5000, is changed to DN 544. If an outbound calling party extension number (544) matches the dial plan pattern, the calling-party extension is converted to the E.164 number 408-555-5044. The E.164 calling-party number appears as the caller ID.

Example 6-11 SRST Dial Plan Example for Mapping Directory Numbers

```
RemoteSite# configure terminal
RemoteSite(config)# call-manager-fallback
RemoteSite(config-cm-fallback)# dialplan-pattern 1 40855550..
    extension-length 3 extension-pattern 5..
```

Since Cisco Unified SRST 8.0, the **dialplan-pattern** command has been used in the opposite way with the addition of the keyword **demote** to the end of the command. In this case, it demotes IP Phone DNs that are specified in E.164 format with a + prefix to shorter extensions, which are to be used internally. External callers place calls to the phones, using E.164 format with a + prefix. If the calls are not natively received in this format from the PSTN (which they rarely are), you have to transform the called number accordingly. Internal users, however, can dial each other by using shorter extensions, which are set up by the **dialplan-pattern** command with the **demote** argument, as shown in Example 6-12.

Example 6-12 SRST Dial Plan Example with the dialplan-pattern Command

```
RemoteSite(config)# call-manager-fallback
Router(config-cm-fallback)# dialplan-pattern 1 +415526....
    extension-length 5 demote
```

In this example, phones are configured with DNs +415526.... and have to be called that way from the outside. Internal users, however, can call each other by using the last five digits (6....).

Note The **dialplan pattern** command with the **demote** argument is also available in CUCME and, hence, can be used for Cisco Unified SRST when CUCME is used in SRST mode.

SRST Dial Plan Voice Translation-Profile Commands for Digit Manipulation

The combination of voice translation-profiles and voice translation-rules creates a powerful tool for modifying numbers so that they match dial plan needs. Example 6-13 shows the configuration commands for voice translation profiles.

Example 6-13 Voice Translation Profile Commands

```
RemoteSite# configure terminal
RemoteSite(config)# voice translation-profile name
RemoteSite(cfg-translation-profile)# translate {called | calling|
    redirect-called | redirect-target| callback} translation-rule-number
```

You define a translation profile for voice calls using the **voice translation-profile** command in global configuration mode. The name parameter of this command defines the name of the translation profile. The maximum length of the **voice translation-profile** name is 31 alphanumeric characters.

You associate a translation rule with a voice translation profile using the **translate** command in **voice translation-profile** configuration mode. The following list defines the keywords and parameter for the **translate** command:

- **called** associates the translation rule with called numbers.
- **calling** associates the translation rule with calling numbers.
- **redirect-called** associates the translation rule with redirected called numbers.
- **redirect-target** associates the translation rule with transfer-to numbers and call-forwarding final destination numbers.
- **callback** associates the translation rule with the number to be used by IP Phones for callbacks.

Note While on a call, IP Phones display the calling-party number. When callbacks are placed from call lists, the callback number (if present) is used for the outbound call and not the calling-party number that was shown while the call was active.

- **translation-rule-number** is the number of the translation rule to use for the call translation. The valid range is from 1 to 2,147,483,647. There is no default value.

Note The prior IOS digit manipulation tool translation rule has been replaced by voice translation-rule. The commands are similar but are incompatible with each other.

SRST Dial Plan Voice Translation-Rule Commands for Number Modification

Example 6-14 shows the configuration commands for voice translation rules.

Example 6-14 Voice Translation Rule Commands

```
RemoteSite# configure terminal
RemoteSite(config)# voice translation-rule number
  router(cfg-translation-rule)# rule precedence /match-pattern/
    /replace-pattern/[type {match-type replace-type} [plan
    {match-type replace-type}]]
```

You define a translation rule for voice calls using the **voice translation-rule** command in global configuration mode. The number parameter identifies the translation rule. The range of the number is from 1 to 2147483647. The choice of the number does not affect usage priority.

You define a translation rule using the **rule** command in voice translation-rule configuration mode. The following list defines the keywords and parameters for the **rule** command, as shown in Example 6-14:

- The parameter *precedence* defines the priority of the translation rule. The range is from 1 to 15.
- The parameter */match-pattern/* is a stream editor (SED) expression used to match incoming call information. The slash (/) is a delimiter in the pattern.
- The parameter */replace-pattern/* is a SED expression used to replace the match pattern in the call information. The slash is a delimiter in the pattern.
- The optional construct *type match-type replace-type* lets you modify the call's number type. Valid values for the *match-type* argument are abbreviated, any, international, national, network, reserved, subscriber, and unknown. Valid values for the *replace-type* argument are abbreviated, international, national, network, reserved, subscriber, and unknown.
- The optional construct *plan match-type replace-type* lets you modify the call's numbering plan. Valid values for the *match-type* argument are any, data, ermes, isdn, national, private, reserved, telex, and unknown. Valid values for the *replace-type* argument are data, ermes, isdn, national, private, reserved, telex, and unknown.

SRST Dial Plan Profile Activation Commands for Number Modification

Voice translation profiles can be bound to dial peers, source groups, trunk groups, voice ports, and the voice service POTS.

Example 6-15 shows the configuration commands for voice translation profile activation.

Example 6-15 Voice Translation Rule Activation Commands

```
RemoteSite# configure terminal
RemoteSite(config)# voice-port 0/1/0:23
RemoteSite(config-voiceport)# translation-profile {incoming | outgoing} name
RemoteSite(config-voiceport)# exit
RemoteSite(config)# call-manager-fallback
RemoteSite(config-cm-fallback)# translation-profile {incoming | outgoing} name
```

In this example, the voice **translationprofile** is bound to a voice port. The voice **translationprofile** can also be bound to all the dial peers, but the voice port needs to be done only once.

You assign a translation profile to a voice port using the **translation-profile** command in **voice-port** configuration mode. The following list defines the keywords and parameter for the **translation-profile** command:

- The keyword **incoming** specifies that this translation profile handles incoming calls.
- The keyword **outgoing** specifies that this translation profile handles outgoing calls.
- The parameter *name* is the name of the translation profile.

In addition to the configuration shown in Example 6-14, the voice translation profiles can be bound to the **call-manager-fallback** Cisco IOS service. The structure of the command is identical.

Note The incoming direction of the voice **translation-profile** bound to the **call-manager-fallback** Cisco IOS service handles the calls coming from IP Phones that are registered with the router.

For more information about voice translation profiles, refer to Cisco TechNotes *Number Translation Using Voice Translation Profiles* at www.cisco.com/en/US/tech/tk652/tk90/technologies_configuration_example09186a00803f818a.shtml and TechNotes *Voice Translation Rules* at www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a0080325e8e.shtml.

SRST Dial Plan Class of Restriction Commands

Calling privileges can be assigned to IP Phones when they are in SRST mode using COR commands. In the absence of COR in SRST dial peers, all phones can dial all numbers.

Example 6-16 shows the dial plan configuration commands for COR as they apply to SRST.

Example 6-16 Class of Restriction Commands

```
RemoteSite# configure terminal
RemoteSite(config)# call-manager-fallback
RemoteSite(config-cm-fallback)# cor {incoming | outgoing} cor-list-name
[cor-list-number starting-number - ending-number | default]
```

The command **cor** configures a COR on dial peers that are associated with DNs. The following list defines the keywords and parameters for the **cor** command:

- The keyword **incoming** defines that a COR list is to be used by incoming dial peers.
- The keyword **outgoing** defines that a COR list is to be used by outgoing dial peers.
- The parameter *cor-list-name* is the COR list name.
- The parameter *cor-list-number* is a COR list identifier. The maximum number of COR lists that can be created is 20, composed of incoming or outgoing dial peers. The first six COR lists are applied to a range of DNs. The DNs that do not have a COR configuration are assigned to the default COR list, as long as a default COR list has been defined.
- The parameters *starting-number - ending-number* define the DN range, such as 2000 to 2025.
- The keyword **default** instructs the router to use an existing default COR list.

Table 6-2 summarizes the functions of COR dialed calls.

Note The complete configuration of COR is handled in *Implementing Cisco Unified Communications Voice over IP and QoS (Cvoice) Foundation Learning Guide*, Fourth Edition. Table 6-2 presents only an overview.

SRST Dial Plan Example

Figure 6-8 shows a multisite topology with a Cisco Unified SRST-enabled Cisco IOS router in the remote site.

Table 6-2 COR Dialing Possibilities

COR List on Incoming Dial Peer	COR List on Outgoing Dial Peer	Result
No COR.	No COR.	The call succeeds.
No COR.	A COR list is applied for outgoing calls.	The call succeeds. By default, the incoming dial peer has the highest COR priority when no COR is applied. If you apply no COR for an incoming call leg to a dial peer, the dial peer can make a call out of any other dial peer, regardless of the COR configuration on the outgoing dial peer.
A COR list is applied for incoming calls.	No COR.	The call succeeds. By default, the outgoing dial peer has the lowest priority. Because some COR configurations exist for incoming calls on the incoming or originating dial peer, it is a superset of the outgoing-call COR configuration for the outgoing or terminating dial peer.
A COR list is applied for incoming calls (a superset of the COR list applied for outgoing calls on the outgoing dial peer).	A COR list is applied for outgoing calls (subsets of the COR list applied for incoming calls on the incoming dial peer).	The call succeeds. The COR list for incoming calls on the incoming dial peer is a superset of the COR list for outgoing calls on the outgoing dial peer.
A COR list is applied for incoming calls (a subset of the COR list applied for outgoing calls on the outgoing dial peer).	A COR list is applied for outgoing calls (supersets of the COR list applied for incoming calls on the incoming dial peer).	The call does not succeed. The COR list for incoming calls on the incoming dial peer is not a superset of the COR list for outgoing calls on the outgoing dial peer.

Figure 6-8 shows a main site with a PSTN number of 511-555-2xxx and a remote site with a PSTN number of 521-555-3xxx. Four digits are used for all internal calls, including calls between the main site and remote site. The remote-site gateway has a single ISDN PRI connection to the PSTN configured on port 0/1/0:23.

For the SRST remote-site configuration shown in Example 6-16, assume that the remote site has only three phones, with one DN each. During SRST fallback, Phone 1 is

configured with directory number 3001 and has unlimited PSTN dialing access. Phone 2 is configured with directory number 3002 and is not be allowed to place international calls. Phone 3 is configured with directory number 3003 and is allowed to place only internal calls. Four-digit dialing to headquarters is configured, and calls should be sent to the main site over the PSTN when in SRST mode.

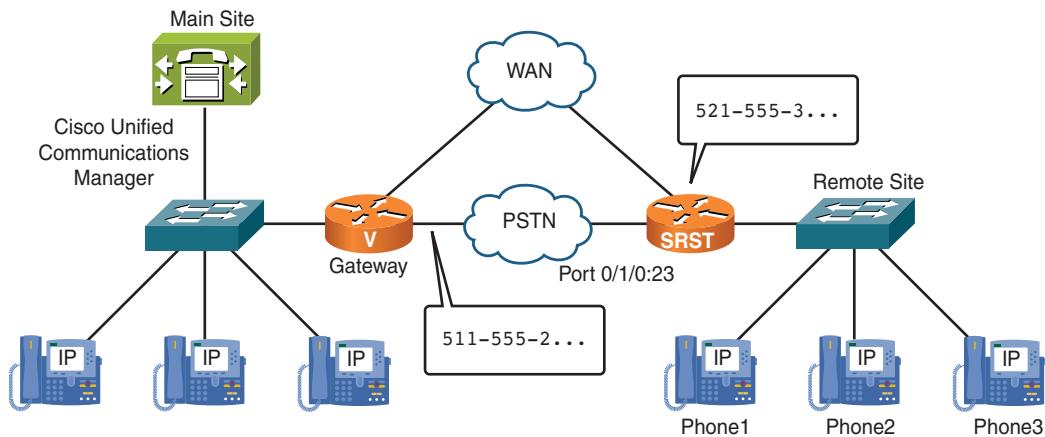


Figure 6-8 SRST Dial Plan Topology

The remote-site router also requires MGCP configurations, as discussed previously, but they are not included in Example 6-17 for simplicity.

Example 6-17 Remote-Site SRST Dial Plan Configuration Example

```

application
global
    service alternate default
!
call-manager-fallback
    ip source-address 10.1.250.101 port 2000
    max-ephones 3
    max-dn 3
    cor incoming phone1 1 3001
    cor incoming phone2 2 3002
    cor incoming phone3 3 3003
    dialplan-pattern 1 5215553...
    extension-length 4
!
dial-peer cor custom
    name internal
    name pstn

```

```
    name pstn-intl
!
dial-peer cor list internal
  member internal
!
dial-peer cor list pstn
  member pstn
!
dial-peer cor list pstn-intl
  member pstn-intl
!
dial-peer cor list phone1
  member internal
  member pstn
  member pstn-intl
!
dial-peer cor list phone2
  member internal
  member pstn
!
dial-peer cor list phone3
  member internal
!
dial-peer voice 1 pots
  description Internal dialing from the PSTN
  incoming called-number .
  direct-inward-dial
  port 0/1/0:23
!
dial-peer voice 9 pots
  description PSTN dial 9 first
  corlist outgoing pstn
  destination-pattern 9T
  port 0/1/0:23
!
dial-peer voice 9011 pots
  description International dial 9 first
  corlist outgoing pstn-intl
  destination-pattern 9011T
  port 0/1/0:23
  prefix 011
!
dial-peer voice 2000 pots
  description Internal 4 digit dialing to HQ
```

```

corlist outgoing internal
translation-profile outgoing to-HQ
destination-pattern 2...
port 0/1/0:23
!
voice translation-rule 1
rule 1 /^2/ /15115552/
!
voice translation-profile to-HQ
translate called 1
!

```

The first part of the SRST configuration includes the **dialplan-pattern** command configured under **call-manager-fallback** configuration mode, which maps the internal four-digit DNs to the E.164 PSTN number.

COR lists are configured for internal destinations called internal, for international PSTN destinations named `pstn-intl`, and for all other PSTN destinations labeled `pstn`. These COR lists are applied to dial peers as outgoing COR lists. Their function is equivalent to partitions in CUCM.

Additional COR lists are configured, one per phone. These are applied as incoming COR lists to phone DNs using the **cor incoming** command in **call-manager-fallback** configuration mode. The configuration shown in Example 6-16 applies the incoming COR list `phone1`, which is equivalent to CSSs in CUCM, to phone 1, which registers with the SRST gateway with a DN of 3001, incoming COR list `phone2` to the phone with DN 3002, and incoming COR list `phone3` to the phone with DN 3003.

Outgoing COR lists are applied to the dial peers that are used as outgoing dial peers: dial peer 9011 for international PSTN calls, dial peer 9 for PSTN calls, and dial peer 2000 for calls to headquarters.

Note For simplicity, Example 6-17 does not show all the outbound dial peers, as shown previously in Example 6-9. Using the destination pattern `9T`, as shown in dial peer 9, is typically avoided when possible for local or national calls to avoid the interdigit timeout associated with the T wildcard.

Note After COR configuration begins on a gateway; if a DN is not assigned the incoming COR list, the DN has unrestricted dialing. In this scenario, “no key” means that you have the “master key”.

Dial peer 1 is configured for inbound dialing from the PSTN with the **incoming called-number** command to identify all destination phone numbers. Direct inward dialing is

enabled, which turns off the second dial tone at ISDN port 0/1/0:23 for external calls dialing in.

The called E.164 numbers (521-555-3xxx) are mapped to four-digit extensions because of the **dialplan-pattern** command that is configured in call-manager-fallback configuration mode. As a result, incoming PSTN calls are sent to the four-digit extensions.

Outgoing calls to phones located at the main site at extensions 2xxx match a destination pattern in dial peer 2000. Dial peer 2000 sends calls to port 0/1/0:23 after performing digit manipulation using the to-HQ voice translation profile. This profile translates the 4-digit called number to an 11-digit E.164 PSTN number. The result is that during SRST fallback, users can still dial 4-digit extensions to reach phones in headquarters.

Summary

The following key points were discussed in this chapter:

- A simplified SRST dial plan has to be implemented on the remote-site gateways to ensure connectivity for remote sites in SRST mode.
- SRST reference is assigned via device pool membership.
- Basic Cisco IOS gateway SRST configuration requires only six configuration steps.
- Cisco IOS gateway MGCP fallback configuration requires only two configuration steps.
- CFUR forwards calls made to unregistered DNs to the defined destination.
- ISDN overlap dialing has to be enabled in countries with open numbering plans.

References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco Unified Communications Manager Administration Guide Release 8.0(1)*, February 2010.

www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_1/ccmcfg/bccm-801-cm.html.

Cisco Systems, Inc. *Number Translation Using Voice Translation Profiles*, February 2006.

www.cisco.com/en/US/tech/tk652/tk90/technologies_configuration_example09186a00803f818a.shtml.

Cisco Systems, Inc. *Voice Translation Rules*, November 2006.

www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a0080325e8e.shtml.

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in the Answers Appendix.

1. When implementing MGCP Fallback and SRST, what configuration is not performed at CUCM?
 - a. Adding SRST references
 - b. Enabling MGCP fallback at the MGCP gateway configuration page
 - c. Configuring CFUR to reach remote-site phones during SRST mode
 - d. Applying SRST references to phones
2. The SRST reference can be applied only per phone at the phone configuration page.
 - a. True
 - b. False
3. Which command is used for SRST configuration at the Cisco IOS router?
 - a. `telephony-server`
 - b. `ccm-manager fallback`
 - c. `service alternate default`
 - d. `call-manager-fallback`
4. Which command is not used for MGCP fallback configuration?
 - a. `ccm-manager fallback-mgcp`
 - b. `application`
 - c. `global`
 - d. `telephony-server`
 - e. `service alternate default`
5. Where do you configure the CFUR-Max-Hop-Counter?
 - a. Service parameter
 - b. Enterprise parameter
 - c. SRST gateway configuration
 - d. Phone configuration
6. How can calling privileges be implemented for individual SRST phones?
 - a. You can do this only when using CUCM Express in SRST mode.
 - b. By preconfiguring the phones that need calling privileges assigned.

- c. By configuring an ephone-dn template.
 - d. By configuring COR lists for directory numbers.
7. What digits will be sent to the PSTN through port 0/1/0:23 in the following SRST dial peer if 9011443335343 is dialed?
- dial-peer voice 9011 pots
description International dial 9 first
corlist outgoing pstn-intl
destination-pattern 9011T
port 0/1/0:23
prefix 011
- a. 9011443335343
 - b. 011443335343
 - c. 443335343
 - d. 3335343
 - e. No digits will be sent to the PSTN.
8. How can remote-site IP Phones be configured to dial four digits to get to headquarters phones in the event of a WAN link failure?
- a. Configure failover dialing in CUCM.
 - b. Configure a translation rule in CUCM for four-digit dialing.
 - c. Configure a voice translation rule on the remote-site router to translate four-digit dialing into the full E.164 number to route over IP.
 - d. Configure a voice translation rule on the remote-site router to translate four-digit dialing into the full E.164 number to route through the PSTN.
10. What is the effect of omitting the **max-ephone** command in call-manager-fallback configuration mode?
- a. An unlimited number of remote IP Phones will register to the SRST router in fallback mode.
 - b. A limited number of remote IP Phones based on router hardware model will register to the SRST router in fallback mode.
 - c. A limited number of remote IP Phones based on the IOS license will register to the SRST router in fallback mode.
 - d. No remote IP Phones will register to the SRST router in fallback mode.

Chapter 7

Implementing Cisco Unified Communications Manager Express (CUCME) in SRST Mode

Cisco Unified Communications Manager Express (CUCME) has many features, benefits, and limitations compared to CUCM. This chapter explains those features and the process of registering IP Phones with CUCME for Survivable Remote Site Telephony (SRST). This chapter also discusses the basic telephony-service commands for configuring **ephones** and **ephone-dns**. This includes some basic hunting, a desirable feature of CUCME in SRST mode over (basic) Cisco Unified SRST.

Upon completing this chapter, you will be able to configure CUCME to provide telephony service, basic hunting, and Music On Hold (MOH) to Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) phones if the connection to the centralized call agent is lost. You will be able to meet these objectives:

- Describe CUCME and the modes in which it can be used
- Describe CUCME versions, their protocol support and features, and the required Cisco IOS Software release
- Describe general CUCME configuration parameters and their functions
- Configure CUCME to support SRST fallback
- Phone provisioning options
- Advantages of CUCME SRST
- Phone registration process
- Configuring CUCME for SRST

CUCME Overview

Cisco Unified Communications Manager Express (CUCME) is an IOS-based IP telephony solution that is an alternative to CUCM for branch offices or small businesses. CUCME is the call-control device using SCCP or SIP to control a few Cisco IP Phones. CUCME

can work independently of CUCM or integrated with SRST, as described in this chapter. CUCME is based on the IOS feature set and does not require any unique router hardware, but it can leverage the modular hardware of the Cisco IOS gateway.

Figure 7-1 shows a deployment of a CUCME router with several phones and devices connected to it. The CUCME router is connected to the public switched telephone network (PSTN) and WAN.

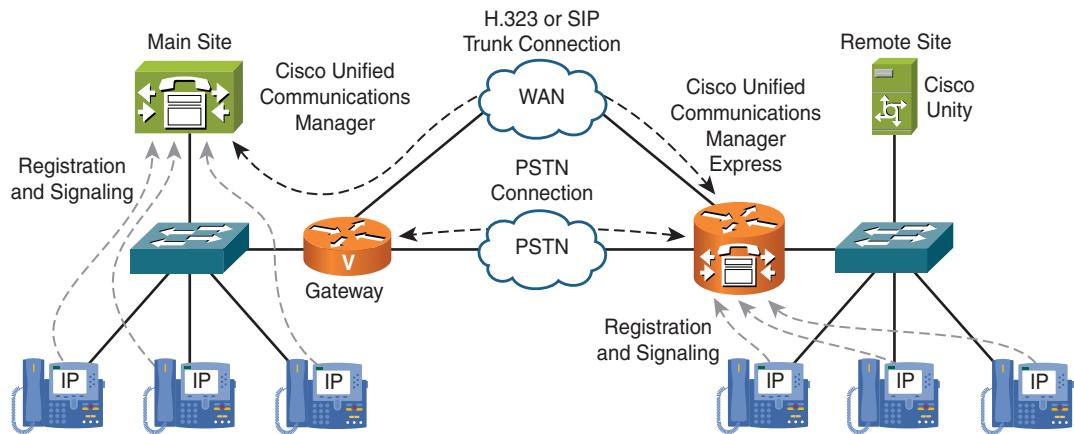


Figure 7-1 Standalone CUCME

CUCME is a feature-rich, entry-level IP telephony solution that is integrated directly into Cisco IOS Software. CUCME allows small-business customers and autonomous small-enterprise branch offices to deploy voice, data, and IP telephony on a single platform for small offices, which streamlines operations and reduces network costs.

CUCME is ideal for customers who have data connectivity requirements and need a telephony solution in the same office on the same device. Whether offered through a managed-services offering of a service provider or purchased directly by a corporation, CUCME provides many of the core telephony features that are required in a small office. CUCME also provides many advanced features that are not available with traditional telephony solutions. Being able to deliver IP telephony and data routing using a single, converged solution allows customers to optimize their operations and maintenance costs, resulting in a cost-effective solution that meets office needs.

A CUCME system is extremely flexible because it is modular. It comprises a router that serves as a PSTN gateway and supports one or more VLANs, which connect IP Phones, phone devices, and PCs to the router.

CUCME in SRST Mode

Figure 7-2 shows a topology that can use SRST fallback support using CUCME. SRST is an IOS feature that enables routers to provide call-handling support for Cisco IP Phones if they lose their connection to a remote primary, secondary, or tertiary CUCM installation, which can occur if the WAN connection to the main site is down.

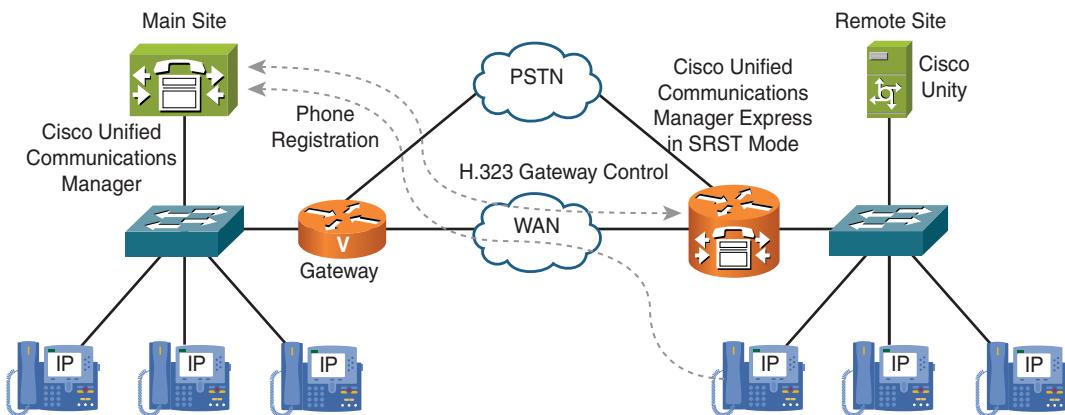


Figure 7-2 CUCME in SRST Mode

When CUCME provides Cisco Unified SRST functionality, provisioning of phones is automatic. Most CUCME features are available to the phones during periods of fallback, including hunt groups, Call Park, and access to Cisco Unity voice messaging services using SCCP. The benefit is that CUCM users gain access to more features during fallback without any additional licensing costs.

Standalone CUCME Versus CUCM and CUCME in SRST Mode

When choosing between standalone CUCME and CUCM or CUCME in SRST mode, consider the differences in features, shown in Table 7-1.

You need to take into account other considerations when choosing the correct system. The server-based CUCM telephony solution also provides scalability for large enterprises. CUCM servers can be grouped in a cluster to provide fault-tolerant telephony for up to 30,000 IP Phones per cluster. Multiple clusters can be configured in an enterprise as previously discussed for larger enterprises. Customers can make use of extensive server-based application programming interfaces (API) with CUCM.

Note Although Cisco IOS gateways can work with CUCM in many configuration options, the IOS gateway never actually replicates the database from the CUCM servers.

Table 7-1 *Standalone CUCME* Versus CUCM and CUCME in SRST Mode*

Feature	Unified CM with Unified CME for SRST	Standalone CUCME
Normal Operation (Unified CM)	SRST Mode (Unified CME for SRST)	
Enterprise size	Medium to large	Multiple medium to small sites. Small.
Clustering	Yes	No.
Centralized call processing	Yes	No. Only within local sites.
Features	All features supported by CUCM	All features supported by Cisco Unified Communications Manager Express.
Feature limitations	None	Features are available only within a local site. Features are available only within a local site.

Both CUCME and CUCM offer voice security through Transport Layer Security (TLS) and IP Security (IPsec). CUCM offers additional voice security with Secure Real-Time Transport Protocol (SRTP).

CUCM is a centralized architecture but also allows for distributed call processing. CUCME is a distributed architecture but also allows centralized call processing for small sites.

CUCM offers a greater choice of voice codecs and video product selection.

CUCME does not support all CUCM features. The CUCM call-processing solution offers feature-rich telephony services to medium or large enterprises. CUCME can serve small deployments on its own or is used as a backup for a centralized call-processing CUCM deployment (CUCME in SRST mode).

The CUCME solution is based on the Cisco access router and Cisco IOS Software. It is simple to deploy and manage, especially for customers who already use Cisco IOS Software products. This allows customers to take advantage of the benefits of IP communication without the higher costs and complexity of deploying a server-based solution.

Although multiple CUCME systems can be interconnected using trunks, the features that are supported across trunks are limited.

Because of the centralized architecture of CUCM, remote-site survivability is extremely important. As previously discussed, Cisco Unified SRST can provide survivability; however, it is limited in terms of telephony features.

To provide a richer feature that is set to IP Phones that are in fallback mode, you can use CUCME in SRST mode. This deployment combines the advantages of CUCM, such as

the centralized configuration and the availability of features to all phones, with the better feature support that CUCME provides versus the standard Cisco Unified SRST in case the site is disconnected from the centralized CUCM cluster.

The CUCM call-processing solution offers feature-rich telephony services to medium or large enterprises. CUCME can serve small deployments on its own or is used as a backup for a centralized call-processing CUCM deployment (CUCME in SRST mode).

The CUCME solution is based on the Cisco access router and Cisco IOS Software. CUCME is simple to deploy and manage, especially for customers who already use Cisco IOS Software products. This simplicity allows customers to take advantage of the benefits of IP communication without the higher costs and complexity of deploying a server-based solution. The number of supported phones is relatively low, however, and heavily depends on the router platform. The number of supported phones ranges from 15 phones on the Cisco 1861 router model to as many as 450 on the Cisco 3945E Integrated Services Router model. (See www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps4625/data_sheet_c78-567246.html for detailed capacity information per router platform.)

Although multiple CUCME systems can be interconnected using trunks, the features supported across trunks are limited.

CUCME cannot be used if certain features are required to operate across multiple sites. These features include CUCM Extension Mobility and Device Mobility, locations-based call admission control (CAC) (including Resource Reservation Protocol [RSVP]-enabled locations), call hunting, call pickup, Presence, and many others. In this case, or simply because of the size of the deployment, CUCM is the better choice.

CUCM is commonly used as the platform for centralized call processing for some sites. In such an environment, IP Phones register to a CUCM across the IP WAN. In this case, CUCME in SRST mode is a better choice than relying on the standard Cisco Unified SRST functionality, because CUCME in SRST mode offers more features than the standard Cisco Unified SRST. In summary, use CUCM when CUCME does not scale to the number of endpoints or does not provide all the required features. If you use CUCM, and the standard Cisco Unified SRST features do not meet the requirements for backup scenarios, use CUCME in SRST mode.

CUCME Features

CUCME delivers capabilities that were previously available only to larger enterprises to the small- or medium-sized business.

CUCME integrates with voice-mail systems such as Cisco Unity, Cisco Unity Connection, Cisco Unity Express, and third-party voice-mail systems, as shown in Figure 7-3.

CUCME can also use the voice gateway features of the ISR router for connectivity to analog phones and faxes, connection to an IP WAN or the Internet, and digital and analog connectivity to the PSTN.

Administration of CUCME can be done using a GUI or command-line interface (CLI).

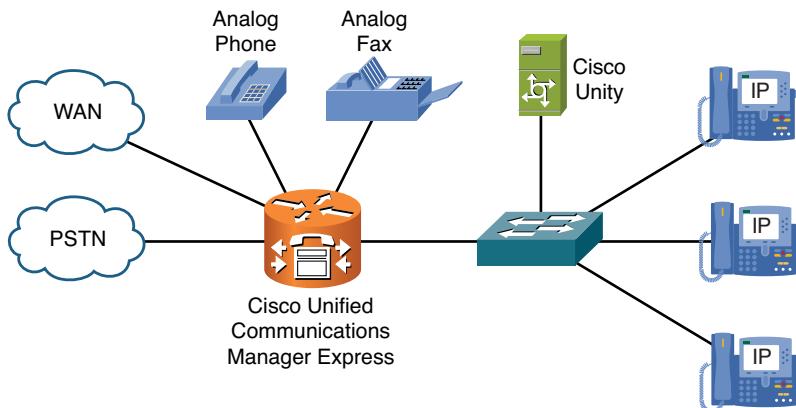


Figure 7-3 CUCME Features

CUCME Features

CUCME also includes features that are similar to legacy low-end private branch exchange (PBX) and key system features, creating a cost-effective, highly reliable, feature-rich IP communications solution for the small office.

The following new features are introduced with CUCME version 8.0:

- **Five additional Music On Hold (MOH) sources:** SCCP phones can be configured to use one of five additional MOH source files that are configured by MOH groups.
- **Support for E.164 numbers and + prefixes:** IP Phones can use E.164 format with a + prefix for their directory numbers (DN).
- **Enhancement of the dialplan pattern command:** You can use the `dialplan pattern` command to allow internal devices to call each other by an internally used shorter number that is derived from a longer DN of the phone (typically in E.164 format with + prefix).
- **Enhancement of voice translation profiles:** When a call is sent to an IP Phone, an additional number (that is, a callback number) is sent to the phone. The phone shows the calling-party number on its display, but uses the callback number for callbacks from call lists.

Other CUCME Features

CUCME also includes the following features that are similar to legacy low-end PBX and key system features:

- Call Transfer, Call Transfer Blocking, paging, intercom, call coverage
- Call Park, Park Call Recall, dedicated park slot per extension, MOH, multicast MOH
- Hunt groups, basic automatic call distribution (B-ACD) and reporting

- Ad-hoc conferencing, retain conference when initiator drops
- Night bell, night service call forwarding
- Headset auto-answer, distinctive ring patterns for internal and external
- Support for Cisco Unified Video Advantage
- Support for Cisco IP Communicator

General Configuration of CUCME

At a minimum, the following commands must be configured to deploy a CUCME system:

- **telephony-service:** This command enters telephony-service configuration mode, where global settings of CUCME are configured.
- **max-ephones:** CUCME must be configured with the maximum number of ephones using the **max-ephones** command in telephony-service configuration mode.
- **max-dn:** CUCME must be configured with the maximum number of extension numbers (ephone-dns) using the **max-dn** command in telephony-service configuration mode.

Note The default value of **max-ephones** and **max-dn** is 0. This default must be modified to allow the configuration of ephones and ephone-dns. The maximum number of supported ephones and ephone-dns is version-specific and platform-specific. The number displayed in Cisco IOS software help “?” command does not always reflect the actual limit.

- **ip source-address:** This command is entered in telephony-service configuration mode. It is used to define the IP address to which CUCME is bound.
- **create cnf-files:** This command is entered in telephony-service configuration mode. It is used to generate XML configuration files for phones.
- **ephone-dn:** This global configuration command is used to create a DN. After this command is entered, the router is in ephone-dn subconfiguration mode.
- **number:** This command defines a DN for an ephone-dn (extension), which can then be assigned to an IP Phone.
- **ephone:** This command is entered in global configuration mode. It is used to create a phone in CUCME.
- **mac-address:** This command is entered in ephone configuration mode. It specifies the device ID of an ephone. When a phone registers with CUCME, it must provide a device ID (which is based on the phone’s MAC address) that is configured in CUCME.
- **type:** This command is entered in ephone configuration mode. It specifies the phone type of this ephone.

- **button:** This command is entered in ephone configuration mode. It is used to assign one or more ephone-dns to an ephone.
- **dialplan-pattern:** This command is entered in telephony-service configuration mode. It is used to map E.164 PSTN numbers to internal extension numbers.

CUCME Basic Configuration

Example 7-1 shows a basic CUCME configuration.

Example 7-1 Cisco Unified CME Basic Configuration

```
telephony-service
  max-ephones 5
  max-dn 10
  ip source-address 10.1.250.102 port 2000
  create cnf-files
!
ephone-dn 6
  number 3001
ephone-dn 7
  number 3002
!
ephone 3
  mac-address 0012.0154.5D98
  type 7960
  button 1:6
ephone 4
  mac-address 0007.0E57.6F43
  type 7961
  button 1:7
!
dialplan-pattern 3 5215553... extension-length 4
!
```

Example 7-1 shows a CUCME configuration of two **ephones**—one with directory number 3001 and one with directory number 3002 with a normal ring, as specified by the `:`. In this simple example, only two Cisco IP Phones are configured to register to CME as an **ephone**. An **ephone** is an Ethernet phone, which is a Cisco IP Phone identified by its burned-in MAC address from manufacturing. The four-digit extensions are expanded to a ten-digit E.164 PSTN address (521-555-3xxx).

CUCME Configuration Providing Phone Loads

CUCME can be configured to provide specific phone loads to IP Phones for each type of phone.

CUCME needs to be configured so that IP Phone firmware files are available through the TFTP server located in router flash. The command `tftp-server flash:filename` allows the specified file that resides in flash memory to be downloaded via TFTP.

Example 7-2 shows a configuration with firmware files made available by the CME router.

Example 7-2 Cisco Unified CME Phone Load Configuration

```
tftp-server flash:apps45.9-0-2ES2.sbn
tftp-server flash:cnu45.9-0-2ES2.sbn
tftp-server flash:cmv45sccp.9-0-2ES2.sbn
tftp-server flash:dsp45.9-0-2ES2.sbn
tftp-server flash:jar45sccp.9-0-2ES2.sbn
tftp-server flash:SCCP45.9-0-2SR1S.loads
tftp-server flash:term45.default.loads
tftp-server flash:term65.default.loads
!
telephony-service
  load 7965 SCCP45.9-0-2SR1S
  load 7945 SCCP45.9-0-2SR1S
!
```

Example 7-2 shows the following Cisco IP Phone firmware files that are made available:

- Cisco Unified IP Phone 7945 with SCCP firmware version 9.0(2)SR1
- Cisco Unified IP Phone 7965 with SCCP firmware version 9.0(2)SR1

To associate a type of Cisco IP Phone with an IP Phone firmware file, use the `load model firmware-file` command in telephony-service configuration mode.

Tip You can see a list of IP Phone models supported by the CUCME router by entering the `load ?` command in telephony-service configuration mode.

Note Firmware filenames are case-sensitive.

CUCME Configuration for Music On Hold

Music On Hold (MOH) is an audio stream played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a CUCME system. This audio stream is intended to reassure callers that they are still connected to their calls. Example 7-3 shows the configuration of MOH with multicast on Cisco Unified CME.

Example 7-3 Cisco Unified CME MOH Configuration

```
telephony-service
  moh moh-file.au
    multicast moh 239.1.1.1 port 16384
!
```

Keep the following points in mind when configuring MOH:

- MOH is enabled by the **moh** command under telephony service.
- For multicast MOH, add the **multicast moh** command.
- CUCME supports only G.711 for MOH.
- Transcoders are required to allow G.729 to be used for MOH.

When the phone receiving MOH is part of a system that uses a G.729 codec, transcoding is required between G.711 and G.729. The G.711 MOH must be translated into G.729. Note that because of compression, MOH using G.729 is of significantly lower fidelity than MOH using G.711. The G.729 codec was designed to accommodate human voice, not more complex sounds from musical instruments.

If the MOH audio stream is also identified as a multicast source, the CUCME router additionally transmits the stream on the physical IP interfaces of the CUCME router that you specify during configuration. This gives external devices access to the MOH audio stream.

Certain IP Phones do not support IP multicast and therefore do not support multicast MOH. You can disable multicast MOH to individual phones that do not support multicast. Callers hear a repeating beep sound when they are placed on hold as an alternative to MOH.

In CUCME Release 4.1 and later releases, the MOH feature is supported when a call is put on hold from a SIP phone and when the user of a SIP phone is put on hold by a SIP, SCCP, or plain old telephone service (POTS) endpoint. The holder (the party who pressed the hold key) or the holdee (the party who is put on hold) can be on the same CUCME group or on a different CUCME group that is connected through a SIP trunk. MOH is also supported for call transfers and conferencing, with or without a transcoding device.

Configuring MOH for SIP phones is the same as configuring MOH for SCCP phones.

Additional MOH Sources

CUCME version 8 introduces the capability of configuring up to five MOH sources in addition to the default MOH source. This allows more than one MOH file to be played to different users put on hold at the same or different times. For example, a user calling into the branch office for customer support put on hold might benefit from a MOH file that has calming music whereas a different caller to the branch site enquiring about a new product put on hold might be best suited for a MOH file with promotional information.

These additional MOH sources can be used by SCCP phones that put calls on hold. Any other entities that put calls on hold (such as basic automatic call distribution [B-ACD] or SIP phones) will use the default MOH source. If live audio feed is used, it can be configured only as the default MOH source.

CUCME can be configured to cache files in RAM. This configuration reduces CPU utilization because flash reads are essentially eliminated after the audio files are loaded to RAM. However, caching audio files in RAM can drastically increase memory consumption. Memory requirements depend on the number and size of MOH files. (There is no limitation on the maximum size of an audio file.) Multiple MOH sources are supported by CUCME, CUCME in SRST mode, and Cisco Unified SRST.

Multiple MOH sources are supported on these platforms: Cisco Unified Communications 500 Series and Cisco 1800, 2800, 2900, 3800, and 3900 Series Integrated Services Routers.

The audio files have to be .au or .wav files in G.711 8-bit mono format, and their minimum size is 100 kb. If multiple flash devices are present in the router, the default flash drive should be used.

The configuration of multiple MOH sources is based on MOH groups. Endpoints that do not support MOH groups or that are not configured to use an MOH group will use the default MOH source.

Note The MOH source is selected based on the configuration of the holder (that is, the phone that puts the call on hold).

Example 7-4 shows an example of a router that is configured with a default MOH audio source and two additional MOH audio sources with multicast for different departments.

Example 7-4 Additional Music on Hold Sources Configuration Example

```
voice moh-group 1
  moh flash:moh1.au
  description MOH: customer services
  multicast moh 239.1.1.1 port 16384
  extension-range 1000 to 1099
  extension-range 1300 to 1399
```

```

!
voice moh-group 2
  moh flash:moh2.au
  description MOH: marketing
  multicast moh 239.1.1.2 port 16384
  extension-range 3000 to 3099
!
telephony-service
  moh-file-buffer 5000
  moh flash:default.wav
  multicast moh 239.1.1.3 port 16384

```

For each department, an MOH group is configured. Within each group, the location of the MOH audio file and the extensions that should use the group has to be configured. In addition, an optional description can be configured and multicast MOH can be enabled for each MOH group.

You configure RAM caching under call-manager-fallback (in the case of Cisco Unified SRST) or under telephony-service (in the case of CUCME). You use the **moh-file-buffer size-in-kb** command for this configuration, and it specifies the maximum size of the MOH RAM cache. The configured limit applies to each audio source file. You cannot enable or disable audio source caching on a per-file basis. The total amount that is used for audio source caching, therefore, depends on the number of configured MOH groups. If all five possible MOH groups and a default audio source are configured, the file buffer size that is allocated will be six times the specified amount. If a configured audio source file is larger than the configured moh-file-buffer, it will not be cached but will be read from flash instead.

Note You can use the **show flash** command to see the size of the MOH files.

Configuring CUCME in SRST Mode

An SRST reference in CUCM can be a standard SRST gateway or a CUCME router. Unlike standalone CUCME, when you are configuring CUCME in SRST mode, no phones have to be configured because they can be learned by Simple Network-Enabled Auto-Provision (SNAP).

However, CUCME in SRST mode allows any combination of the following configurations:

- **Manually configured ephones with associated ephone-dns:** In this case, the phone is fully configured; both the ephone and an ephone-dn, which is associated with the ephone, exist. This is used for phones that require additional configuration settings that cannot be learned from the phone via SNAP. These settings should be applied

only to this phone (or few phones). Therefore, an ephone template or ephone-dn template cannot be used (because these apply to all learned phones and/or DNs).

- **Manually configured ephones with no associated ephone-dn:** This configuration is useful if specific phone configuration parameters are required (which cannot be assigned from a template) but no specific DN is required. If an ephone is preconfigured in CUCME and is not associated with a DN, the DN is not learned via SNAP. Therefore, the phone won't have a DN unless through auto-assignment. This is equivalent to auto-registration in CUCM, where essentially a random DN is assigned to the phones.

Note This combination is not common because it combines the need for specific phone configuration parameters with the dynamic assignment of DNs.

- **Manually configured ephone-dns:** These ephone-dns are not associated with an ephone. The reason to configure the ephone-dn but not the ephone is that only individual ephone-dn configuration is required, but default settings or a single template can be used for the ephone. (This is added after the phone registers.)
- **No manual configuration:** In this case, the ephone-dn and the ephone are learned by SNAP. You can apply configuration settings that are not supported by SNAP to such newly added phones and DNs by configuring the appropriate templates.

Phone-Provisioning Options

Table 7-2 summarizes the phone-provisioning options and shows the relevant configuration parts.

As shown in Table 7-2, if an **ephone** and **ephone-dn** are configured in CUCME, a phone that registers with the configured MAC address gets the complete configuration of the phone and its DN applied as configured in CUCME. CUCME does not use SNAP to configure the phone.

If an **ephone** is configured but not associated with an **ephone-dn**, auto-assignment has to be enabled. Otherwise, the phone does not have a line and cannot place or receive calls. The **ephone-dn** configuration is determined based on the arguments of the **auto-assign** command. SNAP is not used to learn phone settings or DN configuration parameters.

If only **ephone-dns** are configured, the **ephone** configuration is learned by SNAP. The **ephone-dn** configuration that is configured in CUCME is used instead of the phone directory-number configuration provided by SNAP. **ephone** templates (if configured) are applied to the learned **ephone** configuration.

If neither an **ephone** with its MAC address nor a directory number exists for the registering phone, CUCME learns everything, including the **ephone** and **ephone-dn** configuration, by SNAP. **ephone** and **ephone-dn** templates are applied if they are configured.

Table 7-2 Phone-Provisioning Options

	Ephone and Ephone-dn	Ephone and Automatic Assignment	Ephone-dn and SRST Provisioning	Complete SRST Provisioning
Cisco IOS Configuration	ephone 1 mac-address... type 7960 button 1:6 ephone-dn 6 number 3001	ephone 1 mac-address... type 7960 (no button) telephony-service auto assign...	ephone-dn 6 number 3001 telephony-service srst mode auto-provision	telephony-service srst mode auto-provision
Resulting DN Configuration	Existing CUCME configuration	CUCME ephone-dn configuration referenced by automatic assignment	CUCME ephone-dn configuration of matching phone DN	Phone DN configuration plus CUCME SRST ephone-dn template (if used)
Resulting Phone Configuration	Existing CUCME configuration	Existing CUCME configuration	Cisco CUCME ephone template (if used)	Cisco CUCME ephone template (if used)

Advantages of CUCME SRST

Using CUCME in SRST mode has several advantages compared to using standard SRST:

- CUCME provides more telephony features than standard SRST.
- CUCME in SRST mode allows a mix of preconfigured phones and directory numbers for phones and DNs that require individual settings and phones that are not configured but are learned by SNAP.
- The additional features of CUCME can be leveraged by preconfiguring the required individual settings in CUCME to benefit SRST.
- ephone configuration is based on MAC addresses. ephone-dn configuration is based on the directory number.
- All phones and DNs that collectively require identical configuration not provided by SNAP do not have to be preconfigured, but the additional configuration can be applied using templates.
- These features allow flexible configuration of any CUCME feature in a scalable way because only those devices have to be preconfigured, which requires individual settings.

Phone Registration Process

When a phone loses connectivity to its CUCM, it registers to its configured SRST reference.

If that SRST reference is CUCME in SRST mode, the CUCME router first searches for an existing preconfigured **ephone** with the MAC address of the registering phone. If an **ephone** is found, the stored **ephone** configuration is used. No phone configuration settings provided by SNAP are applied, and no **ephone** template is applied. If the **ephone** is configured with one or more **ephone-dns**, the stored configuration is used for the phone's **ephone-dn** or **ephone-dns**. Neither information provided by SNAP nor the **ephone** template configured under **telephony-service** is applied. If the configured **ephone** is not configured with an **ephone-dn**, auto-assignment has to be enabled for the phone to be able to be associated with an **ephone-dn**. SNAP is not an option in this case.

If no **ephone** is found for the MAC address of the registering phone, CUCME adds the **ephone** (and applies the **ephone** template if it is configured) using SNAP. If the directory number exists, it is bound to the added phone; otherwise, the directory number is learned using SNAP. If it is configured, the **ephone-dn** template is applied.

Configuring CUCME for SRST

The configuration of CUCME in SRST mode is performed in **telephony-service** configuration mode, as shown in Example 7-5. As soon as the command **telephony-service** is active, the command **call-manager-fallback** is not accepted by the CLI, and vice versa.

Example 7-5 Configuring CUCME for SRST

```
CMERouter# configure terminal
CMERouter(config)# telephony-service
CMERouter(config-telephony)# srst mode auto-provision {all | dn | none}
CMERouter(config-telephony)# srst dn line-mode {dual | single}
```

To enable SRST mode for CUCME, use the **srst mode auto-provision** command in **telephony-service** configuration mode:

- The keyword **all** includes information for learned ephones and ephone-dns in the running configuration.
- The keyword **dn** includes information for learned ephone-dns in the running configuration.
- The keyword **none** does not include information for learned ephones or ephone-dns in the running configuration. Use this keyword when CUCME is providing SRST fallback services for CUCM.

Note If the administrator saves the running configuration after learning ephones and ephone-dns, the fallback IP Phones are treated as locally configured IP Phones on the CUCME SRST router. This could adversely impact the fallback behavior of those IP Phones.

To specify the line mode for the **ephone-dns** that are automatically created in SRST mode on a CUCME router, use the **srst dn line-mode** command in telephony-service configuration mode:

- The keyword **dual** specifies dual-line ephone-dns.
- The keyword **single** specifies single-line ephone-dns (this is the default).

Note If single-line ephone-dns is used with multiple-line features such as call waiting, call transfer, and conferencing, a phone must have more than one single-line directory number.

Note To specify an **ephone-dn** template to be used in SRST mode on a CUCME router, use the **srst dn template** command in telephony-service configuration mode, as shown in Example 7-6.

Example 7-6 Configuring CUCME for SRST, Continued

```
CMERouter# configure terminal
CMERouter(config)# telephony-service
CMERouter(config-telephony)# srst dn template template-tag
CMERouter(config-telephony)# srst ephone template template-tag
CMERouter(config-telephony)# srst ephone description string
```

To specify an **ephone-dn** template to be used in SRST mode on a CUCME router, use the **srst dn template** command in **telephony-service** configuration mode according to the following points:

- The parameter **template-tag** is the identifying number of an existing **ephone-dn** template. The range is from 1 to 15.
- To specify an **ephone-template** to be used in SRST mode on a CUCME router, use the **srst ephone template** command in **telephony-service** configuration mode. The parameter **template-tag** is the identifying number of an existing **ephone-template**. The range is from 1 to 20.
- To specify a description to be associated with an ephone in SRST mode on a CUCME router, use the **srst ephone description** command in **telephony-service** configuration mode.

The maximum length of the parameter **string** is 100 characters.

CUCME for SRST Mode Configuration

Figure 7-4 shows a topology example of Cisco Unified CME in SRST mode. Example 7-7 shows the SRST Mode configuration. Ten IP Phones are configured, with a current configured maximum of 30 directory numbers among the ten IP Phones.

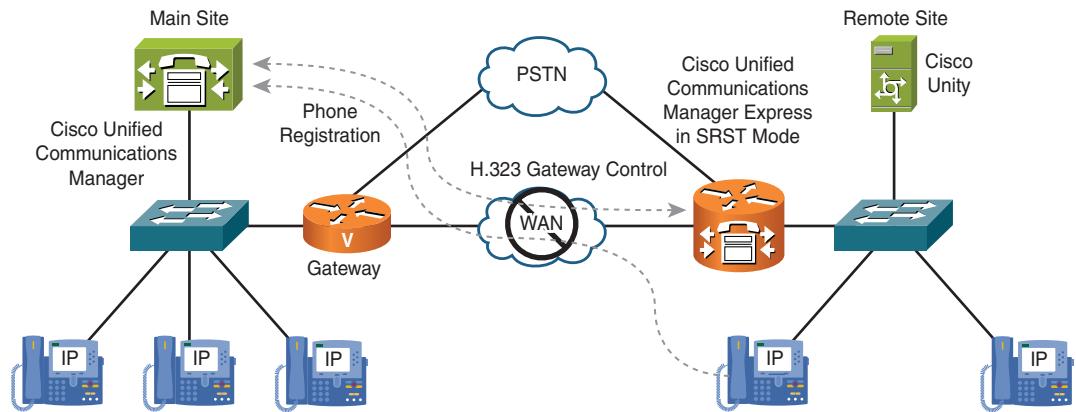


Figure 7-4 CUCME Topology

Example 7-7 CUCME for SRST Mode Configuration

```

CMERouter# configure terminal
CMERouter(config)# telephony-service
CMERouter(config-telephony)# srst mode auto-provision none
CMERouter(config-telephony)# srst dn line-mode dual
CMERouter(config-telephony)# srst ephone template 1
CMERouter(config-telephony)# srst dn template 3
CMERouter(config-telephony)# srst ephone description
CMERouter(config-telephony)# max-ephone 10
CMERouter(config-telephony)# max-dn 30
CMERouter(config-telephony)# ip source-address 10.1.250.102 port 2000
CMERouter(config-telephony)# exit
CMERouter(config)# ephone-template 1
CMERouter(config-ephone-template)# keep-conference local-only
CMERouter(config)# ephone-dn-template 3
CMERouter(config-ephone-template)# hold-alert 25 idle

```

In this example, CUCME uses ephone-template 1 for newly added phones. This template configures conferences to drop if no internal members are left in the conference.

ephone-dns, which are learned using SNAP, are configured to alert the user if a call is on hold for 25 seconds and the phone is idle.

The description of learned phones should be CUCME SRST, and the **ephone-dns** should be dual-mode lines.

Summary

The following key points were discussed in this chapter:

- CUCME cannot be a member of a CUCM cluster.
- CUCME supports Extension Mobility, phone and media security, Busy Lamp Field (BLF), and video.
- Basic configuration of CUCME includes telephony-service configuration, ephone configuration, and ephone-dn configuration.
- The **srst mode** command in telephony-service confirmation mode is required to allow CUCME to learn ephones and ephone-dns via SNAP.

Reference

For additional information, refer to this resource:

Cisco Systems, Inc. *Cisco Unified Communications Manager Express System Administrator Guide*, November 2007 (with updates 2010).
www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html.

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in Appendix A, "Answers Appendix."

1. Which two statements about CUCME are true?
 - a. Cisco IP Phones register with CUCME in standalone mode when CUCME is part of the Cisco Unified CM Group specified in the phone's device pool.
 - b. During SRST fallback, IP Phones register with CUCME in SRST mode when CUCME is configured as the SRST reference for the IP Phone.
 - c. CUCME in SRST mode provides more features than standard SRST to Cisco IP Phones.
 - d. The same platform can serve more phones when running CUCME in SRST mode versus running standard SRST.
 - e. Standalone CUCME routers can be clustered for redundancy.

2. Which two features were added in CUCME version 8.0 that were not available in CME with all previous versions?
 - a. Extension Mobility
 - b. Media Security
 - c. Presence with BLF status
 - d. E.164 support
 - e. Five additional MOH sources
3. Which of the following three commands are not configured in telephony-service configuration mode?
 - a. `create cnf-files`
 - b. `ephone`
 - c. `ephone-dn`
 - d. `max-ephones`
 - e. `max-dn`
 - f. `ip source-address`
 - g. `number`
4. Which statement about CUCME in SRST mode is not true?
 - a. If only the `ephone-dn` is preconfigured, only the `ephone` is learned by SNAP.
 - b. If `ephone` and `ephone-dn` are preconfigured, SNAP is not used.
 - c. If neither the `ephone` nor `ephone-dn` is preconfigured, `ephone` and `ephone-dn` are learned by SNAP.
 - d. If only the `ephone` is preconfigured, only the `ephone-dn` is learned by SNAP.
5. Which of the following statements is the most accurate about the relationship between IOS routers in a remote site and CUCM?
 - a. The CUCM database can be configured to replicate its content onto an IOS router in SRST mode.
 - b. The CUCM database can be configured to replicate its content onto an IOS router in SRST mode on version 8.0 and later.
 - c. The CUCM database can be configured to replicate its content onto an IOS router in SRST mode only with CME.
 - d. The CUCM database cannot be configured to replicate its content onto an IOS router in any mode.

6. Which of the following statements about IOS routers in a remote site is the most accurate?
 - a. **call-manager-fallback** and **telephony-service** should both be configured on the remote router for optimal performance.
 - b. **call-manager-fallback** and **telephony-service** should both be configured on the remote router with standalone CME.
 - c. **call-manager-fallback** and **telephony-service** should both be configured on the remote router to enable the maximum features to remote Cisco IP Phones in fallback mode.
 - d. **call-manager-fallback** and **telephony-service** can never be configured on a remote router at the same time.
7. Which protocol do you need to configure to copy the phone firmware files from the CME router to the Cisco IP Phones?
 - a. FTP
 - b. SFTP
 - c. TFTP
 - d. Secure TFTP
 - e. HTTP
8. What is the benefit of multicast MOH in a remote router?
 - a. Maximum MOH functionality
 - b. Reduced bandwidth utilization when two or more phones are receiving MOH
 - c. Compliance with Internet standards
 - d. Improved audio quality by using G.729

Chapter 8

Implementing Bandwidth Management

Upon completing this chapter, you will be able to implement techniques to reduce bandwidth requirements on IP WAN links in CUCM multisite deployments. You will be able to meet these objectives:

- Describe methods of minimizing bandwidth requirements for Cisco Unified Communications
- Configure CUCM to control the codec used for a call
- Implement local conference bridges to avoid accessing conference bridges over the IP WAN even if all participants are local
- Implement transcenders to allow low-bandwidth codecs to be used when low-bandwidth codecs are not supported by both endpoints
- Implement multicast MOH from branch router flash to avoid MOH streams over the IP WAN

When an IP WAN connects different sites in a Cisco Unified Communications network, bandwidth consumption at the IP WAN should be minimized. Techniques that can help conserve bandwidth on the IP WAN in a multisite deployment include reducing the required bandwidth of voice streams, keeping some voice streams such as local media resources away from the IP WAN, and employing special features such as multicast Music On Hold (MOH) from branch router flash or using transcenders.

This chapter describes all these techniques and features and their implementation.

Bandwidth Management Overview

Valuable IP WAN bandwidth can be conserved by various techniques, including reducing the required bandwidth of voice streams by using Real-Time Transport Protocol (RTP) header compression, a quality of service (QoS) link efficiency mechanism, low-bandwidth audio codecs, or any combination of these solutions.

Note The term Multipoint Control Unit (MCU) is often used in the VoIP industry to refer to a physical device dedicated to mixing multiple RTP audio streams in a conference call. In a Cisco Unified Communications implementation based on Cisco Unified Communications Manager (CUCM) and an Integrated Service Router (ISR), a hardware conference bridge in an IOS router or software conference bridge running in a CUCM server plays the role of an MCU.

Note Refer to the “Quality of Service” module of the *Implementing Cisco Voice Communications and QoS (CVOICE)* book for a more detailed discussion about QoS.

Other options for IP WAN bandwidth management are techniques that influence where voice streams are sent. If three phones, all located at a remote site, establish an ad hoc conference, there is a great difference in bandwidth usage if the conference bridge is located at the remote site local to the phones that are members of the conference. If the conference is located at the main site and has to be accessed over the IP WAN, WAN bandwidth is used inefficiently. In the case of the conference resources at the main site, all three remote IP Phones send their voice stream to the conference bridge over the IP WAN. The conference bridge across the WAN mixes the received audio and then streams it back to all conference members in three separate unicast streams. Although the call appears to be local to the remote site because all conference members are located at that site because of the remotely located conference bridge, the IP WAN is occupied by three calls.

Other bandwidth-management solutions include the use of transcoders or the implementation of special features such as multicast MOH from branch router flash.

Transcoders are devices that can transcode IP voice streams; that is, they change how the audio payload is encoded. For example, transcoding can take a G.711 audio stream and change it into a G.729 audio stream. Transcoders allow the use of low-bandwidth codecs over the IP WAN even if one of the endpoints requires a high-bandwidth codec such as G.711.

Multicast MOH from branch router flash allows a multicast MOH stream to be generated by a Cisco IOS router located at the remote site, instead of being sent over the IP WAN from a centralized MOH server.

CUCM Codec Configuration

To conserve IP WAN bandwidth, low-bandwidth codecs, such as G.729, should be used in the IP WAN. For calls within a LAN environment, high-bandwidth codecs, such as G.711 or G.722, should be used for optimal audio quality. When choosing the right codec for your configuration, it is important to remember that low-bandwidth codecs, such as G.729, are designed for human speech; they do not work well for other audio streams. For example, the audio quality of G.729 can sound poor when used for Music On Hold (MOH).

As stated previously, other methods exist for limiting the bandwidth required for MOH streams. If multicast MOH from branch router flash cannot be used, but MOH streams are not desired on the IP WAN, MOH can be disabled for remote-site phones.

Review of CUCM Codecs

The codec to be used for a call depends on CUCM region configuration. Each device is assigned with a region via the device pool configuration.

For each region, the administrator can configure the codec with the highest permitted bandwidth requirement within a region, to other specifically listed regions, and to all other unlisted regions as well.

When a call is placed between two devices, the codec is determined based on the regions of the two devices and on the devices' capabilities. The devices use the codec that is best supported by both devices and that does not exceed the bandwidth requirements of the codec permitted for the region or regions that are involved in the call. If the two devices cannot agree on a codec when a region configuration allows a G.729 codec but a device on the other end supports only G.711 or G.722, a transcoder is invoked if available. The loss type of a link can also be configured. On links that are configured to be lossy, codecs that are less sensitive to packet loss are preferred over codecs that result in higher quality degradation.

Note For more details about codec selection, refer to *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) Foundation Learning Guide*.

Figure 8-1 shows a sample scenario for codec configuration in CUCM in the locations of company headquarters (HQ) and a company branch site (BR).

In Figure 8-1, phones located at the main site (headquarters) are configured with region HQ_phones. An intercluster trunk that connects to another CUCM cluster and a Session Initiation Protocol (SIP) trunk connecting to an Internet Telephony Service Provider (ITSP) are in region HQ_trunks. The public switched telephone network (PSTN) gateway that is located at HQ is configured with region HQ_gw. At the remote site, phones are in region BR_phones, and the PSTN gateway is in region BR_gw.

CUCM regions are configured in the following way:

- **Within HQ_phones:** G.711 or G.722
- **Within HQ_gw:** G.711 or G.722
- **HQ_phones to HQ_gw:** G.711 or G.722
- **Within BR_phones:** G.711 or G.722
- **Within BR_gw:** G.711 or G.722
- **BR_phones to BR_gw:** G.711 or G.722
- **All others:** G.729

As a result of this configuration, all calls that use the IP WAN between the remote site and headquarters use G.729. Calls that are sent through the intercluster or SIP trunk use G.729 as well. Calls between phones within the main site, calls between phones within the remote site, calls from the main sites' phones to the main sites' PSTN gateway, and calls from remote-site phones to the remote-site PSTN gateway all use G.711 or G.722.

This scenario is configured in CUCM as illustrated in Figure 8-2, which shows the configuration of the HQ_phones and BR_phones regions. Both regions are configured in such a way that calls within the region and calls to the local gateway for regions HQ_gw and BR_gw are allowed to use G.711 or G.722, whereas calls to all other regions are rate limited to G.729.

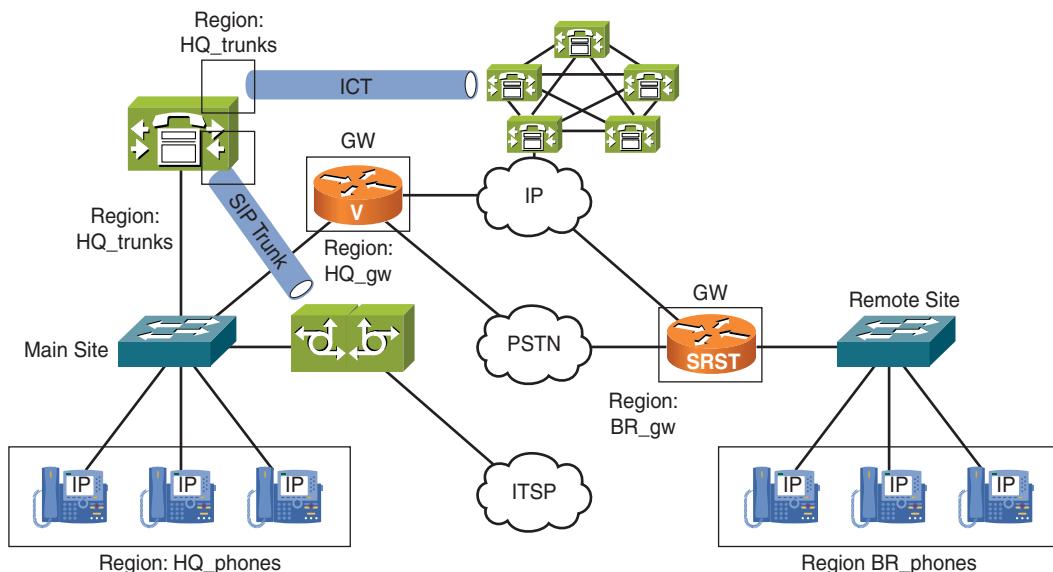


Figure 8-1 Codec Configuration Topology

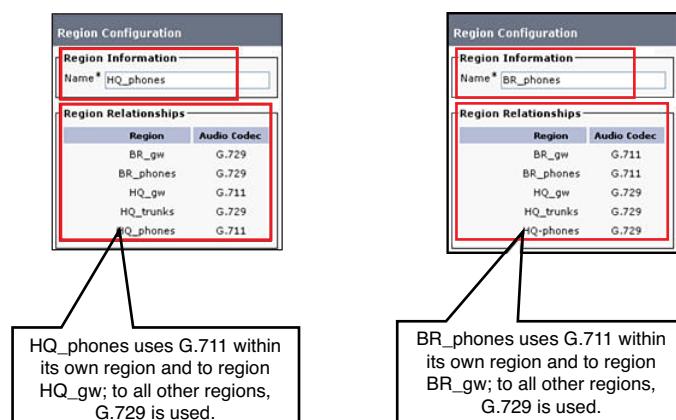


Figure 8-2 CUCM Regions to Configure Codecs

Note The example in Figure 8-2 is only a partial configuration. It does not show the configuration of the other regions.

Local Conference Bridge Implementation

When local conference bridges or media termination points (MTP) are deployed at each site, traffic does not have to cross the IP WAN if all endpoints are located at the same site. Local media resources, such as conference bridges and MTPs, can be implemented by providing appropriate hardware digital signal processors (DSP) in the routers located at the remote sites. All voice gateways require DSPs, but additional DSP resources are required for hardware conference calls and transcoding.

Note Search for the DSP Calculator tool on Cisco.com after logging in with your Cisco.com account for exact calculations of the DSP requirements.

Whether the extra cost of providing the DSP resources for hardware conference calls will pay off depends on the answers to these important questions:

- **Cost of adding DSPs:** Is it necessary to add DSPs to an existing router only, or does the entire platform have to be replaced?
- **Number of devices at the remote site and the likelihood of using applications or features that require access to the media resource that is considered locally deployed:** How many phones are located at the remote site? How often do the phones use features that require a media resource that is currently available only over the IP WAN? What is the maximum number of devices that require access to the media resource at the same time?
- **Available bandwidth and cost of additional bandwidth:** Is there enough bandwidth, or can additional bandwidth be provisioned to accommodate the requirements determined by the preceding factors? How does the cost of adding bandwidth compare to the cost of deploying local DSPs?

Figure 8-3 shows a main site with software and hardware conference resources. At the remote site, DSPs for hardware conference resources are added to the remote-site gateway. Doing this allows the remote-site phones to set up conferences by using local resources instead of always accessing the conference resources located at the main site. For conferencing remote-site members only, no traffic has to be sent across the IP WAN. Even if a few callers from the main site are in the same conference call as the others in the remote site, the WAN utilization is still minimized.

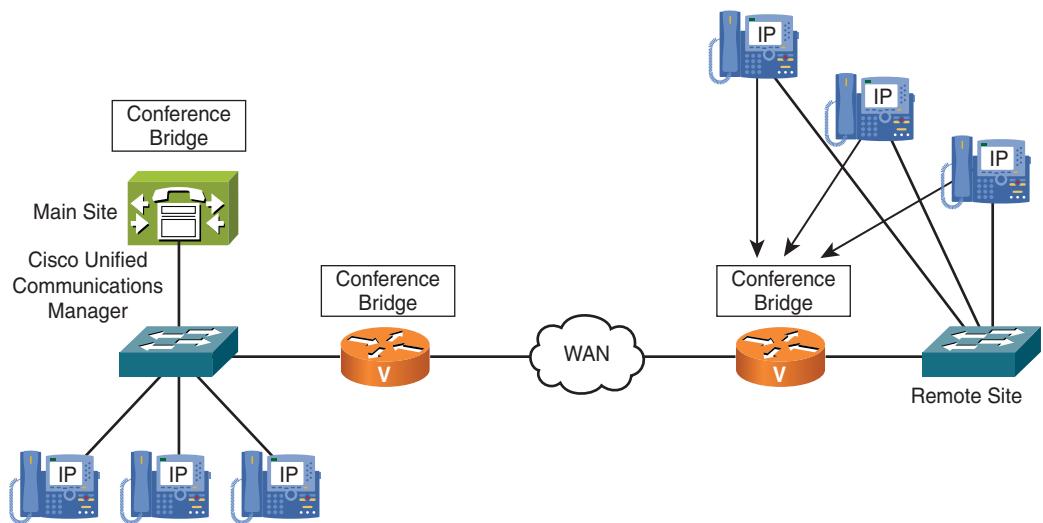


Figure 8-3 Implementing Local Conference Bridges at Two Sites

Note When an ad-hoc conference includes members of different sites, a separate voice stream for each remote member has to be sent across the IP WAN. However, if a MeetMe conference is set up, the users located at the branch site could first establish an ad hoc conference by using a media resource that is local to the branch users by using the DSP resources in their local gateway. Then, they could add a call to the remote MeetMe conference to their local ad hoc conference. In this case, only a single voice stream is sent across the IP WAN connecting the two conferences.

Figure 8-4 illustrates how media resource groups (MRG) and media resource group lists (MRGL) are used logically in CUCM to ensure that main site phones use the conference resources at the main site “HQ” and that remote site “BR” phones use the remote site conference resource when establishing a conference.

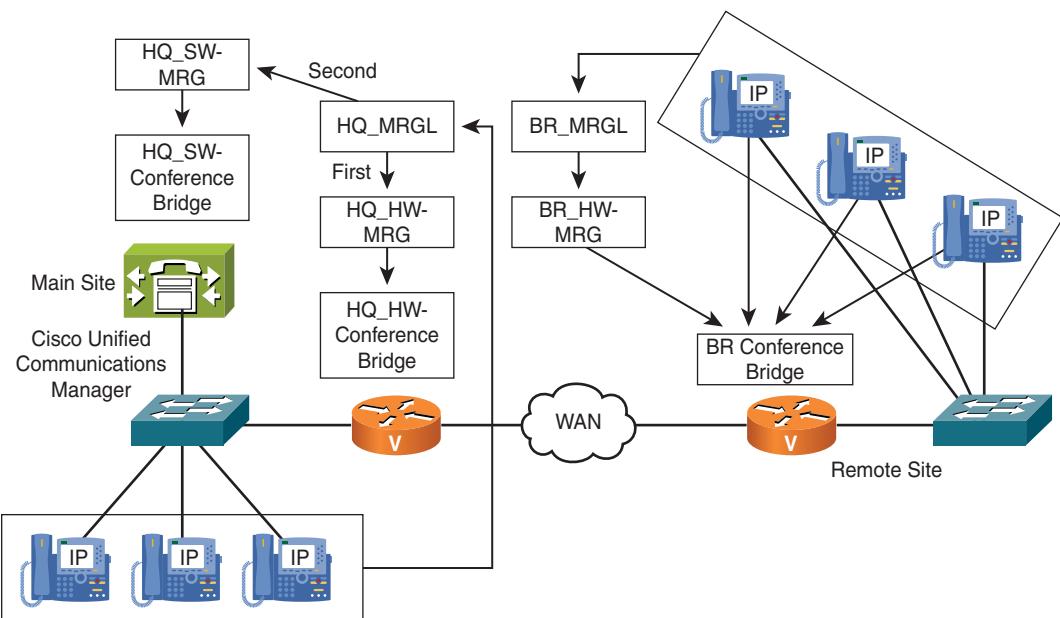


Figure 8-4 Implementing Local Conference Bridges at Two Sites, Continued

The following three MRGs are created:

- **HQ_HW-MRG:** Includes the hardware (HW) conference bridge provided by the voice gateway located at the main site.
- **HQ_SW-MRG:** Includes the software (SW) conference bridge provided by a CUCM server located at the main site.
- **BR_HW-MRG:** Includes the hardware (HW) conference bridge provided by the voice gateway located at the remote site.

HQ_HW-MRG is the first entry of the media resource group list called HQ_MRGL, and HQ_SW-MRG is the next entry. Main site phones are configured with HQ_MRGL. Because media resource groups are used in a prioritized way, main site phones that invoke a conference first use the available hardware conference resources. When all of them are in use, the software conference resources are accessed. Software conference resources run on a CUCM server and use the server CPU to mix the calls. Note that the remote site does not have a software conference bridge because it does not have CUCM servers.

At the remote site, all phones refer to the BR_MRGL, which includes only the BR_HW-MRG. This configuration allows branch phones to use their local conference bridge when they invoke conferences instead of accessing conference resources located across the IP WAN in the main site.

Transcoder Implementation

Transcoders are devices that transcode IP voice streams; that is, they change how the audio payload is encoded. For instance, G.711 IP audio streams are changed into G.729 IP audio streams in real time for a single phone call. Transcoders are deployed to allow the use of low-bandwidth codecs over the IP WAN even if one of the endpoints supports only high-bandwidth codecs, such as G.711. CUCM cannot do transcoding in software and relies on the DSP resources in ISRs.

The transcoder has to be deployed close to the device that supports only G.711 or G.722. That device sends a G.711 or G.722 stream to the transcoder, which encodes the audio to a low-bandwidth codec, such as G.729, all in real time. The G.729 voice stream is then sent from the transcoder to the other device, such as a phone located at a remote site, over the IP WAN. It is important to avoid transcoding more than one time in a single call flow whenever possible because the audio quality may be significantly reduced.

Note It is important for the media resource group list to be configured so that the device that is limited to the higher-bandwidth codec is the one that requests the transcoder media resource. For example, if only G.729 is permitted between two IP Phones, but one IP Phone supports only G.711, the phone using G.729 that cannot comply with the permitted codec is the one that requests a transcoder. Therefore, the media resource group list of this phone requires access to a transcoder, which should be physically located close to the requesting device. Regions have to be set up in such a way that the requesting phone is allowed to use G.711 to the transcoder. This call leg is also subject to region configuration.

As with local conference bridges, these factors must be taken into account before transcoders are deployed:

- **Cost of adding DSPs:** Is it necessary to add DSPs to an existing router only, or does the entire platform have to be replaced?
- **Number of phones at the remote site and the number of calls that are placed to G.711-only phones over the IP WAN:** How many phones are located at the remote site? How often do the phones need to communicate with phones located at the main site that support G.711 only and hence require a transcoder when G.729 must be used over the IP WAN? How many of these calls occur at the same time?

- Available bandwidth and the cost of additional bandwidth: Is there enough bandwidth (or can additional bandwidth be provisioned) to allow G.711 for calls to devices that do not support G.729? How does the cost of adding bandwidth compare to the cost of deploying local DSPs?

Implementing a Transcoder at the Main Site

Figure 8-5 illustrates implementing a transcoder at headquarters for remote-site phones calling in to G.711-only devices in the main site.

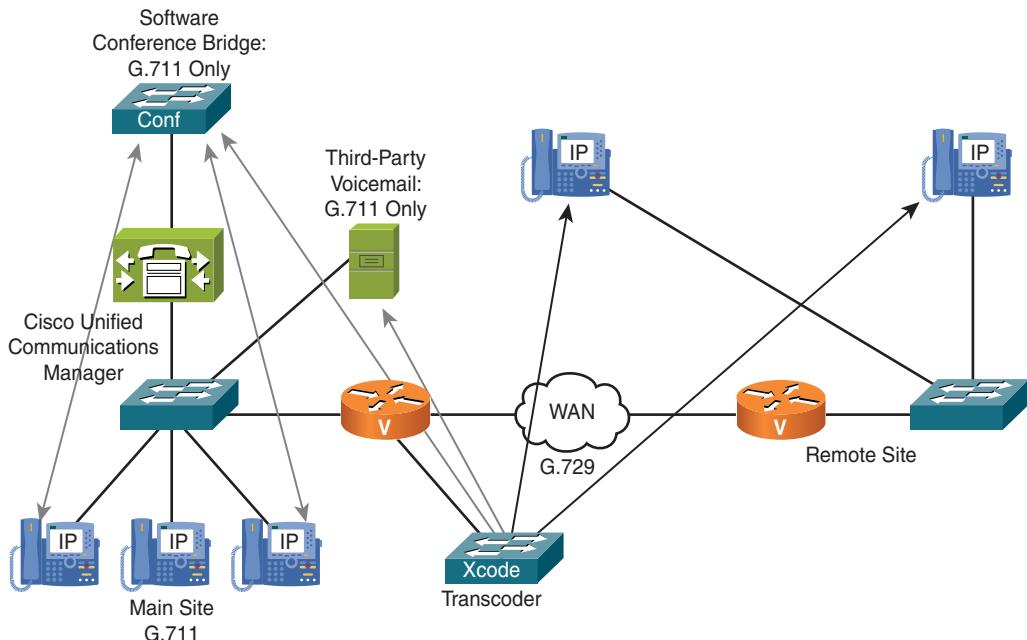


Figure 8-5 Implementing a Transcoder at Headquarters

At the main site, two devices support G.711 only. One is a CUCM software conference bridge, and the other one is a third-party voice-mail application.

Regions are configured in such a way that all voice traffic between the remote site and the main site has to use the G.729 codec.

Because CUCM-based software conference bridges support only G.711, remote site users configured with G.729 are not permitted to join the conference unless transcoding is configured.

If you add a transcoder resource in the main site gateway, which uses the gateway's DSP resources, the remote-site user can now send a G.729 voice stream, saving WAN

bandwidth. The voice stream is transcoded to G.711 and passed to the conference bridge by the transcoder, located in the main site.

The same approach can be used for calls to the G.711-only voice-mail system from the remote site. For example, Cisco Unity Express voice mail supports only G.711.

Figure 8-6 illustrates how the transcoding solution shown in Figure 8-5 is logically implemented in CUCM.

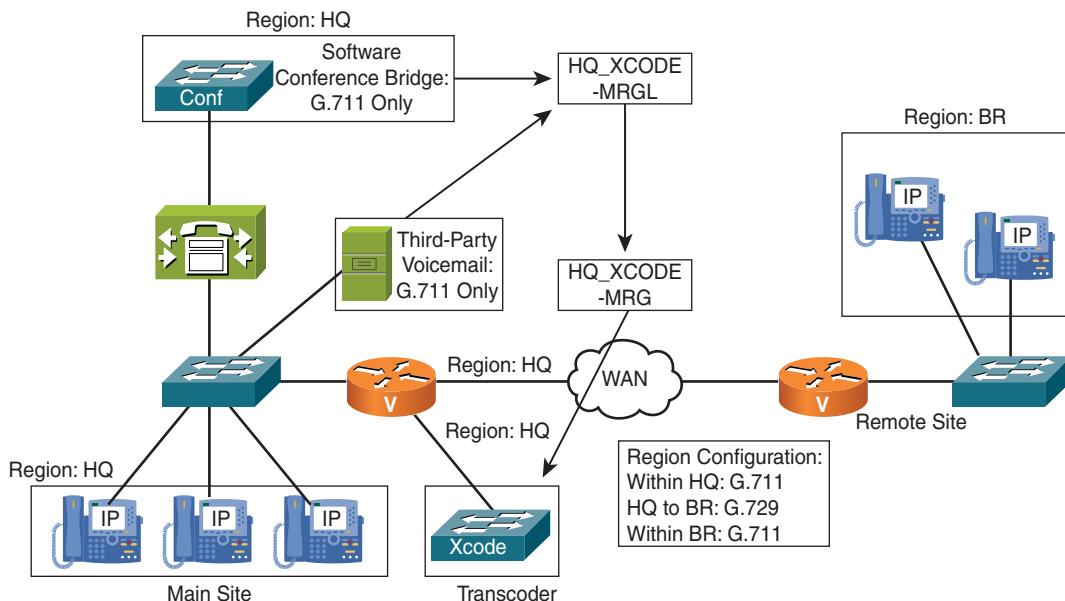


Figure 8-6 Implementing a Transcoder at the Main Site Site, Continued

All main site devices—such as phones, voice-mail system, software conference bridge, and transcoder—are in region HQ. Remote site phones are in region BR.

CUCM region configuration allows G.711 to be used within region HQ and region BR. Calls between regions HQ and BR are limited to G.729.

When a call is placed from a remote site phone to the voice-mail system, CUCM identifies the need for a transcoder based on the capabilities of the devices. In this example, only G.711 is used at the voice-mail system, and the maximum permitted codec over the WAN is G.729. If the device that supports only a codec with higher bandwidth requirements than permitted by the region configuration can access a transcoder, the call is set up and invokes the transcoder resource. The call would fail if a common codec cannot be negotiated during call setup.

Configuration Procedure for Implementing Transcoders

To implement transcoders, perform these steps:

- Step 1.** Add a transcoder resource in CUCM.
- Step 2.** Configure the transcoder resource in Cisco IOS Software.
- Step 3.** Configure media resource groups.
- Step 4.** Configure media resource group lists.
- Step 5.** Assign the media resource group lists to devices, and logically link these in CUCM.

Note Steps 1 and 2 are described in this chapter. Steps 3, 4, and 5—configuring MRG lists and assigning them to devices—are discussed in *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) Foundation Learning Guide*.

Step 1: Add a Transcoder Resource in CUCM

To add a transcoder resource in CUCM navigate to **Cisco Unified CM Administration**, choose, choose **Media Resources > Conference Bridge** and click **Add New**. The Transcoder Configuration window opens, as shown in Figure 8-7. Here, you choose the type of Cisco transcoder media resource. The options are as follows:

- Cisco IOS Enhanced Media Termination Point
- Cisco IOS Media Termination Point
- Cisco Media Termination Point Hardware
- Cisco Media Termination Point

Note The transcoder type depends on the hardware that is used. For example, NM-HDV requires that Cisco IOS Media Termination Point be selected, while newer DSP hardware, such as NM-HDV2, is configured as Cisco IOS Enhanced Media Termination Point.

Transcoder Configuration

Related Links: [Back To Find>List](#) [Go](#)

Transcoder Information

Transcoder: New

IOS Transcoder Info

Transcoder Type*	Cisco IOS Enhanced Media Termination Point	Select transcoder type.
Description	HQ-1 Transcoding Resource	Enter device name and description.
Device Name*	HQ-1_XCODER	Select device pool.
Device Pool*	Default	
Common Device Configuration	< None >	
Special Load Information	default	Leave blank to use

Figure 8-7 Adding a Transcoder Resource in CUCM

Choose the type of Cisco transcoder media resource, enter a device name and description for it, and choose a device pool. The device-pool settings determines the location and region settings and applies them to the transcoder.

The device name has to match the name listed at the Cisco IOS router that provides the media resource. The name is case-sensitive. If the transcoding resource is provided by Cisco IOS Enhanced Media Termination Point hardware, the name can be freely chosen. In all other cases, the name is MTP followed by the MAC address of the interface that is configured to be used for registering the media resource with CUCM.

Step 2: Configure the Transcoder Resource in Cisco IOS Software

Example 8-1 shows a portion of the output display from `show running-config` on the Cisco IOS gateway as it relates to providing hardware transcoding resources to CUCM.

Example 8-1 Configuring the Transcoder Resource in Cisco IOS Software

```
interface Loopback0
    ip address 10.6.9.1 255.255.255.255
!
voice-card 0
    dspfarm
    dsp services dspfarm
!
sccp local Loopback0
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 HQ-1_XCODER
!
dspfarm profile 1 transcode
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  maximum sessions 2
  associate application SCCP
no shutdown

```

In Example 8-1, a Cisco IOS Enhanced Media Termination Point type transcoder can be configured with the following options:

- **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 in interface configuration mode.
- **sccp local:** Skinny Client Control Protocol (SCCP) is required to select the local interface that is used to register the media resources with CUCM. Enter the **sccp local** command in global configuration mode. Although any gateway IP interface with IP connectivity to CUCM works for registration, a loopback interface is strongly recommended.
- **sccp ccm:** Use this command in global configuration mode to use SCCP to add a CUCM server to the list of available servers. You also can set various parameters, including IP address or Domain Name System (DNS) name, port number, and version number.

Note The version used in the **sccp ccm** command is not the CUCM version, but it relates to the DSP version in the ISR.

- **sccp:** To enable the SCCP protocol and its related applications (for example, transcoding and conferencing), use the **sccp** command in global configuration mode. If this command is removed, registration will fail with CUCM.
- **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.

Note The name specified in the Cisco IOS device must match the name in the CUCM exactly because the names are case-sensitive. In addition, it is critical for the DSP resources to register to CUCM with SCCP. If the registration fails, the hardware resources will be unavailable.

Note When a Cisco IOS Enhanced Media Termination Point is being configured, any name can be configured with the associate profile command. When a Cisco IOS conference bridge is being configured, the name cannot be configured. It is CFB(MAC), where (MAC) is the MAC address of the interface that was specified in the **sccp local** command.

- **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 the profile supports, use the **maximum sessions** command in DSP farm profile configuration mode.
- **no shutdown:** If you fail to issue the **no shutdown** command for the DSP farm profile, registration to CUCM does not occur.

To verify the Cisco IOS media resource configuration, use the following **show** commands:

- **show sccp:** Shows you whether the Cisco IOS router successfully established a TCP connection with the configured CUCM or Managers to exchange SCCP signaling messages.
- **show sccp ccm group [group-number]:** Shows you which media resources are registered with the CUCM(s) that are configured in the specified group.
- **show dspfarm profile [group-number]:** Shows you the status of the media resource of the specified profile at the Cisco IOS router.
- **show sccp connections:** Shows you the active RTP streams connected to the DSP resources for hardware conferencing, transcoding, or both.

Multicast MOH from Remote Site Router Flash Implementation

Multicast MOH from remote siterouter flash is a feature that allows multicast MOH streams to be generated by gateways located at remote sites instead of streaming MOH from the main site to a remote site over the IP WAN.

The feature is based on multicast MOH, so CUCM must be configured to use multicast MOH instead of unicast MOH. This configuration is recommended to reduce the load at the MOH server and to reduce bandwidth utilization. This feature multicasts only one stream that can be received by all devices, instead of streaming MOH individually for each endpoint in separate unicast RTP sessions.

Multicast MOH from remote site router flash is a feature of the Survivable Remote Site Telephony (SRST) configuration. Therefore, the remote site router that will generate the multicast MOH stream for the devices located at the remote site has to be configured for SRST. SRST does not have to be active (there is no need for a fallback scenario) because an SRST gateway that is configured for multicast MOH streams MOH continuously, regardless of its state of standby mode or SRST mode.

Because the MOH server located at the main site has to be configured for multicast MOH, multicast routing has to be enabled to allow the multicast stream to be routed from the CUCM server network to the phone network(s). If the MOH server is on the same network that the IP Phones are on, multicast routing is not required. However, such a scenario is not recommended for security reasons, because servers should be separated from endpoints with VLANs.

Each v8.x or later SRST or CUCME router can stream up to six different MOH files. You can configure each of them for multicast MOH or unicast MOH. Therefore, the maximum number of multicast MOH audio sources that can be used per remote site is limited to six. By providing different MOH files for each site, site-specific MOH files can be played for each site. Only G.711 codec is supported by SRST and CUCME.

When multicast MOH is used, IP Phones and CUCM are unaware that the IP Phones listen to locally generated MOH streams. From a signaling perspective, the IP Phone is instructed to listen to a certain multicast stream. The local SRST gateway must generate a multicast MOH stream by using identical settings, such as destination address (multicast group), destination port, and codec.

When using multicast MOH within the main site, you must enable multicast routing on your routers to allow the multicast stream to be routed from the CUCM server network to the phone network or networks. If the MOH server is on the same network that the IP Phones are on, multicast routing is not required, but such a scenario is not recommended for security reasons. (Servers should be separated from endpoints.)

Multicast MOH from Remote Site Router Flash Region Considerations

When multicast MOH is used, remote site IP Phones and CUCM are not aware that the IP Phones listen to locally generated MOH streams. From a signaling perspective, the IP Phone is instructed to listen to a certain multicast stream, and the local SRST gateway has to generate a multicast MOH stream by using identical settings, such as a destination address (multicast group), destination port, codec, and packetization period.

Multicast MOH in SRST gateways and CUCM support only the G.711 codec. Therefore, G.711 must also be configured between the CUCM MOH server and the remote site IP Phones. If CUCM signals a codec other than G.711 to the IP Phone, the IP Phone would not play the locally generated MOH stream because of a codec mismatch. (The signaling would be G.729, but the received RTP stream would be G.711.) To ensure that CUCM sends signaling messages to the phone and instructs it to listen to a G.711 stream, configure regions in this way:

- Put the CUCM MOH server or servers into a dedicated region (for example, MOH).
- Put all remote site devices into a site-specific region (for example, Branch-1).
- Allow G.711 between regions MOH and Branch-1.
- Make sure that region Branch-1 is limited to G.729 for calls to and from all other regions

Multicast MOH from Remote Site Router Flash Address and Port Considerations

Because a single MOH server can stream multiple multicast MOH files, you must specify an initial multicast address and port that is used for the first stream. In addition, you have to choose whether to increment the IP address or port on additional streams. It is recommended that you increment on IP addresses instead of ports. If multiple MOH servers exist within a network, make sure that they do not use overlapping multicast IP addresses and ports for their streams.

For each audio source, four streams are considered for the increment—one per codec: G.711 mu-law, G.711 a-law, G.729, and wideband. This principle always applies, regardless of which MOH codecs have been enabled in the Cisco IP Voice Media Streaming Application service. When you are incrementing on IP addresses, each stream consumes one IP address. In other words, each audio source requires four IP addresses. When incrementing on ports, consider the Real-Time Transport Control Protocol (RTCP). For each audio stream, two separate RTP ports are reserved: one for the actual audio transmission and one for (the optional) RTCP. Therefore, when you are incrementing multicast MOH on ports, each stream consumes two ports. You have to calculate eight port numbers per audio source (two ports per codec).

Audio sources that are not enabled for multicast MOH should nevertheless be considered for the increment of addresses or ports. Audio source 1, which starts with the configured base address and port, requires four IP addresses (or eight ports). The same principle

Table 8-1 Multicast MOH Address and Port Increment Example

Base IP: 239.1.1.1		Increment on IP Address	Increment on Port		
Base Port: 16384	Multicast Enabled	G.711a-law	G.729	G.711a-law	G.729
	G.711a-law, G.729				
Audio Source 1	Yes	239.1.1.2	239.1.1.3	16386	16388
Audio Source 2	No				
Audio Source 3	Yes	239.1.1.10	239.1.1.11	16402	16404
Audio Source 4	No				
Audio Source 5	No				
Audio Source 6	Yes	239.1.1.22	239.1.1.23	16426	16428

applies to each consecutive audio source (audio source 2, audio source 3, and so on), regardless of whether these audio sources are multicast-enabled.

Multicast MOH: Address and Port Increment Example

Table 8-1 shows an example of IP address and port increments for multicast MOH.

The base multicast group is configured for IP address 239.1.1.1 and port 16384. G.711 a-law and G.729 codecs are enabled; audio sources 1, 3, and 6 are multicast-enabled. Table 8-1 shows the IP addresses or ports that are used for the actual multicast MOH streams. Table 8-2 shows how these numbers were derived.

Note The italic numbers in Table 8-2 present the values that are used in the figure. The gray highlighted and bold numbers present the IP address and port number that are actually used in this example.

As you can see from the Table 8-2, audio sources are incremented in ascending order, starting with audio source 1 (live audio at source 0 is not multicast-capable and hence is excluded in the calculation). Codecs are enumerated in the order shown (G.711 mu-law, G.711 a-law, G.729, wideband). For each audio stream, two ports are used: the first one (even-numbered port) for the actual RTP transmission and the subsequent one (odd-numbered port) for the corresponding RTCP.

If you are not sure about the used multicast addresses and ports, you can configure traces for the Cisco IP Voice Media Streaming Application service. Make sure that you

check the Service Initialization check box in the trace configuration. Then, restart the Cisco IP Voice Media Streaming Application service in CUCM. When analyzing the trace output from CUCM, you will find this kind of information, as shown in Example 8-2.

Table 8-2 Multicast MOH Address and Port Calculations

Audio Source	Increment on IP Address (239.1.1.x—Only Last Octet Shown)				Increment on Ports (163xxx—Only Last Octet Shown)			
	G.711 mu-law	G.711 a-law	G.729 Wideband		G.711 mu-law	G.711 a-law	G.729 Wideband	
1	1	2	3	4	384/385	386/387	388/389	390/391
2	5	6	7	8	392/393	394/395	396/397	398/399
3	9	10	11	12	400/401	402/403	404/405	406/407
4	13	14	15	16	408/409	410/411	412/413	414/415
5	17	18	19	20	416/417	418/419	420/421	422/423
6	21	22	23	24	424/425	426/427	428/429	430/431

Example 8-2 Cisco IP Voice Media Streaming Application Trace Output

```
CMOHMgr::KickStartMultiCastStream (1) Starting Multicast
stream, asID = 1, conferenceID = 1, codecType = mulaw,
Multicast ip:port = 239.1.1.1:16384 !
<CLID::Cluster><NID::10.1.1.1>
CMOHMgr::KickStartMultiCastStream (1) Starting Multicast
stream, asID = 1, conferenceID = 1001, codecType = alaw,
Multicast ip:port = 239.1.1.1:16384 !
<CLID::Cluster><NID::10.1.1.1>
```

Note The output that is shown does not match the example in Tables 8-1 and 8-2. It is used only to illustrate which information you will find in the trace output. The number after the KickStartMultiCastStream identifies the audio source. For each enabled codec, you will find information about the used multicast IP address and port. The NID (node ID) shows the IP address of the MOH server. In this example, only G.711 mu-law and G.711 a-law codecs are enabled. Only one audio source (audio source 1) is multicast-enabled. There is a single MOH server at 10.1.1.1.

Tip It is important to know the used multicast IP addresses and ports when you choose the option to prevent multicast traffic from entering the IP WAN by access lists.

Implementing Multicast MOH from Remote Site Router Flash

In the topology shown in Figure 8-8, a MOH server is located at the main site and is configured for multicast MOH. Assume that multicast routing has been enabled in the entire network, including the IP WAN link to the remote site.

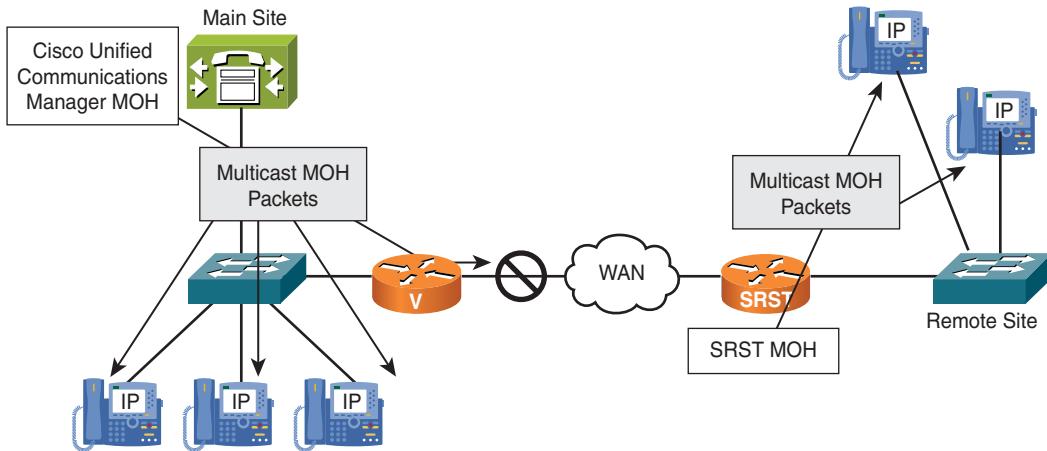


Figure 8-8 *Implementing Multicast MOH from Remote Site Router Flash Example*

The main site router, however, should no longer route multicast MOH to the remote site. The remote site SRST gateway should instead generate multicast MOH streams to the phones located at the remote site.

Because CUCM is unaware that the multicast packets generated by the MOH server at the headquarters are filtered on the IP WAN interface and then locally generated by the branch site SRST gateway, CUCM instructs the IP Phones located at the remote site to join the multicast group IP address that is configured at the CUCM MOH server. To allow the phones to receive MOH for the multicast group IP address they join, the SRST gateway has to be configured to use exactly the same multicast address and port that are used by the CUCM MOH server located at the main site. Example 8-3 shows a portion of the output of `show running-config` at headquarters. Example 8-4 shows a portion of the output of `show running-config` at the branch site.

Example 8-3 Headquarters Gateway Configuration for Multicast MOH

```
ip access-list extended drop-moh
  deny udp any host 239.1.1.1 eq 16384
  permit ip any any
!
interface serial 0/0
  ip access-group drop-moh out
  no ip pim sparse-mode
```

Example 8-4 Branch Site Configuration

```
call-manager-fallback
max-ephones 1
max-dn 1
ip source-address 10.1.5.102
moh moh-file.au
multicast moh 239.1.1.1 port 16384
```

It is assumed that the baseline configuration provides multicast routing in the entire network and that the CUCM MOH server is already configured for multicast MOH.

Note Multicast routing uses Class D addresses for the destination of the MOH RTP streams. The source address streaming multicast MOH is a Class A, B, or C address, never a Class D multicast address.

The multicast MOH stream that is sent toward the branch site needs to be blocked to avoid unneeded WAN utilization. Also, multicast MOH from branch router flash needs to be implemented at the branch site. Of course, if other WAN data traffic is currently being blocked at headquarters in an existing production router, the command line **deny udp any host 239.1.1.1 eq 16384** must be properly integrated with the existing access list.

Therefore, the SRST configuration of the branch site router is extended to include multicast MOH. The SRST configuration uses the same multicast IP address and port that are configured at the CUCM MOH server located at headquarters.

To stop multicast MOH generated by the headquarters CUCM MOH server from being sent over the IP WAN, one of three options can be chosen:

- **Set TTL to a low-enough value at the CUCMMOH server:** If the TTL value in the IP header of the generated multicast MOH packets is set to a low-enough value, the packets are not routed out to the IP WAN. However, if the IP WAN link is one hop away from the CUCM MOH server, and if the main-site phones are also one hop away from the server, this method cannot be used, because the main-site IP Phones would also be affected by the dropped packets. In the current example, Time to Live (TTL) is set to 1, and it is assumed that the IP Phones are in the same VLAN, like the CUCM MOH server.
- **Filter the packets by an IP access control list (ACL):** At the headquarters router, an ACL can be configured that drops the multicast MOH packets at the IP WAN interface.
- **Disable multicast routing at the IP WAN interface:** If you disable multicast routing at the IP WAN interface, multicast packets are not routed out that interface.

Note When multicast MOH in CUCM is configured, it is necessary to specify how to increment multicast streams based on IP addresses or port numbers. Depending on the setting, the IP ACL needs to be configured appropriately to include all possible IP addresses and port numbers. It is recommended that you increment the IP addresses by contiguous numbering. Each enabled codec has a separate MOH stream.

At the branch router, the multicast MOH stream is sent out the interface specified in the **ip source-address** command in call-manager-fallback configuration mode or in telephony-server configuration mode, when CUCM Express in SRST mode is used. Therefore, the multicast MOH stream generated at the remote site router does not have to be blocked at the remote site router WAN interface.

Configuration Procedure for Implementing Multicast MOH from the Remote Site Router Flash

Implementing multicast MOH from remote site router flash involves the following steps:

Step 1. Enable multicast routing in the IP network.

Step 2. Configure multicast MOH in CUCM:

- a. Configure MOH audio sources for multicast MOH.
- b. Configure MOH audio server for multicast MOH.
- c. Enable multicast MOH at the media resource group(s).

Step 3. Enable multicast MOH from remote site router flash at the remote site router.

Step 4. Implement a method to prevent multicast MOH streams from being sent over the IP WAN:

- a. Configure maximum hop value to prevent multicast MOH streams from being sent over the IP WAN.
- b. Use IP ACL at the IP WAN router interface.
- c. Disable multicast routing on the IP WAN router interface.

The configuration procedure describes the implementation of multicast MOH from remote site router flash by first enabling multicast MOH (Steps 1 and 2). Once this works as desired, the configuration is modified so that the multicast MOH stream is generated locally at the remote site router (Step 3) and the multicast MOH stream that is generated by the MOH server is prevented from being sent to the IP WAN.

When enabling multicast MOH at the MOH server, make sure that you set the maximum hop value of the multicast-enabled MOH audio source(s) to a high enough value to allow the multicast MOH packets to be sent all the way to the remote phones.

When choosing Step 4a to preventing the multicast MOH stream of the MOH server from being sent to the IP WAN, you have to use a low-enough value to ensure that the multicast MOH packets generated by the MOH server do not reach the IP WAN.

Note All IP Phones must be able to access the main site CUCM MOH server from their MRG list. This access is required as soon as multicast MOH is configured, whether multicast MOH from remote site router flash is used. If the IP Phones at the remote site do not have access to the CUCM MOH server from their MRG list, CUCM cannot instruct the IP Phones to join the multicast group, and it makes the phone use Tone On Hold instead of MOH.

Furthermore, the Use Multicast for MOH Audio check box has to be checked at the MRG that includes the multicast-enabled MOH server.

Finally, make sure that the G.711 codec is used between the MOH server and the remote site phones, because SRST multicast MOH supports only G.711.

Step 1: Enable Multicast Routing on Cisco IOS Routers

Example 8-5 shows a portion of **show running-config** in the IOS gateway that enables multicast routing at the main site and the remote site.

Example 8-5 Step 1: Enabling Multicast Routing in Cisco IOS Routers

```
ip multicast-routing
!
interface FastEthernet0/0
  description HQ-Voice-Servers
  ip address 10.1.1.101 255.255.255.0
  ip pim sparse-dense-mode
!
interface FastEthernet0/1
  description HQ-Phones
  ip address 10.1.2.101 255.255.255.0
  ip pim sparse-dense-mode
!
interface Serial0/1
  description IP WAN
  ip address 10.1.5.101 255.255.255.0
  ip pim sparse-dense-mode
```

Note The same configuration is required at all remote site routers where multicast is enabled. Use a unique interface description at each router interface.

Two commands are required to enable multicast routing in the network so that multicast MOH streams can be sent:

- **ip multicast-routing:** Configured in global configuration mode. It enables multicast routing on the Cisco IOS router in general.
- **ip pim sparse-dense-mode:** Needs to be configured on each interface where multicast routing should be enabled.

Note The configuration shown in Example 8-5 enables multicast routing in the entire network. When multicast MOH from remote site router flash is used, multicast streams are not sent to the IP WAN. They can be blocked based on the maximum hops parameter (TTL field in the IP header) or by IP ACLs. You can also block multicast streams by disabling multicast routing on the interface, but only if no other multicast routing applications are required in the network.

Also in Example 8-5, the maximum hops parameter cannot be used because the HQ-Phones network and the IP WAN network have the same distance to the HQ-Voice-Servers network. To allow multicast MOH to be sent to the HQ phones, a maximum hop value of 2 is required. This value, however, allows the multicast MOH packets to be sent out on the WAN interface. Therefore, IP ACLs have to be used, or multicast routing must be disabled at the WAN interface (if multicast routing is not required by other applications).

Step 2a: Configure MOH Audio Sources for Multicast MOH

To enable multicast MOH, first multicast MOH must be allowed on MOH audio sources, as shown in Figure 8-9. In **Cisco Unified CM Administration**, choose **Media Resources > Music On Hold Audio Source and Media Resources > Fixed MOH Audio Source**.

Check the Allow Multicasting check box for each MOH audio that is allowed to be sent as a multicast stream. This applies to MOH audio sources and to fixed MOH audio sources.

Note You can find more information about configuring the MOH server and MOH audio sources in *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1)*.

Step 2b: Configure Multicast MOH in CUCM

After multicast MOH on audio sources has been allowed, the MOH server has to be enabled for multicast MOH, as shown in Figure 8-10. In **Cisco Unified CM Administration**, choose **Media Resources > Music on Hold Server**.

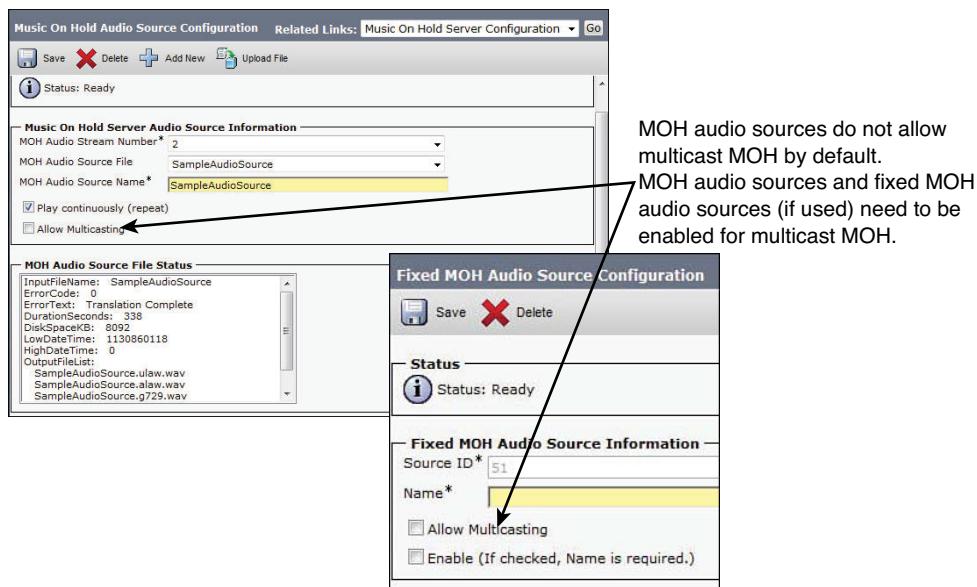


Figure 8-9 Step 2a: Configuring MOH Audio Sources for Multicast MOH

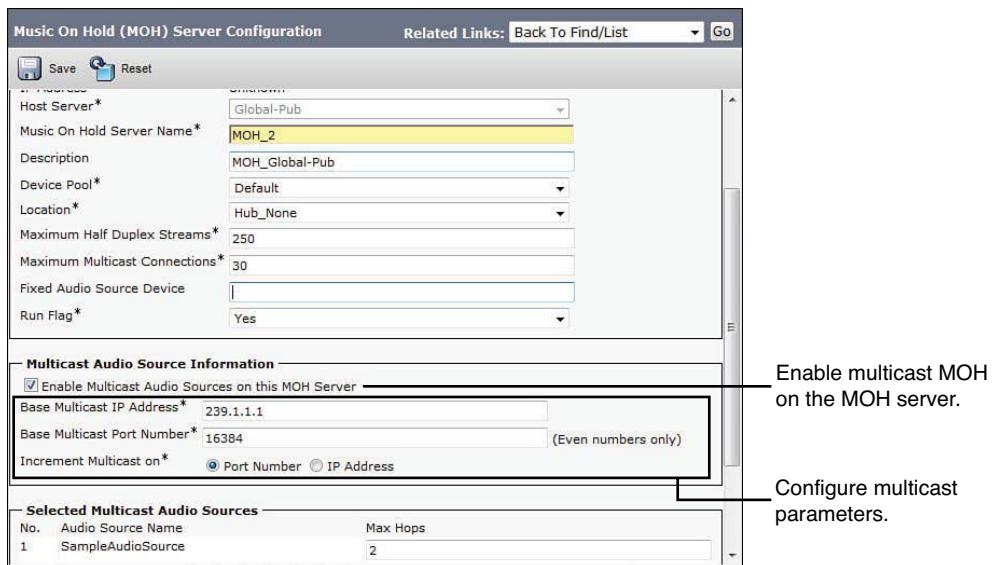


Figure 8-10 Step 2b: Configuring Multicast MOH in CUCM

Figure 8-10 shows how to enable multicast MOH on an MOH server. In the Multicast Audio Source Information section of the MOH Server Configuration screen, check 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 as desired.

Note Recommended practice dictates that you increment multicast on IP address instead of port number to avoid network saturation in firewall situations. Doing this means that each multicast audio source has a unique IP address and helps avoid network saturation. If multiple codecs are enabled for the MOH server, additional IP addresses are in use, with one per codec and per audio source.

Step 2c: Enabling Multicast MOH at the Media Resource Groups

Figure 8-11 shows that the configuration of a Multicast is enabled at the Media Resource Group (MRG). In Cisco Unified CM Administration, choose **Media Resources > Media Resource Group**.

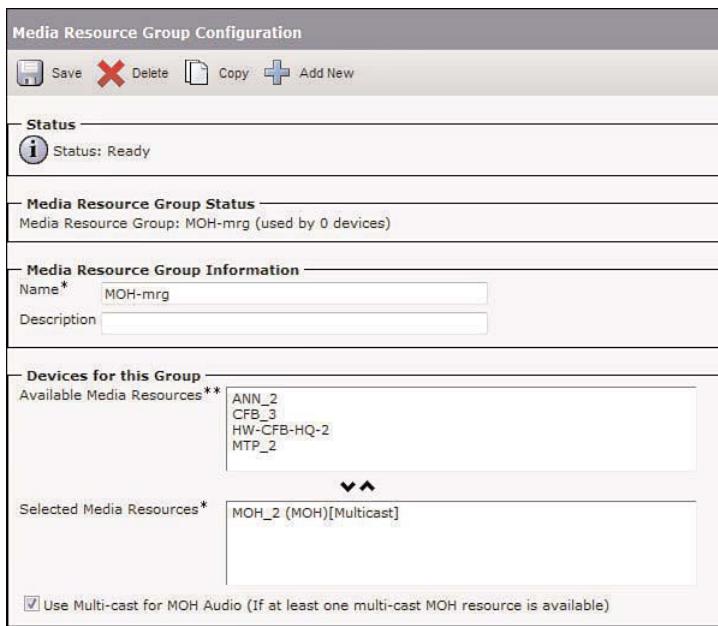


Figure 8-11 Step 2c: Enabling Multicast MOH at the Media Resource Groups

Multicast MOH works only if the multicast enabled MOH server is assigned to a multicast enabled MRG. This MRG will be configured to be a member of an MRGL. The MRGL will then be associated with devices, such as phones.

Step 3: Enable Multicast MOH from Branch Router Flash at the Branch Router

Example 8-6 shows a portion of `show running-config` that demonstrates how to configure a Cisco IOS router for multicast MOH from branch router flash.

Multicast MOH from branch router flash is part of the SRST feature. Therefore, SRST must be configured before you can enable multicast MOH from branch router flash.

Note Additional SRST configuration options were discussed in Chapter 6, “Implementing Cisco Unified SRST and MGCP Fallback.”

Example 8-6 Enabling Multicast MOH from Branch Router Flash at the Branch Router

```
ip multicast-routing
!
call-manager-fallback
  max-ephones 1
  max-dn 1
  ip source-address 10.1.5.102
  moh moh-file.au
  multicast moh 239.1.1.1 port 16384
!
interface FastEthernet0/0
  description BR-Phones
  ip address 10.1.5.102 255.255.255.0
!

interface Serial0/1
  description IP WAN
  ip address 10.1.4.102 255.255.255.0
```

Based on an existing SRST configuration, only two commands are required to enable multicast MOH from branch router flash:

- **moh file-name:** Specifies the MOH audio source file. The specified file must be stored in flash memory of the SRST gateway.
- **multicast moh *multicast-group-address* *port* *port*:** Specifies the multicast address and port that are used for the multicast MOH packets. The specified address and port must exactly match the values that were configured at the MOH server in Step 2b.

Note The SRST gateway permanently streams MOH, regardless of an IP WAN failure or IP Phones being registered with the SRST gateway.

You can configure an additional five MOH streams using MOH group configuration. Refer to Chapter 7, “Implementing Cisco Unified Communications Manager Express (CUCME) in SRST Mode,” for more information about MOH group configuration.

Step 4a: Configure the Maximum Hops to Be Used for MOH RTP Packets

Continue the multicast MOH server configuration by setting the maximum hop value, as shown in Figure 8-12. In Cisco Unified CM Administration, choose **Media Resources > Music on Hold Server**.

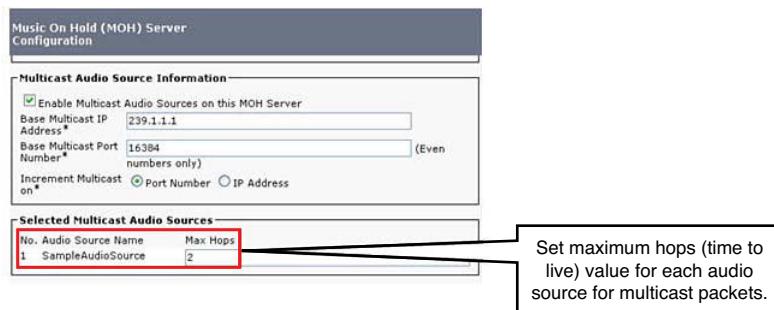


Figure 8-12 Step 4a Configure the Maximum Hops to Be Used for MOH RTP Packets

All MOH audio sources that have been configured for multicasting are listed in the Selected Multicast Audio Sources section of the MOH Server Configuration screen. You can set the Max Hops value for each audio source; the default is 2. This parameter sets the TTL value in the IP header of the multicast MOH RTP packets to the specified value. TTL in an IP packet indicates the maximum number of routers that an audio source is allowed to cross. If Max Hops is set to 1, the multicast MOH RTP packets remain in the subnet of the multicast MOH server. When you use multicast MOH from remote site router flash, you can set Max Hops to a value that is lower than the actual hop count from the MOH server toward the WAN interface of the main site router. This value, however, might conflict with the needs within the main site when IP Phone networks have the same or a higher distance (that is, a higher hop count) to the MOH server than the WAN network. In such a case, one of the other possible methods of preventing the multicast MOH packets that are generated by the MOH server must be used, as described in the following sections.

Step 4b: Use an IP ACL at the IP WAN Router Interface

Example 8-7 shows a portion of `show running-config` that demonstrates how to configure a Cisco IOS router to drop multicast MOH packets by using an IP ACL.

Example 8-7 Step 4b: Using IP ACL at the IP WAN Router Interface

```

ip multicast-routing
!
ip access-list extended drop-moh
  deny ip any host 239.1.1.1 range 16384 16385
  permit ip any any
!
interface FastEthernet0/0
  description HQ-Voice-Servers
  ip address 10.1.1.101 255.255.255.0
  ip pim sparse-dense-mode
!
interface FastEthernet0/1
  description HQ-Phones
  ip address 10.1.2.101 255.255.255.0
  ip pim sparse-dense-mode
!
interface Serial0/1
  description IP WAN
  ip address 10.1.4.101 255.255.255.0
  ip access-group drop-moh out
  ip pim sparse-dense-mode

```

The ACL matches the MOH group address and port number that are used by the MOH server for the MOH RTP packets. The ACL is applied to the IP WAN interface in the outgoing direction and therefore does not allow multicast MOH packets to be sent out the IP WAN.

Note If the MOH server is configured to use more than one codec, the access list has to include additional IP addresses or port numbers. By default, only G.711 is enabled in the Supported MOH Codecs service parameter of the Cisco IP Voice Media Streaming App service. The MOH server can be configured to increment on either IP addresses or port numbers. Also as stated earlier in this chapter, the multicast address and port range that must be filtered depend on several parameters, such as the audio source number, the enabled codecs, and the increment method.

Step 4c: Disable Multicast Routing on the IP WAN Router Interface

Example 8-8 shows a portion of **show running-config** that illustrates how to configure a Cisco IOS router to disable multicast routing at the IP WAN interface.

If no other multicast applications are used over the IP WAN, the simplest way of preventing the multicast MOH packets from being sent to the WAN is to disable multicast routing at the WAN interface.

Example 8-8 Step 4c: Disabling Multicast Routing on the IP WAN Router Interface

```
ip multicast-routing
!
interface FastEthernet0/0
    description HQ-Voice-Servers
    ip address 10.1.1.101 255.255.255.0
    ip pim sparse-dense-mode
!
interface FastEthernet0/0
    description HQ-Phones
    ip address 10.1.2.101 255.255.255.0
    ip pim sparse-dense-mode
!
interface Serial0/1
    description IP WAN
    ip address 10.1.4.101 255.255.255.0
    no ip pim sparse-dense-mode
```

Summary

The following key points were discussed in this chapter:

- Bandwidth-management methods include techniques that reduce required bandwidth of voice streams, techniques that keep voice streams off the IP WAN, and other techniques such as deploying transcoders.
- The highest bandwidth-consuming codec for a call between two devices is determined by the CUCM region configuration of the two devices.
- When you are deploying local conference bridges at multiple sites, use media resource groups and media resource group lists to control which conference bridge is used by which device.
- Transcoders allow low-bandwidth codecs to be used over the IP WAN when low-bandwidth codecs are not supported by both endpoints.
- Multicast MOH from branch router flash is a feature that allows MOH streams to be generated locally at the remote site instead of being sent across the IP WAN from the main site.

References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco Unified Communications System 8.x SRND*, April 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8x.html.

Cisco Systems, Inc. *Cisco Unified Communications Manager Administration Guide Release 8.0(1)*, February 2010.

www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_1/ccmcfg/bccm-801-cm.html.

Cisco Systems, Inc. *Cisco Unified SRST System Administrator Guide*, December 2007.

www.cisco.com/en/US/partner/docs/voice_ip_comm/cusrst/admin/srst/configuration/guide/srstsa.html.

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in Appendix A, "Answers Appendix."

- 1.** Which of the following features does not reduce audio bandwidth utilization in the IP WAN?
 - a.** RTP header compression
 - b.** Low-bandwidth codecs
 - c.** Local media resources
 - d.** Quality of service
- 2.** How can the bandwidth per call be limited in CUCM?
 - a.** By specifying the maximum permitted codec between pairs of regions
 - b.** By specifying the maximum permitted codec between pairs of locations
 - c.** By configuring transcoding
 - d.** By specifying the maximum permitted TTL.
- 3.** When deploying local conference bridges at each site, what is the minimum number of media resource group lists that is required?
 - a.** Number of sites multiplied by (the number of sites minus 1) divided by 2
 - b.** One per site
 - c.** One per site and one per conference bridge
 - d.** One

4. Which device requires access to the transcoder from its media resource group list when transcoding is required for a call?
 - a. Both endpoints of the original call
 - b. The calling device
 - c. The device that supports only codecs not permitted for the original call
 - d. The called device
5. Which statement about multicast MOH from remote site router flash is true?
 - a. Multicast MOH can stream more than one MOH file in SRST v8.x or later.
 - b. Multicast MOH from remote site router flash can also be used for unicast MOH.
 - c. The remote site router with SRST v8.x can stream only a single MOH file and supports G.711 and G.729 only.
 - d. Regions in CUCM have to be configured such that G.711 is allowed between the CUCM MOH server and the remote site phones.
6. Which of the following is the best use of transcoding resources?
 - a. Configure transcoding with DSP resources to use G.711 over the WAN and with G.729 in the LAN.
 - b. Configure transcoding with DSP resources to use G.729 over the WAN and with G.711 in the LAN.
 - c. Configure transcoding with DSP resources on both routers to use G.711 over the WAN and with G.729 in the LAN.
 - d. Configure transcoding with DSP resources on both routers to use G.711 over the WAN and with G.711 in the LAN.
7. Which VoIP signaling protocol or protocol options must be used to configure transcoding resources on a router to communicate with CUCM?
 - a. SIP
 - b. SCCP
 - c. MGCP
 - d. H.323
 - e. SIP and H.323 with CUBE
 - f. Any VoIP signaling protocol

- 8.** Which of the following best describes how multicast MOH streams RTP?
 - a.** A source Class D address streams to a destination Class D address.
 - b.** A source Class A, B, or C address streams to a destination Class D address.
 - c.** A source Class D address streams to a destination Class A, B, or C address.
 - d.** A source Class A, B, or C address streams to a destination Class A, B, or C address.
- 9.** What is the procedure to ensure that branch site phones correctly use the DSP resources for hardware conference calls, which minimizes WAN utilization?
 - a.** Put the branch phones in an MRG that links to an MRGL that links to the branch site conference bridge.
 - b.** Put the branch phones in an MRGL that links to an MRG that links to the branch site conference bridge.
 - c.** Put the branch phones in an MRG that links to an MRGL that links to the headquarters conference bridge.
 - d.** Put the branch phones in an MRGL that links to an MRG that links to the headquarters conference bridge.
- 10.** Which two of the following are acceptable ways to avoid main-site multicast MOH traffic from traversing the IP WAN?
 - a.** Prevent dynamic routing protocols from routing over the WAN.
 - b.** At the main-site router, an ACL can be configured that drops the multicast MOH packets at the IP WAN interface.
 - c.** Disable multicast routing at the IP WAN interface at the main site.
 - d.** Disable multicast routing at the IP WAN interface at the remote site.
 - e.** Use only static routes for IP routing over the IP WAN.

Chapter 9

Implementing Call Admission Control

Upon completing this chapter, you will be able to describe and configure CAC mechanisms and AAR in CUCM. You will be able to meet these objectives:

- Describe the CAC options provided by CUCM
- Implement locations-based CAC in CUCM
- Implement RSVP-enabled locations-based CAC in CUCM
- Implement AAR in order to reroute calls over the PSTN if not enough bandwidth is available for an on-net call
- Implement SIP preconditions on SIP trunks in CUCM
- Implement H.323 gatekeeper-based CAC in CUCM

Implementing multiple-site IP telephony deployments over an IP WAN requires additional planning to ensure the quality and availability of voice calls.

When an IP WAN connects multiple sites in a Cisco Unified Communications deployment, quality of service (QoS) has to be implemented to prioritize voice packets over data packets. However, to avoid an oversubscription caused by too many voice calls, a mechanism is needed to limit the number of calls allowed at the same time between certain locations. Call admission control (CAC) ensures that voice calls do not oversubscribe the IP WAN bandwidth and thus impact voice quality. If CAC is not configured, Cisco Unified Communications Manager (CUCM) assumes that all links everywhere have infinite bandwidth, which can result in oversubscription of WAN links at the expense of audio quality.

This chapter describes how to implement three CAC mechanisms that are provided by CUCM and explains how Automated Alternate Routing (AAR) can be used in some scenarios to reroute calls that were denied by CAC over the public switched telephone network (PSTN) ultimately to the remote site.

CAC Overview

CAC limits the number of calls between certain parts of the network to avoid bandwidth oversubscription, with too many voice calls over WAN links. The default CAC setting in CUCM is disabled, which means that CUCM assumes that there is infinite bandwidth on all links at all times. Limiting the maximum number of calls across a link cannot be achieved by QoS mechanisms alone, because QoS provides only the means to prioritize voice over data traffic. For example, the QoS best-practice mechanism for prioritizing voice of low-latency queuing (LLQ) does not resolve the situation in which too many voice and/or video streams are sent over the network.

If oversubscription occurs, any packets of any voice stream can be affected, not just packets of the particular call or calls that exceed the bandwidth limit. The result is packet delays and packet drops of all voice calls; hence, oversubscription degrades the quality of all voice calls.

Therefore, to ensure good voice quality, CAC must be used to limit the number of voice calls.

CAC in CUCM

CUCM supports different CAC methods, as shown in Figure 9-1.

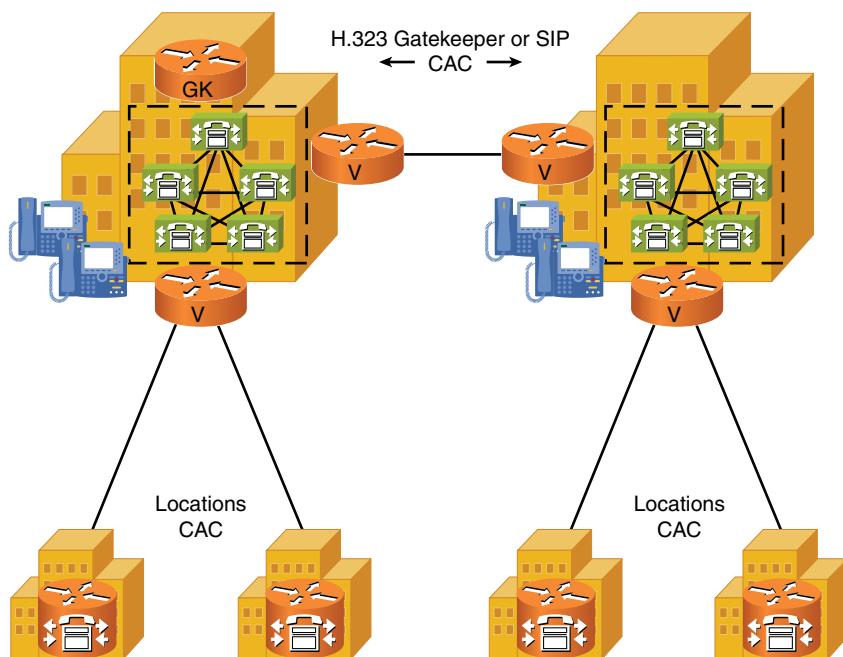


Figure 9-1 CAC in CUCM

In centralized call-processing deployments with CUCM, standard locations and Resource Reservation Protocol (RSVP)-enabled locations can be used to provide CAC. If a call is not admitted by one of these two CAC methods because of bandwidth limitations, AAR can be used to reroute the call over the PSTN as an off-net call instead of just denying the call. AAR provides a service similar to PSTN backup, except that the event is not a call failure on the on-net path but a lack of available bandwidth from a CAC point of view. AAR is designed to work within each CUCM cluster, and it does not apply for calls from within a CUCM cluster to another cluster.

In distributed call-processing environments with two or more CUCM clusters, an H.323 gatekeeper configured with CAC can be used in conjunction with H.323 trunks. Cisco offers two types of H.323-based trunks for gatekeepers: an intercluster trunk (gatekeeper-controlled) and an H.225 trunk (gatekeeper-controlled). If Session Initiation Protocol (SIP) trunks are implemented, you can use SIP preconditions, which allows RSVP-based CAC.

If the call is not admitted by the H.323 gatekeeper, standard backup functionality of route lists and route groups is applied. For example, to route calls that have not been admitted by the gatekeeper to be sent over the trunk, one or more PSTN gateways can be configured in another lower-priority route group of the same route list. In this way, the gatekeeper-controlled trunk is preferred over the PSTN as long as calls are admitted, but if admission is rejected, calls are sent over the PSTN. AAR is not used with gatekeeper CAC. The same principle applies to calls placed through SIP trunks that are configured for SIP preconditions.

Standard Locations

Each device in a CUCM cluster has one location assigned. The assignment can be direct and/or via a device pool. Assigning locations to each device based on the device pool significantly simplifies the CUCM configuration when there are many devices. If both types of assignment are used, the device configuration has higher priority, because it is more specific than the more general device pool.

Calls are limited by permitting a certain bandwidth for all calls coming into and going out of a location. CUCM calculates the actual audio codec bandwidth plus IP overhead (assuming a packetization period of 20 ms). This means that each G.711 call is assumed by the location to be 80 kbps, and a G.729 call is assumed to be 24 kbps. The actual VoIP bandwidth of G.711 and G.729 calls will use more bandwidth than these quantities, but CUCM CAC is configured with these numbers as-is for each call.

Note Calls within a location do not decrease the bandwidth limit, because they are unlimited. Only calls that go out of a location or are received from outside the location are considered by the locations-based CAC algorithm.

The configured bandwidth limit is independent of the call's destination location. Unlike region configuration, in which the maximum permitted codec is configured *for each pair*

of regions, the bandwidth limit of a location applies to *all interlocation calls, regardless of the other location*.

Locations provide CAC for calls within clusters. However, because locations can also be configured for gateways and trunks, they do allow some control over calls leaving the cluster.

Locations-based CAC in CUCM is totally unaware of the network's topology. It is a purely logical assignment and does not reflect the actual topology or the actual bandwidth available.

Locations: Hub-and-Spoke Topology

Figure 9-2 shows a hub-and-spoke CUCM topology with locations-based CAC.

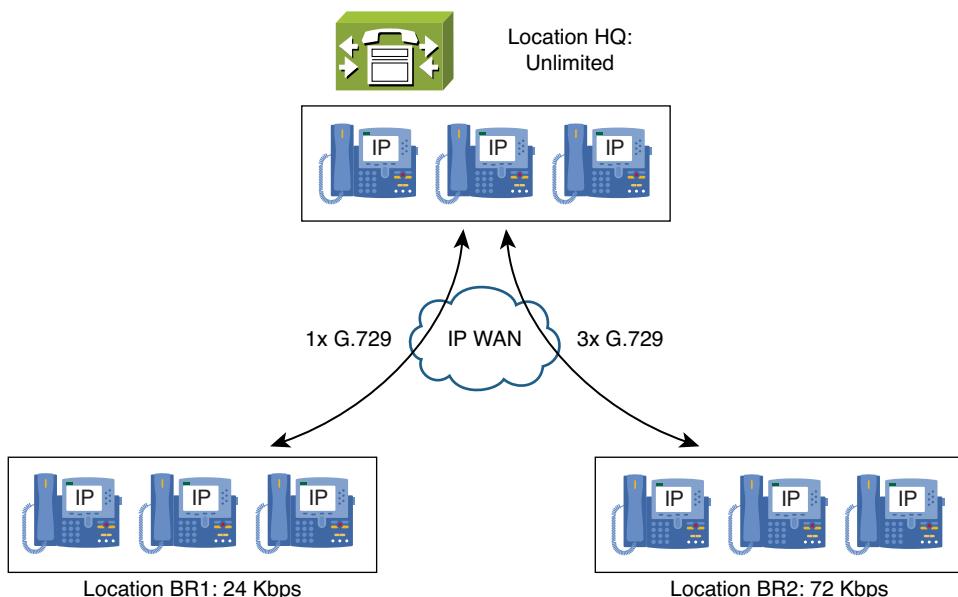


Figure 9-2 Locations with a Hub-and-Spoke Topology

As shown in Figure 9-2, the three sites are headquarters (HQ) and two branches (BR1 and BR2). Assuming that there is a hub-and-spoke WAN provider with no direct connection between the branches, all traffic between branches goes via headquarters.

This scenario is ideal for locations-based CAC, which works relatively well in hub-and-spoke topologies. If the intention is to allow only one G.729 call on the link between BR1 and HQ and three G.729 calls on the link between BR2 and HQ, the following location configuration would work:

- **Location HQ:** Unlimited
- **Location BR1:** 24 kbps (one G.729 call)
- **Location BR2:** 72 kbps (three G.729 calls)

This configuration ensures that no more than one G.729 call will be sent over the IP WAN toward location BR1 and that no more than three G.729 calls will be sent over the IP WAN toward location BR2.

Note The configuration also allows one G.729 call between BR1 and BR2. CUCM CAC is based on a hub-and-spoke topology, in which all calls over the WAN are monitored for CAC as if they go through HQ. Because the configured bandwidth limit does not consider the destination location, the 24-kbps limit of BR1 allows any call to go out or in, regardless of where it goes to or comes from. The headquarters limit is unaffected by such a call. Only locations BR1 and BR2 subtract 24 kbps from their limits. Because locations-based CAC does not provide topology awareness, CUCM does not even know that the call physically flows through headquarters.

Locations: Full-Mesh Topology

Figure 9-3 shows a full-mesh topology with CUCM locations-based CAC.

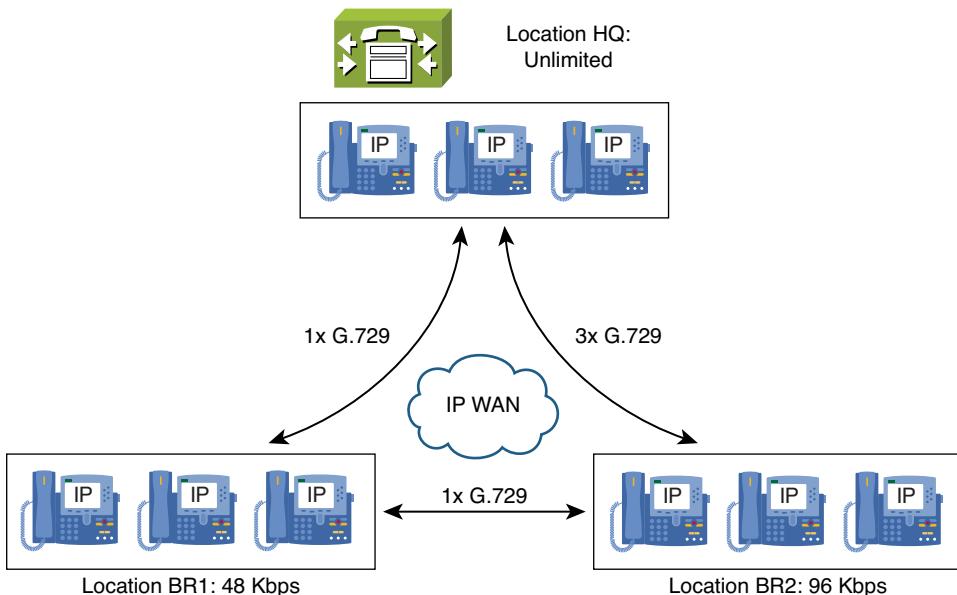


Figure 9-3 Locations with a Full-Mesh Topology

In Figure 9-3, a direct IP WAN link has been added between BR1 and BR2. One G.729 call is allowed on the WAN link from BR1 toward headquarters, one G.729 call is allowed

on the WAN link between BR1 and BR2, and three G.729 calls are allowed on the WAN link from BR2 toward headquarters.

Such a scenario reveals issues that arise when locations-based CAC is used in topologies other than hub-and-spoke. To allow the additional G.729 call that is permitted on the WAN link between BR1 and BR2, the bandwidth limit of these two locations has been increased by 24 kbps, which allows one more G.729 call. Doing this, however, can lead to the following undesirable situations:

- **Two G.729 calls from BR1 to HQ:** Because the BR1 location now has a limit of 48 kbps, it allows two G.729 calls. Location bandwidth limits are not configured per destination, so any call coming into or going out of a location is considered, regardless of the other location involved in the call. Therefore, there is no way to divide the available 48 kbps between one call toward the HQ and one call to BR2.
- **Four G.729 calls from BR2 to HQ:** The same problem occurs with the BR2 location. The additional bandwidth that was added to accommodate the desired call toward BR1 can be used toward the HQ, occupying that link with one more call than intended.

Note The problems encountered here are caused by the fact that the bandwidth limit is configured per location, regardless of the other location where the call goes to or comes from.

Configuration Procedure for Implementing Locations-Based CAC

The implementation of CUCM locations-based CAC involves the following steps:

- Step 1.** Add locations and configure the CAC bandwidth limit.
- Step 2.** Assign locations to devices.

Note To know how much bandwidth has to be calculated per call, regions should be designed and configured to negotiate codecs before locations to implement CAC are implemented.

Locations Configuration Example of a Hub-and-Spoke Topology

Figure 9-4 shows a hub-and-spoke locations-based CAC implementation.

This example has three sites: headquarters and two branches. Each site has its own location (HQ, BR1, and BR2). The physical WAN design is a hub-and-spoke topology where headquarters (HQ) is the hub.

The link between branch 1 and headquarters should not carry more than one G.729 call, and the link between branch 2 and headquarters should not carry more than three G.729 calls. There is no WAN link directly between the WAN sites.

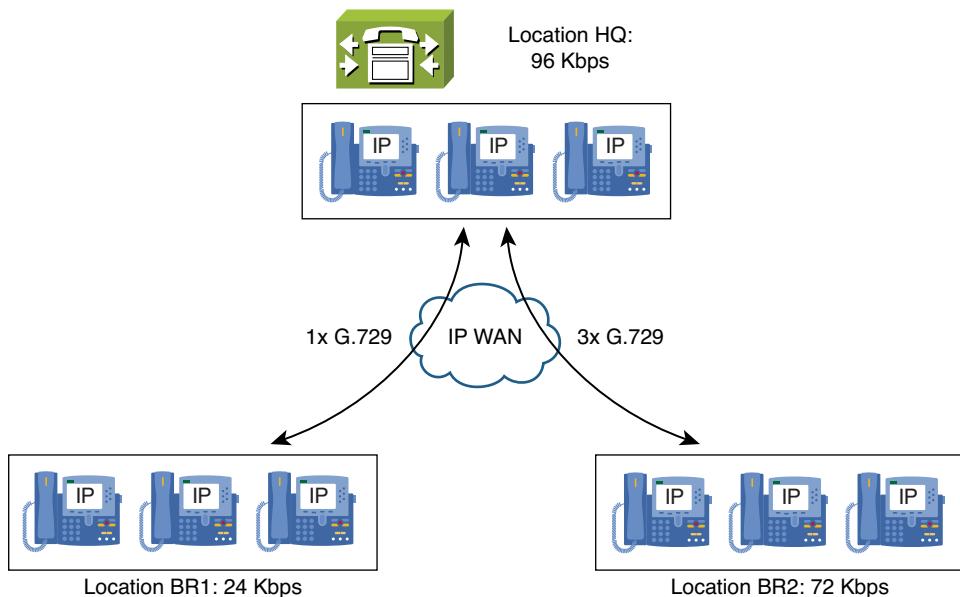


Figure 9-4 Locations Configuration of a Hub-and-Spoke Topology

The following sections demonstrate how to implement locations-based CAC for this scenario.

Step 1: Configure Locations

Figure 9-5 shows how you configure the locations in CUCM. In Cisco Unified CM Administration, choose System > Location.

The screenshot shows the 'Location Configuration' page in the Cisco Unified CM Administration interface. The 'Location Information' section has a red box around the 'Name' field, which contains the value 'BR1'. A callout box with the text 'Enter location name.' points to this field. The 'Audio Calls Information' section has a red box around the 'Audio Bandwidth' field, which shows 'Unlimited' selected and '24' entered. A callout box with the text 'Set bandwidth permitted for calls coming into and going out of location.' points to this field. A note below the bandwidth field states: 'If the audio quality is poor or choppy, lower the bandwidth setting. For ISDN, use multiples of 56 kbps or 64 kbps.'

Figure 9-5 Step 1: Configure Locations in CUCM

One location exists by default: Hub_None. This location is the default location for all devices. To add a new location, click Add New.

In the **Location Configuration** window, enter a name for the location in the **Name** field, and set the bandwidth for audio calls. The default Location bandwidth is unlimited, which means that CAC is disabled by default in CUCM.

Calculations of calls for CUCM CAC include Layer 3 to 7 overhead minus the Layer 2 overhead. This results in a G.729 call calculated with 24 kbps and a G.711 at 80 kbps. The actual bandwidth of a voice call contains the Layer 2 overhead. CUCM's "view" of the call does not include the Layer 2 overhead. Be aware that unless RSVP-enabled locations (which are discussed in a moment) are used, standard locations-based CAC considers calls coming into the location and going out of the location, regardless of the location of the other device.

Step 2: Assign Locations to Devices

Figure 9-6 shows how locations are assigned to devices. In Cisco Unified CM Administration, choose Device > Phone. Select your phone.

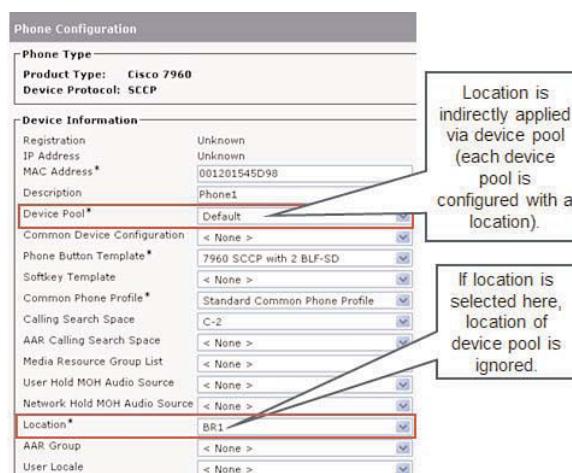


Figure 9-6 Step 2: Assign Locations to Devices

Locations are a mandatory setting in a device pool, and each device needs a device pool assigned. Therefore, a device always has a location assigned indirectly through its device pool. If a device uses a different location than the one specified in its device pool, that location can be chosen at the device itself. A location that is assigned at the device level has higher priority than the location of the device pool. A good way to remember this in Cisco voice technologies is a simple rule: More-specific overrides more-general.

RSVP-Enabled Locations

RSVP-enabled locations are based on CUCM standard locations. RSVP-enabled locations differ from standard locations in two ways. First, RSVP can be enabled selectively between pairs of locations. Because endpoints such as Cisco IP Phones do not support RSVP, the solution requires separate RSVP agents.

An RSVP agent is a device called a Media Termination Point (MTP) through which the call has to flow. RSVP is used only between the two RSVP agents. The Real-Time Transport Protocol (RTP) stream from the IP Phone to the RSVP agent does not use RSVP.

The second and most important difference between RSVP-enabled locations and standard locations is that the use of RSVP makes this CAC mechanism WAN topology-aware, because RSVP will communicate over the WAN. Standard locations do not contain in their configurations details of the WAN topology. RSVP-enabled locations work well with all topologies (full-mesh, partial-mesh, and hub-and-spoke) and adapt to network changes by considering the actual topology. Advantages include consideration of the following:

- **Link failures:** If one link in the IP network goes down and packets are routed on different paths, RSVP is aware of the change and calculates the bandwidth that is now available at the actual routed path.
- **Backup links:** If backup links are added after link failures, or if bandwidth on demand is used to add dial-on-demand circuits, RSVP again is fully aware of the routing path that is currently used and the bandwidth available on each link along that path.
- **Load-share paths:** If load sharing is used, RSVP is aware of the overall bandwidth provided by multiple load-sharing links.

Using RSVP for CAC lets you admit or deny calls based on actual oversubscriptions. The result is always based on the *currently* available bandwidth and interfaces, not on a logical configuration that ignores the physical topology.

Three Call Legs with RSVP-Enabled Locations

When RSVP-enabled locations are used, the end-to-end call is split into three separate call legs, as shown in Figure 9-7.

In Figure 9-7, Phone1, which is in Location A, places a call to Phone2, which is in Location B. CUCM location configuration specifies that RSVP has to be used for calls between these two locations.

CUCM instructs the two involved RSVP agents in Location A and the other in Location B to use RSVP to try to set up the call between each other. If the call is admitted because enough bandwidth is available in the network path between these two devices, the RSVP agents inform CUCM that the RSVP call leg was successfully set up.

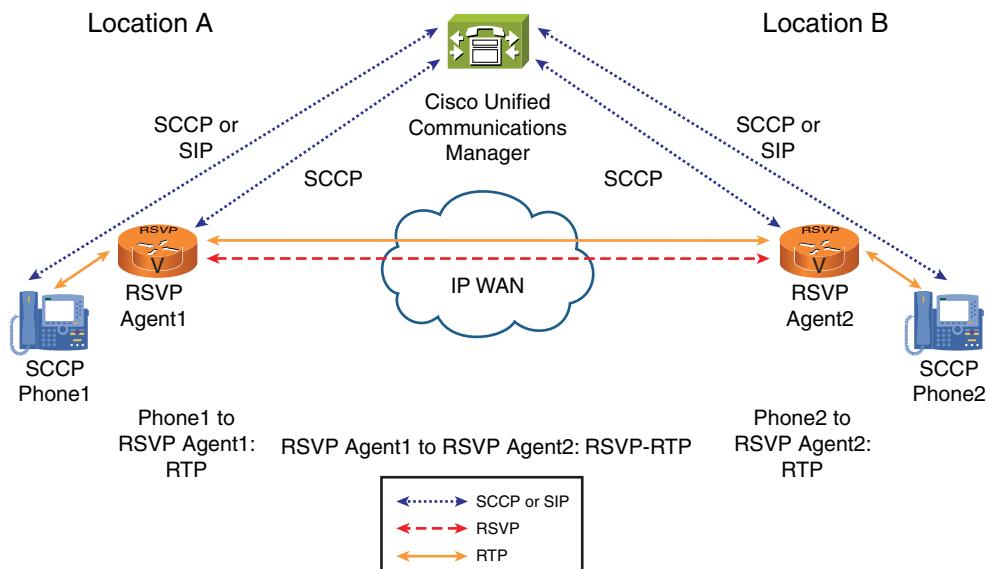


Figure 9-7 Three Call Legs with RSVP-Enabled Locations

CUCM now tells the phones to set up their call legs, each to its respective RSVP agent. If the RSVP call setup between the two RSVP agents is denied, CUCM considers the call to have failed CAC.

It is important to realize that there are three separate RTP streams: Phone1 talks to RSVP Agent1, RSVP Agent1 talks to RSVP Agent2, and RSVP Agent2 talks to Phone2.

RSVP CAC is used only between the RSVP agents. In this case, the RSVP agents are the routers in the two locations, not the Cisco IP Phones.

Characteristics of Phone-to-RSVP Agent Call Legs

Standard location algorithms apply to the call leg between an IP Phone and its RSVP agent, which are usually in the same location. If they are in different locations, standard locations-based CAC is first performed for this call leg between the phone and the RSVP agent. The two RSVP agents try to set up their call leg by using RSVP only if enough bandwidth is available for the IP Phones to reach their RSVP agents.

An RSVP agent registers with CUCM as a special MTP device on an Integrated Service Router (ISR). CUCM uses the media resource group list of the IP Phone to determine which RSVP agent is to be used by which IP Phone. The association of a phone to its RSVP agent is *not* performed by searching for an RSVP agent in the same location as the phone. As mentioned earlier, the IP Phone and its RSVP agent can be in different locations. Only media resource group lists are used to identify the RSVP agent to be used by an IP Phone.

From a design perspective, the RSVP agent on an ISR that is used by a certain IP Phone or group of phones should be as close as possible to the IP Phone or phones. Such a design ensures that no suboptimal paths such as phones are accessing RSVP agents over the IP WAN. In addition, this ensures that RSVP-based CAC performed for the phone to RSVP agent is a short network path, ideally over the LAN only.

The RSVP agent supports pass-through codec configuration, which allows any codec to be used. The benefit is that the codec does not have to be known or supported by the RSVP agent, including secure RTP (SRTP), where the RTP payload is encrypted.

Characteristics of RSVP Agent-to-RSVP Agent Call Legs

The call leg between two RSVP agents uses standard RSVP, as implemented in Cisco IOS routers. The IP network between the RSVP agents is RSVP-enabled, which requires each interface to be configured with a maximum amount of bandwidth that can be used for RSVP calls. When not enough bandwidth is available end to end (between the two RSVP agents in this case), RSVP CAC denies the call.

If RSVP is not enabled on any hop in the path, the CAC algorithm ignores the appropriate link (that is, it is always admitted on this link).

CUCM RSVP agent CAC uses the Integrated Services (IntServ) QoS model for the RSVP call leg. This means that RSVP is used only for CAC (the “control” plane), not with RSVP reservable queues for providing QoS to the streams. Instead, standard low-latency queuing (LLQ) configuration is required to provision QoS for the RTP voice stream (the “data” plane).

The end-to-end call—that is, the incorporation of all three call legs—is established only after the RSVP call leg has been admitted. If the RSVP call leg is not admitted, the call fails because of CAC denial caused by insufficient bandwidth.

RSVP Basic Operation

As shown in Figure 9-8, the RSVP-enabled sender (in this case, an RSVP agent) sends a PATH message toward the RSVP-enabled receiver (again, an RSVP agent in this case) along the path that requests bandwidth for the call to be set up. The receiver responds with a Resv message that is routed back along the path. Each RSVP-enabled device checks to see if the requested bandwidth is available and sends the appropriate information in the downstream path toward the sender. “OK” in Figure 9-8 denotes that RSVP has reserved bandwidth on an interface.

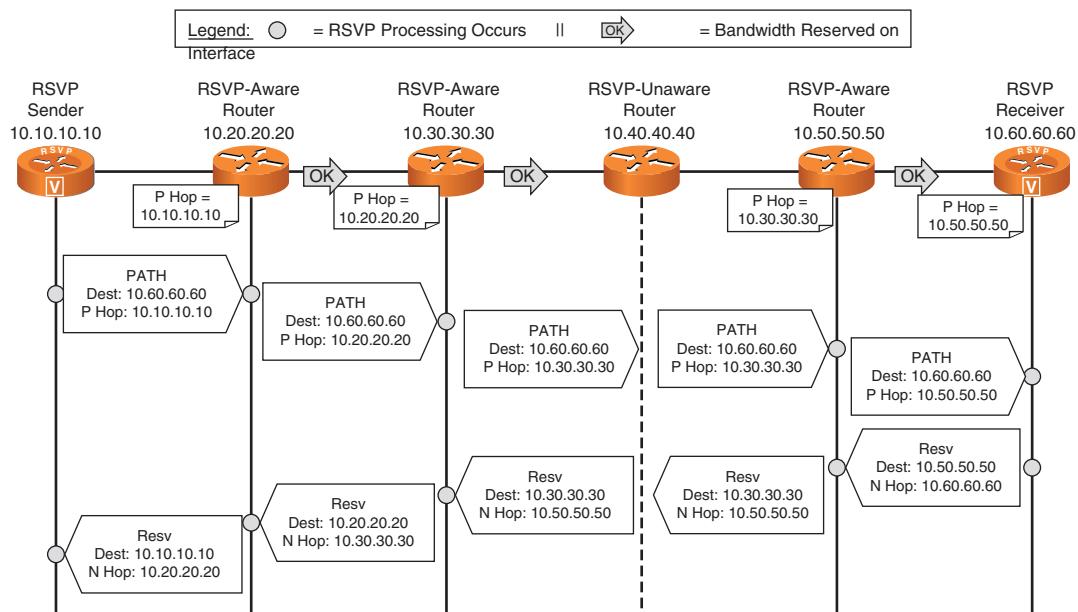


Figure 9-8 RSVP Functionality over Multiple Hops

If no RSVP-enabled device on the path denies the reservation because of insufficient bandwidth, the reservation succeeds, and the call is admitted by RSVP CAC.

A more detailed description of the key RSVP messages follows:

- **Path messages (PATH):** An *RSVP path message* is sent by each sender along the unicast or multicast routes that are provided by the routing protocol. A PATH message is used to store the path state in each node. The path state is used to route reservation request (Resv) messages in the reverse direction.
- **Reservation-request messages (Resv):** A *reservation request message* is sent by each receiver host toward the senders. This message follows in reverse the routes that the data packets use, all the way to the sender hosts. A reservation request message must be delivered to the sender hosts so that they can set up appropriate traffic control parameters for the first hop. RSVP does not send any positive acknowledgment messages.

Other RSVP messages are as follows:

- **Confirmation messages:** *Reservation request acknowledgment messages* are sent when a reservation confirmation object appears in a reservation request message. This

acknowledgment message contains a copy of the reservation confirmation. An acknowledgment message is sent to the unicast address of a receiver host, and the address is obtained from the reservation confirmation object. A reservation request acknowledgment message is forwarded to the receiver hop by hop to accommodate the hop-by-hop integrity-check mechanism.

- **Path error messages:** Result from path messages, and they travel toward senders. Path error messages are routed hop by hop using the path state. At each hop, the IP destination address is the unicast address of the previous hop.
- **Reservation request error messages:** Result from reservation request messages and travel toward the receiver. Reservation request error messages are routed hop by hop using the reservation state. At each hop, the IP destination address is the unicast address of the next-hop node. Information carried in error messages can include the following:
 - Admission failure
 - Bandwidth unavailable
 - Service not supported
 - Bad flow specification
 - Ambiguous path
- **Teardown messages:** *RSVP teardown messages* remove the path and reservation state without waiting for the cleanup timeout period. Teardown messages can be initiated by an application in an end system (sender or receiver) or a router as the result of state timeout. RSVP supports the following two types of teardown messages:
 - **Path teardown:** *Path teardown messages* delete the path state (which deletes the reservation state), travel toward all receivers downstream from the point of initiation, and are routed like path messages.
 - **Reservation-request teardown:** *Reservation-request teardown messages* delete the reservation state, travel toward all matching senders upstream from the point of teardown initiation, and are routed like corresponding reservation request messages.

RSVP-Enabled Location Configuration

Figure 9-9 shows a conceptual example of a CAC implementation configured in CUCM, based on RSVP-enabled locations that will be implemented in the steps listed in the following section.

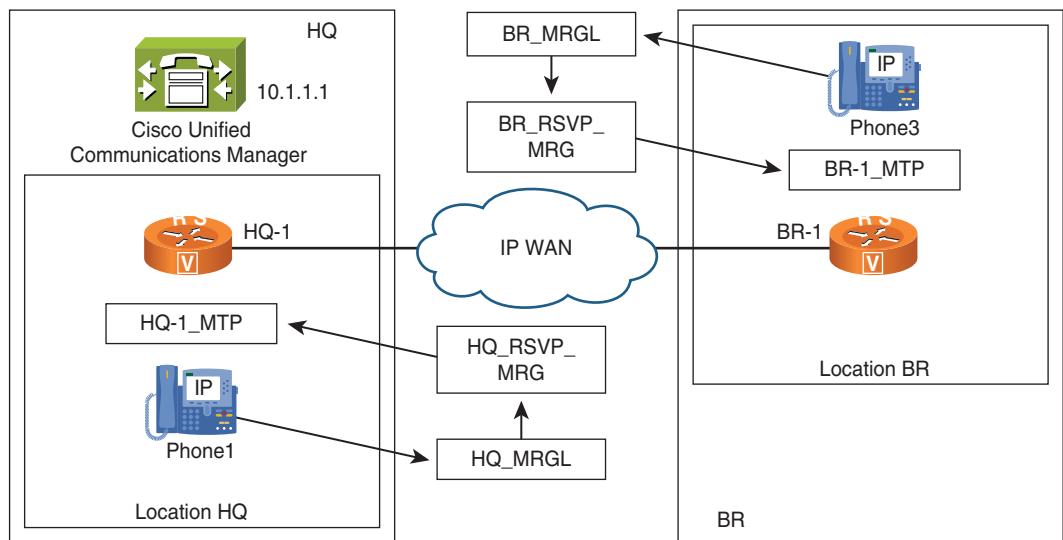


Figure 9-9 *RSVP-Enabled Location CUCM Configuration*

This example has two sites: headquarters (HQ) and branch (BR). Phones located at headquarters are in location HQ, and phones located at the branch are in location BR. RSVP agents exist at each site where HQ-1_MTP is provided by router HQ-1, and BR-1_MTP is provided by router BR-1. The RSVP agents are assigned to their respective locations.

Headquarters phones have media resource group list HQ_MRGL (media resource group list) applied. This media resource group list includes a media resource group named HQ_RSVP_MRGL (media resource group), which includes the HQ-1_MTP RSVP agent media resource. Branch phones have media resource group list BR_MRGL applied. This media resource group list includes a media resource group BR_RSVP_MRGL, which includes the BR-1_MTP RSVP agent media resource.

Regions, although not shown in this figure, are configured so that G.729 has to be used for calls between headquarters phones and branch phones.

Configuration Procedure for Implementing RSVP-Enabled Locations-Based CAC

The implementation of CUCM RSVP-enabled locations involves the following steps:

- Step 1.** Configure RSVP service parameters.
- Step 2.** Configure RSVP agents in Cisco IOS.
- Step 3.** Add RSVP agents to CUCM.
- Step 4.** Enable RSVP between location pairs.

- Step 5.** Configure media resource groups.
- Step 6.** Configure media resource group lists.
- Step 7.** Assign media resource group lists to devices.

Because implementation of media resource groups and media resource group lists (Steps 5 to 7) are discussed in detail in the *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) Foundation Learning Guide* and have been used in earlier chapters, only Steps 1 to 4 are described here.

Step 1: Configure RSVP Service Parameters

The following important RSVP service parameters can be configured:

- **Default Inter-Location RSVP Policy:** This parameter sets the clusterwide default RSVP policy. You can set this service parameter to one of the following values:
 - **No Reservation:** No RSVP reservations get made between any two locations.
 - **Optional (Video Desired):** A call can proceed as a best-effort, audio-only call if failure to obtain reservations for both audio and video streams occurs. The RSVP agent continues to attempt an RSVP reservation for audio and informs CUCM if the reservation succeeds.
 - **Mandatory:** CUCM does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream.
 - **Mandatory (Video Desired):** A video call can proceed as an audio-only call if a reservation for the audio stream succeeds but the reservation for the video stream does not succeed.
- **RSVP Retry Timer:** This parameter defines the interval in seconds after which the RSVP agent retries the reservation if a failure occurs. If you set this parameter to 0, you disable RSVP retry on the system. If the RSVP policy is optional, the call can still proceed even if an RSVP failure occurs during call setup. An RSVP failure indicates insufficient bandwidth at the time of setup, so the call is likely to begin with poor voice quality. However, this condition may be transient, and the automatic reservation retry capability may succeed during the course of the call, at which point adequate bandwidth will be assured for the remainder of the call. The CUCM administrator can configure the icon or message displayed to the user. It should convey something like, “Your call is proceeding despite network congestion. If you experience impaired audio quality, you may want to try your call again later.” If reservation retry succeeds, the icon or message should be removed or replaced by one that conveys a return to normal network conditions and assured audio quality.
- **Mandatory RSVP Mid-Call Retry Counter:** This parameter specifies the mid-call RSVP retry counter when the RSVP policy specifies Mandatory and when the mid-call error-handling option “Call fails following retry counter exceeds” is set. The

default value specifies one time. If you set the service parameter to -1, retry continues indefinitely until either the reservation succeeds or the call gets torn down.

- **Mandatory RSVP Mid-Call Error-Handling Option:** This parameter specifies how a call should be handled if the RSVP reservation fails during a call. You can set this service parameter to the following values:
 - **Call Becomes Best Effort:** If RSVP fails during a call, the call becomes a best-effort call. If retry is enabled, RSVP retry attempts begin simultaneously.
 - **Call Fails Following Retry Counter Exceeded:** If RSVP fails during a call, the call fails after n retries of RSVP if the Mandatory RSVP Mid-Call Retry Counter service parameter specifies n.

Table 9-1 shows the interaction of these policy settings.

Figure 9-10 shows the configuration of the previously described service parameters. It also shows the service parameters that are used to set the Differentiated Services Code Point (DSCP) values that should be used for the RTP packets of calls for which RSVP failed. These parameters can be audio channel (for which RSVP failed at the call setup if the policy was set to Optional) or video or audio channel (if the RSVP failure occurs mid-call and the Mandatory RSVP Mid-Call Error-Handling Option is set to Call Becomes Best Effort).

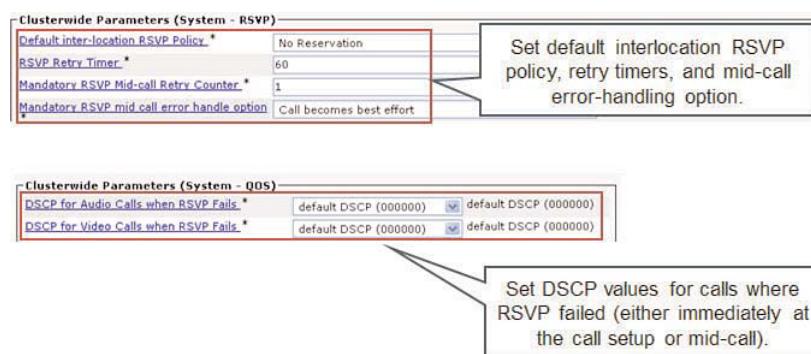


Figure 9-10 Step 1: Configure RSVP Service Parameters

You can configure all these service parameters from **Cisco Unified CM Administration** by choosing **System > Service Parameters** and selecting your CUCM server and the **Cisco CallManager (Active)** service. All these parameters are clusterwide, which means that they apply to all servers in the cluster running the **Cisco CallManager** service.

Table 9-1 *RSVP Policy Settings*

RSVP Policy	When Reservation Failure (Non-Multilevel Precedence and Preemption [MLPP]) Occurs	Mandatory RSVP Mid-Call Error Handling	Mandatory RSVP Retry Counter	Behavior/ Call Result
Mandatory	Audio or video RSVP failure in initial call setup	—	—	Call rejected
Mandatory	Audio or video RSVP failure in mid-call	Call fails following n retry counter exceeded		Call released if reservation does not succeed after n retries
Mandatory	Audio or video RSVP failure in mid-call	Call becomes best effort	n	Call proceeds as best effort, and reservation is retried infinitely
Mandatory (video desired)	Audio RSVP failure in initial call setup	—	—	Call rejected
Mandatory (video desired)	Video RSVP failure in initial call setup	—	—	Call proceeds as audio-only
Mandatory (video desired)	Audio RSVP failure in mid-call	Call fails following n retry counter exceeded		Call released if reservation does not succeed after n retries
Mandatory (video desired)	Video RSVP failure in initial call setup	—	—	Call proceeds as audio-only
Mandatory (video desired)	Audio RSVP failure in mid-call	Call becomes best effort	n	Call proceeds; audio stream in call becomes best effort if reservation does not succeed after n retries

Table 9-1 *RSVP Policy Settings*

RSVP Policy	When Reservation Failure Occurs	Mandatory RSVP Mid-Call Error Handling	Mandatory RSVP Retry Counter	Behavior/ Call Result
Mandatory (video desired)	Video RSVP failure in mid-call	Call fails following retry counter exceeded	n	Call proceeds as audio-only
Mandatory (video desired)	Video RSVP failure in mid-call	Call becomes best effort	n	Call proceeds; video stream in call becomes best effort if reservation does not succeed after n retries
Optional (video desired)	Audio or video RSVP failure in initial call setup	—	—	Call proceeds as audio-only with best effort; RSVP is tried until reservation succeeds or call is torn down
Optional (video desired)	Audio or video RSVP failure in mid-call	—	—	Call proceeds as audio-only; if audio stream had reservation failure, it becomes best effort
Mandatory	Audio or video RSVP failure in initial call setup	—	—	Call rejected

Step 2: Configure RSVP Agents in Cisco IOS Software

Example 9-1 shows a portion of the configuration from `show running-config`, which demonstrates how to configure a Cisco IOS router to enable RSVP agent functionality.

Example 9-1 Step 2: Configure RSVP Agents in Cisco IOS Software

```

!
interface Loopback0
    ip address 10.5.9.1 255.255.255.255
!
sccp local Loopback0
sccp ccm 10.1.1.1 identifier 1 version 7.0+
sccp
!
sccp ccm group 1
    associate ccm 1 priority 1
    associate profile 1 register HQ-1_MTP
!
dspfarm profile 1 mtp
    codec pass-through
    rsvp
    maximum sessions software 20
    associate application SCCP
!
interface Serial0/1
    description IP-WAN
    ip address 10.1.4.101 255.255.255.0
    duplex auto
    speed auto
    ip rsvp bandwidth 40
!
```

As with other Cisco IOS-provided media resources, such as conference bridges and transcoders, the configuration starts with global Skinny Client Control Protocol (SCCP) settings, followed by the CUCM group configuration. Any functional IP address on the router may be chosen for SCCP. However, a loopback interface is a best practice (as shown in Example 9-1), because it is reliable by not being directly associated with any one physical interface. As previously mentioned, the SCCP CCM version is not the CUCM version; instead, it relates to the DSP version on the ISR. The configuration of the media resource is performed in **dspfarm profile** configuration mode. Three commands are specific to the implementation of a software MTP RSVP agent:

- **codec pass-through:** Specifies that the actual content of the RTP stream is not modified. Media resources usually have to interpret and modify the audio stream; examples are transcoders that change the codec of the audio stream, and hardware media termination points that are used to convert out-of-band signaling into in-band dual-tone multifrequency (DTMF). The RSVP agent repackages RTP only at Layers 3 and 4. It terminates the incoming call leg by decapsulating RTP and then reencapsulating the identical RTP into a new call leg. Because this simple repackaging does not require interpreting and modifying the audio payload, which is required with transcoders or hardware media termination points that are used for DTMF, the router can perform this function in software.

- **rsvp:** Specifies that this media termination point is used as an RSVP agent that will set up a call leg to another RSVP agent where RSVP with IntServ over DiffServ has to be used.
- **maximum sessions software sessions:** Specifies the maximum number of sessions for the media resource. Note that the keyword **software** is used. It indicates that this RSVP agent should not use DSPs but that it should perform its function in software: Using software MTP is possible only when codec pass-through has been configured.

After the MTP RSVP agent is set up, you must enable RSVP on the WAN interface or interfaces by using the **ip rsvp bandwidth bandwidth** command. The specified bandwidth determines how much bandwidth (in kbps) is allowed to be reserved by RSVP.

Note The bandwidth reserved for a call depends on the codec that is used. As with standard non-RSVP-enabled CUCM locations, it is 80 kbps for G.711 and 24 kbps for G.729. During call setup, however, the RSVP agent always requests an additional 16 kbps, which is released immediately after the RSVP reservation is successful. Therefore, the interface bandwidth has to be configured in such a way that it can accommodate the desired number of calls, considering the codec that will be used plus the extra 16 kbps. For example, if two G.729 calls are permitted on the interface, 64 kbps must be configured. For two G.711 calls, 176 kbps is required. In Example 9-1, only one G.729 call is permitted.

Note Because RSVP-enabled locations allow RSVP to be used between two RSVP agents that are between the two endpoints of a call, you need to configure at least two RSVP agents in a cluster to make it work. Both agents would be HQ-1 and BR-1, as shown in Figure 9-9. Example 9-1 is for the HQ-1 router.

Step 3: Add RSVP Agents to CUCM

After the RSVP agent function at the Cisco IOS gateway has been configured, the corresponding media resource has to be added to CUCM. Figure 9-11 shows how to add an RSVP agent in CUCM. In Cisco Unified CM Administration, choose **Media Resources > Media Termination Point** and click **Add New**.

In the Media Termination Point Configuration window, choose the type of the media termination point. Currently the only option is Cisco IOS Enhanced Software Media Termination Point. Enter a name and description, and then choose the device pool that should be used.

Note The name of the media termination point has to match the name that was configured at the Cisco IOS router with the **associate profile id register** command entered in **sccp ccm group id** configuration mode. The name is case-sensitive.

Media Termination Point Configuration

Status
(i) Status: Ready

Media Termination Point Information

Media Termination Point Type*	Cisco IOS Enhanced Software Media Termination P
Media Termination Point Name*	HQ-1_MTP
Description	HQ-1 RSVP Agent
Device Pool*	Default

Select media termination point type and device pool.
Enter media termination point name and description.

Figure 9-11 Step 3: Add RSVP Agents to CUCM

Note Because RSVP-enabled locations allow RSVP to be used between two RSVP agents that are between the two endpoints of a call, at least two RSVP agents have to be configured in a cluster to make it work. In our example, these would be HQ-1 and BR-1. Example 9-1 is an example for the HQ-1 router.

Step 4: Enable RSVP Between Location Pairs

After the RSVP agents in Cisco IOS routers are configured and added to CUCM, RSVP has to be enabled between one or more pairs of locations, as shown in Figure 9-12. This task is performed in the Location Configuration window, which can be accessed in CUCM by navigating to **Cisco Unified CM Administration** and choosing **System > Location**.

Choose the location for which RSVP should be enabled for calls to one or more other locations. In the Location Configuration window, under **Modify Setting(s) to Other Locations**, the currently configured location and all other locations are listed.

Choose the **Location** to which RSVP should be used, and then choose the **RSVP Setting**. The options are the same as those for the Default Inter-location RSVP Policy service parameter:

- **No Reservation:** No RSVP reservations get made between any two locations.
- **Optional (Video Desired):** A call can proceed as a best-effort, audio-only call if failure to obtain reservations for both audio and video streams occurs. The RSVP agent continues to attempt an RSVP reservation for audio and informs CUCM if the reservation succeeds.
- **Mandatory:** CUCM does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream as well.

- **Mandatory (Video Desired):** A video call can proceed as an audio-only call if a reservation for the audio stream succeeds but a reservation for the video stream does not succeed.

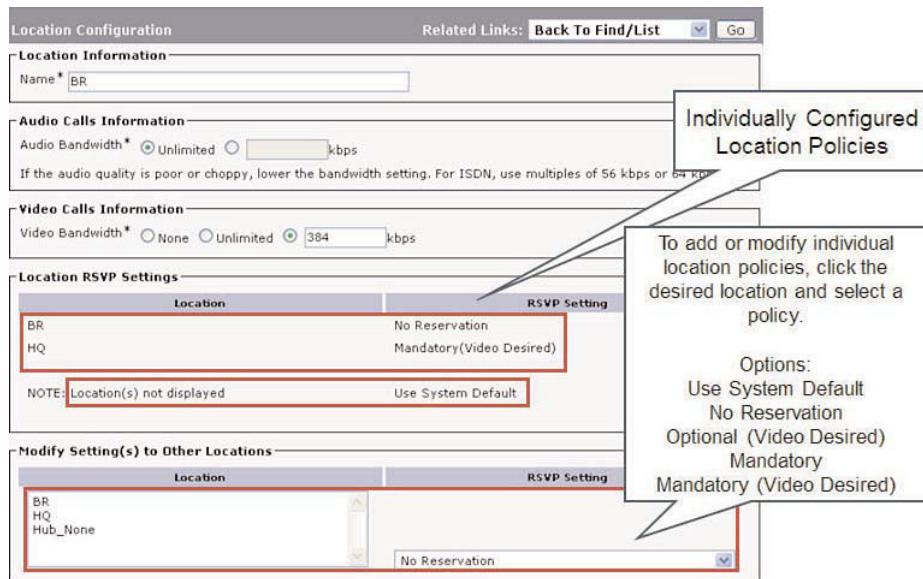


Figure 9-12 Step 4: Enable RSVP Between Location Pairs

In addition, the option Use System Default applies the value of the Default Inter-Location RSVP Policy service parameter for calls to the chosen location.

After you click Save, the changes are displayed in the Location RSVP Settings part of the window. Only locations that are *not* configured to use the system default are listed.

Note RSVP can also be enabled within a location. For the currently configured location, Use System Default is not an option. Only No Reservation, Optional (Video Desired), Mandatory, or Mandatory (Video Desired) can be chosen within a location. The default for calls to Own Location is No Reservation, and to all other locations the default is Use System Default.

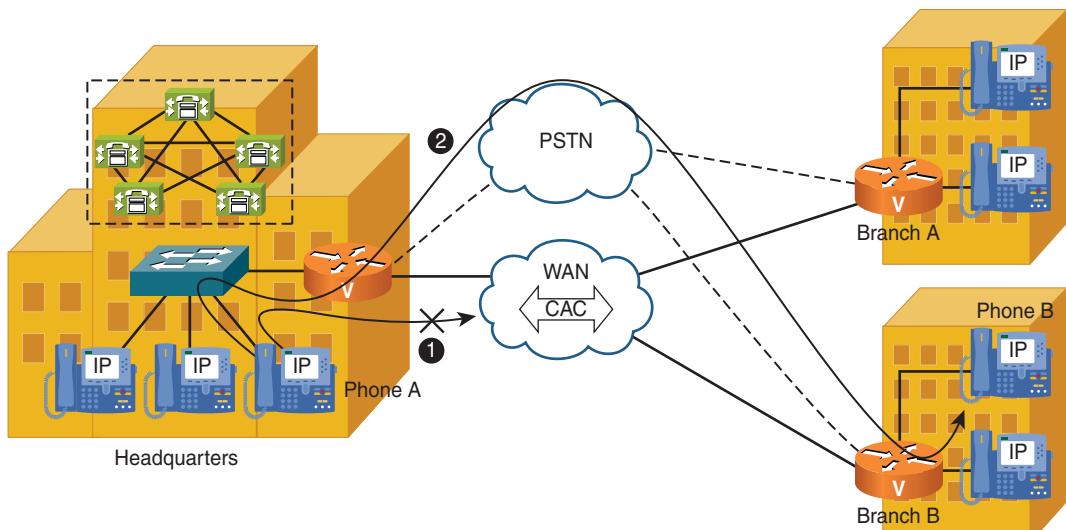
Note When RSVP-enabled locations are used, it is extremely important that the phones use the appropriate RSVP agent. There will be three call legs: The calling phone to its RSVP agent, between the RSVP agents, and the remote RSVP agent to the called phone.

CUCM determines which RSVP agent should be used by a given phone based solely on the media resource group lists assigned to the phones that attempt to establish a call. Errors in the media resource group list configuration can result in suboptimal traffic flows.

Therefore, proper assignment of phones to RSVP agents, by using Media Resource Group Lists (MRGL) and Media Resource Groups (MRG), is extremely important when RSVP-enabled locations are implemented. The sample scenario at the beginning of this configuration section provides all the information needed for how to assign the RSVP agents to the phones. Further configuration of MRGLs and MRGs is covered in detail in the book *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1)*.

Automated Alternate Routing

As illustrated in Figure 9-13, AAR allows calls to be rerouted through the PSTN using an alternate number when CUCM blocks a call because of insufficient location bandwidth from CAC. With AAR, the caller does not need to hang up and redial the called party. Without AAR, the user gets a reorder tone, and the IP Phone displays “Not enough bandwidth.” The administrator can change this Cisco IP Phone display message in CUCM to a different text response.



- ① – Cisco Unified Communications Manager CAC blocks a call over the IP WAN.
- ② – The call is automatically rerouted over the PSTN.

Figure 9-13 AAR Overview

AAR applies to centralized call-processing deployments for internal calls within the same CUCM cluster. For example, if a Cisco IP Phone at company headquarters calls a Cisco IP Phone in branch B, and the available bandwidth for the WAN link between the branches is insufficient as computed by the locations mechanism, AAR can reroute the call

through the PSTN. The audio path of the call would be IP-based from the calling phone to its local headquarters PSTN gateway, time-division multiplexing (TDM)-based from that gateway through the PSTN to the branch B gateway, and IP-based from the branch B gateway to the destination IP Phone.

AAR is transparent to users. It can be configured so that users dial only the four-digit directory number of the called phone without any other user input to reach the destination through an alternative network, such as the PSTN. Digit manipulation through the PSTN must be appropriately configured because four digits will not be routable in the PSTN.

In Figure 9-13, a call is placed from Phone A to Phone B, but the locations-based CAC denies the call because of insufficient bandwidth. With AAR, CUCM now *automatically* composes the required route pattern to reach Phone B via the PSTN and sends the call off-net.

AAR Characteristics

AAR provides a fallback mechanism for calls denied by locations-based CAC or RSVP-enabled locations-based CAC by rerouting calls over the PSTN in the event of CAC failure. AAR is not a feature of Survivable Remote Site Telephony (SRST).

AAR works only for calls placed to internal directory numbers. It does not apply to calls placed to route patterns or feature patterns such as MeetMe or Call Park. However, it does work for hunt pilots and computer telephony interface (CTI) ports. These entities can be configured with an AAR group and an AAR Calling Search Space (CSS).

The alternative number used for the PSTN call is composed of the dialed directory number, a prefix configured per AAR source and destination group, and the external phone number mask of the called device.

Alternatively, calls can be routed to voice mail, or an AAR destination mask can be configured per device that allows any number to be used for the rerouted call. The number specified at the AAR destination mask is also known as the Call Forward No Bandwidth (CFNB) destination.

Note AAR is a fallback mechanism for calls that are denied by locations-based CAC or RSVP-enabled locations-based CAC. It does not apply to voice calls that are denied by gateways because they exceed the available or administratively permitted number of channels. It also does not apply to calls that have been rejected on trunks, such as gatekeeper-controlled H.225 or intercluster trunks. If such calls fail for any reason, fallback mechanisms are provided by route lists and route groups.

AAR is invoked only when the locations-based CAC denies the call because of a lack of network bandwidth. AAR is not invoked when the IP WAN is unavailable or other connectivity issues cause the called device to become unregistered with CUCM. In such cases, the calls are redirected to the target specified in the Call Forward No Answer field of the called device.

AAR Example Without Local Route Groups and Globalized Numbers

Figure 9-14 shows an example of AAR when globalized call routing and local route groups are not being used.

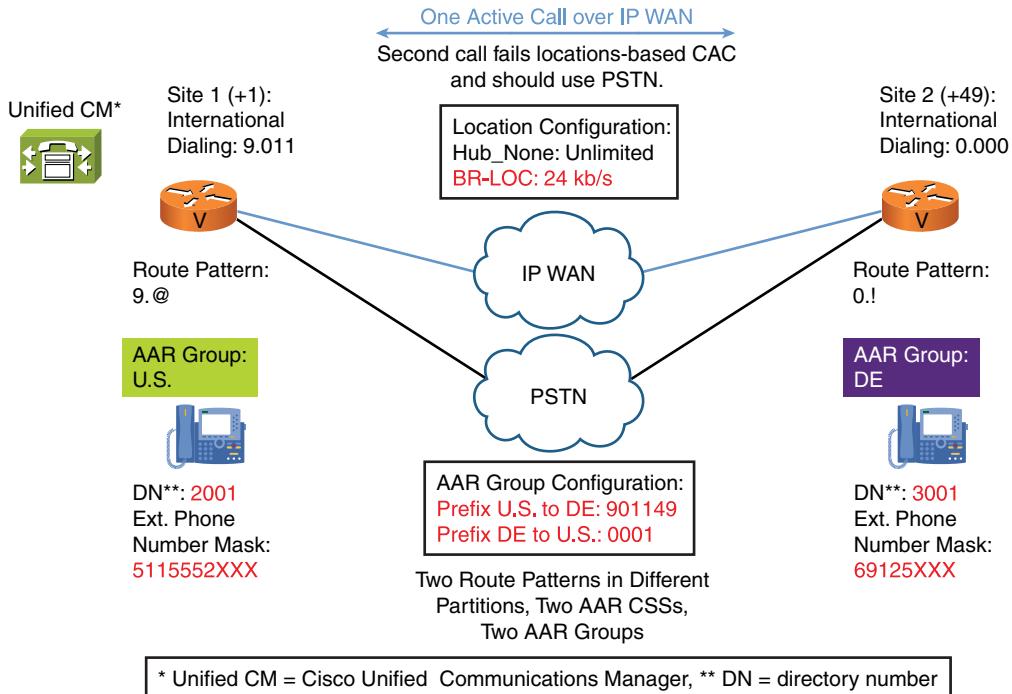


Figure 9-14 AAR Example Without Local Route Groups and Globalized Numbers

There are two sites: one in the United States and the other one in Germany (country codes 1 and 49). At site 1 (country code 1), the access code is 9; at site 2 (country code 49), the access code is 0. Both countries use ten-digit numbers. There are two route patterns: 9. @ for site 1 and 0.! for site 2. Each route pattern is in a site-specific partition, and the phones use site-specific CSSs.

From the perspective of AAR, U.S. phones are configured with a ten-digit external phone-number mask, and phones at the Germany location use national format for the external phone-number mask. U.S. phones are in AAR group U.S., and German phones are in AAR group DE. AAR prefixes are configured as follows:

- Prefix from AAR group U.S. to AAR group DE: 901149
- Prefix from AAR group DE to AAR group U.S.: 0001

The AAR CSS of U.S. phones has access to the 9. @ route pattern; the AAR CSS of German phones has access to the 0.! route pattern.

When a call from a U.S. phone to a German phone is not admitted because of no available bandwidth, the external phone-number mask of the German phone is merged with the DN of the phone. (In this case, the result is 691253001.) Then, the prefix 901149 configured from AAR group U.S. to DE is appended, resulting in a call to 901149691253001, which is processed by the 9.@ route pattern that refers to the U.S. gateway.

In the other direction, an AAR call from a German phone to a U.S. phone composes a dial string of 00015115552001, which is the format used for international calls to the United States. It matches the 0.! route pattern and is sent out using the German gateway.

In summary, this two-site example requires two route patterns in different partitions, two AAR CSSs, and two AAR groups. In a large, worldwide deployment with lots of different numbering plans, the configuration of AAR groups can be complex.

AAR Example with Local Route Groups and Globalized Numbers

Figure 9-15 shows an AAR example where globalized call routing and local route groups are used.

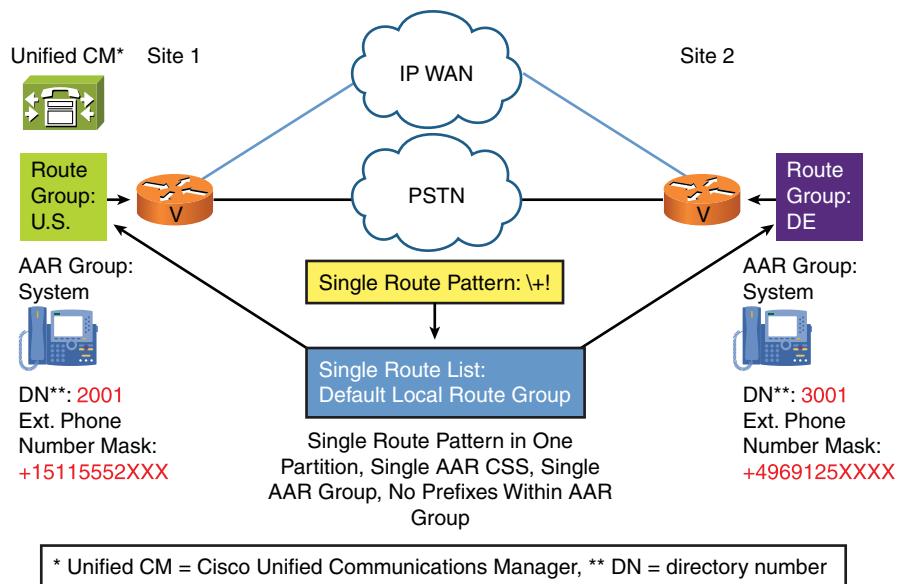


Figure 9-15 AAR Example with Local Route Groups and Globalized Numbers

If the AAR destination mask is entered in the globalized form, and if every AAR CSS is able to route calls to destinations in the globalized form, system administrators can forego the configuration of AAR groups, because their sole function is to determine which digits to prefix based on the local requirements of the PSTN access of the calling phone to reach the specific destination.

With globalized call routing, CUCM can route calls to the PSTN in E.164 format with a + prefix. When you configure the external phone-number mask in this format, no prefixes are required for AAR. To localize the called- and calling-party numbers, implement global transformations for each egress PSTN gateway (like for normal PSTN calls).

Without local route groups, the AAR CSS routes the call through the collocated gateway of the calling phone by matching a site-specific route pattern that refers to a site-specific route list, route group, and gateway. When local route groups and globalized call routing are implemented, the egress gateway does not need to be selected by site-specific AAR CSS, because the egress gateway is determined by the local route group feature.

In summary, when you use globalized call routing with local route groups, AAR implementation is extremely simple: Only a single AAR CSS and AAR group are required and applied to all phones, regardless of their location.

In Figure 9-15, all phones are in the same AAR group (System). No prefix is configured for calls within this single AAR group. There is a single route pattern in E.164 format: \+!. The route pattern refers to the only configured route list, which is configured to use the local route group. Each gateway is referenced from a site-specific route group. U.S. phones use a U.S.-specific device pool with the local route group set to U.S., and German phones use a device pool specific to their country, where the local route group refers to the DE route group. The external phone-number mask in globalized format is +15115222xxxx at U.S. phones and +4969125xxxx at German phones. The AAR CSS is the same for both phones and provides access to the \+! route pattern.

When a call from a U.S. phone to a German phone is not admitted because of no available bandwidth, the external phone-number mask of the German phone is merged with the directory number of the phone (in this case, the result is +49691253001). No AAR prefix is added, so a call is placed to that number. It matches the \+! route pattern, and the local route group is to be used. Therefore, the call is sent to the U.S. gateway, where the called number can be localized by using called-party transformation settings (that is, the number is changed to 49691253001 with a number type of international) that are configured at the gateway.

The same thing happens for calls in the other direction. As a result, +15115552001 is called, and after the called number is localized at call egress—again provided by global transformations at the gateway—a call with a number type of international is placed to 15115552001 (this time through the German gateway).

AAR Considerations

You must consider several important points when implementing AAR. AAR supports the following call scenarios:

- The call originates from an IP Phone within one location and terminates at an IP Phone within another location.
- An incoming call through a gateway device within one location terminates at an IP Phone within another location.

AAR does *not* work with SRST. AAR is activated only after a call is denied by CAC, not by WAN failures.

Using globalized call routing substantially simplifies the implementation of AAR, especially in international deployments.

AAR does not support CTI route points as the origin or destination of calls, and AAR is incompatible with Cisco Extension Mobility for users who roam to different sites.

Note When tail-end hop-off (TEHO) is used, it is important to configure the AAR CSS in such a way that the local gateway is always used for calls being rerouted by using AAR. Calls will fail otherwise, because the call leg to the remote PSTN gateway again runs into the same issue as the initial call: It needs to go over the IP WAN. This typically means it goes out of the location of the originating phone, but doing that is impossible, because no bandwidth is left for the location. This is why the initial call ends up in a CAC failure.

AAR Configuration Procedure

The implementation of AAR involves the following steps:

Step 1. Configure AAR service parameters (Cisco CallManager service).

Step 2. Configure partitions and CCSs.

Step 3. Configure AAR groups.

Step 4. Configure phones for AAR:

a. Apply AAR CSS and (source) AAR group to IP Phones.

b. Configure IP Phone directory number(s):

 Apply (destination) AAR group.

 Set individual AAR destination mask (CFNB).

 Forward to voice mail no bandwidth.

Step 2 is discussed in detail in the book *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1)*.

You need to precisely design partitions and AAR CSS. The AAR CSS of the calling device must include the partition that is necessary to route the redirected call. The call is routed to the number that is composed of the destination directory number, external phone number mask, and AAR prefix (according to the AAR group configuration). If you configure an individual AAR destination mask or forward to voice mail, the AAR CSS has to provide access to these numbers (numbers that are composed of the called directory number and AAR destination mask or voice-mail pilot number).

As previously mentioned, in globalized call routing, AAR configuration is simpler when you use the globalized format at the external phone number mask.

Step 1: Configure AAR Service Parameters

Figure 9-16 shows how to enable AAR and set AAR-related parameters. In Cisco Unified CM Administration, choose System > Service Parameters > Cisco CallManager.

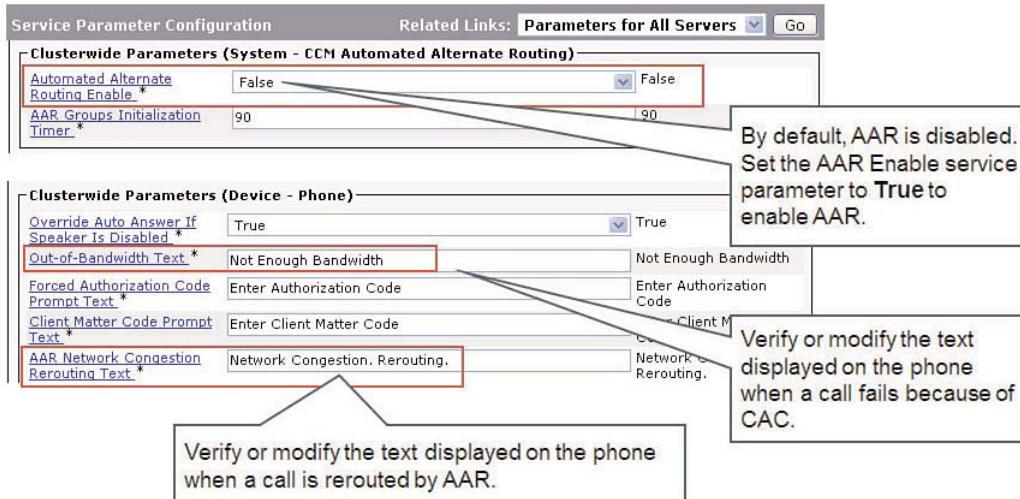


Figure 9-16 Step 1: Configure AAR Service Parameters

You enable AAR by setting the CUCM service parameter Automated Alternate Routing Enable to True. False is the default.

Another AAR-related service parameter is Out-of-Bandwidth Text, where you can specify the text that is displayed on an IP Phone when a call fails because of lack of available bandwidth. With the AAR Network Congestion Rerouting Text parameter, you specify the text that is displayed on an IP Phone when AAR reroutes a call.

Step 2: Configure Partitions and CSSs

The configuration of partitions and CSS is covered in *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1)*.

Step 3: Configure AAR Groups

As shown in Figure 9-17, you configure AAR groups from CUCM in Cisco Unified CM Administration, Call Routing > AAR Groups. Each added AAR group can be configured with a dial prefix for its own group and two dial prefixes for each of the other AAR groups. Configure one for calls going to the other group and one for calls being received from the other group.

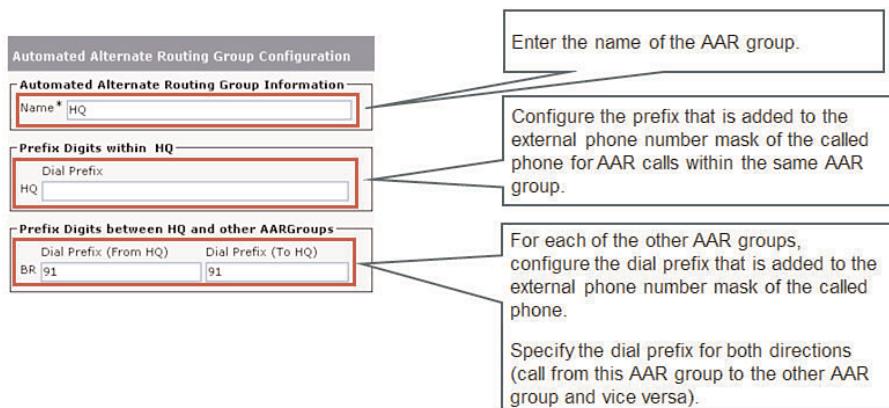


Figure 9-17 Step 3: Configure AAR Groups

In Figure 9-17, there are only two AAR groups. For AAR calls from HQ to BR, a prefix of 0001 is used. For calls in the other direction, a 901149 prefix is used. The AAR configuration that is shown fits a scenario where the HQ site is in Germany and the BR site is in the United States. The external phone-number mask at both sites would use national format.

As a result, an AAR call from Germany to the United States would be placed to 0001 followed by the national number (10 digits). 0 is the PSTN access code in Germany, 00 is the international access code, and 1 is the country code for the United States. An AAR call from the United States to Germany would be placed to the national number of a Germany phone that is prefixed with 901149. 9 is the PSTN access code in the United States, 011 is the international access code, and 49 is the country code of Germany.

Tip The configuration shown in Figure 9-17 does not use globalized call routing. Globalized call routing is recommended in larger multisite environments, especially in international deployments. With globalized call routing, all sites use the same AAR group and no prefixes are required within that group. The external phone number mask is specified in globalized format (E.164 number with + prefix).

Step 4: Configure Phones for AAR

Configure phones for AAR by navigating to **Cisco Unified CM Administration** and choosing **Call Routing > Phone**, as shown in Figure 9-18.

When enabling AAR on a phone, the Phone Configuration window has two possible settings:

- **AAR Calling Search Space:** This CSS is used if a call that originated at this phone is rerouted using AAR.

- **AAR Group:** The AAR group of the phone is the source AAR group, while the AAR group that was set at the directory number is the destination AAR group. It is important to understand this distinction for the configuration of AAR prefixes, because they are configured separately for each pair of AAR source and destination group. If no AAR group is set at the phone, the AAR group of the directory number is used as the AAR source group for this phone.

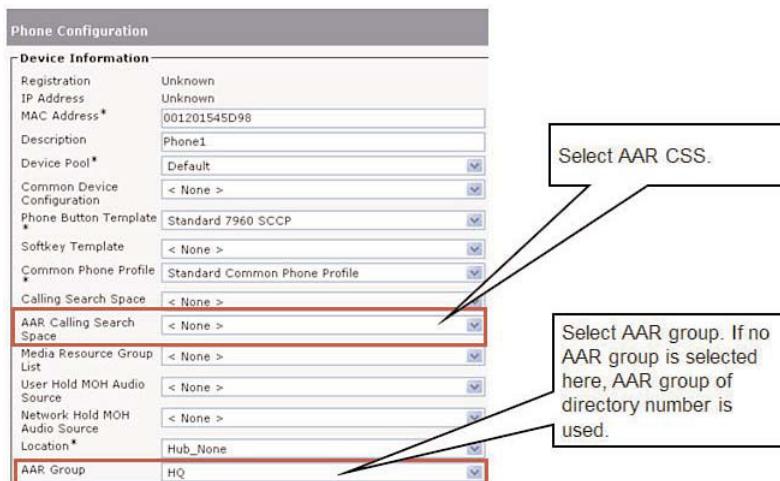


Figure 9-18 Step 4: Configure Phones for AAR

The IP Phone directory numbers in the selected phone must be configured for AAR, as shown in Figure 9-19.

The relevant settings in the Directory Number Configuration window are as follows:

- **Voice Mail:** If this option is activated, calls to this phone are forwarded to voice mail if this directory number cannot be reached because of locations-based CAC.
- **AAR Destination Mask:** If this is set, it is the number where calls are rerouted if this directory number cannot be reached because of locations-based CAC. Because this setting is configured per directory number, it allows *any* destination to be specified. If the mask does not contain *n* wildcard digits, calls are rerouted to the specified number without considering any digits of the directory number. Therefore, this setting is often called CFNB.
- **AAR Group:** An AAR group at the directory number must be set to allow AAR calls to this directory number. The AAR group that is configured at the directory number is the destination AAR group.
- **External Phone Number Mask:** The external phone number mask of the directory number. It should always be set, because it is used by other features, such as digit manipulation at route patterns or route lists.

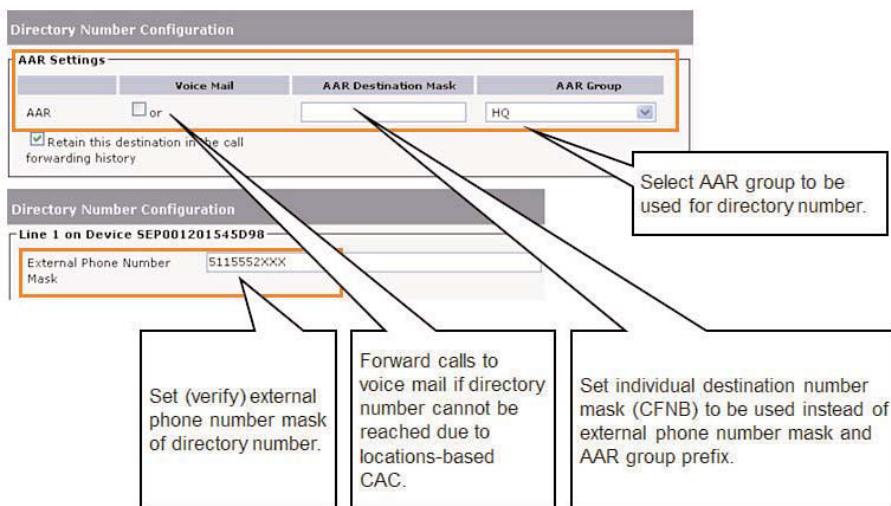


Figure 9-19 Step 4: Configure Phones for AAR, Continued

SIP Preconditions

This topic describes SIP Preconditions and how it is used in CUCM to implement RSVP-based CAC for calls through SIP trunks.

The CUCM implementation of SIP Preconditions is based on RFC 3312, “Integration of Resource Management and SIP,” and RFC 4032, “Update to the Session Initiation Protocol (SIP) Preconditions Framework.” These RFCs describe several types of precondition signaling. CUCM currently supports only precondition signaling for RSVP.

SIP Preconditions applies to SIP trunks and, hence, applies to calls going out of the cluster. Like RSVP-enabled locations, it allows RSVP agents to be used for calls through SIP trunks. It is therefore also referred to as *intercluster RSVP*.

Another term that refers to SIP Preconditions is *end-to-end RSVP*. This term does not mean that RSVP is implemented in the actual endpoints (IP Phones), but it refers to inter-cluster calls. Before SIP Preconditions, intercluster calls using SIP were able to use only local RSVP within a cluster. In this case, an RSVP agent associated with the IP Phone, and another RSVP agent associated with the SIP trunk are used. Such a configuration requires that the phone and trunk be in separate locations, and RSVP needs to be enabled between these two locations. These two RSVP agents, however, were both local to the CUCM cluster and, hence, were not spanning to the other end of the cluster. With SIP Preconditions, RSVP can be used between both ends of the SIP trunk; hence, the name *end-to-end RSVP*.

SIP Preconditions is not limited to intercluster trunks (that is, calls between two CUCM clusters). It can also be used for SIP trunks to CUCME, Cisco IOS gateways, and Cisco Unified Border Elements (CUBE).

CAC Without SIP Preconditions

When not using SIP Preconditions, as shown in Figure 9-20, you can only use RSVP within the local CUCM cluster. Such an implementation is like RSVP-enabled locations, as discussed earlier, except that the two devices involved in the local CUCM cluster are an IP Phone and a SIP trunk (or two SIP trunks).

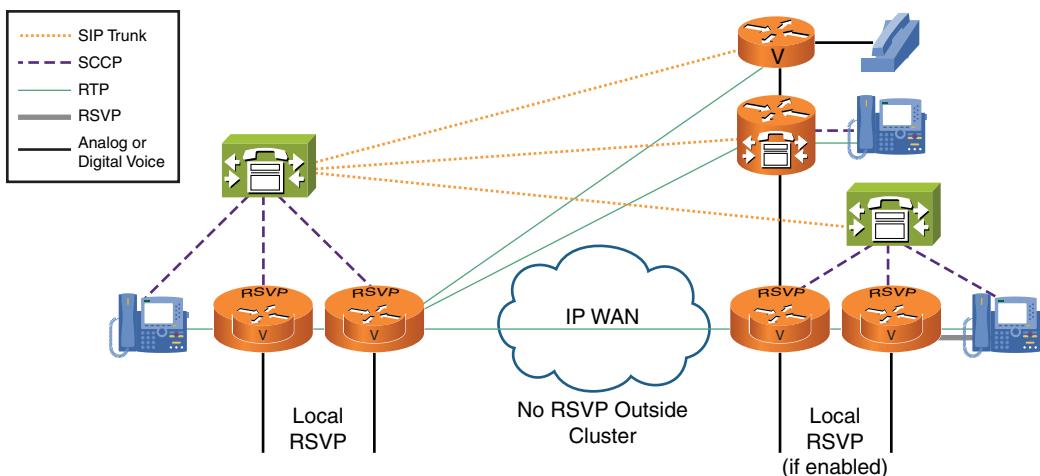


Figure 9-20 CAC Without SIP Preconditions

The IP Phone and SIP trunk are in different locations, and RSVP is enabled between these two locations. The IP Phone refers to its RSVP agent by its MRGL, and the SIP trunk refers to its RSVP agent by its MRGL. RSVP CAC applies between these two RSVP agents. Because all devices are local to the CUCM cluster, this implementation model is called *local RSVP*. If another CUCM cluster is at the other end of the SIP trunk, local RSVP can also be used at that end. The call leg between the two RSVP agents associated with the SIP trunk at each cluster, however, is not subject to RSVP. Therefore, there is no end-to-end RSVP in this case.

If the other end of the SIP trunk is a third-party device, a Cisco IOS SIP gateway, or CUCME, local RSVP applies only to the end of the SIP trunk where CUCM is used.

CAC with SIP Preconditions

Figure 9-21 shows an implementation of end-to-end RSVP-based CAC for SIP trunks with SIP Preconditions.

When both ends of a SIP trunk support SIP Preconditions, the IP Phone and the SIP trunk are in different locations, and RSVP is enabled between these two locations, then end-to-end RSVP is used. As a result, only the RSVP agent associated with the IP Phone

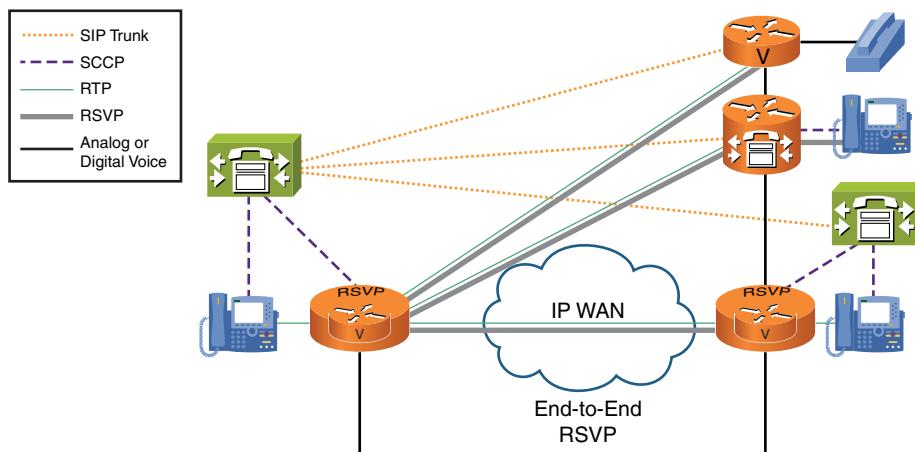


Figure 9-21 CAC with SIP Preconditions

is invoked; no second local RSVP is involved. The RSVP agent of the phone now uses RSVP-based CAC toward the other end of the SIP trunk.

If the other end is another CUCM cluster, the same result happens at that far end—only one RSVP agent is invoked. If the other end is a Cisco IOS router, that router (either CUCME or a Cisco IOS SIP gateway) terminates RSVP at the far end.

With SIP Preconditions, RSVP is now virtually end-to-end. It spans the two call-routing domains and is not limited to the local cluster.

Note Because of proprietary extensions, SIP Preconditions for RSVP-enabled CAC is currently supported only between CUCM, CUCME, and Cisco IOS SIP gateways. Third-party SIP devices are currently not supported.

SIP Preconditions Operation

A call with SIP Preconditions follows the message sequence of RFC 3312 to establish a precondition. Here is a summary of the session-establishment phases:

1. The originating IP Phone places a call to a destination that is reachable through a SIP trunk. According to the location configuration at the originating IP Phone location, RSVP has to be used between the location of the originating IP Phone and the SIP trunk where the call should be routed to.
2. The originating CUCM sends a SIP INVITE message with Session Description Protocol (SDP). The IP address for the media stream in the SDP is set to the IP address of the originating RSVP agent. RSVP is requested in the SDP.
3. The terminating device (for example, a CUCM server of another cluster) responds with a SIP SESSION PROGRESS message with SDP. It provides the IP address of the

terminating RSVP agent, confirms the RSVP request for the forward direction, and sends an RSVP request for the reverse direction.

4. The negotiation of SIP Preconditions for RSVP CAC is completed by SIP PRACK, UPDATE, and OK messages. Then, each of the two RSVP agents attempts an RSVP reservation for its forward direction (that is, toward the other RSVP agent) of the preconditioned bandwidth.
5. If the RSVP reservation is successful, a standard call setup is performed by SIP RINGING, OK, and ACK messages.
6. When the call is answered, the terminating CUCM requests a renegotiation of media capabilities by sending a SIP INVITE message without SDP.
7. The originating CUCM responds with a SIP OK message with SDP. The complete set of supported media capabilities is included in the SDP.
8. The receiving CUCM sends a SIP OK with SDP message, including the selected codec. This codec is now actually used for the end-to-end call.
9. If the selected codec has bandwidth requirements that are different from the requirements used during the SIP Preconditions phase, the RSVP reservation is updated accordingly.
10. The call is now established with three call legs (like with RSVP-enabled locations for calls within a cluster):
 - The call leg between the originating IP Phone and its RSVP agent, where no RSVP-based CAC was performed
 - The middle call leg between the two RSVP agents, where RSVP-based CAC was performed, as previously described
 - The call leg between the terminating IP Phone and its associated RSVP agent, where again no RSVP-based CAC was performed

Note Standard locations-based CAC is performed between the IP Phones and their associated RSVP agents. As a result, the call leg from the IP Phone to its RSVP agent is counted against the maximum bandwidth that is configured at the locations that are applied to the IP Phone and to the RSVP agent.

SIP Preconditions Call Flow Summary

Figure 9-22 illustrates a summarized call flow for SIP Preconditions calls.

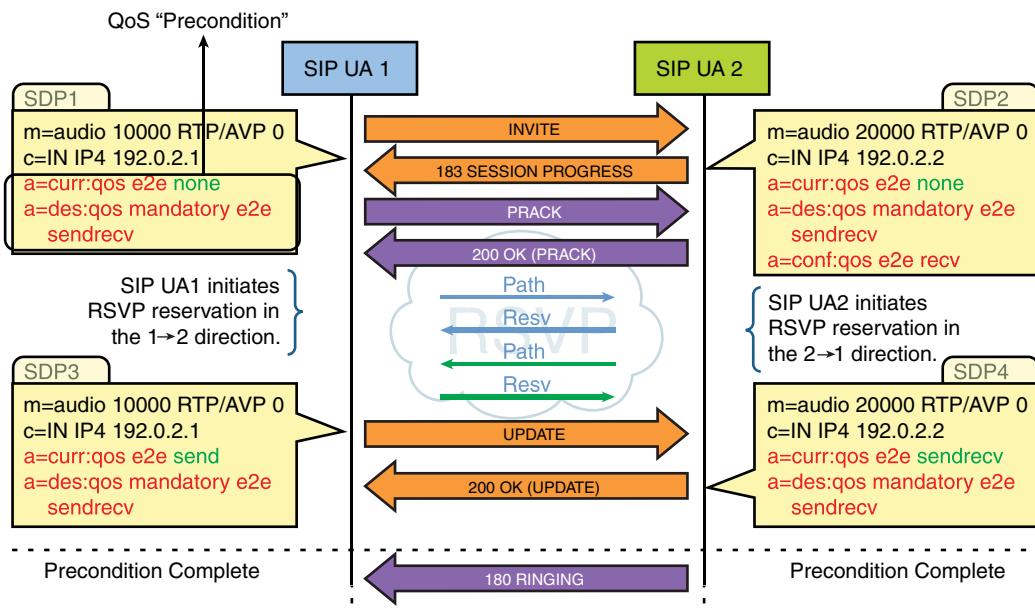


Figure 9-22 SIP Preconditions Call Flow Summary

Figure 9-22 shows the most important components of the first phase of the call setup over a SIP trunk configured for SIP Preconditions. The sequence occurs as follows:

1. The phase starts with the initial INVITE message with the IP address of the originating RSVP agent and the request for RSVP CAC in the SDP.
2. It shows the 183 response message, which confirms the received RSVP CAC request in its SDP. The SDP further includes the IP address of the terminating RSVP agent and the request for RSVP CAC for the reverse direction.
3. This negotiation is completed by the PRACK message, which is sent from the originating side toward the terminating side.
4. RSVP reservations are set up by each RSVP agent for the direction to the other RSVP agent by using RSVP PATH and RSVP Resv messages.
5. The originating side informs the terminating side about the successful RSVP reservation in the SDP of an UPDATE message.
6. The terminating side confirms this information in an OK message with SDP, which includes the same status information for the other direction.
7. The precondition phase is now complete, and the terminating device can send a RINGING message to the originating side.
8. When the call is answered, as shown in Figure 9-23, the terminating side sends an OK message that is confirmed from the other side with an ACK message.

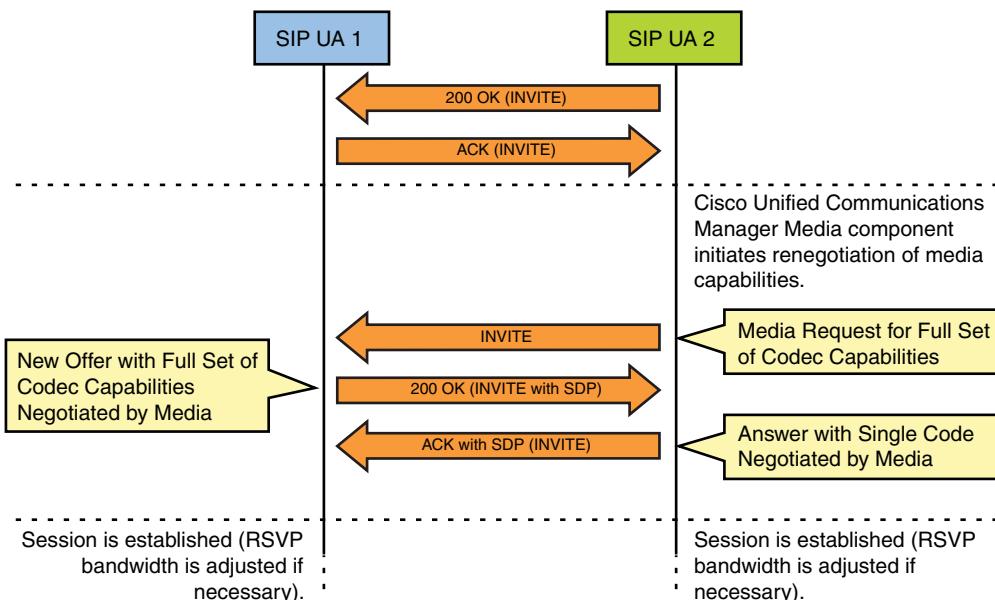


Figure 9-23 SIP Preconditions Call Flow Summary, Continued

9. Now, where the call is formally set up, the terminating side triggers a renegotiation of media capabilities with an INVITE message with no SDP attached.
10. The originating side sends an OK message, including the capabilities of the end device, in its SDP.
11. The terminating side selects a codec and informs the originating side with an ACK message with an attached SDP, including the selected capabilities (codec, packetization size, and so on).
12. If needed, RSVP reservations are updated between the two RSVP agents.

Fallback from End-to-End RSVP to Local RSVP

You can configure QoS fallback to use local RSVP when end-to-end RSVP is not supported by the far end. Fallback applies only in the case where the far end does not support SIP Preconditions. If it supports SIP Preconditions and the RSVP reservation fails, there is no fallback to local RSVP.

If there is QoS fallback, the call is reattempted without SIP Preconditions. CAC reverts to local RSVP, which means that two cluster-internal RSVP agents are used. The call is split into three local call legs:

- One from the originating phone to its RSVP agent
- One from that RSVP agent to the RSVP agent that is associated with the SIP trunk

- One from the RSVP agent that is associated with the SIP trunk, toward the other call-routing domain (where the same action can happen in the case of CUCM)

However, the call leg between the two clusters or between the local cluster and the SIP device on the other end does not use RSVP-based CAC.

The configured RSVP policy determines how calls are processed in certain scenarios:

- When the far end does not support preconditions and QoS fallback is off, the call fails when the RSVP policy is Mandatory or Mandatory (Video Desired). When the RSVP policy is Optional (Video Desired), the call continues without RSVP.
- When the far end does not support preconditions and QoS fallback is on, the configured RSVP policy is applied to local RSVP.
- When preconditions fail on the far end, QoS fallback has no effect. Consequently, the call continues without RSVP when the RSVP policy is Optional (Video Desired), and the call fails when the RSVP policy is either Mandatory or Mandatory (Video Desired).
- When receiving an INVITE with no preconditions and QoS fallback is off, the call fails when the RSVP policy is Mandatory or Mandatory (Video Desired). When the RSVP policy is Optional (Video Desired), the call continues without RSVP.
- When receiving an INVITE with no preconditions and QoS fallback is on, the configured RSVP policy is applied to local RSVP.
- When receiving an INVITE with preconditions, and local QoS (instead of SIP Preconditions) is configured at the receiving SIP trunk, the call fails when the received RSVP policy is Mandatory. If the received RSVP policy is Optional and the local policy is No Reservation, the call proceeds with no RSVP. If the received RSVP policy is Optional, the locally configured policy is applied to local QoS.

In QoS fallback or local QoS configuration, the policies that are applied to local QoS are managed the same way that they are managed for intracluster calls with RSVP-enabled locations.

SIP Preconditions Configuration Procedure

The following steps describe the SIP Preconditions configuration procedure:

Step 1. Follow the standard procedure of RSVP-enabled locations:

- a. Configure RSVP service parameters.
- b. Configure RSVP agents in Cisco IOS Software.
- c. Add RSVP agents to Cisco Unified Communications Manager.
- d. Enable RSVP between location pairs.

- e. Configure Media Resource Groups.
- f. Configure Media Resource Group Lists.
- g. Assign Media Resource Group Lists to devices.

Step 2a. Configure the SIP profile.

Step 2b. Apply *the* SIP profile to trunk.

The configuration for SIP Preconditions is identical to the configuration of RSVP-enabled locations. In addition to the steps required for RSVP-enabled locations, you have to configure the SIP trunks that should use SIP Preconditions for end-to-end QoS.

Note The RSVP agent that is associated with the IP Phone is used for the call leg to the far-end SIP device. If QoS fallback is not enabled, the SIP trunk will never allocate an RSVP agent. If QoS fallback mode is enabled, two local RSVP agents are required in a fallback scenario: one for the IP Phone and one for the SIP trunk. Therefore, the MRGL at the SIP trunk is only required for QoS fallback mode or for when the SIP trunk is not configured for SIP Preconditions at all but is configured to use local QoS.

The first configuration step was described earlier and is not described again. Refer to the section “Configuration Procedure for Implementing RSVP-Enabled Locations-Based CAC” for a description of Step 1.

Step 2a: Configure SIP Profile

Figure 9-24 shows how to configure SIP Preconditions settings at a SIP profile. In Cisco Unified CM Administration choose Device > Trunk.

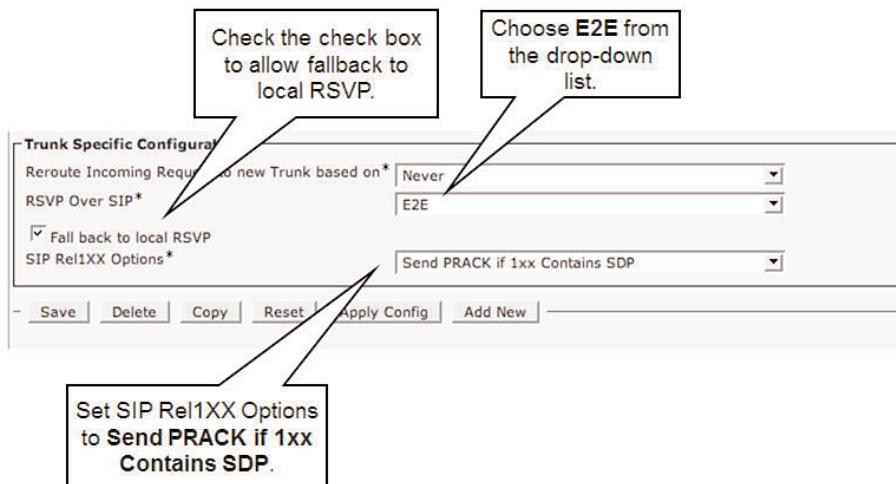


Figure 9-24 Step 2a: Configure SIP Profile

The necessary configuration for SIP Preconditions is applied to SIP trunks via SIP profiles. At the SIP profile, you have to set the SIP Rel1XX Options parameter to **Send PRACK if 1xx Contains SDP**.

Then, you have to set RSVP Over SIP to E2E (end-to-end) when you want to enable SIP Preconditions. If you want the trunk to use only local QoS, you would set the parameter to **Local QoS** instead of to E2E.

When SIP Preconditions is configured (RSVP Over SIP is set to E2E), you can check the check box **Fall back to local RSVP**. This option allows a fallback to local QoS if the far end does not support SIP Preconditions. If SIP Preconditions is supported by the far end and the RSVP reservation fails, there is no fallback to local RSVP.

Note When the other side of the SIP trunk is CUCM, there will never be a fallback to local RSVP. SIP Preconditions is never considered to be unsupported between two CUCM clusters, regardless of whether it has been enabled at the other side. As a consequence, SIP Preconditions always fails and never falls back to local RSVP in such a scenario.

When the other side of the SIP trunk is Cisco IOS device (for example, CUCME), and E2E RSVP is not enabled at that remote router, a fallback to local RSVP is performed, if configured at the local CUCM cluster. If E2E RSVP is not configured on a Cisco IOS device, SIP Preconditions is considered to be unsupported; therefore, local fallback is possible.

Step 2b: Apply SIP Profile to Trunk

Figure 9-25 shows you how to apply the previously configured SIP profile to a trunk. In Cisco Unified CM Administration choose Device > Trunk.

SIP Information	
Destination Address	<input type="text"/>
Destination Address IPv6	<input type="text"/>
<input checked="" type="checkbox"/> Destination Address is an SRV	
Destination Port*	5060
MTP Preferred Originating Codec*	711ulaw
Presence Group*	Standard Presence group
SIP Trunk Security Profile*	-- Not Selected --
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	-- Not Selected --
DTMF Signaling Method*	SIP-Preconditions
	Standard SIP Profile

Figure 9-25 Step 2b: Apply SIP Profile to Trunk

At the SIP trunk, set the SIP profile to the profile that you created earlier.

When the RSVP Over SIP parameter of the SIP profile is set to Local QoS, or fall back to local RSVP is enabled at the SIP profile, the SIP trunk needs to have an MRGL assigned so that it can allocate an RSVP agent for intracluster RSVP-enabled CAC. You can set the MRGL directly at the SIP trunk configuration page, which is located higher up from the SIP Information in Figure 9-25. If it is not set at the trunk, you must set the MRGL at the device pool that is applied to the SIP trunk.

H.323 Gatekeeper CAC

CUCM can connect to other CUCM clusters or to any other H.323 devices via H.323 trunks. H.323 trunks can be configured on their own without using a gatekeeper for address resolution and CAC, or as gatekeeper-controlled trunks. A gatekeeper is an optional H.323 Unified Communications device and is implemented on an ISR. Two types of gatekeeper-controlled trunks can be configured in CUCM:

- **Gatekeeper-controlled intercluster trunk:** This trunk is intended to work with CUCM releases before 3.2, although it can be used on later versions.
- **H.225 trunk:** This trunk can be used to work with CUCM 3.2 or later and all other Cisco or third-party H.323 devices. The H.225 trunk features a peer-discovery mechanism. Hence, it can identify the device located at the other end of the trunk and use the appropriate feature set.

A CUCM gatekeeper-controlled trunk registers as an H.323 gateway with the gatekeeper. Alternatively, it can be configured to register as H.323 terminals. When a trunk is registered, CUCM provides the following information to the gatekeeper, as you can see with the command `show gatekeeper endpoints`:

- **H.323 device type:** The device type can be either gateway or terminal. CUCM is usually configured to register as a gateway.
- **H.323 ID:** Based on the name of the trunk that is configured in CUCM, with the string `_x` at the end. The `x` is a number that uniquely identifies each call-processing CUCM server of the cluster where the Cisco CallManager service is activated.

Note The H.323 ID has to be unique. CUCM keeps the H.323 ID that is used by the members of a cluster unique by adding the individual ending `_x`. Furthermore, because CUCM does not allow multiple trunks to use the same name, no duplicate H.323 IDs can be presented to the gatekeeper from a cluster. However, if the same trunk name is configured in multiple clusters, the call-processing servers of two or more clusters will try to register with the same H.323 ID. The gatekeeper does not allow these duplicate H.323 IDs to register, so the trunk is not operational. Therefore, it is important to use unique trunk names across all CUCM clusters that register with a gatekeeper.

- **H.323 zone:** Used to group devices. Call routing and CAC are performed based on these zones. For example, a default technology prefix can be configured per zone

that identifies the gateway (or gateways) to which calls should be routed when the gatekeeper does not know which gateway to use. Also, CAC can be configured differently for calls within a zone versus interzone calls.

Note The H.323 zone name configured at the gatekeeper-controlled trunk is case-sensitive and has to exist at the gatekeeper.

- Technology prefix: H.323 gateways, including CUCM, can register prefixes. These are number ranges they can route calls to at the gatekeeper. The prefix can consist only of numbers (such as 511), or it can include a technology prefix (such as 1# or 2#). One way of using an H.323 technology prefix is for a gateway to indicate the services it provides by specifying an appropriate technology prefix (for instance, 1# for voice services, 2# for fax services, and so on). Calls that include the technology prefix in their numbers (for example, a call placed to 1#5115551000) can be routed to the gateway in the zone that registered the appropriate technology prefix. Technology prefixes can also be used for TEHO over a gatekeeper-controlled WAN.

As just mentioned, a gatekeeper can be configured to route calls to the gateway or gateways that register with a prefix that is configured to be the default technology. For example, if only one CUCM cluster registers per zone, the trunk in each cluster can be configured with a technology prefix of 1#, and the gatekeeper can be configured to send all calls to the gateway that registered with the configured default technology prefix of 1# in this case. The gatekeeper needs only a configuration of number prefixes, which is a number to find the correct zone. When the outgoing zone is determined, the gatekeeper just sends the call to one of the gateways or CUCM clusters that registered in the zone with the default technology prefix.

Note More information about how a gatekeeper routes call is provided in the *Implementing Cisco Unified Communications Voice over IP and QoS (Cvoice) Foundation Learning Guide*, Fourth Edition book.

H.323 Gatekeeper Used for Call Routing for Address Resolution Only

Figure 9-26 shows an example of gatekeeper-controlled trunks in a distributed CUCM deployment. In the example, two CUCM clusters are shown. Each cluster has an H.225 trunk configured.

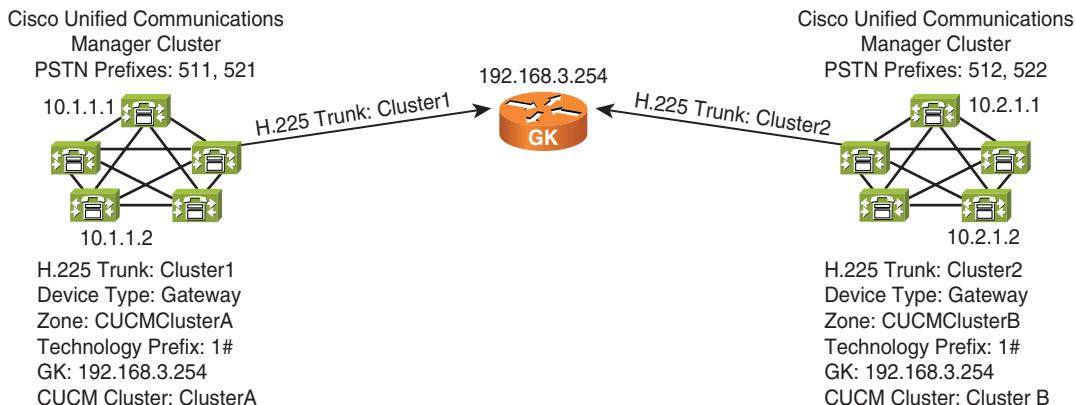


Figure 9-26 H.323 Gatekeeper Used for Call Routing for Address Resolution Only

Note A * is a gatekeeper wildcard that denotes all possible phone numbers, analogous to the gateway of last resort static route in data routing. If a technology prefix is properly entered without the * wildcard, the * often shows up automatically in the IOS configuration after the technology prefix, as illustrated in Example 9-2.

Example 9-2 is a sample of the gatekeeper configuration from `show running-config`. CAC is not configured; therefore, the gatekeeper assumes that infinite bandwidth is available to calls on all WAN links. This example also has no gatekeeper fault tolerance in the form of gatekeeper clustering.

Example 9-2 Sample Gatekeeper Configuration for Call Routing Without CAC

```
gatekeeper
  zone local CUCMClusterA lab.com 192.168.3.254
  zone local CUCMClusterB lab.com 192.168.3.254
  zone prefix CUCMClusterA 511*
  zone prefix CUCMClusterA 521*
  zone prefix CUCMClusterB 512*
  zone prefix CUCMClusterB 522*
  gw-type-prefix 1#* default-technology
  no shutdown
```

The call-processing servers of ClusterA are registered in zone CUCMClusterA, and the call-processing servers of ClusterB are registered in zone CUCMClusterB. This can be verified by using the command `show gatekeeper endpoints`. All endpoints are registered with prefix 1#*, which is configured to be the default technology prefix. You can verify this by using the command `show gatekeeper gw-type-prefix`. The result of these two

commands entered in privileged EXEC mode is shown aggregated as an example into one combined output in Example 9-3.

Example 9-3 Aggregated Output of show gatekeeper Commands

```
show gatekeeper endpoints

show gatekeeper gw-type-prefix

GATEKEEPER ENDPOINT REGISTRATION
=====
H323-ID      IPAddr     ZoneName      Type      Prefix
Cluster1_1   10.1.1.1  CUCMClusterA  VOIP-GW  1#*
Cluster1_2   10.1.1.2  CUCMClusterA  VOIP-GW  1#*
Cluster2_1   10.2.1.1  CUCMClusterB  VOIP-GW  1#*
Cluster2_2   10.2.1.2  CUCMClusterB  VOIP-GW  1#*
```

The H.225 trunks use different names for each cluster to keep the H.323 IDs unique. ClusterA uses Cluster1, and ClusterB uses Cluster2. Each cluster has two call-processing nodes—10.1.1.1 and 10.1.1.2 in ClusterA, and 10.2.1.1 and 10.2.1.2 in ClusterB.

The trunk in ClusterA, with the name Cluster1, is configured with zone ClusterA and technology prefix 1#*. The trunk in ClusterB, with the name Cluster2, is configured with zone ClusterB and the same technology prefix (1#*). Both trunks refer to the IP address of the same gatekeeper of 192.168.3.254.

The gatekeeper has two local zones named CUCMClusterA and CUCMClusterB. It is configured to route calls to prefixes 511 and 521 to zone CUCMClusterA, and to route calls to prefixes 512 and 522 to zone CUCMClusterB. In addition, the gatekeeper is configured to use technology prefix 1#* as the default technology. Therefore, calls to prefixes for which the gatekeeper does not know what gateway to use are routed to the gateway or gateways that registered a technology prefix of 1#*.

This gateway configuration means that the gatekeeper has four gateways registered. Cluster1_1 is the first call-processing server of the CUCM Group that is configured in the device pool of the trunk. Cluster1_2 is the second call-processing server of ClusterA and the two call-processing servers of ClusterB. Note that CUCM automatically gives an added numeric designator of _1 or _2 in the name.

They all use different H.323 IDs because different trunk names have been configured in the two clusters and because CUCM adds the _1 and _2 to the trunk name to uniquely identify the call-processing servers per cluster.

Note If the same trunk name were configured in the two clusters, registrations would fail because of duplicate H.323 IDs.

If the gatekeeper receives an admission request (ARQ) message from one of the H.323 gateways (in this case, a Cisco Unified Communications Server), it looks up its call-routing table of the list of configured zone prefixes to find out in which zone the requested prefix can be found.

Note The command **debug ras** shows the ARQ message followed by an acceptance (ACF) or a rejection (ARJ) based on the CAC settings and number of simultaneous calls. Example 9-2 does not have CAC configured; this is addressed in the next section.

You can verify the list of configured prefixes and their zones using the command **show gatekeeper zone prefix**.

If an ARQ message was sent from 10.1.1.1 to the gatekeeper that requests a call to 5125551234, the gatekeeper determines that the call has to be routed to zone CUCM ClusterB. The only prefix registered by gateways in this zone is 1#*, which is the default technology prefix; it is registered by 10.2.1.1 and 10.2.1.2. Therefore, the gatekeeper chooses one of these two gateways in a round-robin fashion to be the terminating gateway. It tells the originating gateway, the CUCM server of ClusterB that sent the ARQ message, to set up an H.323 call with the determined terminating gateway of 10.2.1.1 or 10.2.1.2.

Note At this point, the gatekeeper is configured only to perform call-routing address resolution. It resolves a dialed number to the IP address where the call has to be routed.

Using an H.323 Gatekeeper for CAC

To use an H.323 gatekeeper for CAC, bandwidth limitations have to be configured. In Cisco IOS, H.323 gatekeeper CAC is implemented by using the **bandwidth** command:

```
router(config-gk)#bandwidth {interzone | total | session}
{default | zone zone-name} bandwidth-size
```

Note The command **bandwidth** exists in other IOS modes as well, such as QoS and interface modes. When used in different IOS modes, this command takes on entirely different meanings.

Table 9-2 lists the parameters used with the **bandwidth** command in gatekeeper mode for configuring CAC options.

Note The bandwidth that is assumed by the gatekeeper for each call is twice the bandwidth of the audio codec. A G.729 call is configured for 16 kbps, and a G.711 call is

configured for 128 kbps. This is not the actual bandwidth seen on the wire, but it's the standard used when configuring gatekeeper CAC to represent a call. Multiple calls are simply calculated as an even multiple of these numbers, 16 and 128. Therefore, it is critical to know which codec is being used when configuring gatekeeper CAC.

Table 9-2 bandwidth Parameters

Syntax	Description
Interzone	Specifies the total amount of bandwidth for H.323 traffic from the zone to any other zone on different gatekeepers.
Total	Specifies the total amount of bandwidth for H.323 traffic allowed in the zone.
Session	Specifies the maximum bandwidth allowed for a session in the zone.
Default	Specifies the default value for all zones.
zone zone-name	Specifies a particular zone by name.
bandwidth-size	Maximum bandwidth. For interzone and total, the range is from 1 to 10,000,000 kbps. For session, the range is from 1 to 5000 kbps.

Bandwidth limitations are configured differently on different Cisco products and for different features. Again, these different settings do not change the bandwidth seen on the wire; they only show the expected configuration on these products all representing the same call. Table 9-3 summarizes how to configure bandwidth limitations for CAC in CUCM.

Table 9-3 Bandwidth Parameters in CUCM and the H.323 Gatekeeper

CUCM Region	CUCM Location	Cisco IOS H.323 Gatekeeper
Audio-Only Call Configuration	Audio codec only	Audio codec bit rate plus Layer 3 overhead
Example: G.711 Call	G.711	80 kbps
Video Call Configuration	Audio codec and video call speed	Video call speed
Example: 384-kbps Video Call	G.711 and 384 kbps	Twice the video call speed
Example: G.729 Call	G.729	768 kbps
		24 kbps
		16 kbps

Note Video calls have not been discussed in this chapter but are shown for completeness.

H.323 Gatekeeper Also Used for CAC

Figure 9-27 shows a sample topology of a Cisco IOS H.323 gatekeeper that has CAC enabled with the configuration in Example 9-4.

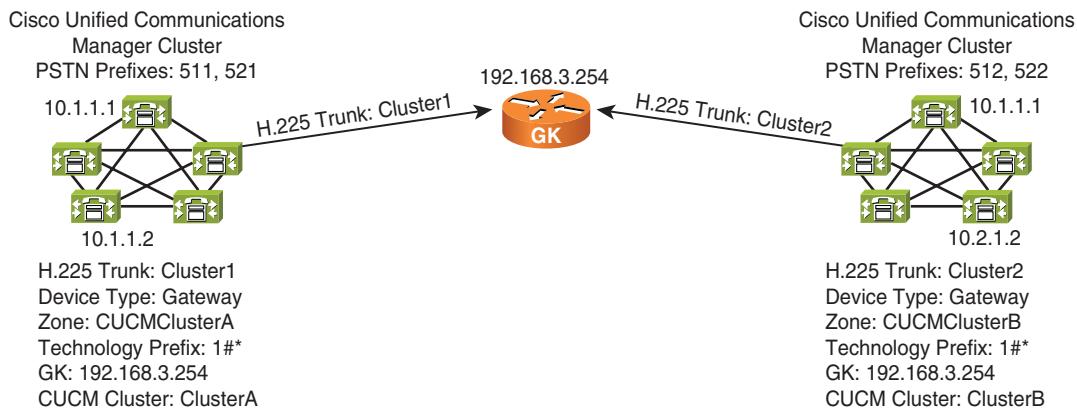


Figure 9-27 H.323 Gatekeeper with Call Admission Control

Example 9-4 shows a sample of the output of `show running-config` of the gatekeeper configuration with CAC.

Example 9-4 H.323 Gatekeeper with CAC Configuration

```
gatekeeper
  zone local CUCMClusterA lab.com 192.168.3.254
  zone local CUCMClusterB lab.com 192.168.3.254
  zone prefix CUCMClusterA 511*
  zone prefix CUCMClusterA 521*
  zone prefix CUCMClusterB 512*
  zone prefix CUCMClusterB 522*
  bandwidth interzone default 64
  bandwidth interzone zone CUCMClusterB 48
  bandwidth session default 128
  bandwidth total zone CUCMClusterB 688
  gw-type-prefix 1#* default-technology
  no shutdown
```

Example 9-4 is based on Example 9-2, but now the H.323 gatekeeper also performs CAC.

The **bandwidth interzone default 64** command specifies that 64 kbps is permitted for calls going out of and coming into a zone. Because no specific zone is specified, but the keyword **default** is used, this setting applies to all zones that are not explicitly configured with a different setting.

The **bandwidth interzone zone CUCMClusterB 48** command specifies that the previously configured default interzone bandwidth limit should not apply to ClusterB but that ClusterB should instead be limited to only 48 kbps. Note again how “more specific” takes precedence over “more general.” The **bandwidth session default 128** command limits the bandwidth to be used per call to a codec that does not require more than 128 kbps. This equates to one G.711 call or eight G.729 calls. Because no different session bandwidth is configured for any specific zone, this default applies to all zones.

The **bandwidth total zone CUCMClusterB 688** command limits all calls of ClusterB, which applies to calls within the cluster and intercluster calls, to a total of 688 kbps. Because ClusterA has neither a **bandwidth total default** command nor a specific **bandwidth total** command, ClusterA has no total limit applied.

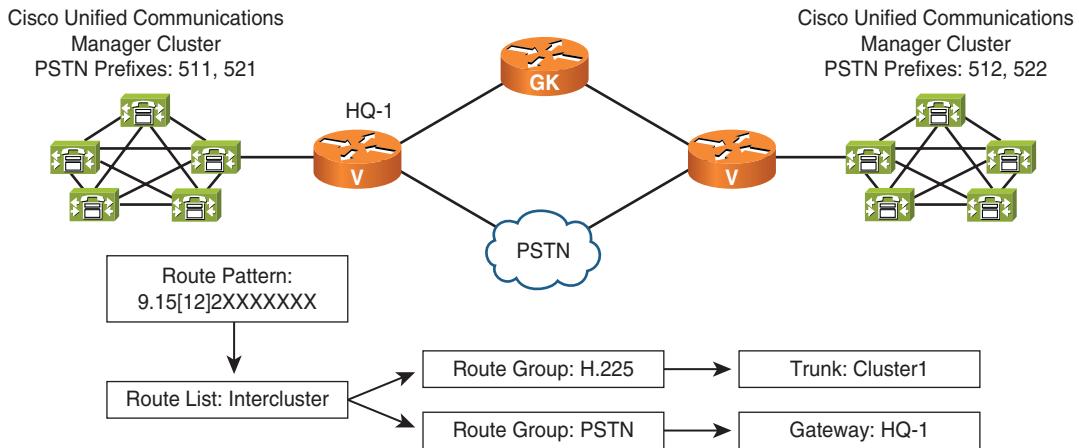
If G.729 is used for interzone calls and G.711 is used for intrazone calls, this configuration effectively would permit the following:

- There can be a maximum of three G.729 calls between ClusterA and ClusterB because ClusterB is limited to 48 kbps based on $3 * 16$ kbps. ClusterA could have four G.729 calls to other zones. However, because the example shows only two zones and the other zone, ClusterB, is limited to three G.729 calls, ClusterA will never be able to use the permitted interzone bandwidth.
- The maximum audio bandwidth is limited to 64 kbps. Calls requiring more bandwidth, for media such as wideband audio codecs or video calls with a video call bandwidth of more than 64 kbps, are not permitted in any zone.
- The total of all calls of both interzone and intrazone calls in zone ClusterB must not exceed 688 kbps. As an example, this configuration allows three G.729 calls to ClusterA based on $3 * 16$ kbps and five G.711 calls within ClusterB based on $5 * 128$ kbps. Intrazone calls in zone ClusterA are unlimited.

Note Some of the **bandwidth** commands in the example are for illustration only and are not useful in this scenario because only two zones are shown. Furthermore, intrazone limitations have been configured but would never apply in this scenario, because the H.323 gateways of CUCM systems only use the gatekeeper for calls to the other cluster. All H.323 gatekeeper bandwidth limitations apply only to calls that are routed by using the gatekeeper. A call between IP Phones of the same cluster does not use the gatekeeper-controlled trunk and therefore is not subject to any of the bandwidth commands entered at the gatekeeper.

Provide PSTN Backup for Calls Rejected by CAC

Backup paths can be provided for calls that are rejected by a gatekeeper because of CAC, as shown in Figure 9-28.



Route lists and route groups provide backup paths if the preferred path fails. In the example, if the calls cannot be established over the H.225 trunk because of CAC, the calls use the PSTN gateway (HQ-1) as backup.

Figure 9-28 Provide PSTN Backup for Calls Rejected by CAC

When a call placed to a gateway or trunk fails, there can be multiple causes. The appropriate device can be down, resulting in a timeout when trying to place a call to an H.323 gateway. CAC can limit a call when an ARQ message is sent to an H.323 gatekeeper.

Also, there can be keepalives that are not exchanged with an MGCP gateway because of lost connectivity. There can be other problems in communicating with the gateway successfully, such as sending H.323 messages to the IP address of an interface other than the one where the H.323 has been bound, or failing gatekeeper registration because of an invalid zone name or because the call is rejected because of lack of resources. The latter may occur when no channel is available on an E1 or T1 trunk, when an administratively configured limit of calls is reached at a dial peer, or because of CAC.

CUCM uses the same backup method for all these types of call failures based on route lists and route groups configured with route patterns. If the currently attempted device of a route group cannot extend the call for any reason, CUCM tries the next device according to the route group and route list configuration for each route pattern.

Therefore, providing a backup for calls that have been rejected because of H.323 gatekeeper CAC is as simple as having a route list and route groups that prefer the gatekeeper-controlled trunk over one or more PSTN gateways. If the call cannot be set up over the trunk, CUCM reroutes the call to the PSTN gateways. Instead of referring to a dedicated PSTN gateway that should be used as a backup, the local route group feature can be

used. Note that AAR is not used in any of these examples because AAR applies only to calls with a single CUCM cluster.

Note For a PSTN backup, you need to perform digit manipulation in such a way that the calling number and (more importantly) the called number are transformed to always suit the needs of the device that is actually used. This transformation can be done at the route list, where digit manipulation can be configured per route group. In the example, the called number, 9 1 511 555-1234, has to be changed to a ten-digit number for the H.225 trunk, because the gatekeeper is configured with area code prefixes without the long distance 1. The called number must also be changed to an 11-digit number if rerouting the call to the PSTN gateway is necessary. A better solution would be using global transformations at the egress devices (H.225 trunk and PSTN gateways). In a large multisite environment or in an international deployment, the implementation of globalized call routing would be the best solution.

Configuration Procedure for Implementing H.323 Gatekeeper-Controlled Trunks with CAC

To implement gatekeeper-controlled trunks for call routing only, add gatekeeper CAC functionality, and provide a backup path, follow these steps:

Step 1. Enable gatekeeper functionality at a Cisco IOS router, and configure the gatekeeper for call routing. This configuration typically includes zones, zone prefixes, and the default technology prefix.

Note More information about gatekeeper configuration is provided in *Implementing Cisco Unified Communications Voice over IP and QoS (Cvoice) Foundation Learning Guide*, Fourth Edition.

Step 2. Add the gatekeeper to CUCM.

Step 3. Add the gatekeeper-controlled trunk, either a gatekeeper-controlled intercluster trunk or an H.225 trunk, to CUCM, and configure the trunk.

Step 4. Configure route groups, route lists, and route patterns to route calls that match a certain route pattern. An example is 9.5[12][12]XXXXXXXX for the examples shown earlier in this topic to the gatekeeper-controlled trunk.

Note Steps 2 through 4 are described in *Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) Foundation Learning Guide*.

To implement gatekeeper-controlled CAC, configure the Cisco IOS gatekeeper with bandwidth commands to enable bandwidth limitations. Typically, this is required only for interzone calls.

Note The command syntax and a sample configuration were shown earlier in this chapter.

To provide backup paths for the gatekeeper-controlled trunk, add PSTN gateways to route groups, and add these gateways to the route lists that are using the gatekeeper-controlled trunks.

Note PSTN backup was configured in earlier examples of this book. More information about gatekeeper configuration is provided in *Implementing Cisco Unified Communications Voice over IP and QoS (Cvoice) Foundation Learning Guide*, Fourth Edition.

Summary

The following key points were discussed in this chapter:

- CAC limits the number of calls to avoid voice-quality issues caused by bandwidth oversubscription because of too many voice calls.
- CUCM locations can be used for CAC within a CUCM cluster that has a hub-and-spoke topology.
- CUCM RSVP-enabled locations provide topology-aware CAC between RSVP agents.
- AAR allows calls that were denied by locations-based CAC to be rerouted over the PSTN.
- H.323 gatekeepers can provide CAC on CUCM H.323 trunks.

References

For additional information, refer to these resources:

Cisco Systems, Inc. Cisco Unified Communications System 8.x SRND, April 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8x.html.

Cisco Systems, Inc. *Cisco Unified Communications Manager Administration Guide Release 8.0(1)*, February 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_1/ccmcfg/bccm-801-cm.html.

Cisco Systems, Inc. Cisco IOS H.323 Configuration Guide Release 15.0 – Configuring H.323 Gatekeepers and Proxies, February 2008, October 2009 (requires a Cisco.com login).

www.cisco.com/en/US/partner/docs/ios/voice/h323/configuration/guide/vh_h323_gkconfig_ps10591_TSD_Products_Configuration_Guide_Chapter.html.

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in the "Answer Appendix."

1. Which of the following two CAC-related features applies to intercluster calls?
 - a. Locations
 - b. H.323 gatekeeper CAC
 - c. AAR
 - d. RSVP-enabled locations
2. Which of the following is an accurate description of a limitation of locations-based CAC?
 - a. Only a total limit for all calls coming into or going out of a location can be configured.
 - b. Locations-based CAC is primarily designed for CAC between two or more CUCM clusters.
 - c. Locations-based CAC can only be configured to allow a maximum of ten calls.
 - d. Locations-based CAC does not have any CAC limitations.
3. Which statement about RSVP-enabled locations is false?
 - a. They adapt to the actual topology considering network changes.
 - b. RSVP provides QoS for each RTP stream.
 - c. The RSVP agent to be used by a phone is determined by the phone's media resource group list.
 - d. The RSVP agent is configured as an MTP in CUCM.
 - e. Cisco IP Phones do not support RSVP.

4. AAR reroutes calls to the PSTN for which two kinds of calls?
 - a. Calls rejected by an H.323 gatekeeper
 - b. Calls rejected by locations-based or RSVP-enabled locations-based CAC
 - c. Calls placed to unregistered phones
 - d. Calls placed to a gateway that is busy
 - e. Calls placed to internal directory numbers
 - f. Calls placed to the PSTN
5. How can calls that are rejected by an H.323 gatekeeper be rerouted using a different path?
 - a. By configuring route lists and route groups with backup devices.
 - b. By putting the gatekeeper-controlled intercluster trunk or H.225 trunk into a location that is set to unlimited.
 - c. This is not possible because AAR supports only internal calls.
 - d. By configuring a second route pattern in the same partition referring to the backup device.
6. Which statement about AAR and SRST is true?
 - a. AAR does not work with SRST.
 - b. AAR works well with SRST in all topologies.
 - c. AAR works well with SRST in only hub-and-spoke topologies.
 - d. AAR works well with SRST in only full-mesh topologies.
7. When a gatekeeper is configured to implement CAC between multiple CUCM clusters, what VoIP signaling protocol is used?
 - a. SIP
 - b. H.323
 - c. MGCP
 - d. SCCP
 - e. SIP and H.323 working together with CUBE

8. Which configuration would give the best user experience if a gatekeeper configured with multiple gatekeeper-controlled intercluster trunks limited additional calls with CAC?
 - a. Ensure that the additional calls blocked with CAC always give the users the reorder tone to train them when best to make calls.
 - b. Use AAR to send additional calls blocked with CAC through the PSTN.
 - c. Use route groups configured with the route lists and route patterns to send additional calls blocked with CAC through the PSTN.
 - d. Use AAR combined with route groups configured with the route lists and route patterns to send additional calls blocked with CAC through the PSTN.
9. Which statement is the most accurate comparing locations-based CAC and RSVP-enabled locations for implementing CAC within CUCM?
 - a. Both methods are optimal for full-mesh topologies.
 - b. RSVP-enabled locations work better with full-mesh topologies than locations-based CAC.
 - c. Locations-based CAC works better with full-mesh topologies than RSVP-enabled locations.
 - d. Both methods are unacceptable for full-mesh topologies.
10. What is the proper syntax to implement CAC on a gatekeeper?
 - a. Use the **bandwidth** command in interface mode.
 - b. Use the **bandwidth** command in gatekeeper mode.
 - c. Use the **cac** command in interface mode.
 - d. Use the **cac** command in gatekeeper mode.
11. Which statement is the most accurate about locations and regions in CUCM?
 - a. Locations configure CAC, and regions negotiate codecs.
 - b. Regions configure CAC, and locations negotiate codecs.
 - c. Both regions and locations together configure CAC.
 - d. Both regions and locations together negotiate codecs.

12. Which protocol or protocols must be configured on the router to enable an IOS RSVP agent to communicate with CUCM?

- a.** SIP
- b.** H.323
- c.** SCCP
- d.** MGCP
- e.** None of the above
- f.** SIP and SCCP working together with CUBE

13. What is the effect of having a non-RSVP-enabled IP router in the path of an RSVP stream?

- a.** The RSVP agents cannot implement CAC.
- b.** The RSVP agents can implement CAC end to end fully, provided that the source and destination agents are properly configured.
- c.** The RSVP agents can implement CAC without a guarantee from the non-RSVP-enabled IP router.
- d.** CAC is not possible at all in this topology.

14. What statement is true about SIP Preconditions?

- a.** SIP Preconditions cannot implement CAC.
- b.** SIP Preconditions requires a gatekeeper for CAC.
- c.** SIP Preconditions supports CAC.
- d.** SIP Preconditions must not be used with RSVP.

This page intentionally left blank

Chapter 10

Implementing Device Mobility

Upon completing this chapter, you will be able to meet the following objectives:

- List the issues with devices roaming between sites
- Describe the Device Mobility feature
- Describe the Device Mobility configuration elements and their interaction
- Describe Device Mobility Operation
- Describe Device Mobility interaction with globalized call routing
- Implement Device Mobility

It is common in multisite environments for some users to roam between sites on a regular basis. When such users take their Cisco Unified Communications endpoints with them, such as Cisco Unified Wireless IP Phones or Cisco IP Communicator (softphone) phones, the standard configuration of their endpoints needs to be adapted to suit the needs of the current physical location. It is important for a professional unified communications solution to provide such a solution.

This chapter describes Device Mobility. This new feature of Cisco Unified Communications Manager (CUCM) allows CUCM endpoints to be dynamically reconfigured based on their actual location as determined by the IP address that is used by the device.

Issues with Devices Roaming Between Sites

Figure 10-1 shows a phone device roaming between two internal sites as a user brings along his phone for business travel.

When users roam between sites, they might take their phones with them. This typically does not apply to Cisco IP Phones, but it's common with softphones such as Cisco IP Communicator running on a laptop or Cisco Unified Wireless IP Phones.

Issues with Roaming Devices

When phones move between different CUCM sites, inaccurate phone settings may occur.

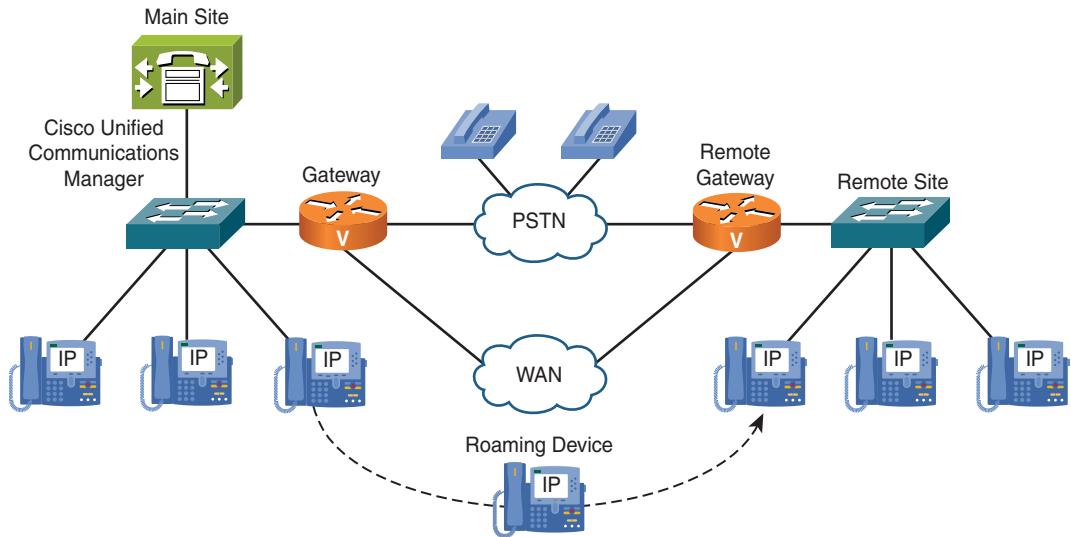


Figure 10-1 Roaming Devices Between Internal Sites

The configuration of an IP Phone includes personal settings and location-dependent settings that are all bound statically to the phone's MAC address and hence to the device itself. Before the CUCM Device Mobility feature was introduced in v6, the physical device location has traditionally been assumed to be constant.

If a phone (or, more likely, a softphone such as IP Communicator) is moved between sites, the location-dependent settings become inaccurate. Some of these settings and their errors are as follows:

- **Region:** Might cause wrong codec settings.
- **Location:** Might cause wrong call admission control (CAC) and bandwidth settings.
- **Survivable Remote Site Telephony (SRST) reference:** Might cause a malfunction of Cisco Unified SRST by pointing to the wrong SRST Integrated Services Router (ISR).
- **Automated Alternate Routing (AAR) group:** Might cause a malfunction of the call redirection on no bandwidth.
- **Calling Search Space (CSS):** Might cause usage of remote gateways instead of local ones.
- **Media Resource Groups and Media Resource Group Lists:** Might cause allocation of wrong media resources, such as conference bridges or transcoders.

Table 10-1 *Device Mobility Solves Issues of Roaming Devices*

Issue Without Device Mobility	Device Mobility Feature to Solve the Issue
When the mobile user moves to a different location, Call Admission Control settings are not adjusted.	Location settings are dynamically assigned.
PSTN gateways to be used are fixed.	Dynamic phone CSS allows for site-independent local gateway access.
SRST reference is fixed.	SRST reference is dynamically assigned.
When the mobile user moves to a different region, codec settings are not adjusted.	Region settings are dynamically assigned.
AAR does not work for mobile users.	The AAR calling search space and the AAR group of the DN are dynamically assigned.
Media resources are assigned location-independently.	The media resource list is dynamically assigned.
AAR has Extension Mobility issues.	Extension Mobility also benefits from dynamic assignment.

For correct settings, CUCM needs to be aware of the physical location of all phones, including roaming devices within the CUCM cluster.

Device Mobility Solves Issues of Roaming Devices

Device Mobility offers functionality that is designed to enhance the mobility of devices within an IP network. Table 10-1 summarizes the challenges and solutions of Device Mobility implemented in CUCM.

Although devices such as IP Phones and IP Communicator still register with the same CUCM cluster with SCCP or SIP, they now will adapt some of their behavior based on the actual site where they are located. Those changes are triggered by the IP subnet in which the phone is located.

Basically, all location-dependent parameters can be dynamically reconfigured by Device Mobility. Thus, the phone keeps its user-specific configuration, such as directory number, speed dials, and call-forwarding settings. However, it adapts location-specific settings such as region, location, and SRST reference to the actual physical location. Device Mobility can also be configured so that dial plan-related settings, such as the device CSS, AAR group, and AAR CSS, are modified.

Device Mobility Overview

The following are key characteristics and features of Device Mobility:

- Device Mobility can be used in multisite environments with centralized call processing within a single CUCM cluster.
- Device Mobility allows users to roam between sites with their Cisco IP Phones, which typically are Cisco IP Communicator or Cisco Unified Wireless Phones.
- IP Phones are assigned with a location-specific IP address by DHCP scopes specific to each location.
- CUCM determines the physical location of the IP Phone based on the IP address used by the IP Phone.
- Based on the physical location of the IP Phone, the appropriate device configuration is applied.

Device Mobility allows users to roam between sites with their IP Phones. Typically, these are Cisco Unified Wireless IP Phones or Cisco IP Communicator Phones.

When the device is added to the network of roaming sites, it is first assigned with an IP address. Because the IP networks are different in each site, CUCM can determine the physical location of the IP Phone based on its IP address.

Based on the physical location of the IP Phone, CUCM reconfigures the IP Phone with site-specific settings.

Dynamic Device Mobility Phone Configuration Parameters

Two types of phone configuration parameters can be dynamically assigned by Device Mobility: Roaming-Sensitive Settings and Device Mobility-Related Settings.

Device Mobility can reconfigure site-specific phone configuration parameters based on the phone's physical location. Device Mobility does not modify any user-specific phone parameters or any IP Phone button settings such as directory numbers or phone services.

The phone configuration parameters that can be dynamically applied to the device configuration are grouped in two categories:

- **Roaming-Sensitive Settings:**
 - Date/Time Group
 - Region
 - Location
 - Connection Monitor Duration

Note The Date/Time Group, Region, Location, and Connection Monitor Duration are configured at device pools only.

- Network Locale
- SRST Reference
- Media Resource Group List (MRGL)

Note The Network Locale, SRST Reference, and Media Resource Group List are overlapping parameters; that is, they can be configured at phones and device pools.

- Physical Location
- Device Mobility Group
- Local Route Group

Note The Physical Location and Device Mobility Group parameters determine which settings should be applied to a roaming phone. The options are none, the roaming-sensitive settings only, or the roaming-sensitive settings and the settings that are related to Device Mobility. They are not phone-configuration parameters themselves, so they are not applied to the phone configuration like the other listed roaming-sensitive settings are. Instead, they are used only at the phone configuration. Consequently, they cannot be overlapping and can be configured only at device pools.

- Device Mobility-Related Settings:
 - Device Mobility CSS
 - AAR CSS
 - AAR Group
 - Calling Party Transformation CSS

Note The Device Mobility CSS, AAR CSS, and AAR Group are overlapping parameters. Therefore, they can be configured at phones and device pools. However, the Device Mobility CSS is called the Calling Search Space only in the Phone Configuration window. It does not overlap with the CSS configured at lines. It relates specifically to a phone's device CSS.

Roaming-sensitive settings are settings that do not have an impact on call routing. Device Mobility-related settings, on the other hand, have a direct impact on call routing, because

they modify the device CSS, AAR group, and AAR CSS. Depending on the implementation of Device Mobility, roaming-sensitive settings only, or both roaming-sensitive settings and Device Mobility-related settings, can be applied to a roaming phone.

Device Mobility Dynamic Configuration by Location-Dependent Device Pools

Figure 10-2 illustrates the location-dependent parameters such as roaming-sensitive settings and Device Mobility-related settings that are configured at device pools. Based on the IP subnet that is used by the phone associated with a device pool, CUCM can choose the appropriate device pool and dynamically apply the location-dependent parameters. With the introduction of Device Mobility, CUCM is aware of the physical location of a device based on its IP address within its IP subnet and applies the appropriate location-specific configuration by selecting the corresponding device pool in the branch site. An IP Phone can only be manually configured to be in one device pool at any one time. In Figure 10-2, the manually configured device pool is referred to as Device Pool Main, and the dynamically assigned device pool from Device Mobility is referred to as Device Pool Remote.

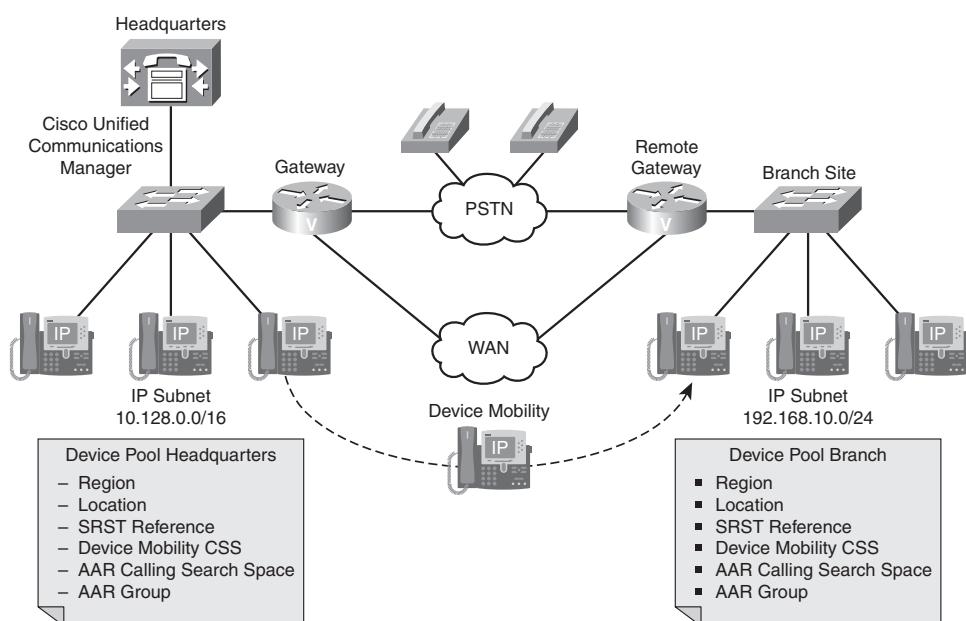


Figure 10-2 Device Mobility with a Dynamic Configuration by Location-Dependent Device Pools

Table 10-2 *Device Mobility Configuration Element Functions*

Configuration Element Name	Configuration Element Function
Device Pool (DP)	Defines a set of common characteristics for devices. The device pool contains only device- and location-related information. One device pool has to be assigned to each device.
Device Mobility Info (DMI)	Specifies an IP subnet and associates it with one or more device pools. DMIs can be associated with one device pool.
Physical Location (PL)	A tag assigned to one or more device pools. It is used to identify whether a device is roaming within a physical location or between physical locations.
Device Mobility Group (DMG)	A tag assigned to one or more device pools. It is used to identify whether a device is roaming within a Device Mobility Group or between Device Mobility Groups.

Device Mobility Configuration Elements

Table 10-2 lists the Device Mobility-related configuration elements and describes their functions. The newly introduced elements are Device Mobility Info (DMI), Physical Location (PL), and Device Mobility Group (DMG).

The DMI is configured with a name and an IP subnet and is associated with one or more device pools. Multiple DMIs can be associated with the same device pool.

The Physical Location and the Device Mobility Group are just tags. They are configured with a name only and do not include any other configuration settings. Both are non-mandatory device pool configuration parameters. Therefore, at the device pool, you can choose no physical location or one physical location and one or no Device Mobility Group. They are used to determine whether two device pools are at the same physical location and/or in the same Device Mobility Group.

Relationship Between Device Mobility Configuration Elements

Figure 10-3 shows an example of how the different Device Mobility configuration elements relate to each other.

Figure 10-3 shows five DMIs for three physical locations—San Jose, New York, and London. They are configured as follows:

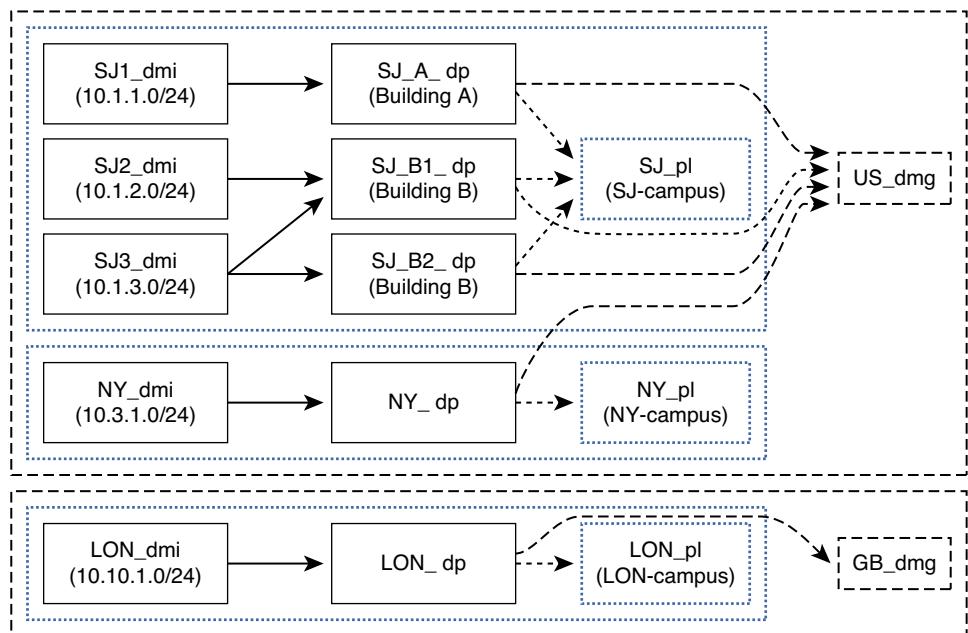


Figure 10-3 Relationship Between Device Mobility Configuration Elements

- **SJ1_dmi:** The IP subnet of this Device Mobility Info is 10.1.1.0/24. This DMI is used at Building A of the San Jose campus and is associated with DP SJ_A_dp.
- **SJ2_dmi:** The IP subnet of this DMI is 10.1.2.0/24. This DMI is used at Building B1 of the San Jose campus and is associated with device pool SJ_B1_dp.
- **SJ3_dmi:** The IP subnet of this DMI is 10.1.3.0/24. Like SJ2_dmi, this DMI is used at Building B1, which is associated with device pool SJ_B1_dp, but it is also used at Building B2 and is associated with device pool SJ_B2_dp.
- **NY_dmi:** The IP subnet of this DMI is 10.3.1.0/24. This DMI is used at the New York campus and is associated with device pool NY_dp.
- **LON_dmi:** The IP subnet of this DMI is 10.10.1.0/24. This DMI is used at the London campus and is associated with device pool LON_dp.

Device pools SJ_A_dp, SJ_B1_dp, and SJ_B2_dp are all configured with the same physical location (SJ_pl) because they are all used for devices located at the San Jose campus.

Device pool NY_dp, serving the New York campus, is configured with physical location NY_pl. Device pool LON_dp, serving the London campus, is configured with physical location LON_pl.

All device pools that are assigned with a U.S. physical location (that is, SJ_A_dp, SJ_B1_dp, SJ_B2_dp, and NY_dp) are configured with Device Mobility Group US_dmg. This setting means that all U.S. device pools are in the same Device Mobility Group. The London campus is in a different DMG: GB_dmg.

In summary, the U.S. Device Mobility Group consists of two physical locations: San Jose and New York. At San Jose, IP subnets 10.1.0.0/24, 10.1.2.0/24, and 10.1.3.0/24 are used; New York uses IP subnet 10.3.1.0/24, and London is configured with IP subnet 10.10.1.0/24. Device Mobility Groups are used to recognize differences in dial patterns in different geographic locations.

Based on the IP address of an IP Phone, CUCM can determine one or more associated device pools and the physical location and Device Mobility Group of the device pool or pools. If an IP Phone uses an IP address of IP subnet 10.1.3.0/24, the device pool has two candidates. However, in this example, the physical location and Device Mobility Group are the same for these two device pools.

Device Mobility Operation

As discussed earlier, each phone is configured with a device pool, similar to previous versions of Cisco CallManager (CCM). This device pool is the phone's home device pool.

IP subnets are associated with device pools by configuring DMIs.

The following occurs when a Device Mobility-enabled phone registers with CUCM with an IP address that matches an IP subnet configured in a DMI:

- The current device pool is chosen as follows:
 - If the DMI is associated with the phone's main or home device pool, the phone is considered to be in its home location. Therefore, Device Mobility does not reconfigure the phone.
 - If the DMI is associated with one or more device pools other than the phone's main or home device pool, one of the associated device pools is chosen based on a round-robin load-sharing algorithm.
- If the current device pool is different from the home device pool, the following checks are performed:
 - If the physical locations are not different, the phone's configuration is not modified.
 - If the physical locations are different, the roaming-sensitive parameters of the current roaming device pool are applied.
 - If the Device Mobility Groups are the same, in addition to different physical locations, the Device Mobility-related settings are also applied, along with the roaming-sensitive parameters.

In summary, the roaming-sensitive parameters are applied when the physical location of the current device pool is different from the physical location of the main or home device pool. The Device Mobility-related settings are also applied when the physical locations are different and the Device Mobility Groups are the same. This occurs when roaming between physical locations within the same Device Mobility Group.

As a consequence, physical locations and Device Mobility Groups should be used as follows:

- **Physical locations:** Configure physical locations in such a way that codec choice and CAC truly reflect the device's current location. Also, local SRST references and local media resources at the roaming site should be used instead of those located at the currently remote home network. Depending on the network structure, IP subnetting, and allocation of services, you may define physical locations based on a city, enterprise campus, or building.
- **Device Mobility Groups:** A Device Mobility Group should define a group of sites with similar dialing patterns or dialing behavior. Device Mobility Groups represent the highest-level geographic entities in your network. Depending on the network size and scope, your Device Mobility Groups could represent countries, regions, states or provinces, cities, or other geographic entities. Device Mobility-related settings that are applied only when roaming within the same Device Mobility Group impact call routing. Therefore, different Device Mobility Groups should be set up whenever a roaming user should not be forced to adapt his dialing behavior. In this case, when roaming between different Device Mobility Groups, the phone Device Mobility-related settings that impact call routing are not modified.

Note When using globalized call routing and local route groups, Device Mobility groups are irrelevant. The reason is that there is no need to change the device-level CSS, the AAR CSS, and the device-level AAR group. The section, “Device Mobility Interaction with Globalized Call Routing” provides more information about the interaction of globalized call routing and Device Mobility.

Device Mobility Operation Flowchart

Figure 10-4 illustrates the flow of Device Mobility operation. Again, DP is the Device Pool, and DMI is the Device Mobility Info (IP subnet). DMG is Device Mobility Group, and PL is the physical location.

The process of a phone registration with Device Mobility is as follows:

1. A phone device attempts to register with CUCM. Phones that do not register with CUCM cannot be part of the CUCM cluster and therefore do not have any Device Mobility configuration. If the phone successfully registers to a CUCM server, continue.
2. CUCM checks whether Device Mobility is enabled for the device. If it isn't, the default behavior applies; go to Step 10. Otherwise, continue.
3. CUCM checks whether the IP address of the IP Phone is found in one of the Device Mobility Groups (DMG). If it is not found, the default behavior applies; go to Step 10. Otherwise, continue.

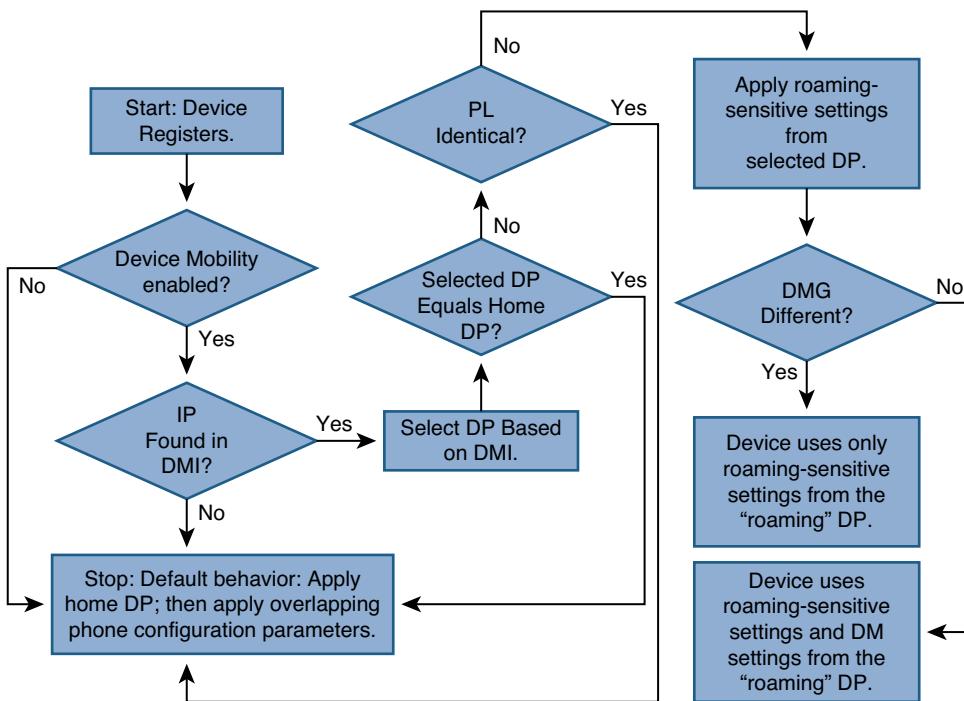


Figure 10-4 Device Mobility Operation Flowchart

4. If the home or main device pool (DP) is associated with the DMI in which the phone's IP address was found, the home or main device pool is chosen. If the home or main device pool is not associated with the DMI in which the phone's IP address was found, the device pool is chosen based on a load-sharing algorithm. The load-sharing algorithm applies if more than one device pool is associated with the DMI.
5. If the chosen device pool is the home or main device pool, the default behavior applies; go to Step 10. Otherwise, continue.
6. If the physical locations of the chosen device pool and the home or main device pool are the same, the default behavior applies; go to Step 10. Otherwise, continue.
7. The roaming-sensitive settings of the chosen device pool of the roaming or remote device pool are used to update the phone's configuration.

Note In this case, overlapping settings that exist at the phone and at the device pool (namely, Media Resource Group List, Location, and Network Locale of the roaming or remote device pool) have priority over the corresponding settings at the phone. This behavior is different from the default behavior in Step 10.

8. If the DMG of the chosen device pool and the home or main device pool are different, the device uses only the roaming-sensitive settings from the "roaming" or

“remote” DP. If they are not different, the device uses the roaming or remote settings and the Device Mobility (DM) settings from the “roaming” or “remote” DP.

Note In this case, all settings are overlapping settings that are Device Mobility-related settings that exist at the phone and device pool. Therefore, the parameters of the roaming or remote device pool have priority over the corresponding settings at the phone. This behavior is different from the default behavior in Step 10.

9. Next, where the phone configuration has been updated with either the roaming-sensitive settings only, or with the roaming-sensitive settings and the Device Mobility-related settings, the phone is reset for the updated configuration to be applied to the phone.

Note This is the end of the process. Step 10 applies only in the conditions outlined in the previous steps.

10. The default behavior is the settings of the home DP, which is the device pool configured on the phone. Some configuration parameters of the device pool can also be set individually at the phone. These overlapping phone configuration parameters are the Media Resource Group List, Location, Network Locale, Device Mobility Calling Search Space (which is just called Calling Search Space at the phone), AAR Calling Search Space, and AAR Group. If these are configured at the phone, implying they are not set to [None], the phone configuration settings have priority over the corresponding setting at the device pool.

Device Mobility Considerations

Roaming-sensitive settings ensure that the roaming device uses local media resources and SRST references. In addition, they ensure the correct use of codecs and CAC between sites. Typically, this is always desired when a device roams between different sites. It is not required when the device moves only between IP subnets within the same site. Therefore, the recommendation is to assign all device pools that are associated with IP subnets (DMI) that are used at the same site to the same physical location. This results in phone configuration changes only when the phone roams between sites (physical locations) and not in a situation where a phone is only moved between different networks of the same site.

Device Mobility-related settings impact call routing. By applying the device CSS, AAR group, and AAR, CSS calls are routed differently. The settings at the roaming device pool determine which gateway will be used for PSTN access and AAR PSTN calls based on the device CSS and AAR CSS. They also determine how the number to be used for AAR calls is composed based on the AAR group.

Such changes can result in different dialing behavior. For instance, when you roam between different countries, the PSTN access code and PSTN numbering plans might be different. For example, to dial the Austrian destination +43 699 18900009, users in Germany dial 0.0043 699 18900009, whereas users in the United States have to dial 9.01143 699 18900009.

German users who roam with their softphones to the United States might be confused when they have to use U.S. dialing rules access code 9 instead of 0 and 011 instead of 00 for international numbers. To prevent this confusion, suppress the application of Device Mobility-related settings. You do this by assigning device pools that are to be used at sites with different dialing rules to different Device Mobility Groups and different physical locations. Now, when a user roams with a device from Germany to the United States, all the roaming-sensitive settings are applied, but the Device Mobility-related settings are not applied. The phone now uses the PSTN gateway and dial rules of its home location even though the user moved to another site. The user does not have to adapt to the dial rules of the local site to which the phone was moved.

Note The preceding statements regarding call routing and dial behavior that are based on Device Mobility-related settings do not apply when globalized call routing is used. The section, “Device Mobility Interaction with Globalized Call Routing,” presents more information about the interaction of globalized call routing and Device Mobility.

Review of Line and Device CSSs

An IP Phone can be configured with a line CSS and a device CSS. If both exist, the partitions configured to the line CSS are considered before the partitions of the device CSS when routing a call. (This is another example of “more specific overrides more general.”)

These two CSSs allow the use of the line/device approach for implementing calling privileges and the choice of a local gateway for PSTN calls. With the line/device approach, all possible PSTN route patterns exist once per location, which is configured with a site-specific partition. This partition is included in the device CSS of the phones and therefore enables the use of a local gateway for PSTN calls. To implement class of service (CoS), PSTN route patterns that should not be available to all users (for example, international calls, long-distance calls, or all toll calls) are configured as blocked route patterns and are assigned to separate partitions. The line CSS of a phone now includes the partitions of the route patterns that should be blocked for this phone. Because the line CSS has priority over the device CSS, the blocked pattern takes precedence over the routed pattern that is found in a partition listed at the device CSS.

Device Mobility and CSSs

Device Mobility never modifies the line CSS of a phone. It does, however, change the device CSS and AAR CSS of a phone when the phone is roaming between different physical locations within the same Device Mobility Group.

The line CSS implements CoS configuration by permitting internal destinations, such as phone directory numbers, Call Park, and Meet-Me conferences, but blocking PSTN destinations. Because the line CSS is not changed by Device Mobility, CoS settings of the device are kept when the device is roaming.

The device CSS is modified when roaming within the same Device Mobility Group. In this case, the device CSS that is used at the home location is replaced by a device CSS that is applicable to the roaming location. This device CSS refers to the local gateway of the roaming site instead of the gateway that is used at the home location.

If the traditional approach of using only one CSS combining CoS and gateway choice is used, the device CSS must be used, because Device Mobility cannot modify the line CSS, and the line CSS has priority over the device CSS. These settings can be modified by Device Mobility.

The AAR CSS can be configured only at the device level. Therefore, it is always correctly replaced when roaming between physical locations within the same Device Mobility Group.

Note When using globalized call routing and local route groups, there is no need for site-specific device-level CSS. More information about the interaction of globalized call routing and Device Mobility is provided in the section, “Device Mobility Interaction with Globalized Call Routing.”

Examples of Different Call-Routing Paths Based on Device Mobility Groups and Tail-End Hop-Off

Table 10-3 shows how calls are routed in different Device Mobility scenarios.

Calls are routed differently depending on the configuration of Device Mobility Groups. Call-routing factors depend on whether Device Mobility-related settings are applied, the dialed destination, and the use of TEHO. In some scenarios, calls might take suboptimal paths.

For example, assume that a user from London roams to the U.S. office with Cisco IP Communicator. For simplicity, assume that there is only one U.S. office.

For the following three scenarios, the home device pool and the roaming device pool are assigned to the same Device Mobility Group, which means that Device Mobility applies Device Mobility-related settings. As a result, PSTN calls placed from the roaming device are treated like PSTN calls of standard U.S. phones.

Table 10-3 Examples of Different Call-Routing Paths Based on Device Mobility Groups and TEHO*TEHO = tail-end hop-off

Scenario	Result
Same DMG, call to PSTN destination close to home location, no TEHO.	The call uses the local PSTN gateway at the roaming location to place a long-distance PSTN call.
Same DMG, call to PSTN destination close to home location, TEHO.	The call uses the IP WAN to the gateway at the home location to place a local PSTN call.
Same DMG, call to PSTN destination close to roaming location.	The call uses the local PSTN gateway at the roaming location to place a local PSTN call.
Different DMG, call to PSTN destination close to home location.	The call uses the IP WAN to the gateway at the home location to place a local PSTN call.
Different DMG, call to PSTN destination close to roaming location, no TEHO.	The call uses the IP WAN to the gateway at the home location to place a long-distance PSTN call.
Different DMG, call to PSTN destination close to roaming location, TEHO.	The call uses the local PSTN gateway at the roaming location to place a local PSTN call.

- If a call to a PSTN destination close to the home location such as a U.K. PSTN number is placed and TEHO is not configured, the call uses the local U.S. PSTN gateway to place an international PSTN call. From a toll perspective, this is a suboptimal solution, because the IP WAN is not used as much as it could be when implementing TEHO. This factor applies not only to the roaming user, but also to U.S. users who place calls to PSTN destinations in Great Britain.
- If the same call to a U.K. PSTN number is placed and TEHO is configured, the call uses the IP WAN to the London site and breaks out to the PSTN at the London gateway with a local call. This solution is the optimal one from a toll perspective.
- If a call to a U.S. destination number is placed, the U.S. gateway is used for a local or national call. This event is optimal from a toll perspective.

Note In all the examples shown that are based on Table 10-3, the user has to dial PSTN destinations by following the NANP dial rules.

For the next three scenarios, the home or main device pool and the roaming or remote device pool are assigned to different Device Mobility Groups. This means that the

Device Mobility-related settings are not applied. Therefore, calls placed from the roaming device are routed the same way as they are when the device is in its home location:

- If a call from the U.S. to a U.K. PSTN destination is placed, the call uses the IP WAN to the London site and breaks out to the PSTN at the London gateway with a local or national call. This solution is the optimal one from a toll perspective.
- If a call from the U.S. to a PSTN destination close to the roaming or remote location such as a U.S. PSTN number is placed and TEHO is not configured, the call uses the IP WAN from the U.S. office to the London site and breaks out to the PSTN at the London gateway to place an international call back to the United States. From a toll perspective, this is the worst possible solution, because the call first goes from the United States to London over the IP WAN, wasting bandwidth, and then goes back from London to the United States via a costly international call.
- If a call from the U.S. to a PSTN destination close to the roaming or remote location such as a U.S. PSTN number is placed and TEHO is configured, the U.S. gateway is used for a local or national call. This event is optimal from a toll perspective.

Note In these three examples, the user has to dial PSTN destinations by following the dial rules of the home or main location (the U.K.).

In summary, when allowing the Device Mobility-related settings to be applied by using the same Device Mobility Group, calls to the home location use a local PSTN gateway to place a long-distance or international call when not implementing TEHO. All other calls are optimal.

When the Device Mobility-related settings are not applied by using different Device Mobility Groups and by not using TEHO, calls to the roaming location first use the IP WAN to go from the roaming location to the home location and then use the home gateway to place a long-distance or international call back to the roaming location. All other calls are optimal.

The discussed scenarios assume that globalized call routing and local route groups are not used. The impact of globalized call routing and local route groups is discussed in the next section.

Device Mobility Interaction with Globalized Call Routing

Local route groups have been introduced with CUCM version 7. When local route groups and globalized call routing (which use local route groups) are not used or supported, Device Mobility is typically implemented:

- Roaming-sensitive settings are always updated when the device roams between different physical locations. These settings are location, region, SRST reference, MRGL, and other parameters that do not affect the selection of the PSTN gateway or the local rules.
- Device Mobility-related settings can be applied in addition to the roaming-sensitive settings (which means that a phone has to roam between different physical locations). The Device Mobility-related settings are device CSS, AAR CSS, and AAR group. The configuration of the device mobility group should determine your decision about whether to apply the Device Mobility-related settings.
- If the device roams between different Device Mobility groups, the Device Mobility-related settings are not updated with the values that were configured at the roaming or remote device pool. This configuration has the advantage that users do not have to adapt to different dial rules between home and roaming location (if they exist). The disadvantage is that all PSTN calls use the home gateway, which can lead to sub-optimal routing.
- If the device roams within the same Device Mobility group, the Device Mobility-related settings are updated with the values of the roaming device pool. This configuration has the advantage that all PSTN calls will use the local (roaming or remote) gateway, which is typically desired for roaming or remote users. However, the users have to use the local dial rules.

Note If TEHO is used, there are no suboptimal paths when using Device Mobility with different Device Mobility groups. When local route groups and globalized call routing are not being used, however, TEHO implementation can be complex, especially when local PSTN backup is desired and when TEHO is implemented in international deployments.

In summary, unless TEHO is used, the implementation of Device Mobility without globalized call routing leads to this situation: Either the home gateway has to be used (when allowing the user to use the home dial rules), or the user is forced to use the dial rules of the roaming site (to use the local gateway of the roaming site).

Advantages of Using Local Route Groups and Globalized Call Routing

Device Mobility benefits from globalized call routing and local route groups, especially when implemented in international environments.

When Device Mobility with globalized call routing is used, there are no changes in the roaming-sensitive settings. Their application always makes sense when roaming between sites. They have no influence on the gateway selection and the dial rules that a user has to follow. The dial plan-related part of Device Mobility, however, changes substantially with globalized call routing. It allows a roaming user to follow the home dial rules for external calls and nevertheless use the local gateway of the roaming site.

This situation is possible because globalization of localized call ingress at the phone occurs. This function is provided by the line CSS of the phone. It provides access to

phone-specific translation patterns that normalize the localized input of the user to global format. The device CSS that was used for gateway selection is obsolete because gateway selection is now performed by the local route group feature.

The AAR CSS and AAR group that are configured at the device level can be the same for all phones as long as the AAR number is always in global format. (You can ensure that it is always in global format by configuring either the external phone number mask or the AAR transformation mask to E.164 format.) In this case, no different AAR groups are required because there is no need for different prefixes that are based on the location of the two phones.

Furthermore, there is no need for different AAR CSS, because the gateway selection is not based on different route lists (referenced from different route patterns in different partitions). Instead, it is based on the local route group that was configured at the device pool of the calling phone.

In summary, when using globalized call routing is used, Device Mobility allows users to use local gateways at roaming sites for PSTN access (or for backup when TEHO is configured) while using their home dial rules. There is no need to apply different device CSS, AAR CSS, and AAR groups, and hence, Device Mobility groups are no longer required.

Example of No Globalized Call Routing with a Different Device Mobility Group

Figure 10-5 shows an example of Device Mobility with different Device Mobility groups in an environment where globalized call routing is not implemented. Also, gateway selection is performed by the device CSS of the IP Phone.

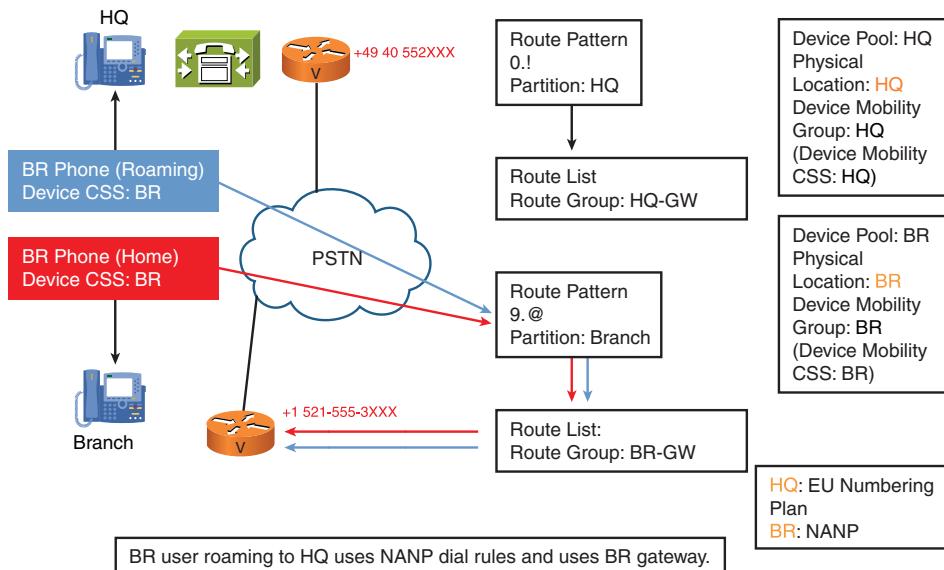


Figure 10-5 Example of No Globalized Call Routing with a Different Device Mobility Group

In this example, there are two sites: The main site (HQ in Figure 10-5) is in Europe, and the branch site (BR) is in the United States. Separate route patterns (representing the different dial rules) are configured in different partitions. The CSS of HQ phones provides access to the HQ gateway, the CSS of BR phones provides access to the BR gateway.

Device Mobility is configured with different Device Mobility groups. This configuration allows BR users who are roaming with their phones to the HQ to use the home dial rules. The device CSS is not updated by Device Mobility, and therefore, the CSS still provides access to the BR route pattern (9.@). However, as a consequence, the BR gateway is used for all PSTN calls.

Example of No Globalized Call Routing with the Same Device Mobility Group

Figure 10-6 shows an example of Device Mobility with identical device mobility groups in an environment where globalized call routing is not implemented. Also, gateway selection is performed by the device CSS of the IP Phone.

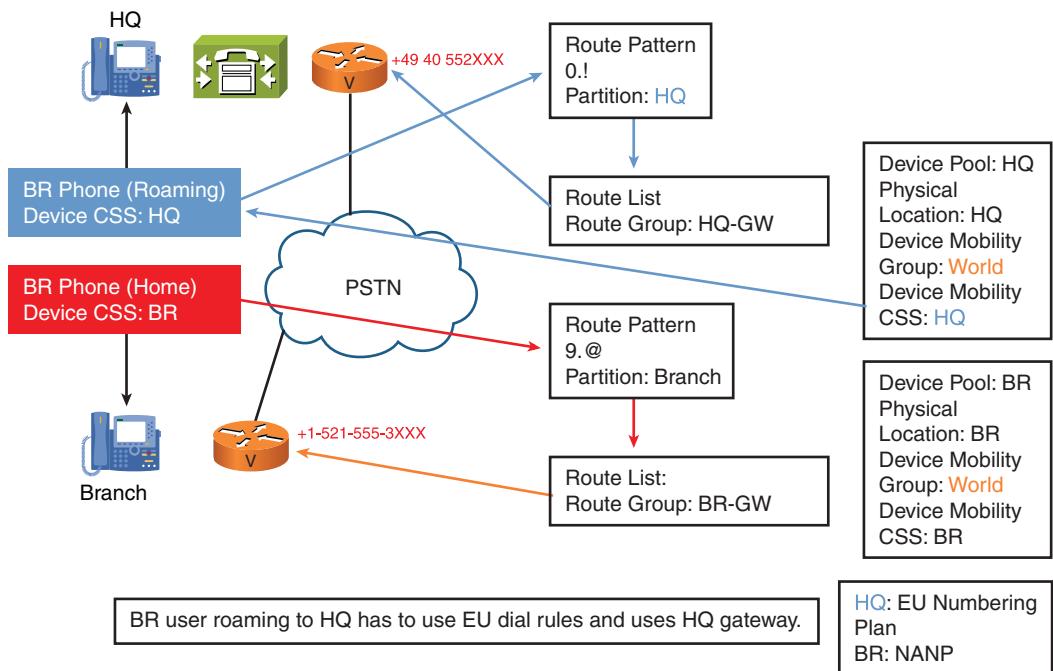


Figure 10-6 Example of No Globalized Call Routing with the Same Device Mobility Group

This example is identical to the previous example with one exception: This time, the Device Mobility group of the home and the roaming device pool are the same. When a BR user roams to the HQ, the device CSS of the phone is updated with the device CSS of the roaming device pool. In the example, CSS BR is changed to HQ. As a consequence, the phone has access to the HQ partition that includes PSTN route patterns in EU dialing format (0.!). Therefore, the roaming user has to follow EU dial rules. Calls to 9.@ are not possible anymore. However, this configuration allows the BR user to use the HQ gateway when roaming to the HQ.

Globalized Call Routing Example

Figure 10-7 shows an example of Device Mobility in an environment where globalized call routing is implemented. Also, gateway selection is performed by the local route group feature.

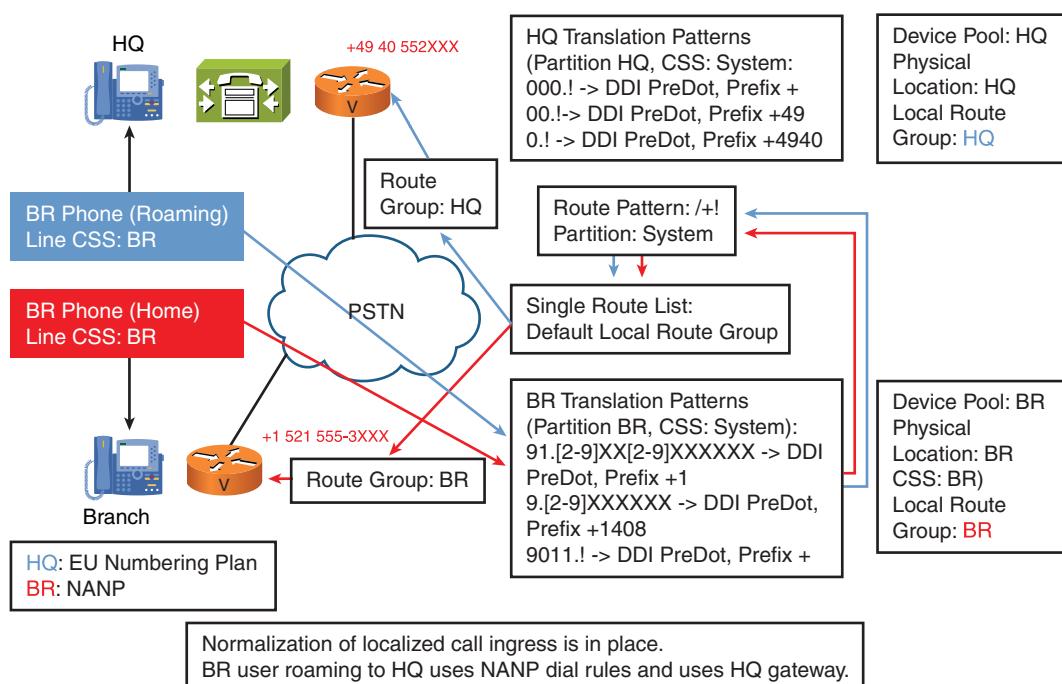


Figure 10-7 Example of Globalized Call Routing with Device Mobility

Figure 10-7 is based on the previous scenario: HQ is in Europe, and BR is in the United States. A BR user will roam to Europe.

However, in this example, globalized call routing has been implemented. Therefore, the (line) CSS of BR phones provides access to translation patterns that convert localized call ingress at the phone (NANP format) to global E.164 format. EU phones have access to translation patterns that convert EU input to global E.164 format.

A single PSTN route pattern (\+!) is configured; it is in a partition that is accessible by all translation patterns.

When a BR user roams to the HQ, the line CSS is not modified; no device CSS is configured at the phone or at the device pool. The Device Mobility groups are also not set (or are set differently).

As a result, there is effectively no change in matching the translation patterns: The BR user still uses NANP dial rules (like at home). The number is converted to international format by translation patterns and matches the (only) PSTN route pattern. The route pattern refers to a route list that is configured to use the default local route group. The default local route group is taken from the roaming device pool. Therefore, if the phone is physically located in the BR office, the local route group is BR; if the phone is roaming to the HQ site, the local route group is HQ. As a result, the local gateway is always used for a PSTN call.

If TEHO was configured, there would be a TEHO route pattern in E.164 format with a leading + sign. The TEHO pattern would refer to a site-specific route list in order to select the correct gateway for PSTN egress. The backup gateway would then again be selected by the local route group feature.

Device Mobility Configuration

The following steps describe how to configure Device Mobility on CUCM:

- Step 1.** Configure physical locations.
- Step 2.** Configure Device Mobility Groups.
- Step 3.** Configure device pools.
- Step 4.** Configure DMIs (that is, IP subnets).
- Step 5.** Set the Device Mobility mode using the following:
 - a.** A CCM service parameter to set the default for all phones.
 - b.** The Phone Configuration window for an individual configuration for each phone.

Steps 1 and 2: Configure Physical Locations and Device Mobility Groups

To configure physical locations and Device Mobility Groups, as shown in Figure 10-8, in CUCM navigate to Cisco Unified CM Administration and choose **System > Physical Location**. For each physical location, a name and a description are configured. Device Mobility Groups are configured under **System > Device Mobility > Device Mobility Group**. For each Device Mobility Group, a name and description are configured.

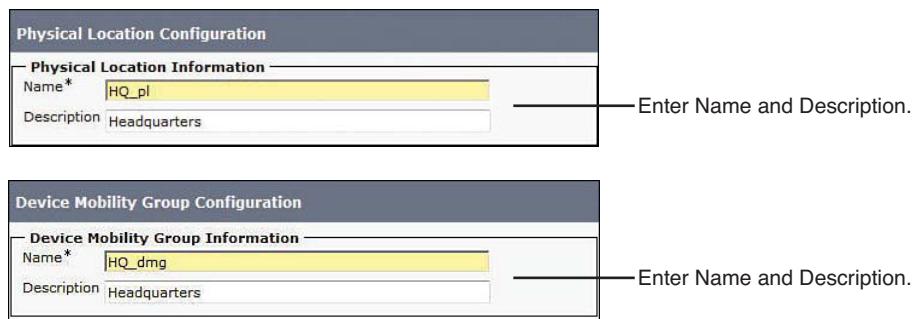


Figure 10-8 Steps 1 and 2: Configure Physical Locations and Device Mobility Groups

Note Device Mobility groups are not necessary when there is no need to change the device level CSS, AAR CSS, and AAR group. This principle applies also when local route groups are used in an environment where all sites share the same dial rules or in an environment where globalized call routing is implemented.

Step 3: Configure Device Pools

To configure a device pool when Device Mobility is used, as shown in Figure 10-9, in Cisco Unified CM Administration choose **System > Device Pool**.

A device pool is configured with a name and a CUCM group. It includes roaming-sensitive settings and Device Mobility-related settings configured under **Device Mobility Related Information**. The physical location and the Device Mobility Group, both configured under **Roaming Sensitive Settings**, are used to decide what settings should be applied to a phone. The options are no settings, the roaming-sensitive settings only, or the roaming-sensitive settings and the Device Mobility-related settings. The physical location and the Device Mobility Group themselves are not applied to the configuration of a phone but are used only to control which settings to apply.

Figure 10-9 does not show the local route group in the roaming-sensitive settings pane. Nevertheless, the local route group is a roaming-sensitive setting and is updated when the physical locations of the home device pool and the roaming device pool are different. The called party transformation CSS is shown in the Device Mobility-related settings pane, but this setting does not apply to IP Phones and hence is no Device Mobility-related setting, although shown as such in Figure 10-9.

Configure roaming-sensitive settings that can be applied to the phone configuration. The Local Route Group is also a roaming -sensitive setting!

Enter name and choose Cisco Unified Communications Manager group.

Device Pool Settings	
Device Pool Name*	HQ_dp
Cisco Unified Communications Manager Group*	Default
Calling Search Space for Auto-registration	< None >
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Local Route Group	< None >
Intercompany Media Services Enrolled Group	< None >

Roaming Sensitive Settings	
Date/Time Group*	CMLocal
Region*	HQ_phones
Media Resource Group List	HQ_mrgl
Location	HQ_Location
Network Locale	United States
SRST Reference*	HQ
Connection Monitor Duration***	
Single Button Barge*	Default
Join Across Lines*	Default
Physical Location	HQ_pl
Device Mobility Group	HQ_dmg

Device Mobility Related Information****	
Device Mobility Calling Search Space	< None >
AAR Calling Search Space	< None >
AAR Group	< None >
Calling Party Transformation CSS	< None >
Called Party Transformation CSS	< None >

Choose physical location and device mobility group to determine whether to apply roaming-sensitive settings and Device Mobility-related settings.

Configure Device Mobility-related settings. The Called Party Transformation CSS is not a Device-Mobility-related setting!

Figure 10-9 Step 3: Configure Device Pools

Step 4: Configure Device Mobility Infos

To configure a device pool when Device Mobility is used, as shown in Figure 10-10, in Cisco Unified CM Administration choose System > Device Mobility > Device Mobility Info. The DMIs are configured with a name, a subnet, and a subnet mask. Then, they are associated with one or more device pools.

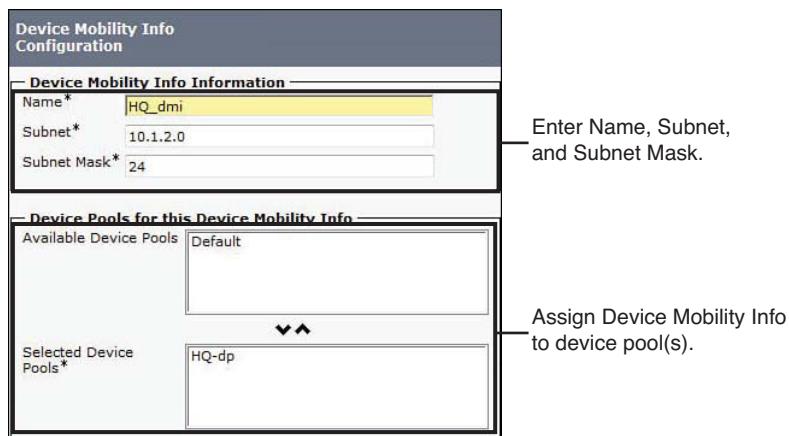


Figure 10-10 Step 4: Configure Device Mobility Info

Step 5a: Set the Device Mobility Mode CCM Service Parameter

Device Mobility is off by default and can be configured per phone. The default for the Device Mobility mode, if it's not set differently at the phone, is set under **System > Service Parameter**, as shown in Figure 10-11. Choose the Cisco CallManager service, and set the Device Mobility Mode to On or Off. Note that Off is the default. The parameter is found in the Clusterwide Parameters (Device - Phone) section.

Clusterwide Parameters (Device - Phone)	
Always Use Prime Line *	False
Always Use Prime Line for Voice Message *	False
Builtin Bridge Enable *	Off
Device Mobility Mode *	On
Auto Answer Timer *	1

Set the default Device Mobility mode for all phones.

Figure 10-11 Step 5a: Set the Device Mobility Mode CCM Service Parameter

Tip There are many entries in CUCM under **System > Service Parameter** after you choose Cisco CallManager. Press Ctrl-F in Internet Explorer and search for the specific title or entry.

Step 5b: Set the Device Mobility Mode for Individual Phones

As shown in Figure 10-12, you set the Device Mobility mode per phone in Cisco Unified CM Administration by choosing Device > Phone.

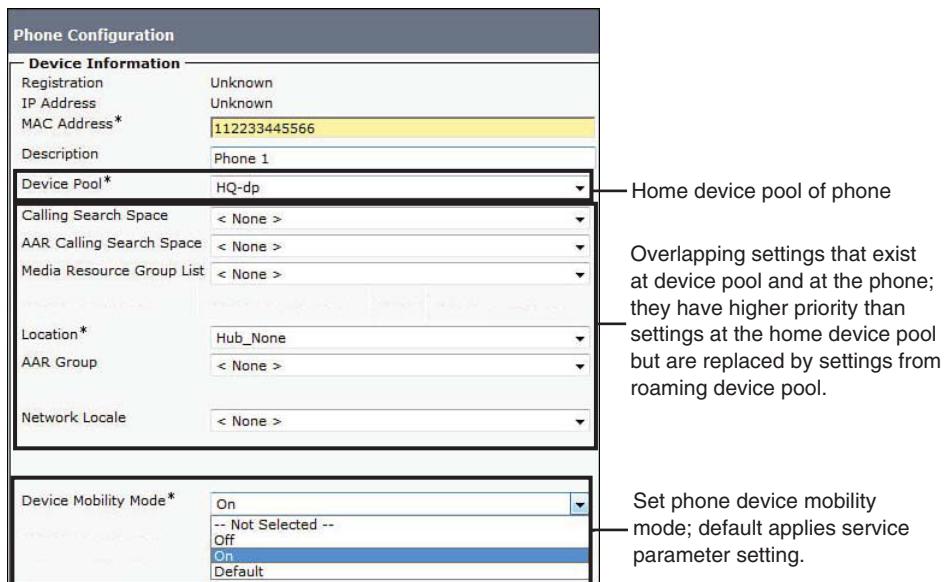


Figure 10-12 Step 5b: Set the Device Mobility Mode for Individual Phones

In the Phone Configuration window, you enable or disable Device Mobility for the phone by either setting the **Device Mobility Mode** to **On** or **Off** or leaving the default value **Default**. If the Device Mobility mode is set to **Default**, the Device Mobility mode is set at the Cisco CallManager service parameter.

Figure 10-12 also shows the configuration of the overlapping parameters, which are parameters that can be configured at both the phone and the device pool. The overlapping parameters for roaming-sensitive settings are Media Resource Group List, Location, and Network Locale. The overlapping parameters for the Device Mobility-related settings are Calling Search Space (called Device Mobility Calling Search Space at the device pool), AAR Group, and AAR Calling Search Space. Overlapping parameters configured at the phone have higher priority than settings at the home device pool and lower priority than settings at the roaming device pool.

Summary

The following key points were discussed in this chapter:

- Issues with roaming devices include inappropriate region, location, time zone, and SRST reference configuration. PSTN calls use the home gateway instead of the local gateway at the roaming site.
- Device Mobility allows roaming devices to be identified by their IP addresses. It also allows configuration settings to be applied that are suitable for the device's current physical location.
- Device Mobility configuration elements are Device Mobility Groups, physical locations, device pools, and DMIs.
- Roaming-sensitive settings are applied to devices that roam between physical locations. In addition, Device Mobility-related settings are applied to devices that roam within the same Device Mobility Group.
- After you configure Device Mobility Groups, physical locations, device pools, and DMIs, you need to enable Device Mobility either clusterwide as a service parameter or individually per phone.

References

For additional information, refer to these resources:

Cisco Systems, Inc. Cisco Unified Communications System 8.x SRND, April 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8x.html.

Cisco Systems, Inc. Cisco Unified Communications Manager Administration Guide Release 8.0(1), February 2010.
[www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_1/ccmfg/bccm-801-cm.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_1/ccmcfg/bccm-801-cm.html).

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in the "Answers Appendix."

1. Which setting is not modified for a laptop with IP Communicator when a user roams between sites when Device Mobility is enabled?
 - a. Region
 - b. Directory number
 - c. Location
 - d. SRST reference

2. Which two statements about the relationship between Device Mobility configuration elements are true?
 - a. Device Mobility Infos refer to one or more device pools.
 - b. Device pools refer to one or more physical locations.
 - c. Device pools refer to one Device Mobility Group.
 - d. Device pools refer to one Device Mobility Info.
 - e. Physical locations refer to Device Mobility Groups.
3. Which statement about Device Mobility operation is false?
 - a. A device pool is selected based on the roaming device's IP address.
 - b. If the selected device pool is the home device pool, no changes are made.
 - c. If the selected device pool is in a different Device Mobility Group than the home device pool, the Device Mobility-related settings of the roaming device pool are applied.
 - d. If the selected device pool is in a different physical location than the home device pool, the roaming-sensitive settings of the roaming device pool are applied.
4. If no device pool settings are configured on the phone, the settings configured on the phone are used.
 - a. True
 - b. False
5. Which two of the following are valid issues that Device Mobility fixes by changing the settings for roaming (mobile) phones in CUCM?
 - a. SRST References for mobile phones are dynamically assigned.
 - b. Phone speed dials for mobile phones are dynamically assigned.
 - c. Phone services for mobile phones are dynamically assigned.
 - d. Region settings for mobile phones are dynamically assigned.
 - e. Call Forward settings for mobile phones are dynamically assigned.
6. Which of the following statements about Device Mobility is the most accurate?
 - a. Device Mobility is essentially the same as Extension Mobility.
 - b. Device Mobility has been available in CUCM and CCM since version 3.0.
 - c. Device Mobility is a new feature added in CUCM v6.x and later.
 - d. Device Mobility greatly enhances Cisco IP Phone services for mobile users.

7. What is the correct configuration relationship between Device Pools and Device Mobility in CUCM?
 - a. IP Phones may optionally be configured to use Device Pools when enabling Device Mobility.
 - b. IP Phones must be configured to use Device Pools when enabling Device Mobility.
 - c. Device pools can optionally be configured to work with Device Mobility.
 - d. Device pools are not used when enabling Device Mobility.
8. Which statement about configuring Device Mobility in a CUCM cluster is true?
 - a. Device Mobility is enabled by default in the cluster and must be enabled for devices in CUCM v6.
 - b. Device Mobility is disabled by default and must be enabled for the CUCM Cluster and then configured for individual devices in CUCM.
 - c. Device Mobility is enabled by default in the cluster and must be enabled for devices in all versions of CCM and CUCM.
 - d. Device Mobility is disabled by default and must be enabled for the CUCM Cluster and then configured for individual devices in all versions of CCM and CUCM.
9. Which three of the following are valid Device Mobility Configuration Elements?
 - a. Device pool
 - b. Region
 - c. Physical location
 - d. Device Mobility Group
 - e. CUCM server
 - f. Cisco IP Phone
10. Which statement is *not* correct about the interaction of Device Mobility and globalized call routing?
 - a. The user of a roaming phone can use the home dial rules.
 - b. The user of a roaming phone can use the home dial rules, but then the home gateway is used all the time.
 - c. The user of a roaming phone can use the roaming gateway.
 - d. The same device mobility group can be used at all device pools.

Chapter 11

Implementing Extension Mobility

Upon completing this chapter, you will be able to describe and configure Extension Mobility to allow roaming users to log in to any device and have the device reconfigured with their personal settings. You will meet these objectives:

- Identify issues with users roaming between sites
- Describe the Cisco Extension Mobility feature
- Describe the Cisco Extension Mobility configuration elements and their interaction
- Describe Cisco Extension Mobility operation
- Configure and implement Cisco Extension Mobility

In multisite environments, it is common for some users to roam between sites on a regular basis. When such users use phones that are provided at the sites they visit, they want to, but traditionally cannot, use their personal phone settings, such as their directory number, speed dials, calling privileges, and Message Waiting Indicator (MWI). A Unified Communications solution can solve this problem.

This chapter describes Extension Mobility, a feature of Cisco Unified Communications Manager (CUCM) that allows CUCM users to log in to an IP Phone and get their personal profile applied, regardless of the device and physical location that they are using.

Issues with Users Roaming Between Sites

Chapter 10, “Implementing Device Mobility,” addressed the situation when users travel to other sites within their organization and bring their phone with them, such as IP communicator on their laptop,. This chapter addresses issues that can occur if users temporarily change their workplace and roam between different sites but do not travel with a device and instead use an available phone at the current location. When users roam between sites and do not have their phone with them as shown in Figure 11-1, they might want to use an available phone at the site they have traveled to. Some organizations call this “hoteling” and often provide offices or cubicles for traveling employees.

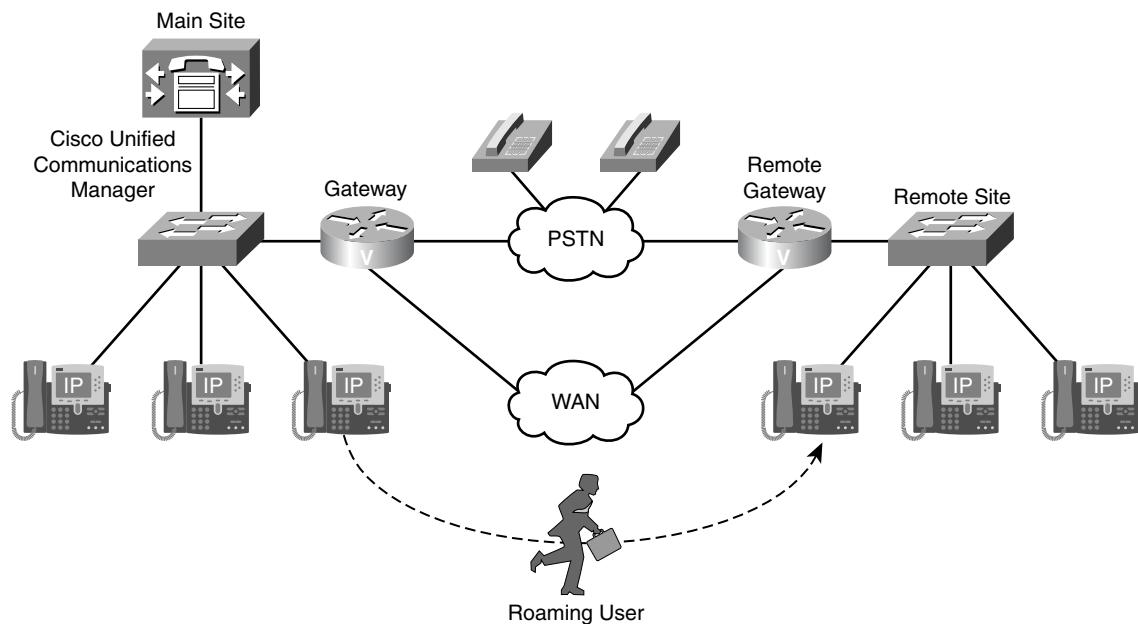


Figure 11-1 Roaming Users

Issues with Roaming Users

Without Extension Mobility, when a user uses a different guest phone in a different site, this leads to the following issues:

- Extensions are traditionally bound to constant devices.
- The user gets the wrong extension on that phone.
- The user gets the wrong calling privileges.
- The user does not have speed dials available.
- The user has the wrong services assigned.
- MWI status does not work with a different extension.

To effectively address these issues, the user would require CUCM to reconfigure the phone that is used with user-specific configuration instead of having device-specific settings applied to the phone.

Table 11-1 Extension Mobility Solves Issues of Roaming Users

Issue Without Extension Mobility	Extension Mobility Feature to Solve the Issue
Extensions are bound to physical devices.	Extensions are bound to device profiles.
Speed dials are assigned to physical devices.	Speed dials are assigned to device profiles.
Services are assigned to physical devices.	Services are assigned to device profiles.
MWI status is defined for physical devices.	MWI status is updated during Extension Mobility login.
Calling privileges are defined for physical devices and locations.	Calling privileges result from merging line settings (device-based) and physical device settings (location-related).

Extension Mobility Solves Issues of Roaming Users

Extension Mobility offers functionality that is designed to enhance the mobility of users within a CUCM cluster. It also resolves the issues of roaming users with Extension Mobility, which are summarized in Table 11-1.

Although the device is not the user's home device, it is reconfigured with user-specific settings that are stored in profiles. This action lets you separate user-specific parameters configured in user profiles from device-specific parameters that are still stored at the phone configuration along with default values for user-specific settings. The phone adapts some of its behavior based on the individual user who is currently using the phone.

The configuration changes are triggered by a user login where the user is identified by a user ID and PIN. The phone configuration adapts to the individual user. When the user stops using the phone, she logs out, and the default configuration is reapplied.

The use of Extension Mobility Device Profiles on a Cisco IP Phone is analogous to a user profile on a computer on most desktop operating systems (OS). When two or more users share the same computer, their login profile customizes their desktop for settings, such as wallpaper, desktop icons, taskbar settings, and so on. Similarly, when two or more traveling users share the same Cisco IP Phone, their login profile customizes their phone settings and functionality.

CUCM Extension Mobility Overview

CUCM Extension Mobility allows users to log in to any phone and get their individual user-specific phone configuration applied to that phone. Thus, users can be reached at their personal directory number, regardless of their location or the physical phone they are using. Extension Mobility is implemented as a phone service and works by default within a single CUCM cluster. With CUCM v8.x or later, Extension Mobility Cross Cluster (EMCC) can be enabled. EMCC is not covered in this book.

The user-specific configuration is stored in device profiles. After successful login, the phone is reconfigured with user-specific parameters, and other device-specific parameters remain the same. If a user is associated with multiple device profiles, he must choose the device profile to be used.

If a user logs in with a user ID that is still logged in at another device, one of the following options can be configured:

- **Allow multiple logins:** When this method is configured, the user profile is applied to the phone where the user is logging in, and the same configuration remains active at the device where the user logged in before. The line number or numbers become shared lines because they are active on multiple devices.
- **Deny login:** In this case, the user gets an error message. Login is successful only after the user logs out at the other device where she logged in before.
- **Auto-logout:** Like the preceding option, this option ensures that a user can be logged in on only one device at a time. However, it allows the new login by automatically logging out the user at the other device.

On a phone configured for Extension Mobility, either another device profile that is a logout device profile can be applied, or the parameters as configured at the phone are applied. The logout itself can be triggered by the user or enforced by the system after expiration of a maximum login time.

Extension Mobility: Dynamic Phone Configuration Parameters

Two types of configuration parameters are dynamically configured when CUCM Extension Mobility is used:

- **User-specific device-level parameters:** These are user-specific phone configuration parameters such as user Music On Hold (MOH) audio source, phone button templates, softkey templates, user locales, Do Not Disturb (DND), privacy settings, and phone service subscriptions. All these parameters are configured at the device level of an IP Phone.
- **Configuration of phone buttons, including lines:** All phone buttons—not only the button types as specified in the phone button template but also the complete configuration of the phone buttons—are updated by Extension Mobility. This update includes all configured lines, with all the line-configuration settings, speed dials, service URLs, Call Park buttons, and any other buttons that are configured in the device profile that is to be applied.

Extension Mobility with Dynamic Phone Configuration by Device Profiles

Figure 11-2 illustrates how user-specific settings roam with the user when the user logs out of one phone at the main site and then logs in to an Extension Mobility-enabled phone located at the remote site.

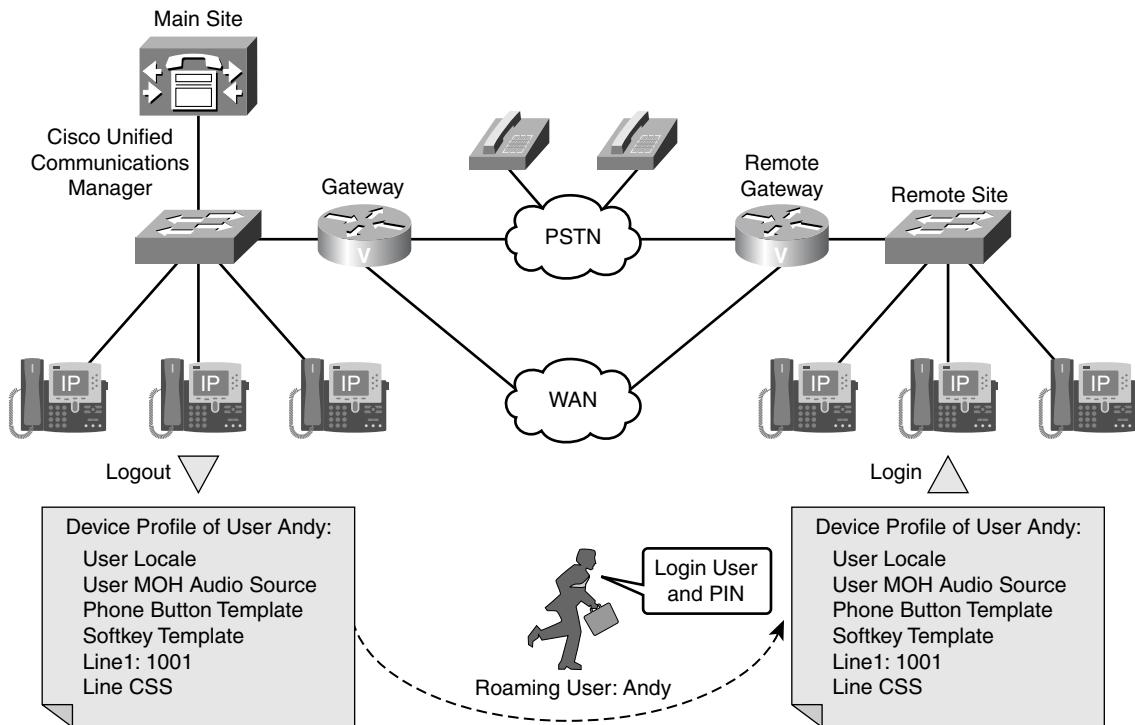


Figure 11-2 Extension Mobility Dynamic Phone Configuration by Device Profiles

As shown in Figure 11-2, the user-specific parameters, such as device-level parameters and all phone button settings including line configurations, are configured in device profiles. Based on the user ID entered during login, CUCM can apply the user's personal device profile and reconfigure the phone with the configuration profile of the individual user who logs in.

With Extension Mobility, CUCM is aware of the end user sitting behind a device and applies the appropriate user-specific configuration based on a device profile associated with the logged-in user.

CUCM Extension Mobility Configuration Elements

Table 11-2 lists the configuration elements related to Extension Mobility and describes their functions. The configuration elements that are introduced with Extension Mobility are the device profile and the default device profile.

The device profile is configured with all user-specific settings that are found at the device level of an IP Phone, such as user MOH audio source, phone button templates, softkey templates, user locales, DND and privacy settings, phone service subscriptions, and all phone buttons, including lines and speed dials. One or more device profiles are applied to an end user in the End User Configuration window.

Table 11-2 Extension Mobility Configuration Elements

Configuration Element Name	Configuration Element Function
Phone	Stores the configuration of physical phones. Configuration parameters include device-specific phone parameters (such as device CSS, location, or MRGL), user-specific phone parameters (such as user MOH audio source, DND, or soft-key template), and (user-specific) button configuration (such as lines or speed dials).
End user	The end user is associated with one or more device profiles. The user ID and the PIN are used to log in to a phone with Extension Mobility.
Device profile	Stores user-specific phone configuration in logical profiles. Configuration parameters include user-specific phone and button parameters (such as lines and speed dials). The parameters of the device profile are applied to a physical phone after a user logs in to the phone using Extension Mobility.
Phone service	Extension Mobility is implemented as a phone service. Hardware phones and device profiles have to be subscribed to the service.
Default device profile	Stores the default device configuration parameters that should be applied when the phone model of a user's device profile is different from the phone model of the phone where the user logs in. A default device profile is automatically created for every phone model that has Cisco Extension Mobility activated and can be viewed by navigating to Cisco Unified CM Administration to Device > Device Settings > Default Device Profile > Device Profile Type (select) > Next.

The default device profile stores default device configuration parameters that are applied by Extension Mobility when there is a mismatch between the actual phone model where the user logs in and the phone model configured in the user's device profile. The default device profile exists once per phone model type and per protocol for SIP and SCCP. All the parameters that cannot be applied from the user's device profile are taken from the default device profile.

For example, a user is associated with a device profile for a Cisco Unified IP Phone 7945 running SCCP. If this user logs on to a Cisco Unified IP Phone 7965 running SIP, some features exist on the target phone that cannot be configured at the Cisco Unified IP Phone 7945 device profile. In this case, the configuration parameters that are unavailable on the user's device profile are taken from the default device profile of the Cisco Unified IP Phone 7945 SCCP.

If a device profile includes more parameters than are supported on the target phone, the additional settings are ignored when the target phone with the user-specific settings is reconfigured.

Note For ease of administration, configuration is much simpler if an organization chooses and standardizes a single Cisco IP Phone model at its different locations for Extension Mobility.

Note The default device profile is not applied if a device profile of a user and the phone on which the user tries to log in are of the same phone model series; for example, Cisco Unified IP Phone 7960, 7961, or 7965.

Note CUCM automatically creates a default device profile for a specific phone model and protocol as soon as Cisco Extension Mobility is enabled on any phone configuration page for this phone model.

Relationship Between Extension Mobility Configuration Elements

As shown in Figure 11-3, an end user is associated with one or more device profiles. For each possible IP Phone model, whether SCCP or SIP, a default device profile can be configured. Because Extension Mobility is implemented as an IP Phone service, all phones that should support Extension Mobility *must* be subscribed to the Extension Mobility phone service to allow a user to log in to the phone. In addition, each device profile *must* be subscribed to the Extension Mobility phone service. This subscription is required to allow a user to log out of a phone.

The Cisco IP Phone models 7940 and 7965 are shown as an example in Figure 11-3, but they are not the only Cisco IP Phones supported in CUCM for Extension Mobility.

CUCM Extension Mobility Operation

The following steps, illustrated in Figure 11-4, describe how Extension Mobility works, how phone model mismatches are handled, and how calling search spaces and partitions are updated when CUCM Extension Mobility is used.

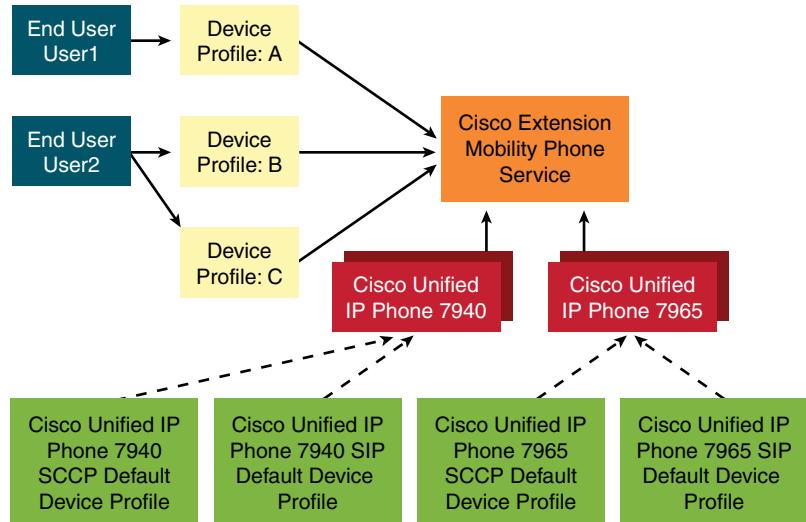


Figure 11-3 Relationship Between Extension Mobility Configuration Elements

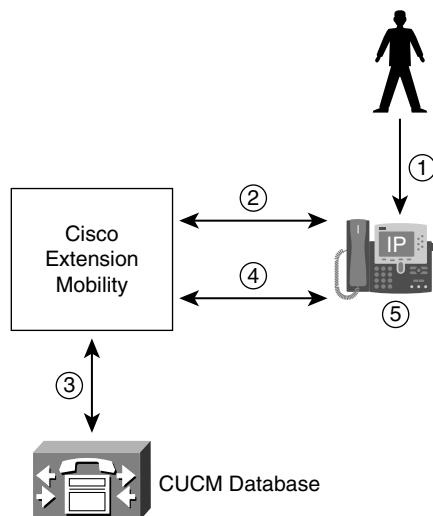


Figure 11-4 Extension Mobility Login Process

When a phone user wants to log in to a phone with Extension Mobility, the following sequence of events occurs:

1. The user presses the Services button on the phone and chooses the Extension Mobility service from the list of phone services available at the phone. The

administrator can name the Extension Mobility service to a different name, in which case that would be the service name the user would select.

2. The Extension Mobility service requires the user to log in using his user ID and PIN. The user enters the required data on the phone by pressing each phone button as many times as needed to select the alphanumeric characters for his user ID and PIN. Therefore, it is suggested to use numerical usernames and PINs to make login easier.
3. If the entered user ID and PIN are correct, Extension Mobility chooses the device profile that is associated with the user.

Note If a user is associated with more than one device profile, all associated profiles are displayed, and the user has to choose the desired profile, as illustrated for User2 in Figure 11-3. Assigning multiple profiles to a user means that the user is provided with a separate device profile for each site. Doing this is common when the traditional approach is used to implement Calling Search Spaces (CSS). Extension Mobility updates only the line configuration, including the line CSS, but not the device CSS. To allow the choice of a local gateway for outbound PSTN calls, a different line CSS has to be applied for each site. In such a scenario, the user chooses a site-specific device profile that differs from the device profile that is used at other sites in its line CSS. The line CSS of such site-specific profiles gives access to route patterns that route PSTN calls to the appropriate local gateway to minimize toll charges. Extension Mobility also works well if the more modern approach of gateway selection of PSTN at the device (phone) level and blocking the CSS at the line level is implemented.

4. CUCM updates the phone configuration with the settings of the chosen device profile. User-specific device-level parameters, lines, and other phone buttons are updated with user-specific settings.
5. The IP Phone is reset and loads the updated configuration.

At this point, the phone can be used just as it would be used in the home location. From the user's phone experience, directory numbers, speed dials, and MWI are all correct, as if the user were still on his home desk phone, regardless of the location and the IP Phone that is used.

Users can log out of Extension Mobility by pressing the **Services** button again and choosing **Logout** in the Extension Mobility service. If users do not log out themselves, the system can be set to automatically log them out after the maximum login time expires. The administrator can configure the CUCM service parameter for the maximum login time. Users can log out only if the Extension Mobility service has been added to their profile.

Users are also automatically logged out of a phone when they log in to another phone and when CUCM is configured for auto-logout on multiple logins. Another option is that the next user of the phone logs out a previous user to be able to log in and have the phone updated with the settings of that new user. After logout, CUCM reconfigures the

phone either with the standard configuration of the IP Phone or by using another device profile, as specified in the Phone Configuration window.

Issues in Environments with Different Phone Models

When different IP Phone models are implemented in a CUCM cluster where Extension Mobility is enabled, an end user may log in to an IP Phone that is a different model than the one configured in the user's device profile, as shown in Figure 11-5.

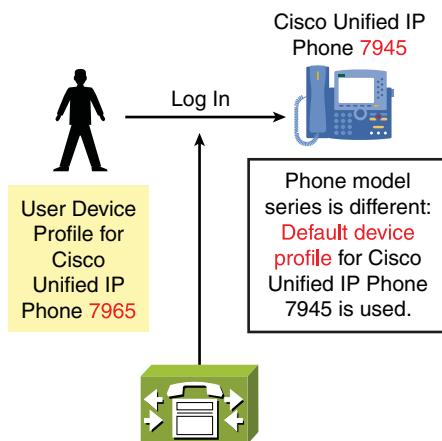


Figure 11-5 Logging into a Different Phone Model with Extension Mobility

Because different phones support different features, when a user logs in to a phone that supports more features than the model associated with the user, the default device profile is used to apply parameters that are supported by the target phone but that are not included in the user's device profile. The default device profile includes phone configuration parameters such as phone button templates, softkey templates, phone services, and other phone configuration settings, but it does not include line or feature button configurations.

The result is that some phone features available on the user's home desk are unavailable on his remote phone when he logs in with Extension Mobility.

Default Device Profile and Feature Safe

Figure 11-6 illustrates the feature safe functionality of Cisco Extension Mobility.

The default device profile is applied only if a user's device profile and the phone on which the user tries to log in are of a different phone model series (for example, Cisco Unified IP Phone Series 794x, 796x, or 797x).

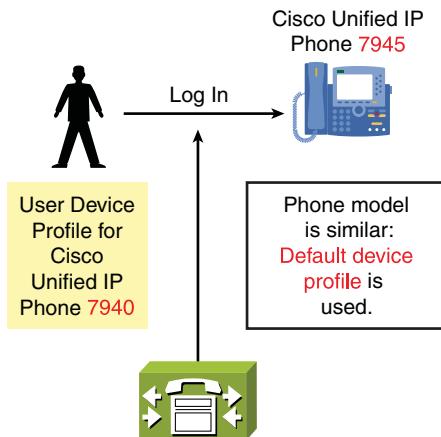


Figure 11-6 Default Device Profile and Feature Safe for Similar Device Profile

When the phone model series of the physical phone and the user device profile are the same, the feature safe function allows different phone models to be used for user device profiles and physical phone models. For example, a user with an associated device profile for a Cisco Unified IP Phone 7940 phone can log into a Cisco Unified IP Phone 7945 phone without having the default device profile applied.

No administrative tasks are required to enable feature safe. Feature safe is independent of the used signaling protocol (SIP or SCCP).

How Cisco Extension Mobility Handles Phone Model Differences

After successful authentication, if the phone model series of the device profile does not match the phone model series of the used phone, the following happens:

1. Device-dependent parameters, such as phone button template and softkey template, from the default device profile are applied to the phone.
2. The system copies all device-independent configuration settings (user hold audio source, user locale, speed dials, and line configuration, except for the parameters that are specified under Line Setting for This Device) from the device profile to the login device.
3. The applicable device-dependent parameters of the device profile of the user are applied. These parameters include buttons (such as line and feature buttons) that are based on the phone button template applied from the default device profile.
4. If supported on the login device, phone-service subscriptions from the device profile of the user are applied to the phone.

5. If the user's device profile does not have phone services configured, the system uses the phone services that are configured in the default device profile of the login device.

For example, the following events occur when a user who has a device profile for a Cisco Unified IP Phone 7960 logs into a Cisco Unified IP Phone 7905:

1. The personal user hold audio source, user locale, speed dials (if supported by the phone button template that is configured in the Cisco Unified IP Phone 7905 default device profile), and directory number configuration of the user are applied to the Cisco Unified IP Phone 7905.
2. The phone button template and the softkey template of the default device profile are applied to the Cisco Unified IP Phone 7905.
3. The user has access to the phone services that are configured in the Cisco Unified IP Phone 7905 default device profile.

Cisco Extension Mobility and CSSs

Cisco Extension Mobility does not modify the device CSS or the Automated Alternate Routing (AAR) CSS (both of which are configured at the device level). Cisco Extension Mobility replaces the line CSS/CSSs that are configured at the phone with the line CSS/CSSs that are configured at the device profile of the logged-in user.

Thus, in an implementation that uses the line/device approach, the following applies:

- The line CSS of the login device is updated with the line CSS of the user. This update is used to enforce the same class of service (CoS) settings for the user, independent of the physical device to which the user is logged in.
- The device CSS of the login device is not updated, and the same gateways (those that were initially configured at the phone before the user logged in) are used for external route patterns. Because the phone did not physically move, the same local gateways should be used for PSTN calls, even when a different user is currently logged into the device.

If the traditional approach is used to implement partitions and CSS, the following applies:

- If only device CSSs are used, the CSS is not updated, and no user-specific privileges can be applied. The user inherits the privileges that are configured at the device that is used for logging in.
- If only line CSSs are used, the line CSS that is configured at the device profile of the user replaces the line CSS of the login device. In a multisite environment, this configuration can cause problems in terms of gateway choice because the same gateway is always used for external calls. To avoid gateway selection problems in such an environment, you should use local route groups.

Alternatives for Mismatching Phone Models and CSS Implementations

To avoid issues with mismatching IP Phone models or with calling privileges when the traditional approach for implementing partitions and CSSs is used, multiple device profiles can be configured per user.

When different phone model series are used, issues can arise when the settings of the default device profile are applied. Different users might require different settings. This problem can be solved by creating multiple device profiles per user. When you configure and associate one device profile (per phone model) with a username, CUCM displays this list of profiles after successful login. The user can choose a device profile that matches the phone model of the login device. However, if many users need to use Cisco Extension Mobility and many different phone models are used, this solution does not scale well.

The same concept can be used as an alternative to the line/device approach for implementing CSSs. A separate device profile can be created per site and is configured with the appropriate CSS to allow local gateways to be used for external calls. Again, the user chooses the corresponding device profile after logging in, and the correct CoS and gateway choice are applied without depending on a separate line and device CSS. The recommendation, however, is to use the line/device approach in a multisite environment, because that approach simplifies the dial plan and scales better.

Note When using the traditional CSS approach with only one CSS applied at the line, use local route groups to prevent gateway-selection problems.

CUCM Extension Mobility Configuration

The following steps are required to configure Extension Mobility in CUCM. They are explained in detail in the following sections:

- Step 1.** Activate the Cisco Extension Mobility service in CUCM for the cluster.
- Step 2.** Set Cisco Extension Mobility service parameters.
- Step 3.** Add the Cisco Extension Mobility phone service.
- Step 4.** Create default device profiles for all phone models used.
- Step 5.** Create device profiles, and subscribe them to the Cisco Extension Mobility phone service.
- Step 6.** Create end users, and associate them with device profiles.
- Step 7.** Enable Extension Mobility for phones, and subscribe the phones to the Cisco Extension Mobility service.

Step 1: Activate the Cisco Extension Mobility Feature Service

Activate the Cisco Extension Mobility feature service by choosing **Tools > Service Activation** in CUCM Serviceability, as shown in Figure 11-7. Extension Mobility is disabled by default on a new CUCM Cluster installation.

Service Name	Activation Status
Cisco CallManager	Activated
Cisco Tftp	Activated
Cisco Messaging Interface	Deactivated
Cisco Unified Mobile Voice Access Service	Deactivated
Cisco IP Voice Media Streaming App	Deactivated
Cisco CTIManager	Deactivated
Cisco Extension Mobility	Activated
Cisco Extended Functions	Deactivated
Cisco Dialed Number Analyzer	Deactivated
Cisco DHCP Monitor Service	Deactivated

Figure 11-7 Step 1: Activate the Cisco Extension Mobility Service

Note Starting with CUCM version 6.0, Cisco Extension Mobility is considered a user-facing feature and can be activated on any server in a CUCM cluster to provide a redundant Cisco Extension Mobility environment.

Step 2: Set Cisco Extension Mobility Service Parameters

The Cisco Extension Mobility service has several configurable service parameters. Choose **System > Service Parameters** in CUCM, as shown in Figure 11-8. Select your CUCM server, and select **Cisco Extension Mobility (Active)**. Press the **Advance** button on the bottom to see all the options shown in Figure 11-8.

Choose Server and select Cisco Extension Mobility Service.

Parameter Name	Parameter Value	Suggested Value
Enforce Maximum Login Time *	False	False
Maximum Login Time *	8:00	8:00
Multiple Login Behavior *	Multiple Logins Not Allowed	Multiple Logins Not Allowed
Alphanumeric User ID *	True	True
Remember the Last User Logged In *	False	False
Clear Call Log *	False	False

There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

Enable or disable alphanumeric user IDs, remembering the last logged in user, and clearing the call log on logout.

Enable or disable auto-logout after expiration of maximum login time.

Set the multiple login behavior: Allowed, disallowed, or auto-logout.

Figure 11-8 Step 2: Set Cisco Extension Mobility Service Parameters

If the Enforce Maximum Login Time parameter is set to True, the user is automatically logged out after the Maximum Login Time expires. The Multiple Login Behavior parameter specifies how to handle users who log in to a device but are still logged in at another device. Three options exist: Login can be denied, login can be allowed, or the user can be automatically logged out from a phone where she logged in earlier and did not log out.

Alphanumeric user IDs can be enabled or disabled. The phone can remember the last logged-in username. This username can be presented as a default on the next login if you set the Remember the Last User Logged In parameter. Finally, call lists can be preserved or cleared at logout, depending on the setting of the Clear Call Log service parameter.

Note All these parameters are clusterwide service parameters of the Cisco Extension Mobility service. You can access them from CUCM Administration by choosing System > Service Parameters.

Step 3: Add the Cisco Extension Mobility Phone Service

Add the Cisco Extension Mobility phone service, as shown in Figure 11-9.

Cisco Extension Mobility is implemented as a phone service. Therefore, it needs to be added to the available phone services in CUCM. To add the Cisco Extension Mobility phone service, in CUCM Administration, choose Device > Device Settings > Phone

The screenshot shows the 'IP Phone Services Configuration' page. In the 'Service Information' section, the 'Service Name*' field is set to 'EM Logon / Logoff', 'ASCII Service Name*' is also 'EM Logon / Logoff', 'Service Description' is 'Extension Mobility Logon Logoff Service', and 'Service URL' is '10.80.80.10:8080/emapp/EMAppServlet?device=#DEVICENAME#'. A note to the right explains that the URL should be 'http://Server IP_Address:8080/emapp/EMAppServlet?device=#DEVICENAME#'. Below this, under 'Enable', the 'Enable' checkbox is checked, and the 'Enterprise Subscription' checkbox is unchecked.

Enable the Cisco Extension Mobility IP phone service

Enter service name and service description; enter Cisco Extension Mobility service URL: http://Server IP_Address:8080/emapp/EMAppServlet?device=#DEVICENAME#

Figure 11-9 Step 3: Add the Cisco Extension Mobility Phone Service

Services and select Add New. Configure the Cisco Extension Mobility service with a service name and description, and then enter the service URL:

`http://IP address of server:8080/emapp/EMAppServlet?device=#DEVICENAME#`

Note The service URL is case-sensitive and must be entered exactly as worded, except that you replace the “*IP address of server*” in the URL above with the actual IP address of your CUCM server with Extension Mobility enabled. Be sure not to change anything else when entering this URL.

Step 4: Create Default Device Profiles

If multiple phone models are used for Extension Mobility, you might want to enable default device profiles.

To configure a default device profile, as shown in Figure 11-10, in CUCM Administration, choose Device > Device Settings > Default Device Profile. First, you must choose the product type, which is the phone model, select Next, and then select the device protocol and select Next again. Then, you can configure the settings on the default device profile.

Default Device Profile Configuration

Status
Status: Ready

Default Device Profile Information

Product Type:	Cisco 7965
Device Protocol:	SCCP
Device Profile Name:	Cisco 7965 SCCP
Description:	
User Hold MOH Audio Source	< None >
User Locale	< None >
Phone Button Template*	-- Not Selected --
Softkey Template	< None >
Privacy*	Default
Single Button Barge	Default
Join Across Lines	Default
Always Use Prime Line*	Default
Always Use Prime Line for Voice Message*	Default
<input type="checkbox"/> Ignore Presentation Indicators (internal calls only)	
<input type="checkbox"/> Do Not Disturb	
DND Option*	Use Common Phone Profile Setting
DND Incoming Call Alert	< None >
Extension Mobility Cross Cluster CSS	< None >

Multilevel Precedence and Preemption (MLPP) Information

MLPP Domain	< None >
MLPP Indication*	Default
MLPP Preemption*	Default

Select phone model and protocol.

Select default phone configuration for the selected phone type.

Figure 11-10 Step 4: Create Default Device Profiles

Note The available configuration options depend on the phone model and protocol you choose. The default device profile does not include phone button configuration (for example, lines or features buttons), but it does include the phone button template.

Step 5a: Create Device Profiles

To create and configure device profiles, in CUCM Administration, choose **Device > Device Settings > Device Profile**, as shown in Figure 11-11. Select **Add New**. After choosing the phone model and protocol, you can configure user-specific device configuration parameters. After the phone button template is configured, the appropriate buttons can be configured. The **Device Profile Name** will be unique for each Extension Mobility user. Repeat this step in full with a unique name for each user that will use Extension Mobility.

In the Device Profile Configuration window, choose **Subscribe/Unsubscribe Services** from the Related Links in the upper right of the window, and click **Go**. Then, choose the phone service you added in Step 3, click **Next**, and enter the name with which the phone

service should be displayed in the list of phone services at the IP Phone after the Services button is pressed. Click **Subscribe**, and then click **Save**. The device profile is now subscribed to the Cisco Extension Mobility service.

Configure phone lines and buttons.	Select phone model and protocol.	Enter device profile name and description.

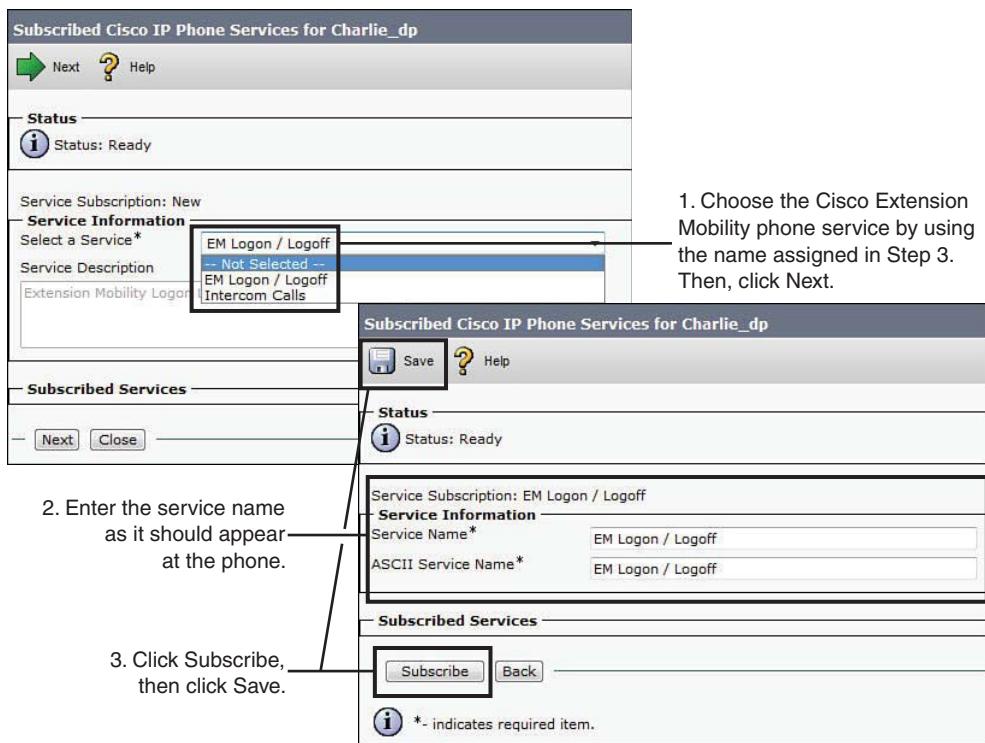


Figure 11-12 Step 5b: Subscribe the Device Profile to the Cisco Extension Mobility Phone Service

Caution If the device profile is not subscribed to the Cisco Extension Mobility service, users do not have access to Cisco Extension Mobility phone service after they log in and their device profile has been applied. As a result, users can no longer log out of Cisco Extension Mobility at the phone. Therefore, make sure that you do not forget to subscribe the phones (see Step 7b)—and the device profiles—that you use for Cisco Extension Mobility to the Cisco Extension Mobility phone service. Since CUCM version 7, an enterprise subscription can be enabled at each phone service. If an enterprise subscription is enabled, the corresponding phone service applies to all phones and device profiles.

Step 6: Associate Users with Device Profiles

In the End User Configuration window, which you get to by choosing **User Management > End User**, choose the device profile or profiles that you want to associate with the user in the list of Available Profiles. Click the down arrow to add them to the list of Controlled Profiles, as shown in Figure 11-13. You can also set the Default Profile. Repeat this step for every user you want to set up with Extension Mobility.

End User Configuration

Save Add New

User Information

User ID*	CharlieS
Password	*****
Confirm Password	*****
PIN	*****
Confirm PIN	*****
Last name*	Sweetland
Middle name	
First name	Charlie
Telephone Number	
Mail ID	
Manager User ID	
Department	
User Locale	English, United States
Associated PC	
Digest Credentials	
Confirm Digest Credentials	

Device Information

Controlled Devices	
Available Profiles	Charlie_dp
CTI Controlled Device Profiles	

Extension Mobility

Available Profiles	
Controlled Profiles	Charlie_dp
Default Profile	Charlie_dp
Presence Group*	Standard Presence group
SUBSCRIBE Calling Search Space	< None >
<input checked="" type="checkbox"/> Allow Control of Device from CTI	
<input type="checkbox"/> Enable Extension Mobility Cross Cluster	

Figure 11-13 Step 6: Associate Users with Device Profiles

Step 7a: Configure Phones for Cisco Extension Mobility

Next, the phone has to be enabled for Cisco Extension Mobility and subscribed to the Cisco Extension Mobility phone service. Figure 11-14 shows the first part of enabling Cisco Extension Mobility on a phone. Choose **Device > Phone**, scroll down in the phone settings, and check the **Enable Extension Mobility** check box to enable Cisco Extension Mobility. Then, choose a specific device profile or the currently configured device settings to be used during the logout state. The recommendation is to use the current device settings. Repeat this step for every phone in the CUCM cluster that Extension Mobility users will use.

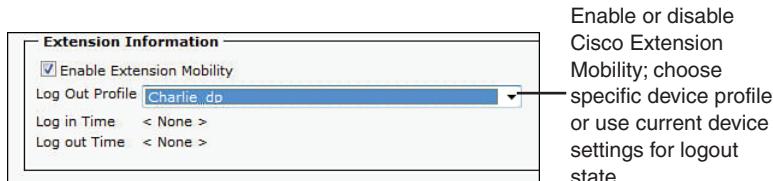


Figure 11-14 Step 7a: Configure Phones for Cisco Extension Mobility

Note If you choose a device profile as a logout profile, you will not be able to delete it until it is unassigned from the phone as it was assigned in Figure 11-14.

Step 7b: Subscribe the Phone to the Extension Mobility Phone Service

The last step of Cisco Extension Mobility configuration is to subscribe the IP Phone to the Cisco Extension Mobility phone service. This is the same as the process that was explained in Step 5, where the device profile was subscribed to the Cisco Extension Mobility service. In the Phone Configuration window, use the related link **Subscribe/Unsubscribe Services** to open the Subscribed Cisco IP Phone Services window and subscribe to the service, as shown in Figure 11-15. Repeat this step for every phone in the CUCM cluster that Extension Mobility users will use.

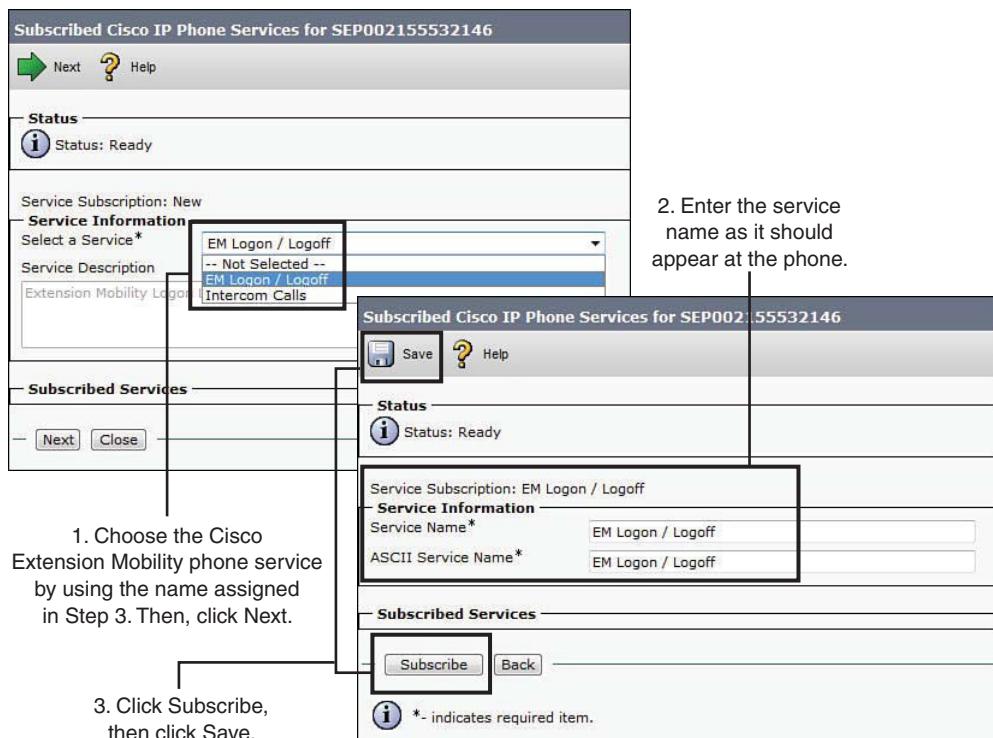


Figure 11-15 Step 7b: Subscribe the Phone to the Cisco Extension Mobility Phone Service

Tip If you have correctly configured Extension Mobility on a phone, and if you press Services on the phone to log in to Extension Mobility, you might not get any response on a new Cisco IP Phone. The solution is to do a full-factory default restore on the IP Phone. Unplug the IP Phone, plug it back in while holding the # key. Then, press 1 2 3 4 5 6 7 8 9 * 0 #. The full reset takes about 10 minutes with several phone reboots. Be patient. This factory default restore does not change any CUCM configurations for the IP Phone.

Summary

The following key points were discussed in this chapter:

- The Device Mobility and Extension Mobility features of CUCM allow users to roam between sites.
- Extension Mobility enables users to log in to IP Phones and apply their profiles, including extension number, speed dials, services, MWI status, and calling privileges.

- The user's device profile is used to generate the phone configuration in the login state.
- Seven steps are needed to configure Extension Mobility.

References

For additional information, refer to these resources:

Cisco Systems, Inc. Cisco Unified Communications System Release 8.x SRND. San Jose, California, April 2010.

www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8xsrnd.pdf.

Cisco Systems, Inc. *Cisco Unified Communications Manager Administration Guide Release 8.0(2)*. San Jose, California, March 2010.

www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmcfg/bccm.pdf.

Cisco Systems, Inc. *Cisco Unified Communications Manager Features and Services Guide Release 8.0(2)*. San Jose, California, March 2010.

www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmfeat/fsgd.pdf.

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in the Answers Appendix.

1. Which of the following is not a problem when users roam between sites and use guest phones in a hoteling office where Extension Mobility is not enabled?
 - a. The phone they use uses the wrong location and region settings.
 - b. The user gets the wrong extension on that phone.
 - c. The user gets the wrong calling privileges from his or her home desk phone.
 - d. The user does not have his or her speed dials available.
2. Which two settings cannot be updated when you use Extension Mobility?
 - a. Phone button template
 - b. Softkey template
 - c. Device CSS
 - d. Network locale
 - e. Phone service subscriptions
 - f. Phone lines and speed dials

- 3.** Which three of the following are not configuration elements relevant to Extension Mobility configuration?
 - a.** Location
 - b.** Phone
 - c.** End user
 - d.** Device security profile
 - e.** Device pool
 - f.** Device profile
 - g.** Phone service
- 4.** Which two of the following are Cisco-recommended approaches to implementing calling privileges when using Extension Mobility?
 - a.** Configure the line(s) of the user's device profile with a CSS that includes blocked route patterns for the destinations the user should not be allowed to dial.
 - b.** Do not configure a device CSS in this case.
 - c.** Do not configure a line CSS in this case.
 - d.** Configure the device with a CSS that includes all PSTN route patterns pointing to the local gateway.
 - e.** Configure the line(s) of the physical phone with the CSS that includes blocked route patterns for the destinations the user should not be allowed to dial.
- 5.** Which two of the following happen if the user logs into a device but is still logged into another device?
 - a.** If the multiple login behavior service parameter is set to Not Allowed, the second login fails.
 - b.** If the multiple login service parameter is set to auto-logout, the user is automatically logged out of the other device.
 - c.** If the multiple login behavior enterprise parameter is set to allowed, the login succeeds, and the user is logged out at the other device.
 - d.** If the multiple login behavior enterprise parameter is set to prompt, the user is asked whether he wants to be logged out at the other device first.
 - e.** The login fails independent of any CUCM Extension Mobility configuration.

6. Which of the following best describes a user using CUCM Extension Mobility prior to CUCM v8.x?
 - a. An employee travels to a remote site in the same company CUCM cluster and logs in on a Cisco IP Phone to make a PSTN call from the remote location.
 - b. An employee travels to a remote site in the same company CUCM cluster and uses IP communicator on her laptop to make a PSTN call from the remote location.
 - c. An employee travels to a remote site in the same company on a different CUCM cluster and logs in on a Cisco IP Phone to make a PSTN call from the remote location.
 - d. An employee travels to a remote site in the same company on a different CUCM cluster and uses IP communicator on his or her laptop to make a PSTN call from the remote location.
7. What role do device profiles play in a CUCM cluster?
 - a. It is optimal to configure for users who do not travel but who want to best use their IP Phone Services.
 - b. It is optimal to configure for users who travel to other sites but who want to best use their IP Phone Services.
 - c. It is optimal to configure for users who do not travel but who want to use the maximum number of their phone features.
 - d. It is optimal to configure for users who travel to other sites and who want their home site phone settings to be available remotely.
8. Which statement about configuring Extension Mobility in a CUCM cluster is true?
 - a. Extension Mobility is enabled by default on the CUCM cluster but needs to be configured for each user.
 - b. Extension Mobility is not enabled by default on the CUCM cluster and must be enabled on a CCM server and configured for each user.
 - c. Extension Mobility is not enabled by default on the CUCM cluster and must be enabled on all CUCM servers and configured for each user.
 - d. Extension Mobility is enabled by default on the CUCM cluster but needs to be enabled for all CUCM servers and configured for each user.

- 9.** Which implementation example of Extension Mobility would result in the simplest CUCM administrator configuration while maintaining maximum user Cisco IP Phone features for roaming users?
 - a.** Allow different users to own any Cisco IP Phone model they choose for their homes site and for hoteling.
 - b.** Standardize on different Cisco IP Phone models for each location to best suit the business models of different sites.
 - c.** Standardize on the 7965 Cisco IP Phone model to be used for all sites.
 - d.** Standardize on the 7905 Cisco IP Phone model to be used for different sites.
- 10.** In CUCM v8.x and later, Extension Mobility Cross Cluster (EMCC) is a supported feature.
 - a.** True.
 - b.** False.

Chapter 12

Implementing Service Advertisement Framework (SAF) and Call Control Discovery (CCD)

Upon completing this chapter, you will be able to meet the following objectives:

- Describe what SAF is, what CCD is, and how CCD uses SAF
- Describe the characteristics of SAF
- Describe the characteristics of CCD
- Describe how CCD works
- Describe how to implement SAF and CCD
- Describe the special considerations for using SAF and CCD

In large deployments with many call agents, dial plan implementation can be complex. New in CUCM version 8.0 and later, Cisco Service Advertisement Framework (SAF) and Call Control Discovery (CCD) can be configured to allow call agents to propagate call-routing information to the network and learn routes from the network. Thus, SAF and CCD facilitate the deployment of large Cisco Unified Communications solutions by greatly simplifying dial plan implementation. Prior to CCD and SAF, all call routing entries had to be manually configured.

With the increasing deployment of Cisco Unified Communications solutions, dial plans have become more complex to implement, especially in large enterprises that consist of numerous call-control devices. Some examples of these call-control devices are Cisco Unified Border Element (CUBE), Cisco Unified Survivable Remote Site Telephony (SRST), Cisco Unified Communications Manager (CUCM), CUCM Express (CUCME), and Cisco IOS gateways.

To simplify dial plan implementation in large deployments, it is desirable that call-control devices dynamically exchange call-routing information so that no any-to-any static configuration is required. Cisco SAF allows services to be propagated through SAF-enabled network devices. Cisco CCD is the first application that uses SAF to dynamically advertise services in a Cisco Unified Communications implementation for the

reachability of internal directory numbers and public switched telephone network (PSTN) backup numbers.

This chapter explains how SAF works, describes its components, and shows how to configure it. This chapter also describes how CCD uses SAF to dynamically exchange call-routing information and how you can implement CCD in CUCM and in Cisco IOS Software.

SAF and CCD Overview

Figure 12-1 shows an overview of dial plans in large networks, comparing traditional static configurations on the left and dynamic configurations with SAF and CCD on the right.

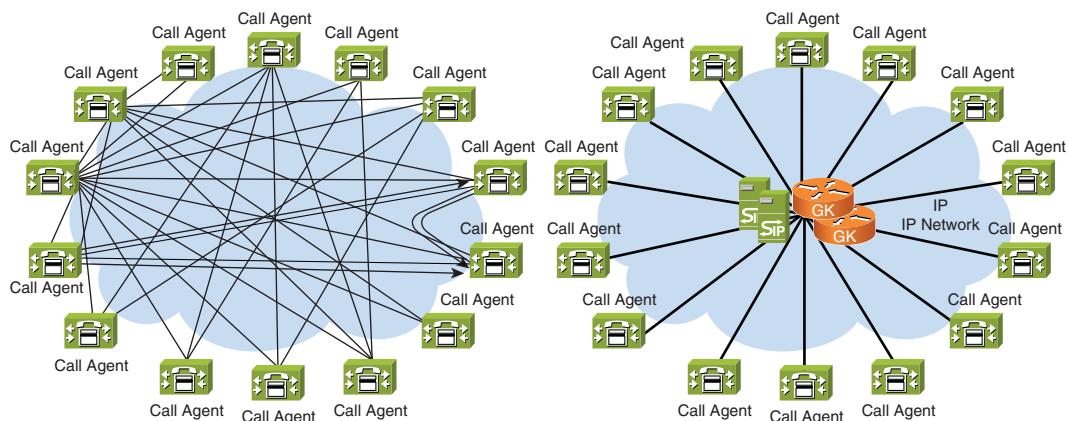


Figure 12-1 Dial Plans in Large Networks Comparing Static to Dynamic Configurations

In large networks with many call agents, such as CUCME, CUCM clusters, CUBE, Cisco Unified SRST, and Cisco IOS gateways, the implementation and maintenance of dial plans can be complex, as shown in Figure 12-1 on the left with a full-mesh configuration.

The use of H.323 gatekeepers or Session Initiation Protocol (SIP) network services can reduce this complexity; however, dial plan implementation still does not scale well in large deployments with purely static configurations.

Dial Plan Scalability Issues in Large Networks

Prior to CCD and SAF, the main scalability issues in large Unified Communications networks are caused because call-routing information has to be configured separately at each call-routing domain.

Without centralized services (such as H.323 gatekeepers or SIP network services), a full-mesh configuration is required. In other words, each call control domain must be

configured with call-routing information toward all other call-routing domains. This implementation model does not scale at all and is therefore suitable only for smaller deployments.

In a hub-and-spoke deployment model, call-routing information for each call-routing domain is configured only once at the centralized call-routing entity. This centralized call-routing entity can be a SIP network service or an H.323 gatekeeper. Such a solution scales better than full-mesh topologies; however, it can introduce a single point of failure and therefore requires redundant deployment of the centralized service. In addition, the centralized call routing still has to be manually configured with static entries. For example, if telephone-number ranges or prefixes are changed at one of the call-routing domains, these changes also have to be manually performed at the centralized call-routing service. Furthermore, PSTN backup has to be implemented independently at each call-routing domain.

In summary, there is no dynamic exchange of call-routing information between call-routing domains with H.323 or SIP, and there is no automatic PSTN backup.

Scalable Dial Plan Solution for Large Networks

The problem of dynamically distributing reachability information is known also in areas other than telephony call routing. As an example, in routed IP networks, routing has changed from simple static routing to large, fully dynamic clouds, such as the Internet.

The solution for scalable IP routing is provided by dynamic routing protocols, such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP). IP routers have local networks that are attached. They advertise these locally known networks to other routers so that all routers can automatically learn about all available networks and the path to get to those networks.

Now, with CUCM v8.x and later, the same concept can be used to distribute call-routing information in a Cisco Unified Communications implementation. Each call-routing domain advertises locally known telephone numbers or number ranges. Because local numbers are typically used by internal patterns (using VoIP) and via the PSTN, each call-routing domain advertises both the internally used numbers and the corresponding external PSTN numbers.

Cisco CCD, a new feature that was introduced with CUCM version 8, provides exactly such a service. It allows CUBE, Cisco Unified SRST, CUCM, CUCME, and Cisco IOS gateways to advertise and learn call-routing information in the form of internal directory numbers and PSTN numbers or prefixes.

CCD Overview

Figure 12-2 provides an overview of CCD in a SAF-enabled IP network.

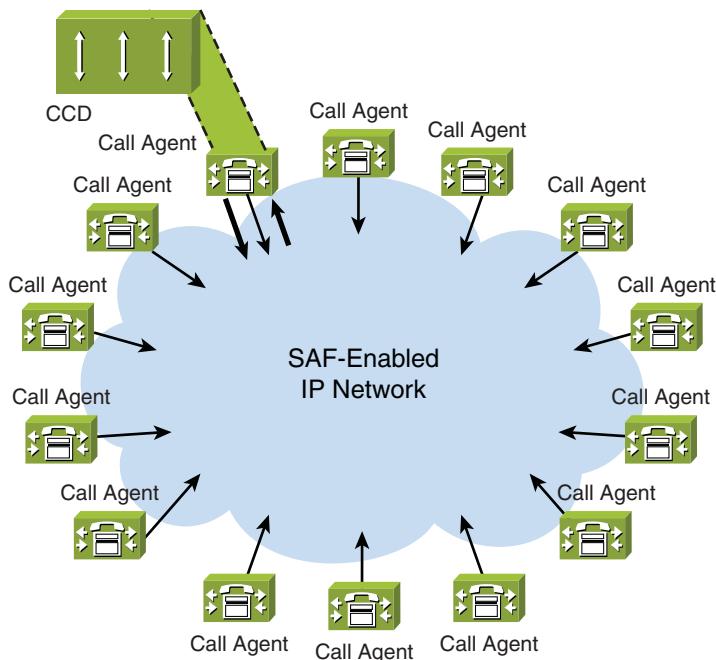


Figure 12-2 CCD and SAF Overview

With CCD, each CCD-enabled call agent advertises locally found directory numbers or directory-number ranges and their corresponding PSTN numbers or prefixes to the SAF-enabled network. In addition, each CCD-enabled call agent learns call-routing information from the network.

SAF is used to propagate information within the SAF-enabled network. SAF forwarders interact with CCD-enabled call agents (that is, SAF clients). A SAF forwarder learns information from a SAF client. SAF forwarders exchange learned call-routing information with each other so that the SAF-enabled network is aware of all learned call routes. SAF forwarders do not only learn from SAF clients, but they also advertise all learned information to SAF clients. That way, all SAF clients are aware of all available call-routing information—internal directory numbers and their corresponding PSTN numbers.

SAF Characteristics

Figure 12-3 shows an overview of the components of SAF.

SAF is a network-based, scalable, bandwidth-efficient, real-time approach to service advertisement and discovery.

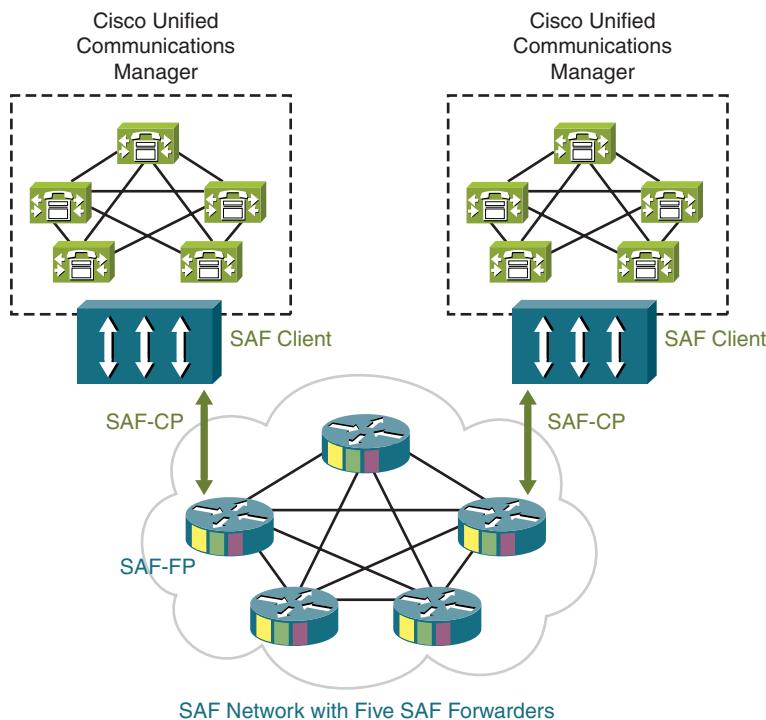


Figure 12-3 Components of SAF

SAF can be used to advertise and learn any service to and from the SAF-enabled network. CCD is the first Cisco application that uses SAF. As previously mentioned, the devices within the SAF network are SAF forwarders. They are responsible for propagating services within the network. SAF forwarders do not interpret the service information itself; they guarantee only the fast and reliable exchange of the information. SAF forwarders use the SAF Forwarding Protocol (SAF-FP) between each other.

SAF forwarders can interact with SAF clients. A SAF client is an entity that processes SAF service data. A SAF client can independently advertise (generate) SAF service information to be propagated in the network or subscribe to (receive) SAF service information. A SAF client communicates with one or more SAF forwarders using the SAF Client Protocol (SAF-CP). With CCD, the SAF client is a call agent, such as CUBE, Cisco Unified SRST, CUCM, CUCME, and Cisco IOS gateways.

Cisco SAF forwarders use IP multicast to automatically discover and communicate as peers with other Cisco SAF forwarders on a LAN. On networks that do not support IP multicast, SAF forwarders can connect statically as peers by creating unicast point-to-point adjacencies with SAF neighbors.

SAF Client Types

Figure 12-4 illustrates the two available CCD SAF client types.

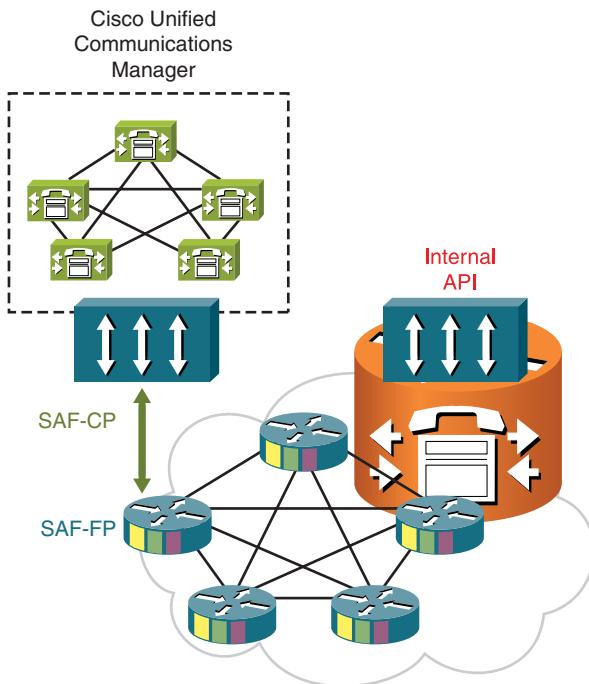


Figure 12-4 SAF Client Types

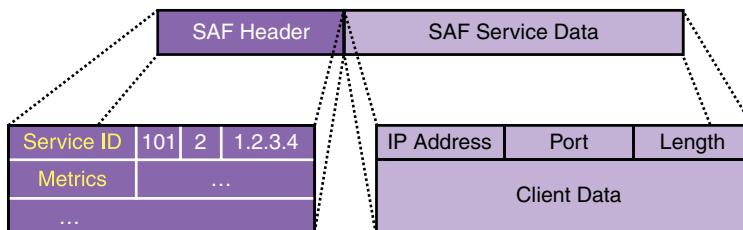
A SAF forwarder is always a Cisco IOS router. Remember that SAF forwarders do not process the propagated service information. Their function is to propagate the information within the SAF network and pass it to SAF clients.

SAF clients then interpret the service information. With CCD, the SAF client is a call-control device, which sends and receives call-routing information. Depending on the type of call-control device, the CCD device can be an internal or external SAF client:

- **External SAF client:** The SAF client and the SAF forwarder are two different devices. They use the SAF-CP for communication. An example of a CCD external SAF client is CUCM.
- **Internal SAF client:** The SAF client and the SAF forwarder are two different functions within the same device—a Cisco IOS router. They use an internal application programming interface (API) for communication. Examples of CCD internal SAF clients are CUBE, Cisco Unified SRST, CUCME, and Cisco IOS gateways.

SAF Message Components

Figure 12-5 shows the two components of a SAF message.



- Relevant to SAF forwarders
- Identifies service type and unique instance
- Used by forwarders to propagate advertisements
- Metrics used to avoid loops
- Relevant to SAF clients
- Service-specific information
- Transparent to forwarders
- Client data depends on service type

Figure 12-5 SAF Message Components

A SAF message consists of two components:

- **SAF header:** The SAF header is relevant mainly to SAF forwarders. It identifies the service type (for example, CCD) and includes information that is relevant for the dynamic distribution of SAF services, such as metrics and loop detection information.
- **SAF service data:** SAF service data is relevant only to the SAF client. A SAF forwarder cannot interpret the SAF service data. SAF service data includes the IP address and port of the advertising SAF client and detailed client data that describes the advertised service. With CCD, client data includes call-routing information, such as directory numbers, the IP address of the call-control device, the signaling protocol to use to communicate with the call-control device, PSTN prefixes, and so on.

SAF Routing Characteristics

The SAF-FP uses features and functions of the Cisco proprietary EIGRP for SAF routing. Features and mechanisms that are used and known from EIGRP include the Diffusing Update Algorithm (DUAL) to prevent loops, reliable transport over IP (IP protocol 88), support for authenticated updates, and incremental, event-triggered updates for fast convergence and low-bandwidth consumption. Configurable parameters that relate to these EIGRP-derived features include bandwidth percent, hello interval, holdtime, split horizon, maximum hops, and metric weights.

Although SAF routing behaves similarly to that of EIGRP, it is independent of the used IP routing protocol. SAF works over static routing, and in networks that use dynamic routing protocols, such as EIGRP, OSPF, and BGP.

Note SAF-FP is a “service” routing protocol, not an IP routing protocol. SAF-FP routes information about services over IP networks. It is based on EIGRP technology and takes advantage of many of the features historically developed for EIGRP-based IP routing, applying this functionality to the distribution of service information.

SAF Neighbor Relationships

Figure 12-6 illustrates how SAF forwarders can connect to each other.

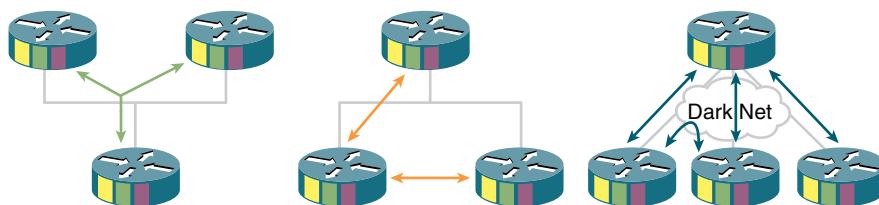


Figure 12-6 SAF Neighbor Relationships

SAF forwarders can be, but do not have to be, directly neighboring devices. There are three configuration options:

- **Multicast:** When multiple SAF forwarders are connected via a broadcast-capable medium, such as a LAN using Ethernet in the example on the left in Figure 12-6, they can communicate to each other via multicasts. This communication allows a dynamic neighbor discovery because there is no need to statically configure the Layer 2 adjacent neighbors.
- **Unicast:** When it is not desired that all SAF devices on a broadcast-capable medium automatically discover each other, SAF forwarders can be configured to send updates only to statically configured neighbors via unicast messages, as shown in the middle example in Figure 12-6.
- **Static:** When SAF forwarders are not Layer 2 adjacent—that is, when one or more IP hops are between them—these nonadjacent neighbors have to be statically configured. No discovery is possible. See the two bottom-right routers in the example in the right of Figure 12-6 for an illustration of non-Layer 2 adjacent SAF forwarders.

In Figure 12-6, the left example shows three routers that are connected to an Ethernet; however, the left and middle example should not build adjacencies among each other in a full-mesh fashion. Instead, they should communicate only in a hub-and-spoke fashion. (One router communicates with both of the others, and the other two routers do not communicate directly with each other.)

Cisco SAF forwarders can be located anywhere within the network, but they are normally located at the edges, or boundaries, of a network.

SAF Client and SAF Forwarder Functions

SAF clients register to the network, more precisely to a SAF forwarder. They can publish services (that is, advertise information) to the SAF network or subscribe to services (that is, request information) from the SAF network. To allow the SAF client and the SAF forwarder to quickly detect dead peers (for example, if the device was powered off), they exchange keepalives.

SAF forwarders propagate updates that are received from SAF clients that publish services to other SAF forwarders. They send updates to SAF clients, which subscribe to their services. In addition, SAF forwarders exchange hellos with other SAF forwarders to detect dead peers.

CCD Characteristics

Figure 12-7 illustrates the characteristics of CCD and how CCD forwarding and requesting that services are used in CUCM.

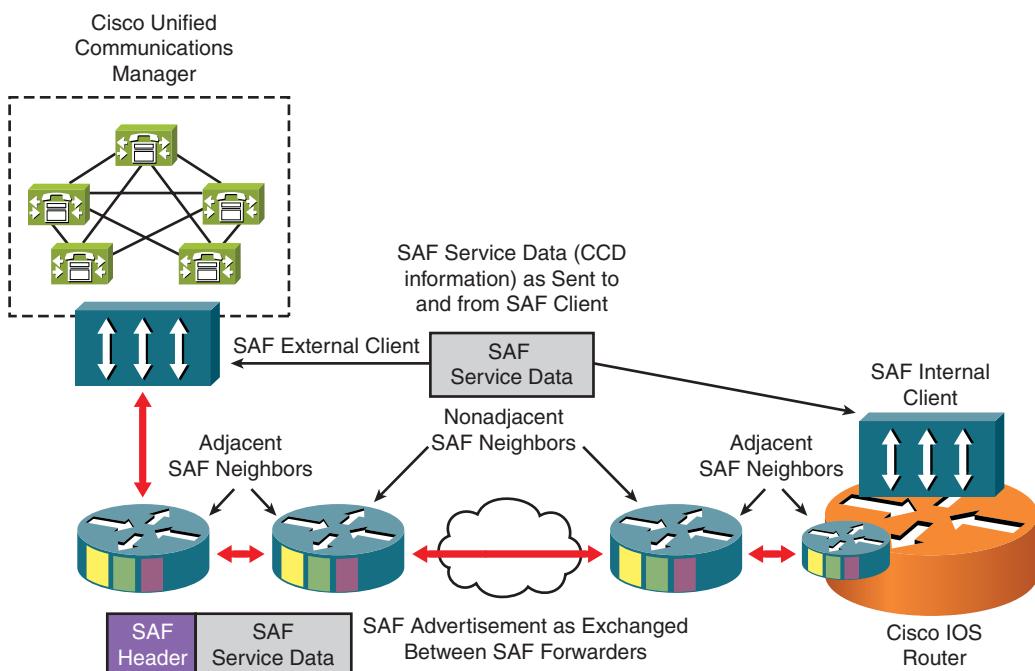


Figure 12-7 CCD Overview

CCD is a function of call agents. It allows call agents to advertise locally known internal directory numbers and the corresponding PSTN numbers to other CCD-enabled

call agents. CCD uses SAF for distributing call-routing information over the SAF-enabled network.

A CCD-enabled call agent is configured to send its locally configured directory-number range as a SAF service to a SAF forwarder. The CCD SAF client generates SAF service data (call-reachability information) and passes it on to the SAF forwarder that will propagate the information within the SAF network. All SAF forwarders that have SAF subscribing clients attached send the SAF service data to their clients. From a CCD perspective, all SAF clients exchange SAF service data (call-routing information).

You can compare the SAF service data with TCP or User Datagram Protocol (UDP), which establish an end-to-end communication between IP endpoints. Likewise, CCD-enabled call agents exchange call-routing information via the end-to-end service data exchange.

The SAF header can be compared to the IP header. It is also interpreted at intermediate nodes (SAF forwarders); although, these intermediate network nodes do not process the payload (that is, the SAF service data).

CCD enables call agents to exchange call-routing information. The information that is relevant consists of the following components:

- **Dial plan information:** Includes internally used directory numbers (potentially with internal prefixes, such as site codes), the IP addresses of the respective call agents, and the signaling protocol that the call agents will use. All this information is advertised by call agents that are propagated throughout the network by SAF and then learned by other call agents.
- **Reachability information:** This dynamic routing for call-reachability information drastically simplifies dial plan implementations in large networks. There is no need for a static full-mesh configuration and no need even for the configuration of a centralized call-routing service (such as an H.323 gatekeeper or a SIP network service). You must configure only the internal number range that should be advertised per call agent at the respective call agent. CCD and SAF then ensure that the locally known numbers are distributed among all call agents.

When rerouting over the PSTN is desired, call agents are configured not only to advertise their internally used number ranges, but also with the corresponding PSTN numbers. The PSTN number is not advertised as a distinct number; it is advertised by a PSTN failover digit-transformation rule (known as a ToDID rule). A ToDID rule describes how the internally used number has to be manipulated to get to the associated PSTN number. A ToDID rule consists of two components:

- **Number of digits to be stripped:** The first part of a ToDID rule is the number of digits to be stripped from the internally used number. For example, if site-code dialing is used and the internally used number to reach a block of directory numbers is 8-408-2XXX, you might want to strip the leading 8408 before prefixing the necessary digits to directory-number range 2XXX. In this case, your ToDID rule starts with 4: because the four leading digits should be stripped.

- **Prefix to be added to the (deflated) internal number:** The second part of a ToDID rule is the prefix that should be added to the internally used number after digit stripping has been performed. In the previous example, if the PSTN direct inward dialing (DID) range of the internally used directory-number range 2XXX (dialed as 8-408-2XXX from other sites) is 408 555-2XXX, the prefix would be 408555. Usually, E.164 format with a + prefix represents the PSTN number, so the configured prefix would be +140855.

In the given example, the complete ToDID rule would be 4:+1408555 because the numbers to be stripped and the prefix are separated by a column.

By advertising only the locally present internal numbers and the corresponding ToDID rule at each call agent, the dial plan implementation of large networks is extremely simplified. If there are any changes at a call agent, you have to change only the advertised number (range) and its ToDID rule at the affected call agent. All other call agents will dynamically learn the changes.

CCD Services in CUCM

The CCD advertising service is configured with the directory numbers that will be advertised. In CUCM, they are configured by *hosted* directory-number ranges. Each hosted directory-number range is configured with its PSTN failover information (the ToDID rule for the hosted directory-number range). In addition, the signaling protocol and the IP addresses of the call agents have to be advertised. They are configured by a trunk. The trunk can be a SAF-enabled H.323 intercluster trunk (ICT) or a SAF CCD SIP trunk. CCD advertises call routes with one or more call agent IP addresses. The IP addresses to be advertised are determined by the device pool that is applied to the SAF-enabled trunk.

Note The trunk is not used to advertise call routes. Call routes are advertised by CCD and SAF and not via H.323 or SIP. The trunk determines the IP addresses of the call agents and the supported signaling protocols, in case another call agent wants to establish a call to a learned call route.

The CCD that is requesting service is responsible for subscribing to call-routing information from its SAF forwarder. It allows CUCM to learn routes from the SAF-enabled network. Only one CCD that is requesting service exists per CUCM cluster. However, like the advertising service, it can be configured to accept patterns that are reachable via SIP or H.323, depending on the associated trunk or trunks.

The service advertises the call negotiation information for these trunks, including the dynamic port number for the H.323 trunk, the standard port 5060 for the SIP trunk, and the SIP route header information. The Adaptive Security Appliances (ASA) do not have application inspection for the SAF network service. When CUCM uses a SAF-enabled H.323 trunk to place a call, the ASA cannot inspect the SAF packet to learn the ephemeral port number used in the H.225 signaling. Therefore, in scenarios where call traffic from

SAF-enabled H.323 trunks traverses the ASAs, ACLs must be configured on the ASAs to allow this signaling traffic. The ACL configuration must account for all the ports used by the H.225 and H.245 signaling. ACL configuration is not required when SAF-enabled SIP trunks with the standard 5060 port are used.

Note Like the trunks that are associated with CCD advertising services, the trunks that are associated with the CCD that is requesting services are not used to learn patterns via SIP or H.323. They determine the outbound capabilities for calls that are placed to learned destinations. If the CCD that is requesting service is associated only with an H.323 trunk, learned routes that are to be reached via SIP are not added to the call-routing table of the receiving CUCM.

The CUCM nodes of the cluster that is permitted to place outbound calls to learned routes are determined by the device pool that is applied to the trunk that is associated with the CCD requesting service.

Processing Received Routes in CUCM

You can configure a filter that is applied to received routes to deny the learning of routes by using these criteria:

- **Learned pattern prefix:** The received patterns are compared with the configured prefix, starting with the left-most digit. By using a learned pattern prefix for blocking received routes, you can filter internally used numbers by their leading digits—for example, by their site code.
- **Learned pattern:** The received pattern is checked in its entire length. If it matches the configured learned pattern, it will not be added to the local call-routing table.
- **Remote call control identity:** Each call agent has a so-called SAF client ID. By setting the remote call-control identity, you can filter received routes that are based on the ID of the advertising call agent.
- **Remote IP:** By setting this filter, you can block routes that are based on the advertising IP address.

You can configure one or more criteria when setting up a filter; however, as soon as one criterion is matched, the learned route is filtered.

The same destination number can be learned multiple times. It might be advertised by different call agents. It might allow SIP and H.323 to be used for setting up the call. (Both signaling protocol capabilities are advertised separately.) It also might be reachable at multiple IP addresses (of the same call agent, in the case of a CUCM cluster). If a route is learned multiple times, CUCM will load share the outbound calls to the corresponding destination among all possible paths (that is, by protocol and remote IP addresses).

All learned routes are put into one configurable partition. All devices that should have access to learned routes need that partition included in their Calling Search Space (CSS).

Sometimes, the IP path for a learned route might not be available, and a ToDID rule might have been advertised with the hosted directory number. In that situation, a call to the transformed number (a ToDID rule that is applied to the advertised pattern) is placed with the Automated Alternate Routing (AAR) CSS of the calling device.

Note PSTN backup for CCD is completely independent from AAR. AAR places PSTN backup calls for cluster-internal destinations when the IP path cannot be used because of insufficient bandwidth as indicated by call admission control (CAC). Only the AAR CSS is reused for CCD PSTN backup. Otherwise, CCD PSTN backup does not interact with AAR at all. For example, CCD PSTN backup works even when AAR is globally disabled by the corresponding Cisco CallManager service parameter.

CCD Operation

Figure 12-8 illustrates how CCD works for on-net calls and how CCD reroutes calls to the PSTN if the IP path is not available.

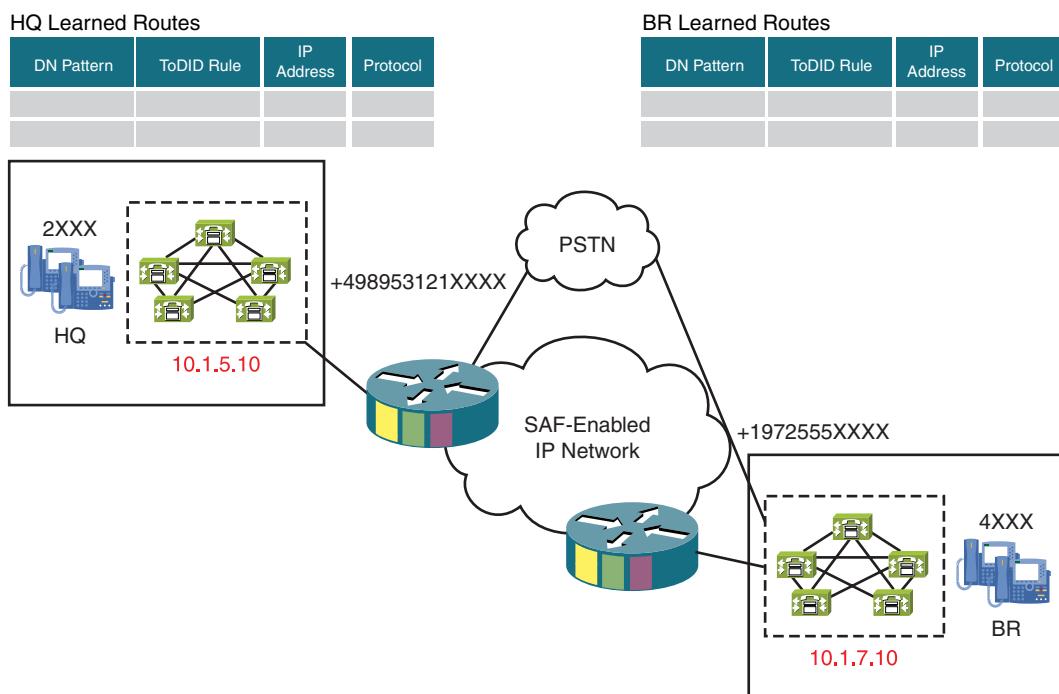


Figure 12-8 CCD Base Configuration for PSTN Rerouting When the IP Path Is Down

Figure 12-8 shows the base configuration. There are two sites, each with a CUCM cluster. One site (HQ) is located in Germany, and it has a DID range of +498953121XXXX. The other site (BR) is located in Brazil, and it has a DID range of +1972555XXXX.

Internally, range 2XXX is used. The other site (BR) is in the United States; it has a DID range of +1972555XXXX. Internally, the directory-number range 4XXX is used.

CCD Propagation of HQ Routes

Figure 12-9 illustrates how HQ routes from one CUCM cluster are propagated to the BR site of another CUCM cluster.

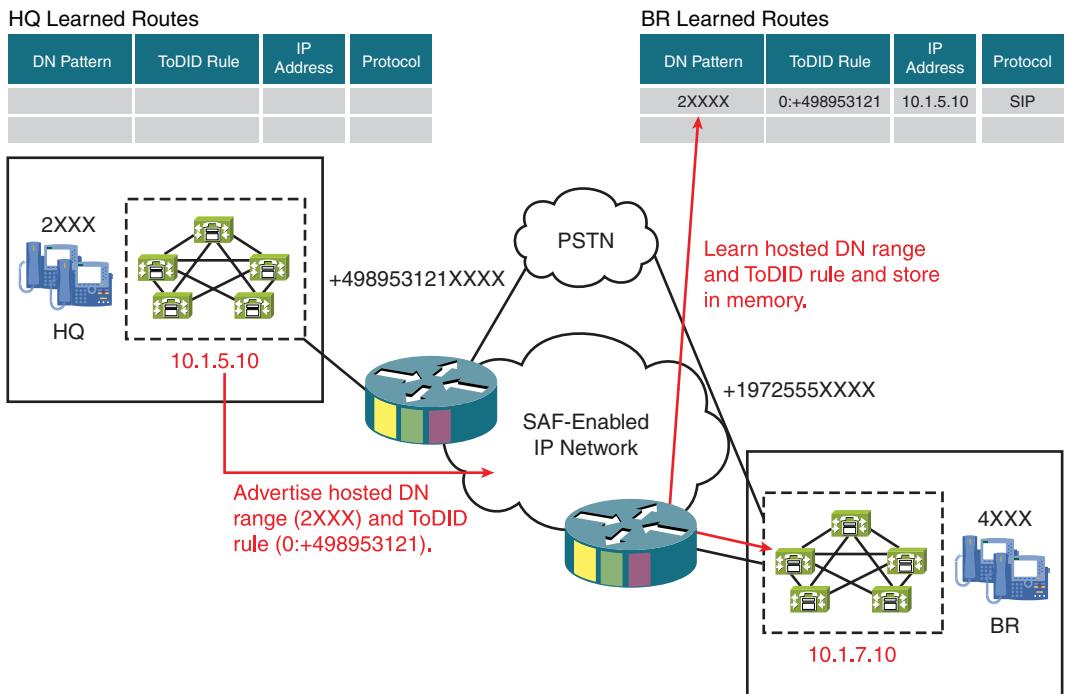


Figure 12-9 CCD Propagation of HQ Routes

The CUCM cluster at the HQ site advertises its directory-number range 2XXX with a ToDID rule of 0:+498953121 to its SAF forwarder. The SAF network propagates this new route throughout the network, and the SAF forwarder at the BR site sends the information to the BR CUCM cluster. The call routing table of the BR cluster is populated with the directory-number pattern 2XXX and a ToDID rule of 0:+498953121.

At the advertising site, only a SIP trunk has been associated with the CCD advertising service.

Therefore, the BR cluster learns the route only for SIP.

CCD Propagation of BR Routes

Figure 12-10 illustrates how BR routes are propagated to the HQ site.

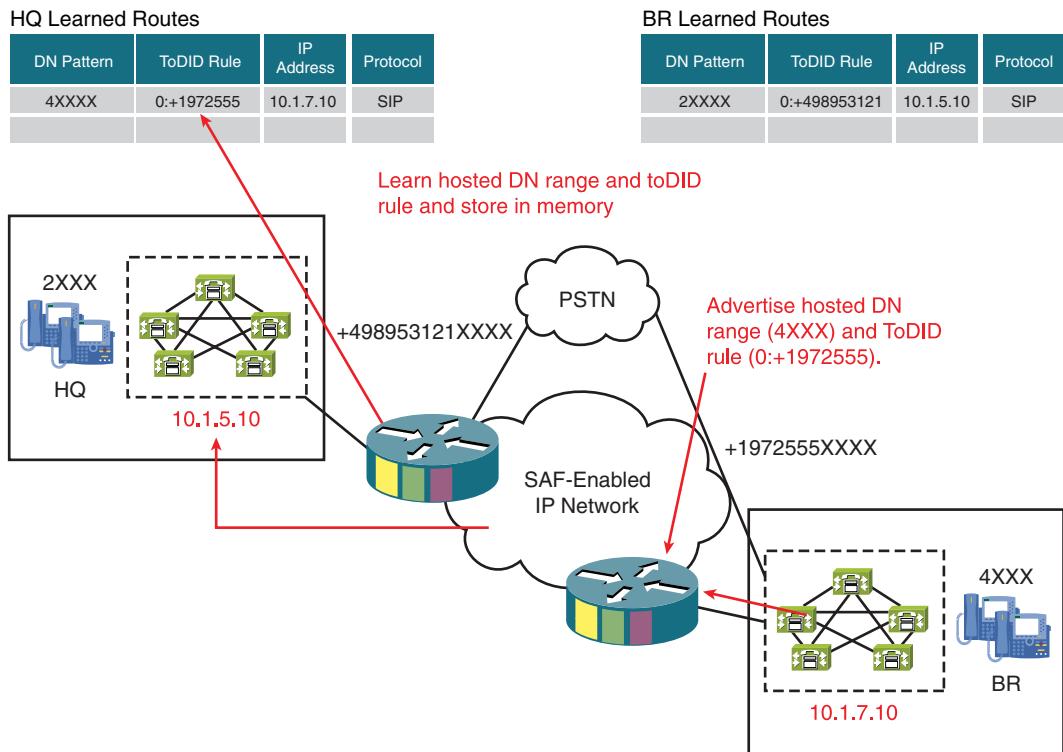


Figure 12-10 CCD Propagation of BR Routes

The CUCM cluster at the BR site advertises its directory number range 4XXX with a ToDID rule of 0:+1972555 to its SAF forwarder. The SAF network propagates this new route throughout the network, and the SAF forwarder at the HQ site sends the information to the HQ CUCM cluster. The call-routing table of the HQ cluster is populated with the directory-number pattern 4XXX and a ToDID rule of 0:+1972555.

Again, only a SAF-enabled SIP trunk is associated with the CCD advertising service at the originating site. Therefore, the HQ cluster learns the route only for SIP.

At this point, the network is in a converged state, because all sites know about the routes of all other sites.

CCD Call from HQ to BR

Figure 12-11 illustrates the call flow for a call from the HQ to the BR site.

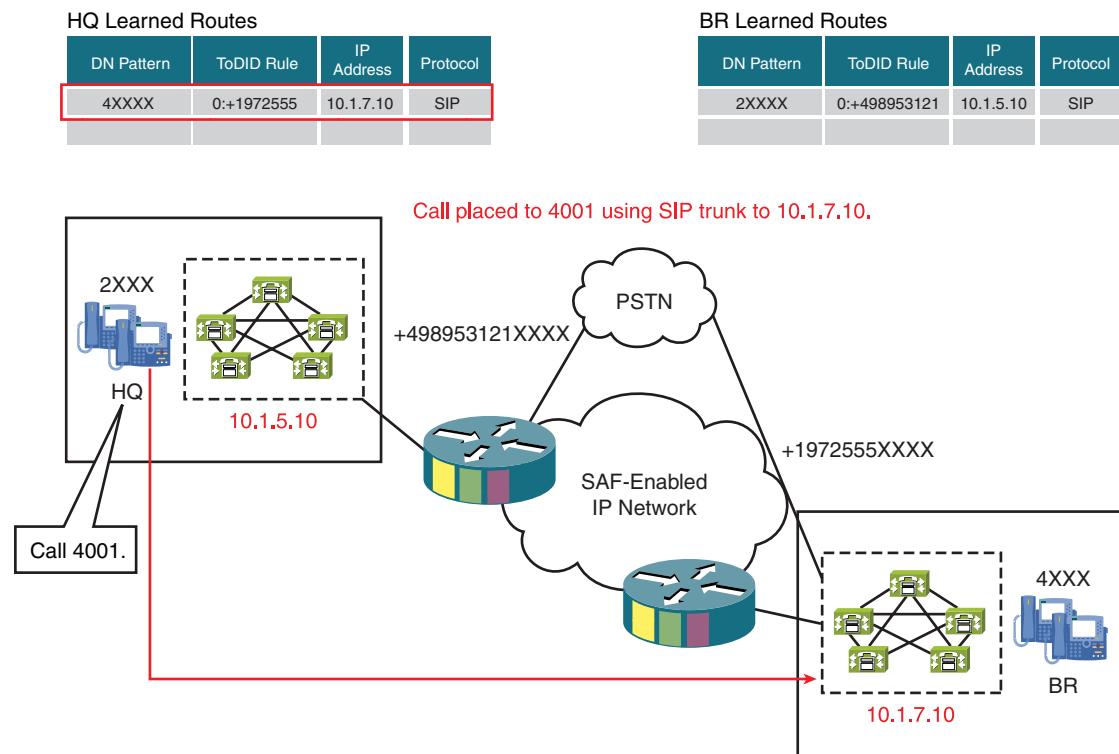


Figure 12-11 CCD Call from the HQ to BR

The HQ site dials 4001. The called number is found in the call-routing table of the HQ CUCM cluster.

Note All learned routes are put into the same configurable partition. The CSS of the calling phone must have access to this partition for the call to work. If the calling phone does not have access to the partition that includes all learned patterns and there is no match in any other partition, the call fails.

CUCM identifies the matched pattern as a CCD-learned pattern. According to the learned route, the call has to be set up through a SAF-enabled SIP trunk, of which the destination IP address is dynamically created to the destination IP address as learned by CCD (in this case, 10.1.7.10).

The call is now set up over the IP network.

CCD with a Link Failure at BR

Figure 12-12 demonstrates how CCD manages a link failure between the SAF client and its SAF forwarder at the BR site.

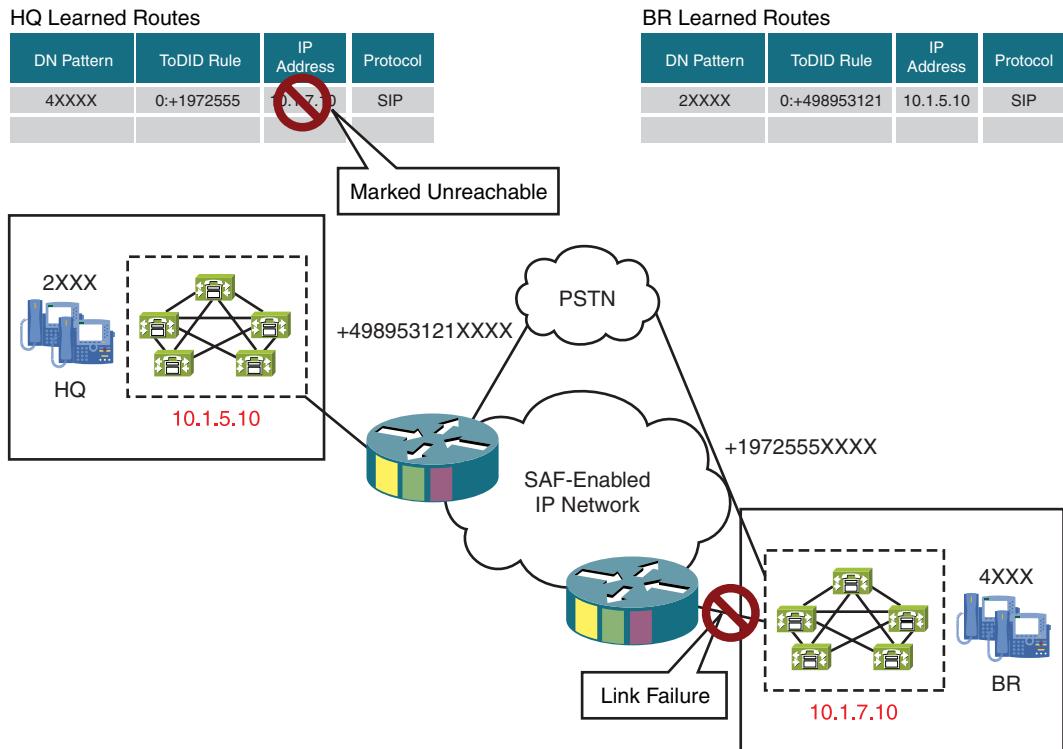


Figure 12-12 CCD Link Failure at BR

When the connection between the SAF client and the SAF forwarder at the BR site is broken, the SAF forwarder at the BR site detects this problem that is based on the missing keepalives of the registered SAF client.

The BR SAF forwarder sends an update throughout the SAF-enabled network so that all SAF forwarders are aware that the *IP path* to 4XXX is currently unavailable. Other than in IP routing, the learned route is not removed, but only the IP path is marked unreachable.

All SAF forwarders that have registered SAF clients now pass this update on to their SAF clients so that all SAF clients in the network can mark the IP path to 4XXX as unreachable.

As shown in Figure 12-12, the call-routing table at the HQ site also gets updated accordingly.

CCD for Call from HQ to BR During Link Failure

Figure 12-13 demonstrates the call flow for a call from the HQ site to the BR site during a link failure at the BR site.

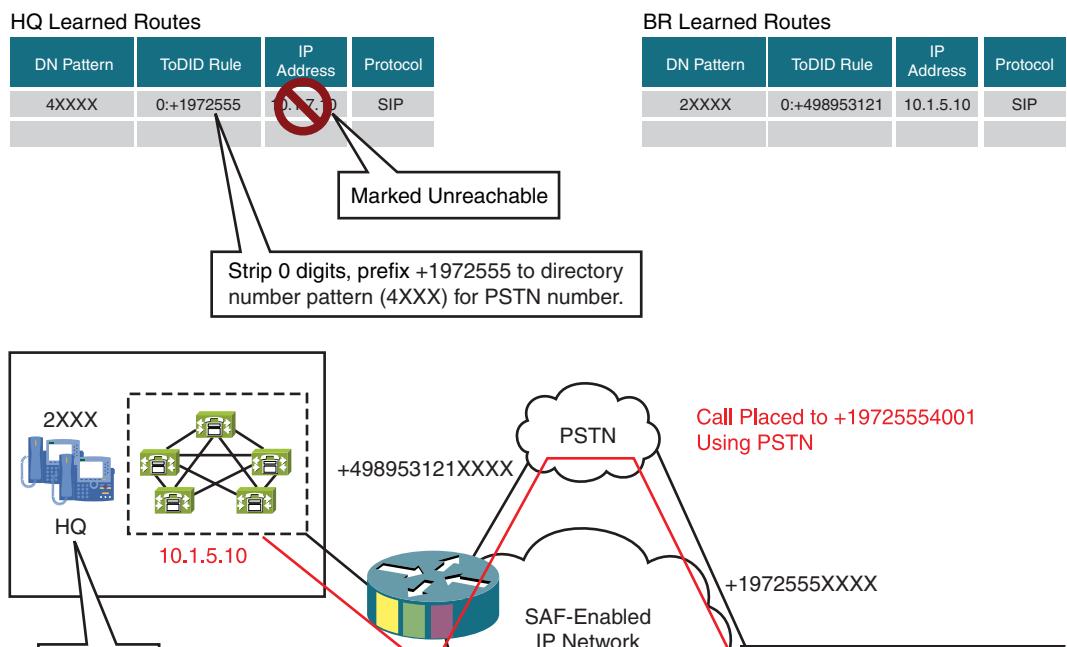


Figure 12-13 CCD for Call from HQ to BR during IP Link Failure

When a user at the HQ site dials 4001 during the link failure at the BR site, the called number is still found in the call-routing table of the HQ CUCM cluster. However, the IP path is marked as unreachable; therefore, the call cannot be set up over the IP network with the use of a SIP trunk.

CUCM now checks whether there is a ToDID rule associated with the learned pattern. In this case, a ToDID rule of 0:+1972555 has been learned. CUCM does not strip any digits (because of the 0 in front of the : [column]), but it adds the prefix +1972555 to the dialed directory number 4001. The resulting number +19725554001 is now matched in the call-routing table of CUCM, where a match is found in a PSTN route pattern.

Note The CSS used for the PSTN backup call is the AAR CSS of the calling phone. The route pattern, route list, route group, and gateway for PSTN access has to be in place for PSTN backup to work. Furthermore, the PSTN route pattern must be in a partition that's reachable from the AAR CSS of the calling phone.

In Figure 12-13, the ToDID rule results in globalized PSTN numbers (E.164 format with a + prefix). Therefore, a PSTN route pattern that matches this format (for example, \+.!) has to be in place. If all sites share the same PSTN dial rules—for example, all sites are within the North American Numbering Plan (NANP)—you could also configure ToDID rules that result in PSTN patterns with a PSTN access code, followed by a national access code, followed by the 10-digit PSTN number. In this case, your PSTN route pattern would have to be 91[2-9]XX[2-9]XXXXXX.

The call is now set up over the PSTN.

Note If the learned pattern was removed when the IP path became unavailable, the originating site would not know what PSTN number to use for the backup call. By default, a route is completely removed only if it has not advertised for 48 hours.

SAF and CCD Implementation

The first main configuration task is to enable SAF in Cisco IOS routers in the network. You have to configure SAF forwarder functionality on a Cisco IOS router. All SAF forwarders must share the same SAF autonomous system number. You can specify the interface that the SAF forwarder should use.

When using internal SAF clients, perform these main configuration tasks:

Step 1. Configure a trunk profile and specify the interface and the protocol to use for call signaling.

Note The IP address (interface) that is used for call signaling can be different from the IP address that is used by the SAF forwarder.

Step 2. Configure the directory-number blocks to be advertised.

Step 3. Configure a call-control profile that refers to the directory-number blocks and the trunk profile to use.

Step 4. Configure the actual CCD process (channel) that refers to the SAF forwarder by its autonomous-system number. Then, perform these tasks:

- Enable the CCD advertising service by referring to the call control profile.
- Enable the CCD requesting service.

Step 5. Configure a VoIP dial peer that refers to the SAF.

When implementing external SAF clients, you must perform these high-level configuration tasks:

Step 1. At the SAF forwarder (Cisco IOS router), add the external SAF client (CUCM):

- Specify the SAF ID, username, and password of the external client.
- Map the external SAF client to the SAF autonomous system.

Step 2. At the external SAF client (CUCM), add the SAF forwarder (Cisco IOS router). Specify the SAF ID, username, and password, as configured at the SAF forwarder.

Step 3. Configure CCD at the external SAF client:

- Configure a SAF SIP or a SAF H.323 trunk.
- Configure the hosted DN patterns and hosted DN groups.
- Configure the CCD advertising service.
- Configure the CCD requesting service and the partition to be used for learned patterns.

Note These steps are elaborated on later in this chapter.

External SAF Client Configuration Elements

Table 12-1 shows the configuration elements of an external SAF client and their functions.

Table 12-1 External SAF Client Configuration Elements

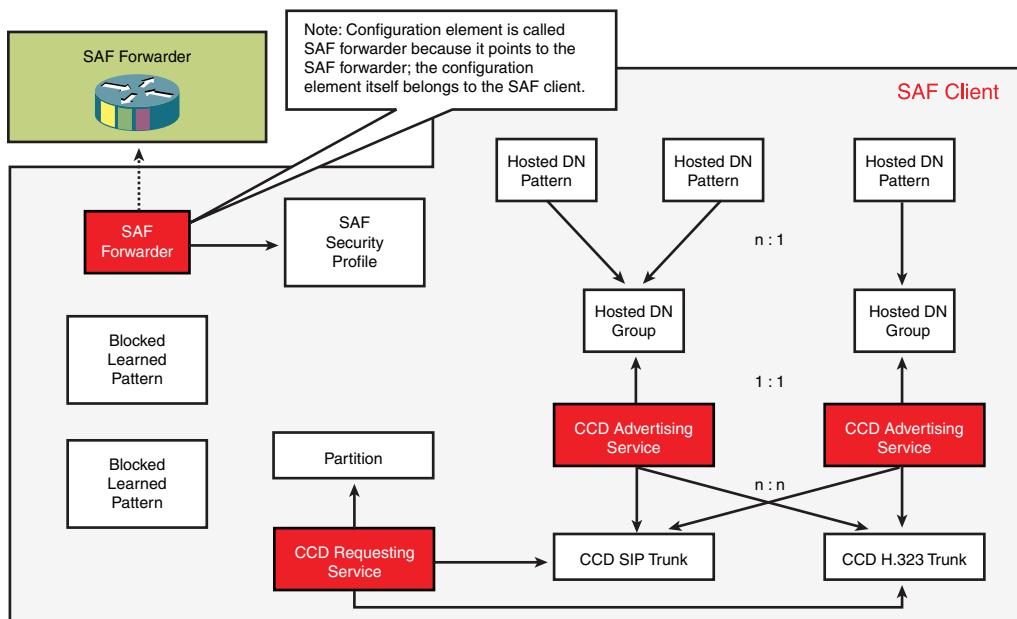
Configuration Element Name	Configuration Element Function
SAF security profile	Configured with username and password. Referenced from SAF forwarder.
SAF forwarder	Points to SAF forwarder. Configured with IP address of SAF forwarder. Refers to SAF security profile.
SAF trunks	One SAF SIP trunk and one SAF H.323 trunk can be configured. They are not configured with a destination address. The rest of the configuration is similar to normal SIP and H.323 trunks.
Hosted DN group	Configured with PSTN failover strip digits and PSTN failover prepend digits. Refers to hosted DN patterns.
Hosted DN pattern	Directory number or directory-number range to be advertised. Configured with PSTN failover strip digits and PSTN failover prepend digits; if not configured, hosted DN group configuration is used. Applied to hosted DN group.

Table 12-1 External SAF Client Configuration Elements

Configuration Element Name	Configuration Element Function
CCD advertising service	Refers to hosted DN group, SAF SIP trunk, and SAF H.323 trunk.
CCD requesting service	Configured with route partition, learned pattern prefix, and PSTN prefix. Refers to SAF trunks.
Blocked learned patterns	Configured with remote IP, remote call control identity, and learned pattern or learned prefix.

Note You can configure the CCD advertising service and the CCD requesting service independently. The configuration of blocked learned patterns is optional.

Figure 12-14 illustrates the relationship of external SAF client configuration elements and how they relate to each other.

**Figure 12-14 Relationship of External SAF Client Configuration Elements**

Note You can configure only a single CCD-requesting service in your cluster. You can configure multiple blocked learned patterns, SAF forwarders, and SAF security profiles. You can configure one CCD SIP trunk and one CCD H.323 trunk. Only one trunk is required.

Internal SAF Client Configuration Elements

Table 12-2 illustrates the configuration elements of an internal SAF client, their functions, and the ways they interact with each other.

Table 12-2 Internal SAF Client Configuration Elements

Configuration Element Name	Configuration Element Function
Trunk profile	profile trunk-route: Configured with interface whose IP address should be used for signaling when setting up SAF calls.
DN block profile	profile dn-block: Configured with patterns to be advertised (internal number and number used for PSTN backup).
Call control profile	profile callcontrol: Refers to DN block profiles and trunk profile.
SAF client “channel”	channel: Configured with SAF client ID and autonomous system. Advertising and requesting services are enabled; the advertising service refers to the call control profile.
Dial peer	dial-peer voice: Configured with destination-pattern .T and session-target saf. This is the incoming and outgoing dial peer for a call sent to or received from SAF trunks.

Note You can configure the advertising service and the requesting service independently of each other.

Figure 12-15 illustrates the relationships of internal SAF client configuration elements.

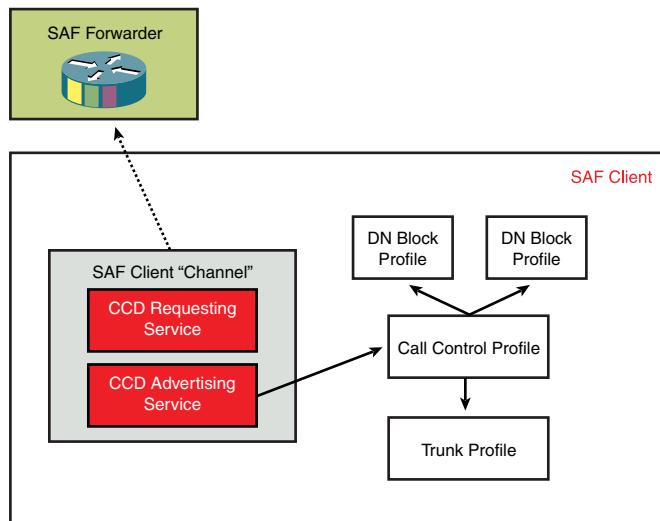


Figure 12-15 Relationship of Internal SAF Client Configuration Elements

Note The configuration shown in Figure 12-15 is one that you can do multiple times, if multiple SAF forwarder processes are configured in separate autonomous systems. Each SAF client “channel” has to refer to another SAF autonomous system. The CCD advertising service of a single SAF client channel can refer to multiple call-control profiles. This capability allows the configuration of two trunk profiles (one SIP and one H.323 trunk per call control profile). Only one trunk is required.

SAF Forwarder Configuration Procedure

The configuration procedure of the SAF forwarder is as follows:

Step 1. Configure SAF forwarder (mandatory). For example:

```

Interface Loopback1
    IP Address 10.1.1.1 255.255.255.255
!
router eigrp SAF
!
    service-family ipv4 autonomous-system 1
!
```

```

sf-interface Loopback1
topology base
exit-sf-topology
exit-service-family

```

In this configuration, a SAF forwarder is configured with autonomous system 1. All SAF forwarders that will exchange information with each other have to be in the same autonomous system.

For the command `router eigrp SAF`, the entry SAF is an EIGRP process ID that only has local significance to this router.

You use the `sf-interface` command to bind the SAF process to the specified interface used by the SAF forwarder. If the router has multiple interfaces, it is recommended that you use a loopback interface, as shown in this example.

Step 2. Configure SAF forwarder to support external SAF client (if used). For example:

```

router eigrp SAF
!
service-family ipv4 autonomous-system 1
!
sf-interface Loopback1
topology base
exit-sf-topology
external-client HQ_SAF
exit-service-family
!
service-family external-client listen ipv4 5050
external-client HQ_SAF
username SAFUSER
password SAFPASSWORD

```

Each allowed external client must be listed in the `service-family` section. In addition, the username and password that the external client should use must be specified in the `service-family external-client` section.

Note If you want to allow multiple nodes of a CUCM cluster to act as SAF clients, each of them needs a unique client name. You can either configure each of them individually with separate node names or use a SAF client ID in CUCM, which is `client-ID@`. The `@` sign instructs CUCM to add a unique node number so that the actual client IDs are `client-ID@1`, `client-ID@2`, and so on.

At the SAF forwarder, you can either create individual entries or add the keyword `base-name` to the `external-client client-ID` command. Do not specify the `@` sign at the SAF forwarder; only add the keyword `basename` to the `external-client` command, and the specified client ID will be permitted with any suffixes of `@` followed by a number.

External SAF Client Configuration Procedure

The following steps are the configuration procedure of an external SAF client in CUCM:

- Step 1.** Configure SAF security profile.
- Step 2.** Configure SAF forwarder.
- Step 3.** Configure SAF trunk.
- Step 4.** Configure hosted DN group.
- Step 5.** Configure hosted DN pattern.
- Step 6.** Configure CCD advertising service.
- Step 7.** Configure CCD requesting service and partition.
- Step 8.** Configure CCD blocked learned patterns (optional).
- Step 9.** Configure CCD feature parameters (optional).

The last two configuration steps are optional, as noted. You do not have to configure the CCD advertising service and the CCD requesting service if you want only to advertise or learn call routes (exclusively).

Step 1: Configure SAF Security Profile

Figure 12-16 shows how to configure a SAF security profile in CUCM. In Cisco Unified CM Administration, choose **Advanced Features > SAF > SAF Security Profile**.

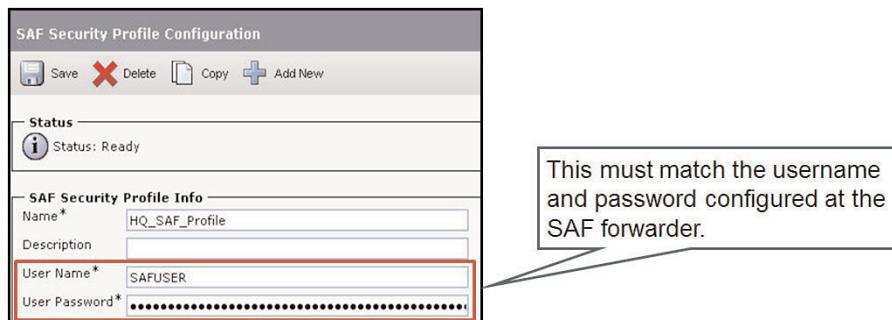


Figure 12-16 Step 1: Configure SAF Security Profile

Make sure that the username and the password match the username and password that were just configured at the SAF forwarder.

Step 2: Configure SAF Forwarder

Figure 12-17 shows how to add a SAF forwarder to CUCM. In Cisco Unified CM Administration, choose Advanced Features > SAF > SAF Forwarder.

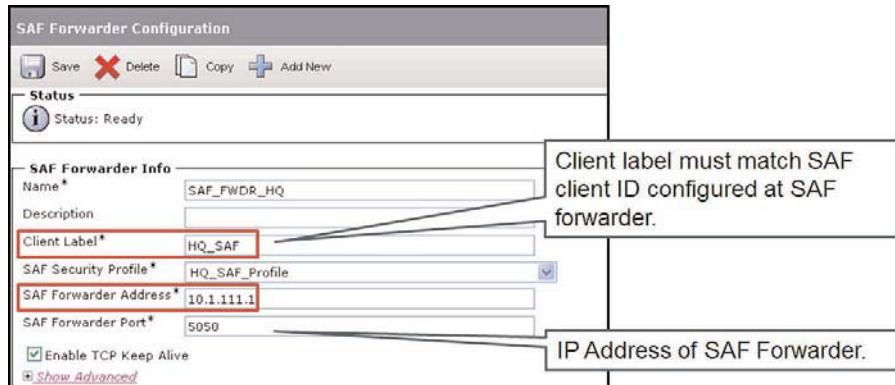


Figure 12-17 Step 2: Configure SAF Forwarder

The destination IP address has to match the one of the interface that is specified with the **sf-interface** command at the SAF forwarder.

If you want to register with more than one SAF forwarder, click the **Show Advanced** link, which allows you to configure multiple SAF forwarders and associate individual members of the cluster selectively with the configured SAF forwarders.

Note If you want to allow multiple nodes of a CUCM cluster to act as SAF clients, each one needs a unique client name. You can either configure each of them individually with separate node names or use a SAF client ID in CUCM, which is **client-ID@**. The @ sign instructs CUCM to add a unique node number so that the actual client IDs are **client-ID@1**, **client-ID@2**, and so on.

At the SAF forwarder, you can either create individual entries or add the keyword **basename** to the **external-client client-ID** command. Do not specify the @ sign at the SAF forwarder; only add the keyword basename to the **external-client** command, and the specified client ID will be permitted with any suffixes of @ followed by a number.

Step 3: Configure SAF-Enabled SIP Trunk

Figure 12-18 shows how to add a SAF-Enabled SIP trunk in CUCM. In Cisco Unified CM Administration, choose Device > Trunk > Add New.

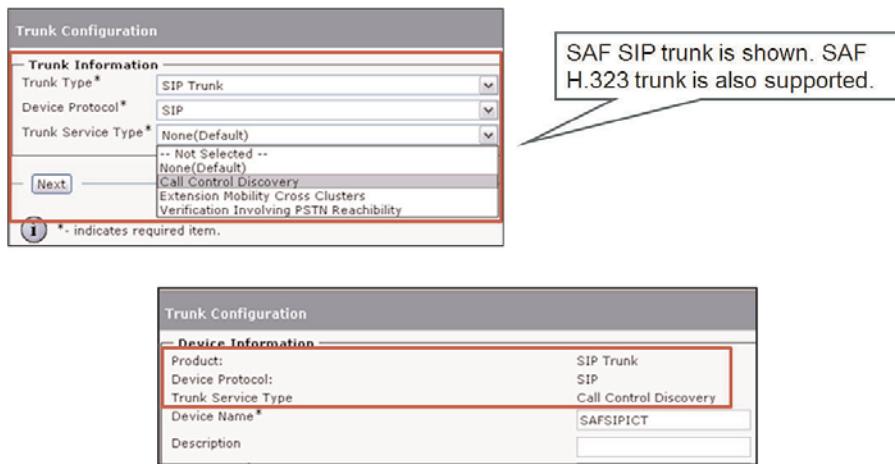


Figure 12-18 Step 3: Configure a SAF Trunk

You can configure one SAF-enabled SIP trunk, as shown in Figure 12-18, or one SAF-enabled H.323 trunk, but you need to create only one of each trunk type. With a SAF-enabled H.323 trunk, you have to first add a standard nongatekeeper-controlled ICT and check the Enable SAF checkbox. After the check box is checked, the IP address field is disabled. The reason is that the configured trunk does not refer to a particular destination IP address but instead acts as a template for a dynamically created trunk once a SAF call is placed. The destination IP address is then taken from the learned SAF service data.

Note Global E.164 number starting with a + are not supported across H.323 trunks. It is recommended to use SIP trunks when doing global routing.

The same concept applies to the SAF-enabled SIP trunk. The only difference is that the SAF-enabled SIP trunk is a special trunk service type, which is selected before the trunk configuration page is shown. Therefore, there is no extra check box like there is at the nongatekeeper-controlled ICT. The SAF-enabled SIP trunk also does not have a destination IP address field. The SAF-enabled SIP trunk must use a nonsecure profile.

You can have one SAF-enabled H.323 or one SAF-enabled SIP trunk.

Step 4: Configure Hosted DN Group

Figure 12-19 shows the configuration of a hosted DN group in CUCM. In Cisco Unified CM Administration, choose Call Routing > Call Control Discovery > Hosted DN Group.

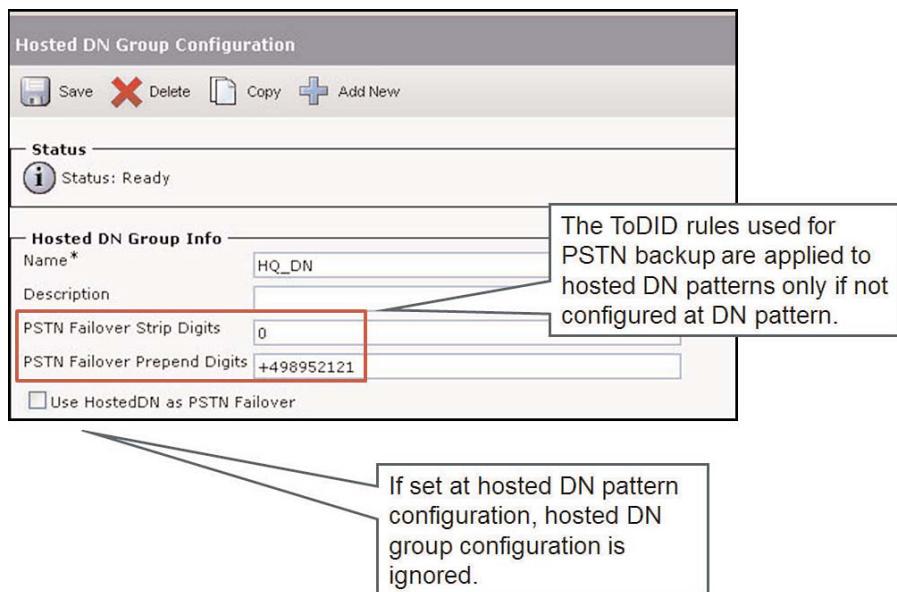


Figure 12-19 Step 4: Configure a Hosted DN Group

The hosted DN group will be referenced from hosted DN patterns. If all (or at least most) of the associated hosted DN patterns share the same ToDID rules, you can configure the ToDID rule at the hosted DN group. The settings of the hosted DN group are applied to the hosted DN patterns if the hosted DN pattern parameters are unset.

Select the **Use Hosted DN as PSTN Failover** check box to create a ToDID rule of 0:. As a result, the number that is to be used for PSTN backup is identical to the internally used number. Usually, this result occurs only when tail-end hop-off (TEHO) patterns are advertised.

Step 5: Configure Hosted DN Pattern

Figure 12-20 shows the configuration of a hosted DN pattern in CUCM. In Cisco Unified CM Administration, choose Call Routing > Call Control Discovery > Hosted DN Pattern.

Hosted DN patterns refer to a hosted DN group. As previously mentioned, if the parameters at the hosted DN pattern are unset, the parameters of the hosted DN group are applied. When the PSTN Failover Strip Digits field is set to 0 and the PSTN Failover Prepend Digits field is empty, both fields are considered unset. The configuration

example shown in Figure 12-20 does not generate a ToDID rule of 0:, but it applies the settings of the configured hosted DN group.

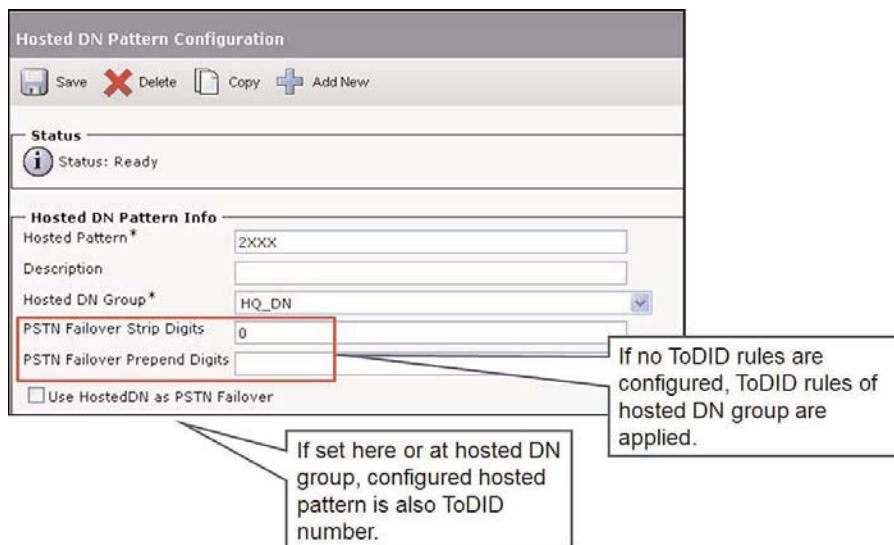


Figure 12-20 Step 5: Configure a Hosted DN Pattern

At the hosted DN group, the same logic applies. If the PSTN Failover Strip Digits field is set to 0 and the PSTN Failover Prepend Digits field is empty at the hosted DN pattern and at the hosted DN group, the no ToDID rule is advertised. As a result, there is no PSTN backup when the IP path is unavailable.

If you want to advertise a ToDID rule of 0:, the number that should be used for backup is identical to the internally used number (for example, when TEHO patterns are advertised). Therefore, you must check the Use Hosted DN as PSTN Failover check box.

Step 6: Configure CCD Advertising Service

Figure 12-21 shows the configuration of the CCD advertising service in CUCM. In Cisco Unified CM Administration, choose Call Routing > Call Control Discovery > Advertising Service.

You need to configure one CCD advertising service for each configured hosted DN group. Each CCD advertising service can use the SAF-enabled SIP trunk or the SAF-enabled H.323 trunk. One trunk has to be specified. Multiple CCD advertising (and the CCD requesting service) can refer to the same SAF-enabled trunks.

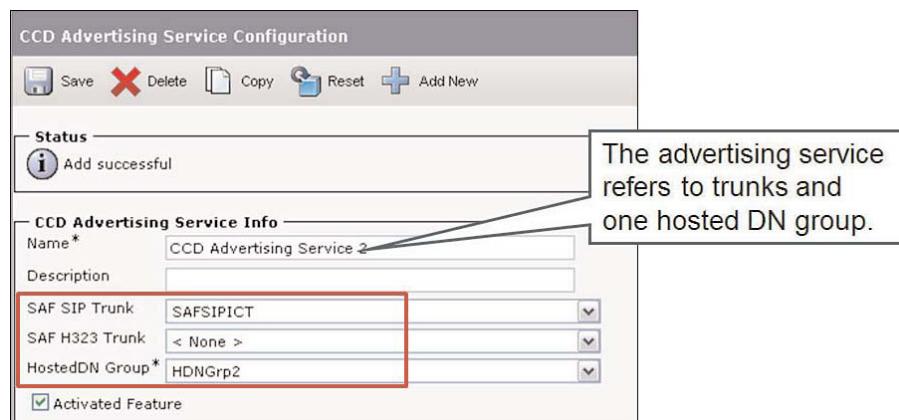


Figure 12-21 Step 6: Configure a CCD Advertising Service

Step 7: Configure CCD Requesting Service and Partition

Figure 12-22 shows the configuration of the CCD requesting service in CUCM. In Cisco Unified CM Administration, choose Call Routing > Call Control Discovery > Requesting Service.

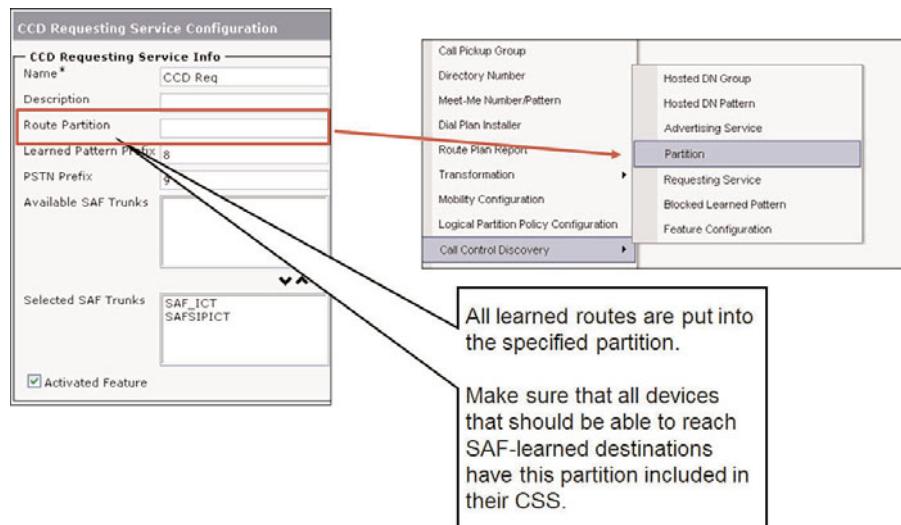


Figure 12-22 Step 7: Configure a CCD Requesting Service and Partition

You can configure only one CCD requesting service. You have to enter the partition into which all learned routes should be put. You must first create the partition as shown in Figure 12-22.

In addition to creating the partition, you can configure the CCD requesting service with a learned pattern prefix and a PSTN prefix. These prefixes are applied to all learned DN patterns and to all learned ToDID rules, respectively.

Finally, the CCD that is requesting service is referred to the SAF-enabled SIP or to the SAF-enabled H.323 trunk.

If you associate the CCD requesting service with only one type of trunk, all received routes that are reachable by the other (unconfigured) protocol type are ignored. They are not added to the call-routing table.

Step 8: Configure CCD Blocked Learned Patterns

Figure 12-23 shows the configuration of the CCD blocked learned patterns in CUCM. In Cisco Unified CM Administration, choose Call Routing > Call Control Discovery > Blocked Learned Pattern.

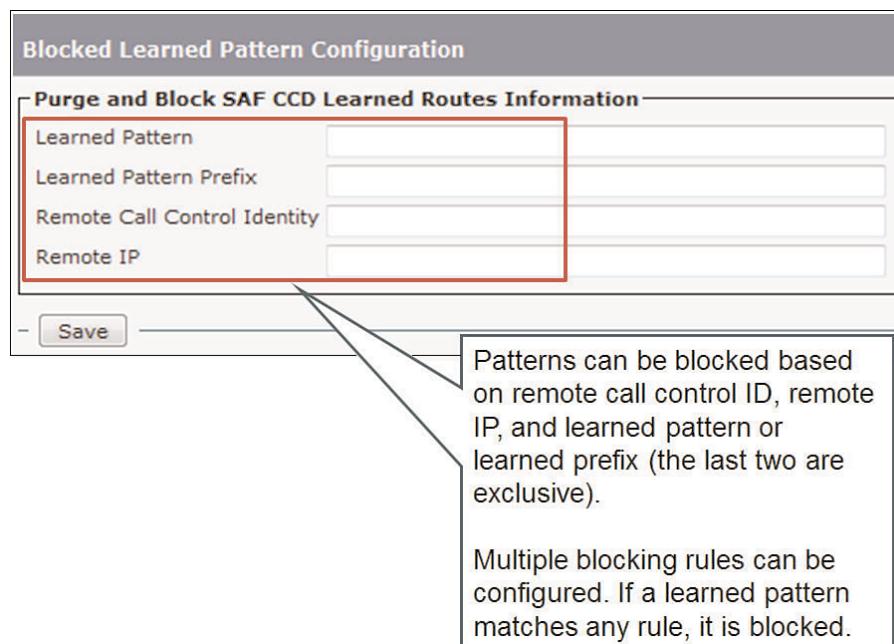


Figure 12-23 Step 8: Configure CCD Blocked Learned Patterns

CCD blocked learned patterns are optional. If CCD blocked learned patterns are configured, all routes that match any of the configured criteria are blocked. As a result, they are not added to the call-routing table.

In Figure 12-23, you can configure a filter that is applied to received routes to deny the learning of routes by using these criteria:

- **Learned pattern:** The received pattern is checked in its entire length. If it matches the configured learned pattern, it will not be added to the local call-routing table.
- **Learned pattern prefix:** The received patterns are compared with the configured prefix, starting with the left-most digit. By using a learned pattern prefix for blocking received routes, you can filter internally used numbers by their leading digit (for example, by their site code).
- **Remote call control identity:** Each call agent has a so-called SAF client ID. By setting the remote call-control identity, you can filter received routes that are based on the ID of the advertising call agent.
- **Remote IP:** By setting this filter, you can block routes that are based on the advertising IP address.

Step 9: Configure CCD Feature Parameters

Figure 12-24 shows the configuration of CCD feature parameters in CUCM. In Cisco Unified CM Administration, choose Call Routing > Call Control Discovery > Feature Configuration.

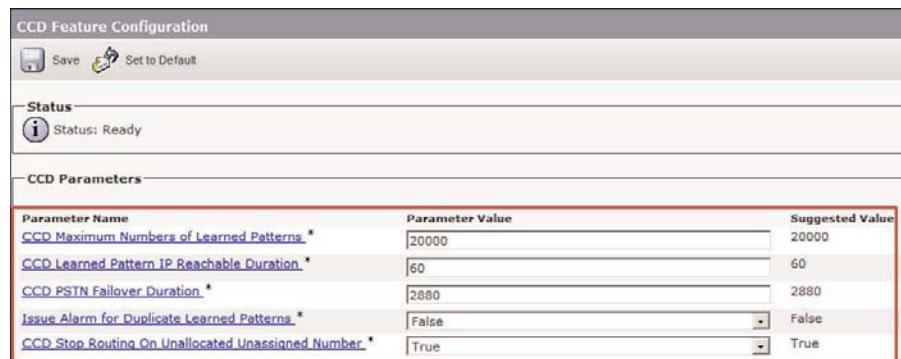


Figure 12-24 Step 9: Configure CCD Feature Parameters

CCD blocked learned patterns are optional. If CCD blocked learned patterns are configured, all routes that match any of the configured criteria are blocked. As a result, they are not added to the call-routing table.

Here are the configurable CCD feature parameters:

- **CCD Maximum Numbers of Learned Patterns:** Specifies the number of patterns that this CUCM cluster can learn from the SAF network. The higher the number of

allowed learned patterns, more memory and CPU-processing power is required. Balance the need for the number of learned patterns in your system with the resources of your deployment hardware components to guide you in setting the value in this parameter. When CUCM attempts to learn more patterns than are allowed by the value set in this parameter, the alarm CCDLearnedPatternLimitReached is issued. The default value is 20,000.

- **CCD Learned Pattern IP Reachable Duration:** Specifies the number of seconds that learned patterns stay active (IP reachable), and CUCM marks those patterns as unreachable. PSTN failover occurs when CUCM cannot communicate with the SAF forwarder because of IP connectivity issues for the duration that is specified in this parameter. For example, this parameter is set to 20 seconds. When CUCM cannot communicate with the SAF forwarder after more than 20 seconds, all calls to learned patterns fail over to the PSTN according to the learned ToDID rule. PSTN failover continues until IP connectivity to the SAF forwarder is restored. CUCM automatically detects the restored connectivity to the SAF forwarder. CUCM then falls back to the IP path of routes as soon as the routes are received with the appropriate reachability information again. When the time specified by this parameter elapses, CUCM marks the learned patterns as unreachable. If enabled, the CCD PSTN Failover Duration service parameter timer starts, which allows patterns that have been marked as unreachable through IP to instead be reached through PSTN failover. The default value is 60 seconds.
- **CCD PSTN Failover Duration:** Specifies the number of minutes that calls that are placed to learned patterns that have been marked unreachable are routed through PSTN failover and are then purged from the system. For the duration specified in this parameter to start counting down, another service parameter, CCD Learned Pattern IP Reachable Duration, must first have expired. The expiration of that parameter indicates that IP connectivity is down between the SAF forwarder and CUCM, and that all learned patterns are marked unreachable. Then, when the duration in this parameter, CCD PSTN Failover Duration, expires, all learned patterns are purged from the system. Also, calls to purged patterns are rejected (the caller hears a reorder tone or a This Number Is Unavailable announcement). Setting this parameter to 0 means that PSTN failover is disabled. If the SAF forwarder cannot be reached for the number of seconds defined in the CCD Learned Pattern IP Reachable Duration service parameter, and no failover options are provided through the PSTN, calls to learned patterns immediately fail. Setting this parameter to 525,600 means that PSTN failover will never expire and, as a result, learned patterns will never be purged because of a loss of communication with the SAF forwarder. The default is 2880 minutes (48 hours).
- **Issue Alarm for Duplicate Learned Patterns:** Determines whether CUCM issues an alarm called DuplicateLearnedPattern when it learns duplicate patterns from different remote call-control entities on the SAF network. The default value is False.
- **CCD Stop Routing on Unallocated Unassigned Number:** Determines whether CUCM continues to route calls to the next learned call control entity (if advertised

by multiple call agents) when the current call control entity rejects the call with the cause code for Unallocated/Unassigned Number. An unallocated number represents a hosted directory number that does not exist in the current call control entity. The default value is True.

Internal SAF Client Configuration Procedure

The following steps are the configuration procedure of an internal SAF client on an IOS router:

- Step 1.** Configure trunk profile.
- Step 2.** Configure directory-number blocks to be advertised.
- Step 3.** Configure call-control profile.
- Step 4.** Configure advertising service.
- Step 5.** Configure requesting service.
- Step 6.** Configure VoIP dial peer referring to SAF.

You can do the configuration steps listed in the figure multiple times, if multiple SAF forwarder processes are configured in separate autonomous systems. Each SAF client channel that is configured with the advertising and the requesting service has to refer to another SAF autonomous system.

The CCD advertising service of a single SAF client channel can refer to multiple call-control profiles. This capability allows the configuration of two trunk profiles (one SIP and one H.323 trunk per call-control profile). Only one trunk is required.

Step 1: Configure Trunk Profile

Example 12-1 shows the configuration of a trunk profile in Cisco IOS Software from global configuration mode.

The trunk profile is configured with the interface that should be used for call signaling. It is configured also with the protocol type (in this case, SIP) and the transport parameters (TCP versus UDP, and port number).

You can configure one SIP trunk or one H.323 trunk.

Example 12-1 Configuring the Trunk Profile in Cisco IOS Software

```

Interface Loopback1
  IP Address 10.1.1.1 255.255.255.255
!
router eigrp SAF
!
  service-family ipv4 autonomous-system 1
!
```

```

sf-interface Loopback1
topology base
exit-sf-topology
exit-service-family
!
voice service saf
profile trunk-route 1
session protocol sip interface loopback1 transport tcp port 5060

```

Step 2: Configure Directory-Number Blocks

Example 12-2 shows the configuration of directory-number blocks in Cisco IOS Software from global configuration mode. Each directory-number block is configured globally with a ToDID applied to all extensions that are listed later. The command to configure a directory-number block is **profile dn-block tag alias ToDID-prefix strip ToDID-strip**. The subsequent command to add extensions is **pattern tag type extension pattern**.

Example 12-2 Configure Directory-Number Blocks

```

router eigrp SAF
!
service-family ipv4 autonomous-system 1
!
sf-interface Loopback1
topology base
exit-sf-topology
exit-service-family
!
voice service saf
profile trunk-route 1
session protocol sip interface loopback1 transport tcp port 5060
!
profile dn-block 1 alias-prefix 1972555
pattern 1 type extension 4XXX

```

Note The *ToDID-strip* argument stands for the number of digits to be stripped; the *ToDID-prefix* argument stands for the prefix to be added to the internal number after stripping digits.

Neither the *ToDID-prefix* argument nor the *pattern* argument support the use of the + sign. If you want to advertise a number with a + sign, you must use the command **pattern tag type global pattern**. Again, you cannot enter the + sign in the *pattern* argument; however, because of the type global, a + sign is prefixed to the configured *pattern*. The ToDID of global patterns is always unset.

Step 3: Configure Call-Control Profile

Example 12-3 shows the configuration of the call-control profile in Cisco IOS Software from global configuration mode.

Example 12-3 *Configure Call-Control Profile*

```
router eigrp SAF
!
service-family ipv4 autonomous-system 1
!
sf-interface Loopback1
topology base
exit-sf-topology
exit-service-family
!
voice service saf
profile trunk-route 1
  session protocol sip interface loopback1 transport tcp port 5060
!
profile dn-block 1 alias-prefix 1972555
  pattern 1 type extension 4XXX
!
profile callcontrol 1
dn-service
trunk-route 1
dn-block 1
```

The call-control profile refers to one or more directory-number blocks and to a particular trunk. The call-control profile will be used in the next step to specify that the listed directory-number blocks should be advertised at the specified trunk or trunks (if two of them are used). Another command that you can enter under **dn-service** is **site-code site-code extension-length length**. It allows a site code to be prefixed to all configured extensions referenced by the call-control profile. The **extension-length** argument sets the number of digits (starting with the least-significant digit) that should be preserved from the configured extension before the site code is added.

Step 4: Configure Advertising Service

Example 12-4 shows the configuration of the advertising service in Cisco IOS Software from global configuration mode.

Example 12-4 Configure Advertising Service

```

router eigrp SAF
!
service-family ipv4 autonomous-system 1
!
sf-interface Loopback1
topology base
exit-sf-topology
exit-service-family
!
voice service saf
profile trunk-route 1
  session protocol sip interface loopback1 transport tcp port 5060
!
profile dn-block 1 alias-prefix 1972555
  pattern 1 type extension 4XXX
!
profile callcontrol 1
dn-service
  trunk-route 1
  dn-block 1
!
channel 1 vrouter SAF asystem 1
  publish callcontrol 1

```

You configure the advertising and requesting services under **channel tag vrouter EIGRP-ID asystem AS**. The **EIGRP-ID** argument refers to the name that was assigned to the router EIGRP process (SAF, in the example). The **AS** argument is the AS number that was assigned to the EIGRP service family.

To enable the advertising service itself, you use the command **publish callcontrol tag**. The **tag** argument refers to the tag that was applied to the previously configured call-control profile. Effectively, you configure the call-control profile (which determines which directory numbers should be advertised by which trunk protocol) by the SAF process identified by the autonomous-system number.

Step 5: Configure Requesting Service

Example 12-5 shows the configuration of the advertising service in Cisco IOS Software from global configuration mode.

Example 12-5 Configure Requesting Service

```

router eigrp SAF
!
service-family ipv4 autonomous-system 1
!
sf-interface Loopback1

```

```

        topology base
        exit-sf-topology
        exit-service-family
    !
    voice service saf
        profile trunk-route 1
            session protocol sip interface loopback1 transport tcp port 5060
    !
    profile dn-block 1 alias-prefix 1972555
        pattern 1 type extension 4XXX
    !
    profile callcontrol 1
        dn-service
            trunk-route 1
            dn-block 1
    !
    channel 1 vrouter SAF asystem 1
        subscribe callcontrol wildcarded
        publish callcontrol 1

```

You can also configure the requesting service under **channel tag vrouter EIGRP-ID asystem AS**. Use the **subscribe callcontrol wildcarded** command to enable the learning of routes that are advertised by the SAF process that matches the autonomous-system number specified at the channel configuration level.

Step 6: Configure VoIP Dial Peer

Example 12-6 shows the configuration of a dial peer that refers to SAF-learned routes in Cisco IOS Software from global configuration mode.

Example 12-6 Configure VoIP Dial Peer

```

router eigrp SAF
!
service-family ipv4 autonomous-system 1
!
sf-interface Loopback1
topology base
exit-sf-topology
exit-service-family
!
voice service saf
profile trunk-route 1
    session protocol sip interface loopback0 transport tcp port 5060

```

```

!
profile dn-block 1 alias-prefix 1972555
    pattern 1 type extension 4XXX
!
profile callcontrol 1
    dn-service
        trunk-route 1
        dn-block 1
!
channel 1 vrouter SAF asystem 1
    subscribe callcontrol wildcarded
    publish callcontrol 1
!
dial-peer voice 2045 voip
    destination-pattern .T
    session target saf

```

The configuration of this dial peer is like the configuration of a dial peer that refers to a **session target ras** command when an H.323 gatekeeper is used. The destination pattern **.T** stands for all learned routes. The rest of the dial peer configuration is used as a template for the outgoing dial peer that is used on outbound SAF calls, and for the incoming dial peer that is used on inbound SAF calls.

If you have other dial peers that also represent learned routes, the **preference** command determines which dial peer should be treated with higher priority.

CCD Considerations

The following additional considerations must be accounted for in a CCD and SAF implementation:

- Monitoring SAF-learned routes
- CSS used for PSTN backup calls
- SRST implementation with CCD
- CCD integration with static routing
- Cisco IOS SAF client limitations when advertising +
- TEHO implementation with CCD
- Globalized call routing and trunk types

- SAF in CUCM clusters that use clustering over the WAN
- Other SAF and CCD considerations

The following sections address these CCD considerations.

Monitoring Learned Routes from CUCM in RTMT

SAF-learned routes are not visible by any tool in the CUCM Administration web page. The only way to view SAF-learned routes is by using the Cisco Unified Real-Time Monitoring Tool (RTMT).

Figure 12-25 shows an example of SAF-learned routes that are displayed by Cisco Unified RTMT. The ToDID rule 0: means that the “internal” pattern and the pattern that is used for PSTN backup are the same pattern. This principle usually applies when advertising TEHO patterns are advertised. The ToDID rules that are empty mean that there is no PSTN backup path for the respective learned patterns.

Learned Pattern						
Select a Node CUCM801Pub1 ▾						
Pattern	TimeStamp	Status	Protocol	AgentId	IP Address	ToDID
\+14087071222	2010/03/11 18:56:33	Reachable	SIP		10.1.132.1(5060)	
\+14087071222	2010/03/11 18:56:33	Reachable	H323		10.1.132.1(1720)	
300X	2010/03/12 08:03:27	Reachable	SIP	StandAloneCluster	10.1.5.11(5060)	0+44228822
3XXX	2010/03/12 08:03:27	Reachable	H323	StandAloneCluster	10.1.5.11(33143)	0+44228822
400X	2010/03/11 18:56:33	Reachable	SIP		10.1.132.1(5060)	0.1972555
4XXX	2010/03/11 18:56:33	Reachable	H323		10.1.132.1(1720)	0.1972555
\+44201	2010/03/11 18:56:33	Reachable	SIP	StandAloneCluster	10.1.5.11(5060)	0
\+44201	2010/03/11 18:56:33	Reachable	H323	StandAloneCluster	10.1.5.11(33143)	0

Figure 12-25 Monitoring SAF-Learned Routes from CUCM in RTMT

Monitoring Learned Routes in CUCME

Example 12-7 shows the output of the SAF-learned routes in Cisco IOS Software configured as CUCME with the command `show voice saf dndp all`. Note that only a call agent can interpret SAF service data; SAF forwarders cannot interpret SAF service data. Therefore, this command works only on Cisco IOS routers that are internal SAF clients and SAF forwarders.

The output shows two types of patterns: extensions (with a ToDID) that were learned from a device other than a Cisco IOS device; and global patterns, which include a + sign and no ToDID information (most likely advertised by another Cisco IOS internal client).

Example 12-7 Monitoring Learned Routes in CUCME

```
BR2# show voice saf dndp all
-
Last successful DB update @ 2010:03:12 16:03:27:838

***** Private Dialplan Partition *****

Pattern - 2XXX
```

```

Primary Trunk-Route(s) ID : 273 274
Alias-Route(s) Prefix/Strip-Len : +498952121/0

Pattern - 3XXX
Primary Trunk-Route(s) ID : 270 269
Alias-Route(s) Prefix/Strip-Len : +44228822/0

***** Global (E164) Dialplan Partition *****

Pattern - +4420!
Trunk-Route(s) ID : 271 272

Pattern - +16505051234
Trunk-Route(s) ID : 270 269

```

CCD PSTN Backup CSS

When a learned pattern is marked unreachable and a ToDID is advertised with the pattern as shown in Figure 12-26, a PSTN backup call is placed. The CSS that is used for this call is the AAR CSS.

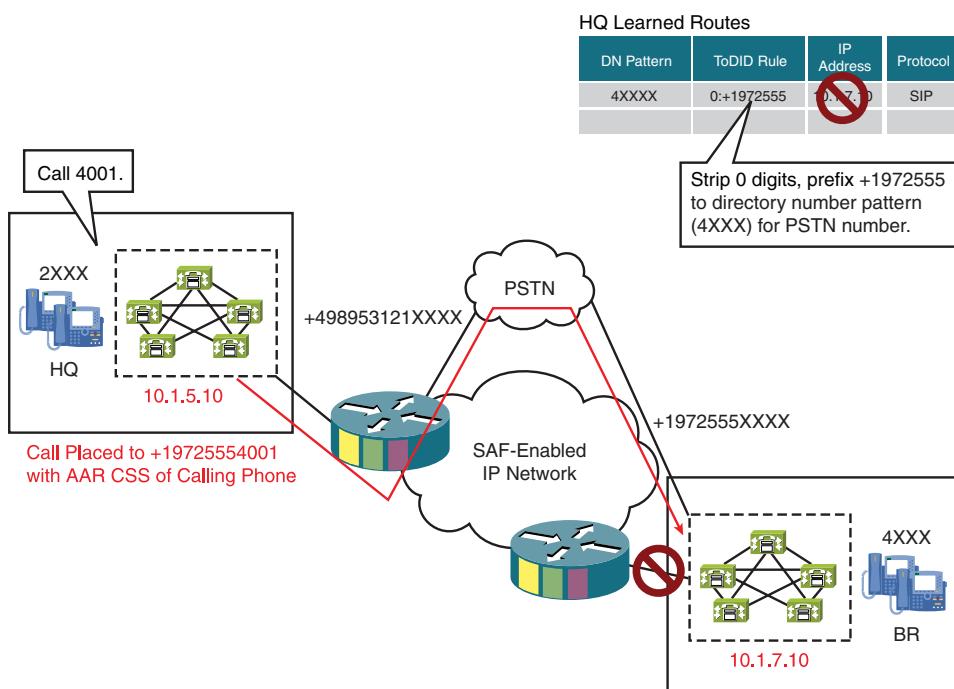


Figure 12-26 CCD PSTN Backup CSS

Make sure that the AAR CSS is set at all phones, so that PSTN backup calls for CCD-learned patterns will work. Also, ensure that the number that is composed of the directory-number pattern and the ToDID rule is routable. (In other words, a route pattern matches the number dialed.)

Note PSTN backup for CCD is completely independent from AAR. AAR places PSTN backup calls for cluster-internal destinations when the IP path cannot be used because of insufficient bandwidth, as indicated by CAC.

Only the AAR CSS is reused for CCD PSTN backup. Otherwise, CCD PSTN backup does not interact with AAR at all. For example, CCD PSTN backup works even when AAR is globally disabled by the corresponding Cisco CallManager service parameter.

SRST Considerations

A Cisco Unified SRST gateway does not need to advertise any internal directory numbers because the SRST site is reachable only via the PSTN. It is the responsibility of CUCM to know how to route calls to cluster-internal directory numbers when they are not reachable over the IP WAN, as shown in Figure 12-27.

- SRST subscribes to the CCD service but does not publish any patterns
- During WAN failures, SRST uses learned patterns to transparently reroute calls over the PSTN.

New York SRST Routing Table

DN Pattern	ToDID Rule	IP Address	Protocol
8408XXXX	4:+1408555	10.1.1.1	SIP
8415XXXX	4:+1415777	10.1.1.1	SIP
8449XXXX	4:+1949222	10.1.1.1	SIP

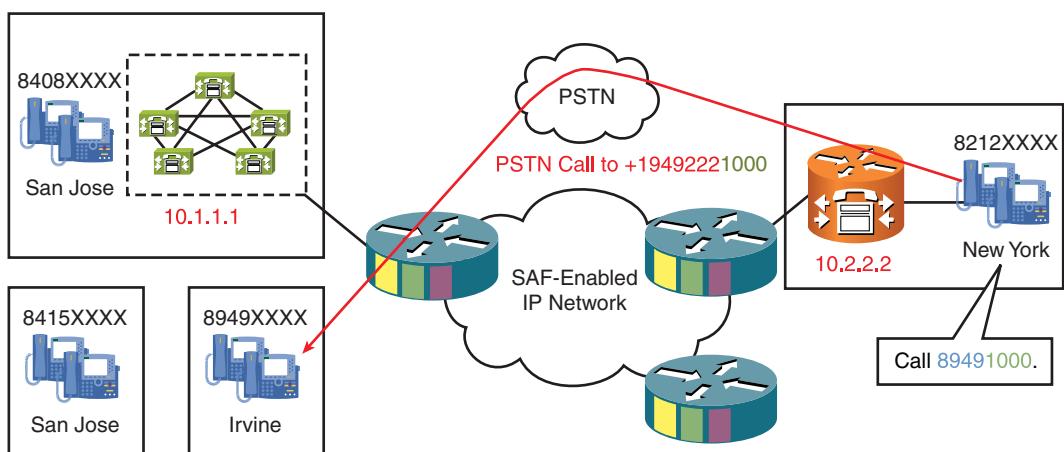


Figure 12-27 SRST Considerations with SAF and CCD

However, the Cisco Unified SRST gateway needs a local dial plan that allows end users to place calls to other sites by dialing the internal directory number of the other site. Cisco Unified SRST then must transform the internally used directory numbers to the corresponding PSTN numbers so that the call can be rerouted over the PSTN. This local dial plan does not have to be configured manually when CCD is used. Instead, Cisco Unified SRST can subscribe to SAF and learn all internally known directory-number ranges and the corresponding ToDID rules. Cisco Unified SRST learns these routes while there is no network problem. At this time, the learned patterns are not used because the Cisco Unified SRST gateway does not route any calls; CUCM controls all IP Phones and performs call-routing services.

After IP connectivity is broken, IP Phones fall back to the Cisco Unified SRST gateway and, when registered, the Cisco Unified SRST gateway has to route calls. Because the gateway has learned all available internally used directory numbers with the corresponding ToDID rules, it can now route to the respective PSTN number any calls that are based on the dialed internal directory number.

In Figure 12-27, the Cisco Unified SRST gateway learned three patterns while IP connectivity was working: 8408XXXX with a ToDID rule of 4:+1408555, 8415XXXX with a ToDID rule of 4:+18415, and 8949XXXX with a ToDID rule of 4:+1949222.

When a user dials 89491000 while the gateway is in SRST mode, the IP path is marked unreachable because of the loss of IP connectivity. Therefore, the ToDID rule is applied: It strips the first four digits and adds the prefix +1949222 so that the number used for the PSTN backup call is +19492221000.

The only static configuration required at the Cisco Unified SRST gateway is an outbound dial peer that routes calls starting with + toward the PSTN.

CCD and Static Routing Integration Considerations

All routes learned by CCD are put into the same configurable partition. If this partition is listed first in the CSS of the calling phones, it has higher priority for equally qualified matches than partitions that are listed later.

Such a configuration allows learned routes to take precedence over statically configured backup routes. You have to make sure that backup routes in later partitions are not more specific than learned routes because the order of partitions is relevant only if the matches are equally qualified.

Be aware that routes in later partitions are considered only after learned routes are removed from the call-routing table.

When CUCM loses IP connectivity to its SAF forwarder, it waits for 60 seconds until it considers the IP path to be unavailable. You can configure this time by configuring the **CCD Learned Pattern IP Reachable Duration** feature parameter by navigating in **Cisco Unified CM Administration > Call Routing > Call Control Discovery > Feature Configuration**. During that time, calls to learned patterns fail.

After the timer expires, CUCM starts another timer, the CCD PSTN Failover Duration. The default value for this timer is 48 hours. During this time, CUCM tries to place a CCD PSTN backup call. If no ToDID has been advertised, CUCM assumes that there is no PSTN backup path and that, therefore, calls will fail.

The learned route is purged only after the expiration of the timer. Then, another (statically configured backup) pattern, which is in a partition listed after the CCD partition, can be matched. If you want to use locally configured static backup patterns, either disable CCD PSTN backup by setting the CCD PSTN Failover Duration timer to 0, or set the timer to a lower value than the default (two days) by navigating in **Cisco Unified CM Administration** to **Call Routing > Call Control Discovery > Feature Configuration**.

Cisco IOS SAF Client Considerations When Using Globalized Call Routing

Cisco IOS internal SAF clients have limited support regarding the + sign in advertised routes. In fact, the + sign cannot be configured in either the directory-number pattern or the ToDID rule. The only way to advertise a pattern with + is to use the **pattern tag type global** command instead of the **pattern tag type extension** command. In this case, however, the ToDID is always unset, regardless of the configured alias prefix at the directory-number block profile, as illustrated in Table 12-3.

When a CCD-enabled CUCM uses globalized call routing for PSTN access, the mentioned limitation of Cisco IOS internal SAF clients causes issues because the backup PSTN number is not in a format that CUCM can route to the PSTN.

The workaround is to make sure that CCD PSTN backup calls can be routed to the PSTN even if the number that results from the ToDID rule does not start with +.

Table 12-3 Cisco IOS SAF Client Considerations When Using Globalized Call Routing

Cisco IOS Configuration	DN Pattern and ToDID	Limitation
profile dn-block 1 alias-prefix 197255	4XXX 0:197255	The + is not supported in alias-prefix or extension.
pattern 1 type extension 4XXX		PSTN backup cannot be advertised with +.
profile dn-block 2 pattern 1 type global 14087071222	+14087071222 (no ToDID)	The + is added to patterns configured with type global. Global patterns always have ToDID unset. There is no PSTN backup for global patterns.

Note Cisco IOS Software has limitations only in advertising patterns that include the + sign. Cisco IOS Software can process received patterns that include a + sign without any problems or limitations.

Solution for PSTN Backup Advertised in E.164 Format Without Leading +

Figure 12-28 illustrates the workaround for CCD PSTN backup calls to PSTN destinations that are in E.164 format *without* a + prefix.

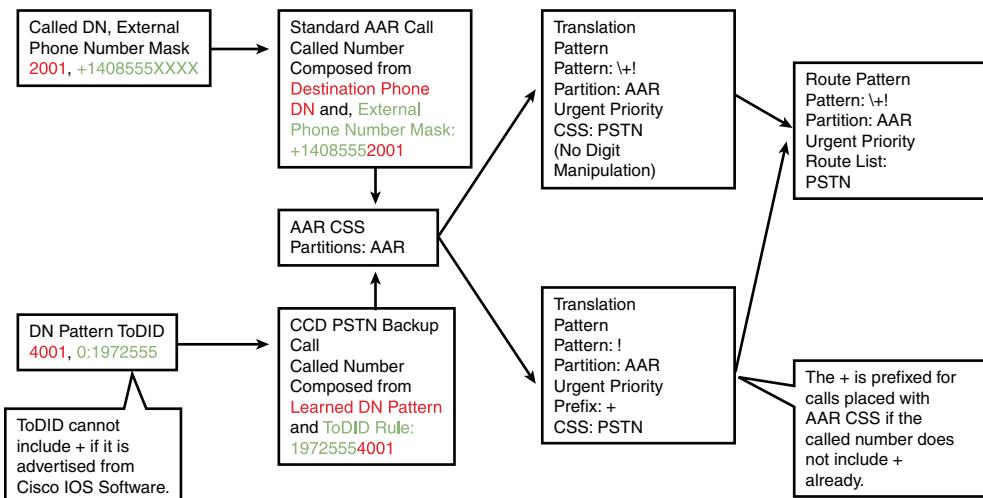


Figure 12-28 Solution for PSTN Backup Advertised in E.164 Format Without a Leading +

It is a desirable goal, but it can be cumbersome to add all possible E.164 numbers to the overall dial plan of CUCM. However, because CCD PSTN backup calls are always placed using the AAR CSS of the calling phone, you can add one translation pattern ! to a partition that is accessible only from the AAR CSS. At that pattern, you can prefix a + to the called-party number and set the CSS of the translation pattern to a CSS that has access to the global PSTN route pattern (+!).

That process solves the issue with CCD PSTN backup calls. However, if AAR is enabled, it will break AAR, assuming that the AAR implementation is based on globalized call routing. If the external phone number mask of the destination phone is in E.164 format *with* a + prefix, AAR calls would not work anymore. The reason is that they use the same CSS and therefore would also match the ! translation pattern that prefixes a +. In this case, AAR calls would be placed to E.164 numbers with two + signs. To also make AAR CSS calls work, you have to add a second translation pattern into the same partition that is only accessible from the AAR CSS. This second translation pattern \+! is not configured with any digit manipulation but uses the same CSS as the other translation pattern (!). As a consequence, AAR calls are passed to the \+! route pattern without any digit manipulation (by matching the more specific \+! translation pattern, which does not prefix a +). CCD PSTN backup calls do not match the \+! translation pattern and are therefore routes, as previously explained.

Note The described solution is only a workaround. The implementation of advertised patterns in Cisco IOS Software may change in the future so that + can be configured in the advertised pattern and in the ToDID rule. If so, you should change from the described workaround to the solution that allows CCD PSTN backup calls to be placed to globalized numbers.

TEHO Considerations

TEHO destinations are located at the PSTN only; they do not exist internally at all. The advertised directory number is a PSTN number. When globalized call routing is enabled, this number has to be in E.164 format with a + prefix.

Calls to PSTN destinations will match the learned directory number and are therefore sent to the TEHO site over the IP WAN. In case the IP WAN is down, the local gateway should be used as a backup. This situation requires having a ToDID rule of 0:. With this rule, the CCD PSTN backup number is identical to the learned directory number. When the IP path is marked as unreachable, the same number would be called using the AAR CSS of the calling phone.

In CUCM, generate a ToDID rule of 0: by checking the **Use Hosted DN as PSTN Failover** check box, as previously shown in Figure 12-19. In Cisco IOS Software, you cannot set the ToDID to 0:.

Furthermore, if globalized call routing is to be used, you are forced to use global patterns, which do not allow any ToDID rule to be advertised.

When TEHO pattern is advertised without a ToDID rule, local TEHO backup does not work. You could only configure static local backup routes by putting similar patterns into partitions that are listed later in the phone CSS. However, such patterns are used only after the learned pattern has been completely purged. By default, this process occurs after the expiration of the CCD PSTN Failover Duration timer, which is 48 hours by default.

Based on these issues, it is recommended that you do not advertise TEHO patterns from Cisco IOS Software if the + is required and local backup is desired.

Trunk Considerations When Using Globalized Call Routing

As previously mentioned, you can configure one SAF-enabled SIP trunk or one SAF-enabled H.323 trunk in CUCM and in Cisco IOS Software. If both types of trunk are used by the advertising SAF client and both are used at the requesting SAF client, all routes are learned twice, once per protocol. When placing a call to such a route, loadsharing occurs. This means that half of the calls are set up using SIP, and half of the calls are signaled by H.323.

When implementing TEHO and using globalized call routing, TEHO calls are expected to be received with a + prefix. The reason is that they are advertised that way and the incoming VoIP call can be routed back out to the PSTN at the TEHO gateway when the called number is in globalized format.

H.323 trunks, however, do not send the + sign. When a call is received (or placed) through an H.323 trunk and the called number includes a +, the + sign is stripped. This does not happen on SIP trunks.

When you rely on the + to be received through the H.323 trunk, you have to configure incoming called-party settings at the H.323 trunk. Consequently, the + is prefixed before the received called-party number is matched in the call-routing table without the +.

If you have a SIP and an H.323 trunk, and you do not prefix the + at the H.323 trunk because of the load-sharing algorithm, every second call would fail (H.323), whereas the other half of calls would work (SIP). These apparently inconsistent errors are difficult to troubleshoot.

Note When you expect to receive VoIP calls to internal directory numbers and globalized (PSTN) numbers, make sure that your incoming called-party settings prefix only the + to the called numbers where it is required. You can either refer to the ISDN type of number or use global transformations to control which called-party numbers you can modify.

CUCM Clusters and CCD Configuration Modes

When you are configuring a CUCM cluster with one or more SAF forwarders, by default, all CUCM nodes applied to the SAF-enabled trunk or trunks via the device pool register with the configured SAF forwarder. The two CUCM CCD configuration modes, as illustrated in Figure 12-29, are

- **Basic configuration mode:** All CUCM servers use the same primary or secondary SAF forwarders.
- **Advanced configuration mode:** Multiple sets of forwarders can be configured and individually applied to CUCM servers. This mode is required when clustering over the WAN deployment model is used.

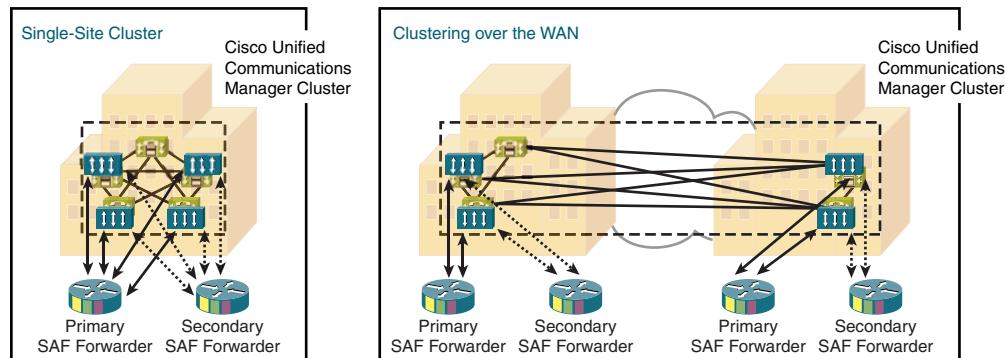


Figure 12-29 CUCM CCD Configuration Modes

First, make sure that each local node uses a different SAF client ID. You can easily check the nodes by using a SAF client name that ends with @. In this case, each node uses the configured name that is followed by @ and a unique node ID. At the SAF forwarder, you have to add the **basename** keyword to the end of the SAF **external-client *client-ID*** command, or you have to manually configure all names that are used by the nodes in your cluster.

In some cases, you may not want all nodes that should use SAF register with all configured SAF forwarders. For example, as shown in Figure 12-29, when you use clustering over the WAN, you typically want to register nodes only with their local SAF forwarders. For that configuration, click the **Show Advanced** link at the SAF forwarder configuration page.

At the advanced configuration mode page, you can associate individual members of the cluster selectively with the configured SAF forwarders.

Other SAF and CCD Considerations

Here are some other SAF and CCD considerations you need to take into account in your design:

- If you do not assign a trunk when you configure the CCD requesting service, CUCM will not subscribe to the SAF forwarder. No routes will be learned.
- Each hosted DN pattern must be globally unique.
- If a trunk is assigned to a route group or is associated with a route pattern, you cannot enable SAF on the trunk, and vice versa.
- You cannot enable SAF on SIP trunks that use authenticated or encrypted security profiles.

Summary

The following key points were discussed in this chapter:

- Dynamic distribution of call-routing information simplifies dial plan implementation in large or very large networks.
- SAF allows any services to be advertised to and learned from a SAF-enabled network.
- CCD allows call agents to advertise the internal directory numbers that they serve, along with the appropriate PSTN numbers, using SAF.
- When a learned VoIP route to a directory number becomes invalid, the call is automatically rerouted over the PSTN.

- SAF and CCD implementation includes the configuration of SAF forwarders and SAF clients. SAF clients can be internal or external to the Cisco IOS router used as a SAF forwarder.
- Special considerations that relate to SAF and CCD implementation include deployments using SRST, TEHO, globalized call routing, and environments that have a SAF SIP trunk and a SAF H.323 trunk.

References

For additional information, refer to these resources:

Cisco IOS Service Advertisement Framework Configuration Guide 15.1.

www.cisco.com/en/US/docs/ios/saf/configuration/guide/saf_cg_ps10592_TSD_Products_Configuration_Guide_Chapter.html.

Cisco Systems, Inc. *Cisco Unified Communications System 8.x SRND*, April 2010.
www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8x.html.

Cisco Systems, Inc. *Cisco Unified Communications Manager Administration Guide Release 8.0(1)*, February 2010.

www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_1/ccmcfg/bccm-801-cm.html.

Review Questions

Use these questions to review what you've learned in this chapter. The answers appear in the "Answers Appendix."

1. Which two devices do *not* support CCD?
 - a. Cisco Unified SRST
 - b. Cisco IOS gateway
 - c. CUBE
 - d. Cisco IOS gatekeeper
 - e. CUCM
 - f. CUCME
 - g. Cisco IOS Catalyst switches
2. Which two statements are true about SAF?
 - a. SAF forwarders interpret the SAF header and SAF service data.
 - b. An internal SAF client is collocated with a SAF forwarder.
 - c. An internal SAF client resides in CUCM.

- d.** SAF clients do not have to be Layer 2–adjacent.
 - e.** SAF requires EIGRP to be used as the IP routing protocol.
- 3.** Which two statements are *not* true about CCD?
 - a.** Call-routing information is learned by the CCD requesting service.
 - b.** Call-routing information is advertised by the CCD advertising service.
 - c.** Load balancing occurs among trunk protocols and learned remote IP addresses.
 - d.** Learned call-routing information can be placed into different partitions that are based on the remote call control identity.
 - e.** Learned call-routing information can be placed into different partitions that are based on the remote IP address.
- 4.** Which is a valid purpose of the ToDID rule in CCD?
 - a.** The ToDID rule describes how to manipulate the learned DN pattern to get to the number that should be used for a PSTN backup call if the CCD path is unavailable.
 - b.** The ToDID rule describes how to manipulate the learned DN pattern to get to the number that should be used for a PSTN backup call when the CCD path is available.
 - c.** The ToDID rule describes how to manipulate the internal DNs to get to the number that should be used for a PSTN backup call if the CCD path is unavailable.
 - d.** The ToDID rule describes how to manipulate the internal DNs to get to the number that should be used for a PSTN backup call when the CCD path is available.
- 5.** Which is *not* a configuration step when implementing SAF in CUCM?
 - a.** Configure SAF forwarder.
 - b.** Configure SAF trunk.
 - c.** Configure CCD advertising and requesting service.
 - d.** Configure hosted DN group and hosted DN pattern.
 - e.** Configure DN block profile.
 - f.** Configure blocked learned patterns.

- 6.** Which CSS is used for CCD PSTN backup calls?
 - a.** Line CSS of the originating phone
 - b.** Device CSS of the originating phone
 - c.** CSS of the SAF trunk
 - d.** AAR CSS of the originating phone
 - e.** CSS of the PSTN gateway
- 7.** Upon which protocol is Cisco SAF and CCD built?
 - a.** BGP
 - b.** OSPF
 - c.** RIP
 - d.** EIGRP
- 8.** Where are the SAF-learned routes in headquarters viewed by the administrator?
 - a.** CUCM Administration.
 - b.** CUCM Serviceability.
 - c.** They cannot be viewed.
 - d.** RTMT.

This page intentionally left blank

Answers Appendix

Chapter 1

- 1. D
- 2. C
- 3. C
- 4. C
- 5. C
- 6. D
- 7. A
- 8. C
- 9. C

Chapter 2

- 1. D
- 2. C
- 3. B and C
- 4. D and E
- 5. A
- 6. A

7. B and C

8. C

9. C

10. B

Chapter 3

- 1. B
- 2. C and D
- 3. B
- 4. C
- 5. B

6. B and C

7. A

8. C

9. C

Chapter 4

- 1.** C
- 2.** D
- 3.** D and E
- 4.** A and C
- 5.** B
- 6.** D
- 7.** D and G
- 8.** C and D
- 9.** A

Chapter 7

- 1.** B and C
- 2.** D and E
- 3.** B, C, and G
- 4.** C
- 5.** D
- 6.** D
- 7.** C
- 8.** B

Chapter 5

- 1.** C
- 2.** B and D
- 3.** D
- 4.** C and D
- 5.** B
- 6.** B
- 7.** B
- 8.** B and C

Chapter 8

- 1.** D
- 2.** A
- 3.** B
- 4.** C
- 5.** A
- 6.** B
- 7.** B
- 8.** B
- 9.** B

10. B and C

Chapter 6

- 1.** B
- 2.** B
- 3.** D
- 4.** D
- 5.** A
- 6.** D
- 7.** B
- 8.** D
- 9.** D

Chapter 9

1. B and D
2. A
3. D
4. B and E
5. A
6. A
7. B
8. C
9. B
10. B
11. A
12. C
13. C
14. C

Chapter 10

1. B
2. A and C
3. C
4. A
5. A and D
6. C
7. B
8. B
9. A, C, and D
10. B

Chapter 11

1. A
2. C and D
3. A, D, and E
4. A and D
5. A and B
6. A
7. D
8. B
9. C
10. A

Chapter 12

1. D and G
2. B and D
3. D and E
4. A
5. E
6. D
7. D
8. D

This page intentionally left blank

Index

A

- AAR (Automated Alternate Routing),** 44, 255-263
 - characteristics, 256-259
 - configuring, 260-263
- activation commands, MGCP fallback,** 158-159
- advantages**
 - of CUCME SRST, 194
 - of globalized call routing, 50-51
 - of TEHO, 116
- advantages of QoS, 25-26**
- annunciators, disabling, 29-30**
- availability, challenges to CUCM**
 - multisite deployment, 6-7**
 - solutions, 38-44

B

- B2BUA, 128**
- bandwidth**
 - CFNB, 44**
 - challenges to CUCM multisite

- deployment, 3-5, 26-38**
- managing, 201-202**
 - local conference bridge implementation, 205-208*
 - transcoder implementation, 208-214*
- CAC (Call Admission Control),** 234-235
 - calls, limiting, 37-38
 - H.323 gatekeeper CAC, 273-283
 - locations-based, 235-283
 - full-mesh topology, 237-238*
 - hub-and-spoke topology, 236-237*
 - RSVP-enabled locations, 241-255*
- SIP Preconditions, 264-273, 270-273**
- call egress, 104**
- call flow, SIP Preconditions, 267-269**
- call ingress, 104**
- call preservation, 126**

C

- call routing, globalized call routing, 46-51**
 - advantages, 50-51
 - phases, 48-50
- CCD (Call Control Discovery), 343-346, 381-390**
 - characteristics, 351-353
 - operation, 355-361
 - PSTN backup, 387-388
 - services, 353-355
 - TEHO, 388
- CEF (Cisco Express Forwarding), 3**
- centralized call processing dial plans, 84**
 - site code requirements, 88-89
- CFNB (Call Forward on No Bandwidth), 44**
- CFUR (Call Forwarding Unregistered), 42-43, 142-146**
 - with globalized call routing, 145-146
 - interaction with globalized call routing, 143
 - SRST, configuring dial plans, 161-162
 - without globalized call routing, 143-144
- challenges to CUCM multisite deployment, 1-18**
 - availability challenges, 6-7
 - bandwidth challenges, 3-5
 - solutions, 26-38*
 - dial plan challenges, 7-16
 - optimized call routing, 14-15*
 - overlapping and nonconsecutive numbers, 9-10*
 - PSTN backup, 14-15*
 - PSTN requirements, 15-16*
- scalability, 17**
- solutions, 45-46**
- variable-length numbering plans, 12-13**
- mobility solutions, 44-45**
- quality challenges, 2-3**
- QoS, 24-26**
- security challenges, 17-18**
 - solutions, 51-52*
- characteristics**
 - AAR, 256-259
 - of SAF, 346-347
- Cisco IOS gateways**
 - MGCP fallback, configuring, 158-160
 - protocols, comparing, 59
 - PSTN access, implementing, 90-93
 - SRST, configuring, 154-158
- Cisco Unified SRST**
 - E.164 support, 138-139
 - example configuration, 157-158
 - multiple MOH support, 139-146
 - versions and support, 137-138
- class of restriction commands, SRST dial plan configuration, 173-178**
- client types (SAF), 348**
- codecs**
 - configuring, 202-204
 - low-bandwidth, solutions to multisite CUCM deployment challenges, 27-29
- commands, dialplan-pattern, 169**
- comparing Cisco IOS gateway protocols, 59**
- configuration elements, Extension Mobility, 321-323**

configuring

- AAR, 260-263
- CUCM
 - codecs*, 202-204
 - Extension Mobility*, 329-338
 - MGCP gateway*, 64-68
- CUCME, 187-192
 - MOH*, 191-192
 - phone registration process*, 195
 - phone-provisioning options*, 193
 - SRST*, 195-196
 - SRST mode*, 192-193
- Device Mobility, 309-313
 - elements*, 295-297
 - by location-dependent device pools*, 294
- dial plans
 - for CUCM SRST support*, 160-161
- gatekeeper-controlled intercluster trunks, 77-79
- H.225 trunks, 77-79
- H.323 gateway, 69-71
- IP phones, local PSTN gateway usage, 93-94
- MGCP fallback, 151-152
 - on Cisco IOS gateways*, 158-160
- multicast MOH from remote site router flash, 215-229
- RSVP-enabled locations (CAC), 245-255
- SAF, 361-390
 - external client*, 367-376
 - forwarders*, 365-366
 - internal client*, 376-381
- SIP Preconditions, 270-273
- SRST, 151-153
 - CFUR dial plans*, 161-162
 - on Cisco IOS gateways*, 154-158
 - open numbering plans*, 167-169
- transcoders, 31-32
- connectivity to remote sites, ensuring, 140-141
- CSSs, 301-302
- CUBE (Cisco Unified Border Element), 51-52
- CUCM (Cisco Unified Communications Manager)
 - annunciators, disabling, 29-30
 - CAC, 234-235
 - RSVP-enabled locations*, 241-255
 - CCD, services, 353-355
 - challenges to multisite deployment, 1-18
 - availability challenges*, 6-7
 - bandwidth challenges*, 3-5
 - dial plan challenges*, 7-16
 - quality challenges*, 2-3
 - codecs, configuring, 202-204
 - connections, 58-64
 - Extension Mobility, 319-321
 - configuring*, 329-338
 - H.323 gateway, implementing, 68-71
 - locations-based CAC, 235-283
 - full-mesh topology*, 237-238
 - hub-and-spoke topology*, 236-237
 - MGCP gateway, configuring, 64-68
 - phone registration process, 195
 - phone-provisioning options, 193
 - remote-site redundancy, 123-124
 - technologies*, 124-126

- SRST, 127-133
 - configuring*, 152-154
 - dial plans, configuring*, 160-161
 - Max Forward UnRegistered Hops to DN parameter*, 162
 - SRST mode, advantages, 194
 - CUCME (Cisco Unified Communications Manager Express)**, **181-185**
 - configuring, 187-192
 - features, 185-187
 - MOH sources, 191-192
 - SRST, configuring, 195-196
 - SRST mode, 183-185
 - configuring*, 192-193
-
- D**
- default device profile (Extension Mobility)**, 326-329
 - defining translation rules, 171
 - deploying CUCM, challenges to, 1-18
 - Device Mobility**, 291
 - configuration elements, 295-297
 - configuring, 309-313
 - CSs, 301-302
 - interaction with globalized call routing, 304-309
 - operation, 297-304
 - phone configuration parameters, 292-294
 - roaming, 289-291
 - dial peer commands, SRST dial plans**, **164-167**
 - dial plans**
 - CCD, 345-346
 - characteristics*, 351-353
 - operation*, 355-361
 - challenges to CUCM multisite deployment, 7-16
 - optimized call routing*, 14-15
 - overlapping and nonconsecutive numbers*, 9-10
 - PSTN requirements, 15-16
 - scalability, 17
 - solutions, 45-46
 - variable-length numbering plans*, 12-13
 - international multisite CUCM deployment
 - with centralized call processing*, 84
 - with distributed call processing*, 84-89
 - globalized call routing*, 103-110, 115-118
 - globalized call routing, implementing*, 102-103
 - implementing*, 83
 - localized call ingress at phones, implementing*, 110-112
 - PSTN backup for on-net intersite calls, implementing*, 95-97
 - selective PSTN breakout*, 93-94
 - TEHO**, *implementing*, 97-98
 - TEHO with local route groups**, 100-101
 - TEHO without local route groups**, 98-100
 - MGCP fallback, requirements, 139-143
 - SAF**
 - characteristics*, 346-347
 - client types*, 348
 - configuration elements*, 362-365
 - forwarders*, 351
 - messages*, 349

neighbor relationships, 350
routing characteristics, 349-350
scalability, 344-345
SRST, 163-164
class of restriction commands,
173-178
dial peer commands, 164-167
open numbering plans, 167-169
requirements, 139-143
dialplan-pattern command, 169
DID (Direct Inward Dialing), 10-11
digit manipulation
PSTN backup of on-net intersite calls,
requirements, 95-97
requirements, site-code dialing, 87-88
SRST dial plan configuration, 170-172
disabling annunciators, 29-30
distributed call processing dial plans,
requirements, 84-89

E

E.164 addressing, 10-11, 104
emergency dialing, globalized call
routing example, 112-115
ensuring connectivity to remote sites,
140-141
examples
CAC, full-mesh topology location
configuration, 238-240
Cisco IOS gateway configuration for
MGCP, 66-68
Cisco Unified SRST configuration,
157-158
of Device Mobility, globalized call
routing, 308-309
of globalized call routing, emergency

dialing, 112-115
MGCP fallback configuration,
159-160
SRST dial plans, 173-178
of TEHO
with local route groups, 100-101
without local route groups,
98-100
Extension Mobility, 317-320
configuration elements, 321-323
configuring, 329-338
feature safe, 326-329
operation, 323-326
external SAF client, configuring,
367-376

F

fallback for IP phones, 41-42
feature safe (Extension Mobility),
326-329
features, CUCME, 185-187
FIFO (first in, first out) queuing, 3
forwarders (SAF), 351
configuring, 365-366
full-mesh topology, locations-based
CAC, 237-238
locations, example configuration,
238-240

G

gatekeeper-controlled intercluster
trunks, 63
configuring, 77-79
globalized call routing, 46-51
advantages, 50-51
emergency dialing example, 112-115
implementing, 102-103

interaction with CFUR, 143
 interaction with Device Mobility, 304-309
 interdependencies, 115-118
 number formats, 103-110
 phases, 48-50

H

H.225 trunks
 configuring, 77-79
 implementing, 75-76
H.323 gatekeeper CAC, 273-283
H.323 gateway
 configuring, 69-71
 implementing, 68-71
H.323 trunks, 61-64
hub-and-spoke topology, locations-based CAC, 236-237

I

implementing
 globalized call routing, 102-103
H.225 trunks, 75-76
H.323 gateway, 68-71
 local conference bridges, 205-208
 localized call ingress at phones, 110-112
 MGCP gateway, 64-68
 multicast MOH from remote site router flash, 215-229
 PSTN access in Cisco IOS gateways, 90-93
 PSTN backup for on-net intersite calls, 95-97
 selective PSTN breakout, 93-94

SIP trunks, 74-75
TEHO, 97-98
 transcoders, 208-214
incoming calls
 PSTN, 104
 transforming with ISDN TON, 90-93
intercluster trunks, implementing, 75-76
interdependencies, globalized call routing, 115-118
internal SAF client, configuring, 376-381
international multisite CUCM deployment, dial plans, 83
 globalized call routing, 102-110, 115-118
 localized call ingress at phones, implementing, 110-112
 PSTN backup for on-net intersite calls, implementing, 95-97
 selective PSTN breakout, implementing, 93-94
TEHO
implementing, 97-98
with local route groups, 100-101
without local route groups, 98-100
 with centralized call processing, 84

IP phones

configuring to use local PSTN gateway, 93-94
 fallback, 41-42

ISDN TON (type of number), transforming incoming calls, 90-93

J-K-L

large network dial plan scalability, 344-345
 limiting CAC calls, 37-38
 local conference bridges, implementing, 205-208
 localized call ingress at phones, implementing, 110-112
 localized E.164, 104
 locations-based CAC, 235-283
 low-bandwidth codecs, solutions to multisite CUCM deployment challenges, 27-29

M

managing bandwidth, 201-202
 local conference bridge implementation, 205-208
 transcoder implementation, 208-214
 manual Cisco IOS MGCP gateway configuration, 65
Max Forward UnRegistered Hops to DN parameter (CUCM), 162
MCU (Multipoint Control Unit), 202
 messages, SAF, 349
 MGCP fallback, 39-40, 124-126, 133-137
 activation commands, 158-159
 configuring, 151-152
on Cisco IOS gateways, 158-160, 163
 dial plan requirements, 139-143
MGCP gateway, implementing, 64-68
 mixed conference bridges, solutions to multisite CUCM deployment challenges, 32

mobility
 device roaming, 289-291
 solutions to multisite CUCM deployment challenges, 44-45
MOH (Music On Hold)
 Cisco Unified SRST, multiple MOH support, 139-146
 CUCME, configuring, 191-192
 multicast MOH, 202
from remote site router flash, configuring, 215-229
 solutions to multisite CUCM deployment challenges, 33-37
multicast MOH, 202
 from remote site router flash, configuring, 215-229
multiple MOH support (Cisco Unified SRST), 139-146
multisite CUCM deployment. See also **international multisite CUCM deployment**, dial plans
 challenges to
availability challenges, 6-7
bandwidth, 3-5
dial plan challenges, 7-16, 12-13
dial plans, 17
quality challenges, 2-3
security, 17-18
 connections, 57-64
H.323 trunks, 61-64
SIP trunks, 60-61
 globalized call routing, 46-51

N

NANP (North American Numbering Plan), 92
 neighbor relationships (SAF), 350
 nongatekeeper-controlled intercluster trunks, 63
 normalization
 localized call ingress from phones, 106-107
 localized call ingress on gateways, 106-107
 number formats, globalized call routing, 103-110
 number globalization, 104
 number localization, 104
 number normalization, 104

O

open numbering plans, SRST dial plan configuration, 167-169
 optimized call routing, challenges to multisite CUCM deployment, 14-15
 outgoing PSTN calls, 104
 overlapping numbers, challenges to CUCM multisite deployment, 9-10

P

phases of globalized call routing, 48-50
 phone configuration parameters (Device Mobility), 292-294
 phone registration process (CUCME), 195
 phone-provisioning options (CUCME), 193
 PSTN access, implementing in Cisco IOS gateways, 90-93

PSTN backup, 39

for CCD, 355
 challenges to multisite CUCM deployment, 14-15
 for on-net intersite calls, implementing, 95-97
 PSTNs, requirements, 15-16

Q

QoS (quality of service), 24-26
 quality, challenges to CUCM multisite deployment, 2-3
 queuing, 3
 queuing delay, 3

R

redundancy, remote-site redundancy, 123-124
 Cisco Unified SRST, 139-146
 MGCP fallback, 126, 133-137
 SRST, 127-133
 technologies, 124-126
 references (SRST), 153
 phone registration process, 195
 regions, CUCM codec configuration, 203-204
 remote-site redundancy, 123-124
 Cisco Unified SRST
 E.164 support, 138-139
 multiple MOH support, 139-146
 versions and support, 137-138
 MGCP fallback, 126, 133-137
 configuring, 151-152, 158-160
 configuring on Cisco IOS gateways, 163
 dial plan requirements, 139-143

SRST, 127-133
Cisco IOS gateway configuration, 154-158
configuring, 151-154
configuring on Cisco IOS gateways, 163
CUCME, configuring, 195-196
dial plan dial peer commands, 164-167
dial plan requirements, 139-143
dial plans, configuring in CUCM, 160-161
open numbering plans, 167-169
references, 153
switchover signaling, 129-130
timing, 132-133
voice translation-profile commands, 170-172
 technologies, 124-126
requirements
 distributed call processing dial plans, 84-89
 remote-site redundancy configuration, 151-152
roaming, 289-291
 Device Mobility
CSSs, 301-302
interaction with globalized call routing, 304-309
Extension Mobility, 317-320
configuration elements, 321-323
operation, 323-326
routing characteristics (SAF), 349-350
RSVP-enabled locations (CAC), 241-255
 configuring, 245-255

S

SAF (Service Advertisement Framework), 343-344
 characteristics, 346-347
 client types, 348
 configuration elements, 362-365
 configuring, 361-390
 external client, configuring, 367-376
 forwarders, 351
configuring, 365-366
 internal client, configuring, 376-381
 messages, 349
 neighbor relationships, 350
 routing characteristics, 349-350
scalability
 of dial plans, 17
 of dial plans in large networks, 344-345
security, challenges to CUCM multisite deployment, 17-18
 solutions, 51-52
selective PSTN breakout, implementing, 93-94
services, CCD, 353-355
SIP (Session Initiation Protocol), trunks, 60-61
 implementing, 74-75
SIP Preconditions, 264-273
 call flow, 267-269
 configuring, 270-273
 operation, 266-267
site-code dialing
 centralized call processing dial plans, 88-89
 digit manipulation requirements, 87-88

- implementing for multisite dial plans with distributed call processing, 86
 - SNAP (Simple Network Auto Provisioning), 42**
 - solutions to multisite CUCM deployment challenges**
 - availability solutions, 38-44
 - bandwidth solutions, 26-38
 - CAC calls, limiting*, 37-38
 - disabled annunciators*, 29-30
 - low-bandwidth codecs*, 27-29
 - mixed conference bridges*, 32
 - MOH*, 33-37
 - transcoders*, 30-32
 - dial plan solutions, 45-46
 - mobility solutions, 44-45
 - security solutions, 51-52
 - SRST (Survivable Remote Site Telephony), 123, 127-133**
 - CFUR, configuring dial plans, 161-162
 - configuring, 151-153
 - on Cisco IOS gateways*, 154-158, 163
 - CUCME, configuring, 195-196
 - dial plans
 - class of restriction commands*, 173-178
 - components*, 163-164
 - dial peer commands*, 164-167
 - open numbering plans*, 167-169
 - requirements*, 139-143
 - voice translation-profile commands*, 170-172
 - dial plans, configuring in CUCM, 160-161
 - Max Forward UnRegistered Hops to DN parameter (CUCM), 162
 - references, 153
 - switchover signaling, 129-130
 - timing, 132-133
 - SRST mode (CUCME), 183-185**
 - advantages, 194
 - configuring, 192-193
-
- ## T
-
- TEHO (tail-end hop-off), 14-15, 388**
 - advantages, 116
 - examples
 - with local route groups*, 100-101
 - without local route groups*, 98-100
 - implementing, 97-98
 - timing, SRST, 132-133**
 - ToDID rules, 352**
 - TON (type of number), transforming incoming calls, 90-93**
 - transcoders, 202**
 - configuring, 31-32
 - implementing, 208-214
 - solutions to multisite CUCM deployment challenges, 30-32
 - transforming incoming calls using ISDN TON, 90-93**
 - translation rules, defining, 171**
 - trunks**
 - gatekeeper-controlled intercluster trunks, configuring, 77-79
 - H.225, implementing, 75-79
 - H.323, 61-64
 - intercluster trunks, implementing, 75-76
 - SIP, 60-61
 - implementing*, 74-75

U-V-W-X-Y-Z

variable-length numbering plans, 10-11

challenges to CUCM multisite deployment, 12-13

versions and support, Cisco Unified SRST, 137-138

voice translation-profile commands, SRST dial plan configuration, 170-172

VoIP, call preservation, 126

This page intentionally left blank



Cisco Learning Network

Free Test Prep and Beyond.

- Access review questions
- Watch Quick Learning Modules (QLMS)
- Search for jobs and network with others
- Take self-assessments
- Participate in study groups
- Play online learning games

Register for a free membership
and get started now.

www.cisco.com/go/learningnetwork

Cisco Learning Network

A social learning site brought to you by Learning@Cisco



ciscopress.com: Your Cisco Certification and Networking Learning Resource

Cisco Press is the only authorized publisher for Cisco certification and network technology self-study resources.

CERTIFICATION INFO: CCENT | CCNA | CCNA Concentrations | CCNP | CCDA | CCDP | CCSP | CCVP | CCIE

STORE | NEWSLETTERS | SERIES

CISCO NETWORKING ACADEMY

On INFORMIT:
REFERENCE LIBRARY—Browse full Cisco Press books
CERTIFICATION REFERENCE GUIDE—Weekly updates on IT certifications

CCENT 640-822 Network Simulator

The CCENT 640-822 Network Simulator is a state-of-the-art, interactive simulation software. It allows you to practice your networking skills with 96 structured labs designed to help you learn by doing—the most effective method of learning. This software download will be accessible via your ciscopress.com Account page after purchase.
Special Offer
Receive the CCNA ICND2 640-816 Network Simulator Upgrade free when you purchase the CCENT 640-822 Network Simulator. The upgrade will be available in April.
Visit the product page for details.

CCNA Security 640-553 Cert Flash Cards

Cert Flash Cards Online provides cert card review, learning, and exam practice that is a valuable late-stage tool to help you succeed on your certification exam. CCNA Security Cert Flash Cards Online consists of a custom flash card application loaded with 250 questions that test your skills and enhance retention of exam topics.
Visit certflashcardsonline.com to see a demo and try it free.

OnCertification Video Podcasts

Study tips, reviews, screencasts, and conversations with Cisco certification insiders on test-prep technologies.
Recent Episodes:
Introducing Safari Bookbag for the iPhone By Tim Warner
Test-Taking Skills Clinic Exam 640-802: Cisco CCNA By Tim Warner
See all OnCertification podcast episodes on InformIT.com

Network World's Cisco Subnet

Cisco Subnet is the independent voice of Cisco customers for Cisco news, blogs, discussion groups, security alerts, Cisco Press book giveaways, and more. This month, Network World is giving away *Voice over IP Security* by Patrick Park and *CCNA Wireless Official Exam Certification Guide* by Brandon Carroll. Enter to win a copy.
Brandon Carroll and Patrick Park are blogging for Cisco Subnet during February.

Safari Books Online

Online access to books, videos, and tutorials from Cisco Press, Addison-Wesley, Prentice Hall, Sams, IBM Press, Exam Cram, and Que—plus O'Reilly Media, Microsoft Press, and Wiley—starting as low as \$22.99.
START YOUR FREE TRIAL →

Connect with Cisco Press authors and editors via Facebook and Twitter, visit informat.com/socialconnect.

Subscribe to the monthly Cisco Press newsletter to be the first to learn about new releases and special promotions.

Visit ciscopress.com/newsletters.

While you are visiting, check out the offerings available at your finger tips.

—Free Podcasts from experts:

- OnNetworking
- OnCertification
- OnSecurity



Podcasts

View them at ciscopress.com/podcasts.

—Read the latest author **articles** and **sample chapters** at ciscopress.com/articles.

—Bookmark the Certification Reference Guide available through our partner site at informat.com/certguide.

Quick Links

- Book Support
- Chapters & Articles
- Contact Us
- Facebook Group | Facebook Fan Page
- Newsletters
- Partners & Resources
- Product Support Team
- Register a Book
- RSS Feeds
- Search
- Twitter
- User Groups

Become a Member
The Cisco Press membership program offers you exclusive discounts and members-only content. Sign up with your e-mail address and complete a user profile to join the site.

Most Popular

- CCNA Official Exam Certification Library (CCNA Exam 640-802), 3rd Edition**
By Jennifer C. Baker \$53.99 (Save 10%)
- CCNA Preparation Library, 7th Edition**
By Stephen McQuerry \$85.50 (Save 10%)
- Network Security Technologies and Solutions (CCIE Professional Development Series)**
By Yusuf Bhaiji \$72.00 (Save 10%)

See All Most Popular Books

Search →
BROWSE before you buy & FIND the content you need!

Look for the Search icon above the book cover on any product page to take a look inside!

Just Released

- CCENT 640-822 Network Simulator: Software Download**
By Pearson Certification \$74.99
- Designing Cisco Network Service Architectures (ARCH), 2nd Edition**
By Keith Hutton, Mark Schofield, Diane Teare \$63.00 (Save 10%)
- Power of IP Video, The: Enhancing Quality of Visual Networking**
By Jennifer C. Baker, Felicia Brych-Dalke, Mike Mitchell, Nader Nariani \$40.50 (Save 10%)

See All Books

Coming Soon

- CCNA 640-802 Network Simulator**
By Pearson Certification \$134.99 (Save 10%)

See All Coming Soon Books

ARE YOU ON facebook ?

DO YOU twitter ?
Join and follow Pearson imprints today!