IP COMMUNICATIONS

Configuring Cisco Unified Communications Manager and Unity

A Step-by-Step Guide

ciscopress.com

David Bateman

Configuring Cisco Unified Communications Manager and Unity Connection:

A Step-by-Step Guide

David Bateman

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Configuring Cisco Unified Communications Manager and Unity Connection: A Step-by-Step Guide

David Bateman

Copyright © 2011 Cisco Systems, Inc.

Cisco Press logo is a trademark of 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 May 2011

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

ISBN-10: 1-58714-226-0

ISBN-13: 978-1-58714-226-0

Warning and Disclaimer

This book is designed to provide information about configuration and administrative tasks related to Communications Manager and Unity. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The 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

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales.

For more information please contact: U.S. Corporate and Government Sales
1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside 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

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Project Editor: Mandie Frank

Editorial Assistant: Vanessa Evans

Designer: Sandra Schroeder

Indexer: Tim Wright

Cisco Representative: Erik Ullanderson

Cisco Press Program Manager: Anand Sundaram

Development Editor: Marianne Bartow

Technical Editors: David Mallory, Toby Sauer

Copy Editor: John Edwards

Proofreader: Apostrophe Editing Services

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, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

About the Author

David J. Bateman is a certified Cisco Systems instructor and the director of curriculum development for Skyline-ATS. He has more than 20 years of internetworking experience. For more than 10 years, David was a senior LAN/WAN engineer, working on small, medium, and large networks. Later in his career, he took on the responsibility of running the business operations of a technical services company, while maintaining his existing client base. David has always enjoyed sharing his knowledge, and in 1999, he added to his list of accomplishments by becoming a technical seminar leader. After many successful seminars, he decided to become a full-time Cisco instructor for Skyline Advanced Technology Services. He has been teaching and implementing Cisco voice technologies since 2000. David's years of real-world technical and business knowledge allow him to bring a unique perspective to the classroom, where he not only delivers critical technical knowledge but can also explain how technologies can be used to address various business issues.

About the Technical Reviewers

David L Mallory, CCIE No. 1933, is a technical leader for Learning@Cisco, where he is responsible for content development strategy. For the last seven years, David has been primarily focused on UC certifications and was the technical lead for the Cisco 360 Learning Program for CCIE Voice. Prior to joining Learning@Cisco, David was a systems engineer supporting global accounts. David is a frequent presenter at Cisco Live and has obtained four CCIEs—Routing & Switching, WAN Switching, Security, and Voice.

Toby Sauer is the lead voice instructor and voice curriculum manager for Skyline Advanced Technology Services. He brings 30 years of experience in the traditional voice, data, and VoIP arenas. Toby has been involved in Cisco VoIP since the beginning, working with traditional VoIP, and he was involved in the earliest installations of Cisco Communications Manager. He has installed many different implementations of Communications Manager and was responsible for converting most of the Midwest's Cisco offices from traditional PBX to Communications Manager.

Toby became a Cisco voice instructor in 2000. As the Communications Manager product continued to grow and develop, he was a key instructor to many of the original deployment partners.

Toby currently holds CCNP-Voice, CCNA-Voice, CCNA-RS, CCSI, and various partner-level certifications. He teaches all the Cisco Standard Voice courses and many custom variations of these courses.

Dedications

I'd like to dedicate this book to my parents, who taught me unconditional love; to my wife, Nikki, who is my life, my love, my all; and to Matthew, a young man that I am proud to call my son.

Acknowledgments

There are a number of people that I would like to thank in helping me complete this book. Often the greatest help that can be received is when someone is willing to sacrifice so that you can succeed. With this in mind, I would like to thank my wife, Nikki. She has sacrificed many beautiful summer days that we could have spent out on the motorcycle so that I could work on this book. She sacrificed hours each week reading what I had written in order that I might deliver a more readable copy to the editors. I know it was not always fun for her, but it helped me complete this book. Without her sacrifice, this book would not have been possible.

I would also like to thank the technical editors. Their keen insight and willingness to ask me what the heck I was thinking on some subjects have helped make this a much better book than it was when I first wrote it.

Of course I'd like to thank those at Skyline-ATS, where I work. I would especially like to thank them for the skill they showed in increasing my workload as deadlines for the book drew near. I guess they figured I would do better under pressure. But seriously, I would like to thank Mike Maudlin and Mike Zanatto for their understanding and cooperation during this project. I also need to thank all the others that I worked with at Skyline-ATS. The awesome amount of knowledge that we hold as a team is incredible, and to have such a resource at my disposal has been invaluable.

A big thank-you to the folks at Cisco Press: Brett Bartow, who assisted from the beginning of this project and was always there to remind me of upcoming deadlines long enough in advance so that I had time to either meet the deadline or come up with a really good excuse. Also Marianne Bartow, who acted as my development editor and was always helpful and encouraging.

Thanks one and all for all you've done.

Contents at a Glance

Part I Communications Manager Configuration

Chapter 1 CUCM and Unity Connection Overview 1

Chapter 2 Preparing CUCM for Deployment 41

Chapter 3 Deploying Devices 77

Chapter 4 Implementing a Route Plan 151

Chapter 5 Configuring Class of Service and Call Admission Control 193

Chapter 6 Configuring CUCM Features and Services 231

Part II Messaging Configuration

Chapter 7 Unity Predeployment Tasks 295

Chapter 8 User/Subscriber Reference 377

Chapter 9 Call Management 495

Chapter 10 Implementing Unity Networking 567

Chapter 11 Exploring Unity/Connection Tools 587

Part III Leveraging the Power of Communications Manager and Unity

Chapter 12 Maximizing CUCM and Unity/Connection 627

Appendix Additional Reference Resources 651

Index 657

Table of Contents

Part I Communications Manager Configuration

Chapter 1 CUCM and Unity Connection Overview 1

Ensuring a Reliable Foundation 2

Infrastructure Overview 3

Inline Power 4

Voice VLANs 4

CDP Support 4

Voice Gateways 4

Creating a Reliable VoIP Infrastructure 5

Communications Manager Overview 7

Defining Communications Manager Components 8

Communications Manager Business Edition 10

Communications Manager Devices 10

Phones 11

Gateways Overview 12

Gatekeepers 14

Media Resources 15

Conference Bridge (CFB) 15

Transcoders 16

MoH 16

Annunciator 16

Understanding Communications Manager Deployment Models 17

Single-Site 17

Multisite WAN with Centralized Call Processing 17

Multisite WAN with Distributed Call Processing 17

Route Plan Overview 18

Typical Call Flow 19

Wildcards 20

Calling Privileges 21

Unified Messaging Overview 22

Software Architecture 23

Unity Software Architecture 23

Unity Connection Architecture 25

Following the Call Flow 25

Exploring Call Handlers 26

Defining Various Types of Users 29
Unity Connection Users 29
Unity Subscribers 30
User Parameters 31
Networking Overview 33
Unity Networking 33
Unity Connection Networking 35
Securing the Environment 35
Securing the Operating System 35
Communications Manager Security Issues 36
Unity Security Issues 38
Summary 39

Chapter 2 Preparing CUCM for Deployment 41
Configuring Communications Manager for Maximum Performance 41
Activating Communications Manager Services 42
Configuring Communications Manager's Enterprise Settings 43
Removing DNS Dependencies 48
Defining Enterprise Parameters 50
General Parameters 50
Communications Manager Administrator Parameters 52
CCMUser Parameters 53
CDR Parameters 55
Localization Parameters 55
Multi-Level Precedence and Pre-Emption (MLPP) Parameters 55
Security Parameters 56
Prepare Cluster for Roll Back 57
Phone URL Parameters and Secured Phone URL Parameters 57
User Search Parameters 58
CCM Web Services Parameters 59
Trace Parameters 59
User Management Parameters 60
Service Manager TCP Ports Parameters 60
CRS Application Parameters 60
Cluster Domain Configuration 60
Denial-of-Service Protection 60
TLS Handshake Timer 60
Cisco Support Use 60

IPv6 Configuration Modes 60
Cisco Syslog Agent 61
CUCReports Parameters 61
Logical Partitioning Configuration 61
Preparing Communications Manager for Device Registration 62
Device Pools 62
Common Device Configuration 66
Creating Communications Manager Groups 66
Defining Date/Time Groups 69
Configuring Regions 70
Building Device Pools 72
Summary 75

Chapter 3 Deploying Devices 77
Adding Clients 78
Defining Device Settings 78
Phone Button Templates 78
Softkey Template 80
Device Defaults 83
Adding Phones 84
Autoregistration 86
Manually Adding Phones 89
Add a Line to a Phone 99
Using BAT to Add Devices 106
Activating the BAT Service 107
BAT CSV and Template Overview 108
Creating a CSV File for BAT 110
Adding Phones Using BAT 113
Adding Phones Using TAPS 118
Adding Gateways 119
Adding H.323 Gateways 119
Device Information 121
Call Routing Information—Inbound Calls 123
Call Routing Information—Outbound Calls 124
Geolocation 125
Intercompany Media Engine 126
Incoming Calling/Called Party Settings 126
Adding MGCP Gateways 126

Adding IOS MCGP Gateways 127
Adding Non-IOS MGCP Gateways 132
Adding Intercluster Trunks 143
Device Information 144
Call Routing Information—Inbound Calls 147
Call Routing Information—Outbound Calls 147
Remote Cisco Communications Manager Information 149
UUIE Configuration 149
Geolocation Configuration 149
Summary 150

Chapter 4 Implementing a Route Plan 151
Understanding Call Flow 152
Understanding Route Groups and Route Lists 154
Creating Route Groups 157
Creating a Route List 158
Understanding Route Patterns 163
Creating Basic Route Patterns 166
Using Pattern Wildcards to Create a Basic Dial Plan 171
Advanced Route Plan Components and Behavior 173
Creating Route Filters 174
Creating Translation Patterns 179
Creating CTI Route Points 183
Adding a Line to a CTI Route Point 185
Directory Number Information 185
Directory Number Settings 186
AAR Settings 187
Call Forward and Pickup Settings 187
Park Monitoring 189
MLPP Alternate Party Settings 189
Line Settings for All Devices 190
Line Settings for This Device 190
Multiple Call / Call-Waiting Settings 190
Forwarded Call Information Display 191
Summary 191

Chapter 5 Configuring Class of Service and Call Admission Control 193
Rights and Restrictions 193
Understanding Call Search Spaces and Partitions 193

Creating Calling Search Spaces and Partitions 202
Applying Calling Search Spaces and Partitions 205
Assigning a CSS to a Phone 206
Assigning a CSS to a Line 206
Assigning a CSS to a Gateway or Trunk 207
Assigning a Partition to a Line (Directory Number) 209
Assigning a Partition to a Pattern 210
Implementing Call Admission Control 211
Configuring CAC for a Distributed Deployment 211
Configuring a Gatekeeper 213
Configuring a Gatekeeper-Controlled Trunk 215
Call Routing Information—Outbound Calls 219
Gatekeeper Information 220
Configuring CAC for a Centralized Deployment 221
Creating Locations 221
Assigning a Location to Devices 223
Special Services Configuration 224
Special Services Overview 224
Configuring Special Services Route Patterns 225
Summary 229

Chapter 6 Configuring CUCM Features and Services 231
Configuring Features 231
Creating Call Pickup Groups 231
Add a Call Pickup Number 232
Assign a Call Pickup Group to a Line 234
Creating Meet-Me Patterns 235
Creating Call Park Numbers 237
Creating Directed Call Park Numbers 239
Creating Intercoms 240
Creating Intercom Partitions 241
Intercom Calling Search Spaces 241
Creating Intercom Numbers 241
Assigning an Intercom DN to a Phone 242
Creating Forced Authorization Codes 244
Create a Forced Authorization Code 244
Assign a Forced Authorization Code to a Route Pattern 245
Configuring Client Matter Codes 246

Create a Client Matter Code 246
Assign a Client Matter Code to a Route Pattern 247
Configuring Voice Ports and Profiles 248
Creating Users 259
Configuring Advanced Services 262
Implementing Advanced Features 263
Configuring IP Phone Services 263
Extension Mobility 265
Creating and Managing Media Resources 273
Configuring an MOH Server 273
Assign an MOH Audio Source to a Phone 276
Creating Conference Bridges 276
Configuring MTPs 279
Creating Transcoders 279
Configuring Annunciators 281
Media Resource Management 282
Assign a Media Resource Group List to a Phone 285
Assign a Media Resource Group List to a Device Pool 286
Configuring Remote Site Failover 286
SRST Overview 287
Configuring SRST 287
Creating an SRST Reference to a Device Pool 288
Assign an SRST Reference to a Device Pool 290
Configuring AAR 290
Creating an AAR Group 291
Assign an AAR Group to a Line 292
Summary 294

Part II Messaging Configuration

Chapter 7 Unity Predeployment Tasks 295
Accessing and Navigating Unity Administrator 296
Accessing and Navigating Unity Connection Administrator 301
Unity Integration Verification 304
Communications Manager Integration 305
Voicemail Port Configuration 305
Unity Telephony Integration Manager (Communications Manager) 307

SIP Integration 311
SIP Configuration 311
Unity Telephony Integration Manager (SIP) 312
PIMG/TIMG Integration 315
PIMG/TIMG Configuration 315
Unity Telephony Integration Manager (PIMG/TIMG) 315
Defining Unity System Configuration 317
Creating Schedules and Holidays 318
View and Change a Schedule 319
Add a Schedule 320
Define a Default Schedule 320
Add a Holiday 321
Modify or Delete a Holiday 322
Defining Configuration Settings 322
Settings 322
Software Versions 326
Recordings 326
Contacts 328
Phone Languages 328
GUI Languages 330
Message Security 330
Message Subjects 330
Configuring Authentication Settings 331
Configuring Ports 332
Configuring Unity System Access and Policies 334
Defining Account Polices 334
Configuring Class of Service 337
Adding a CoS 337
Modifying a CoS 338
Creating and Managing Unity Public Distribution Lists 347
Creating Public Distribution Lists 347
Managing PDL Members 350
Unity Connection Integration Verification 351
Communications Manager Integration 351
Defining Unity Connection System Configuration 354
Defining General Configuration 355
Defining Mailbox Quotas 358

Configuring Message Aging Policy 359
Creating Schedules and Holidays 361
View and Change a Schedule 361
Configuring Unity Connection System Access and Policies 363
Configuring Authentication Rules 363
Configuring Restriction Tables 366
Configuring CoS 368
Understanding Roles 371
Defining the Dial Plan 372
Summary 375

Chapter 8 User/Subscriber Reference 377
Defining Various Types of Subscribers 377
Exchange 378
Networked Subscribers 378
Unity Connection Users 378
Creating Users 378
Exploring Templates 379
Creating Unity Subscriber Templates 381
Configuring Subscriber Template Profile Settings 384
Configuring Subscriber Template Account Settings 386
Configuring Subscriber Template Passwords Settings 386
Configuring Subscriber Template Conversation 388
Configuring Subscriber Template Call Transfer 394
Configuring Subscriber Template Greetings 398
Configuring Subscriber Template Caller Input 402
Configuring Subscriber Template Messages Settings 405
Configuring Subscriber Template Distribution Lists Settings 407
Configuring Subscriber Template Message Notification Settings 408
Configuring Subscriber Feature Settings 412
Creating New Unity Subscribers 414
Importing Unity Subscribers 417
Creating Unity Connection User Templates 420
Configuring User Template Basics Settings 424
Configuring Password Settings 426
Configuring Template Passwords 427
Configuring Roles 427
Configuring User Template Transfer Rules 427

Configuring User Template Messages Settings 430
Configuring User Template Message Actions 432
Configuring User Template Caller Input 434
Configuring User Template Mailbox Settings 435
Configuring User Template Phone Menu 437
Configuring User Template Playback Message Settings 439
Configuring User Template Send Message Settings 442
Configuring User Template Greetings 444
Configuring User Template Post-Greeting Recording 446
Configuring User Template Message Notification Settings 447
Creating New Unity Connection Users 451
Importing Unity Connection Users 454
Unity Connection Contacts 456
Creating Unity Connection Contact Templates 456
Creating Unity Connection Contacts 457
Managing Users 460
Managing User Access 460
Unlocking an Account 460
Resetting Passwords 461
Changing a Subscriber's Extension 462
Changing a Subscriber's CoS 463
Granting Access to Licensed Features (FaxMail, Text-to-Speech, CPCA) 463
Granting Additional System Access Rights 465
Managing Call Transfer and Greetings 466
Allowing Screening and Hold Options 466
Changing Maximum Greeting Length 467
Enabling and Disabling Greetings 468
Modifying Caller Input Options 469
Managing Message Access, Notification, and Indication 472
Allowing Subscribers to Send to Distribution Lists 473
Allowing Messages Deleted from the Phone to Be Saved in the Deleted Items Folder 474
Enabling Live Reply for a Subscriber 474
Creating Private Lists 475
Configuring Message Notification 476
Adding Alternate Extensions 480
Adding Alternate Names 482

Assigning External Service Accounts (Unity Connection Only) 483
Add SMTP Proxy Addresses (Unity Connection Only) 483
Changing Maximum Outside Caller Message Length 484
Adjusting Urgent Message Marking 484
Enable MWI on Another Extension 485
Adding and Removing Users from a Distribution List 486
Conversation Management Settings 487
Changing Menus from Full to Brief 487
Changing How a User Searches for Other Users 488
Changing What Message Count Is Played to a User 489
Changing the Order in Which Messages Are Played 490
Changing What Header Information Is Heard While Listening to Messages 492
Summary 493

Chapter 9 Call Management 495
Understanding Call Flow 495
Call Flow Architecture 496
Call Handler Overview 497
Creating Basic Call-Routing Systems 499
Call Handlers 500
Creating and Configuring Unity Call Handlers 500
Configuring Unity Call Handlers 502
Profile Settings 502
Call Transfer Settings 504
Greetings Settings 507
Configuring Call Handler Caller Input Settings 510
Configuring Call Handler Messages Settings 513
Creating and Configuring Unity Connection Call Handlers 514
Configuring Unity Connection Call Handlers 516
Configuring Call Handler Basics Settings 517
Configuring Call Handler Transfer Rules 518
Configuring Call Handler Caller Input 520
Configuring Call Handler Greetings 522
Configuring Call Handler Post-Greeting Recording 525
Configuring Call Handler Messages Settings 525
Configuring Call Handler Owners 526

Directory Handlers 527
Configuring Unity Directory Handlers 528
Directory Handler Search Options Settings 529
Directory Handler Match List Options Settings 531
Directory Handler Caller Input Settings 533
Configuring Unity Connection Directory Handlers 534
Unity Connection Directory Handler Greeting 539
Configuring Auto-Attendant 540
Creating Advanced Call-Routing Systems 542
Using Interview Handlers 543
Creating and Configuring Interview Handlers in Unity 543
Creating and Configuring Interview Handlers in Unity Connection 546
Creating an Audio Text Application 549
Remotely Managing Call Handlers 551
Configuring Call Routing 552
Creating and Configuring a Call Routing Rule in Unity 553
Creating and Configuring a Call Routing Rule in Unity Connection 557
Managing Restriction Tables 560
Configuring Unity Restriction Tables 561
Configuring Unity Connection Restriction Tables 563
Summary 565

Chapter 10 Implementing Unity Networking 567
Unity Networking Overview 567
Networking Components 568
Locations 568
Message Addressing 568
Network Subscribers 568
Voice Connector 568
Interoperability Gateway 569
Schema Extensions 569
Unity-to-Unity Networking Overview 569
Unity–to–Legacy Voicemail Networking Overview 570
Unity Networking Configuration 571
Defining Digital Networking 571
Unity to Non-Unity Networking Concepts 577
Defining AMIS Networking 577

Defining VPIM Networking 578
Defining Bridge Networking 580
Unity Connection Networking Overview 581
Networking Unity Connection to Unity Connection 582
Networking Unity Connection to Unity 583
Networking Unity Connection to Other Systems 585
Summary 586

Chapter 11 Exploring Unity/Connection Tools 587
Using Unity Tools 587
Unity Web-Based Tools 587
Monitoring 588
Reports 592
Subscriber Reports 593
System Reports 595
Using Advanced Tools 599
Administration Tools 600
Audio Management Tools 608
Diagnostic Tools 609
Reporting Tools 612
Switch Integration Tools 613
Using Unity Connection Tools 614
Unity Connection Administration Tools 614
Task Management 615
Bulk Administration Tool 616
Custom Keypad Mapping 617
Migration Utilities 618
Grammar Statistics 618
SMTP Address Search 619
Show Dependencies 619
Unity Connection Reports 619
Phone Interface Failed Logon Report 622
Users Report 622
Message Traffic Report 622
Port Activity Report 622
Mailbox Store Report 622
Dial Plan Report 623
Dial Search Scope Report 623

User Phone Login and MWI Report 623
User Message Activity Report 623
Distribution Lists Report 623
User Lockout Report 623
Unused Voice Mail Accounts Report 624
Transfer Call Billing Report 624
Outcall Billing Detail Report 624
Outcall Billing Summary Report 624
Call Handler Traffic Report 624
System Configuration Report 625
SpeechView Activity Report By User 625
SpeechView Activity Summary Report 625
Summary 626

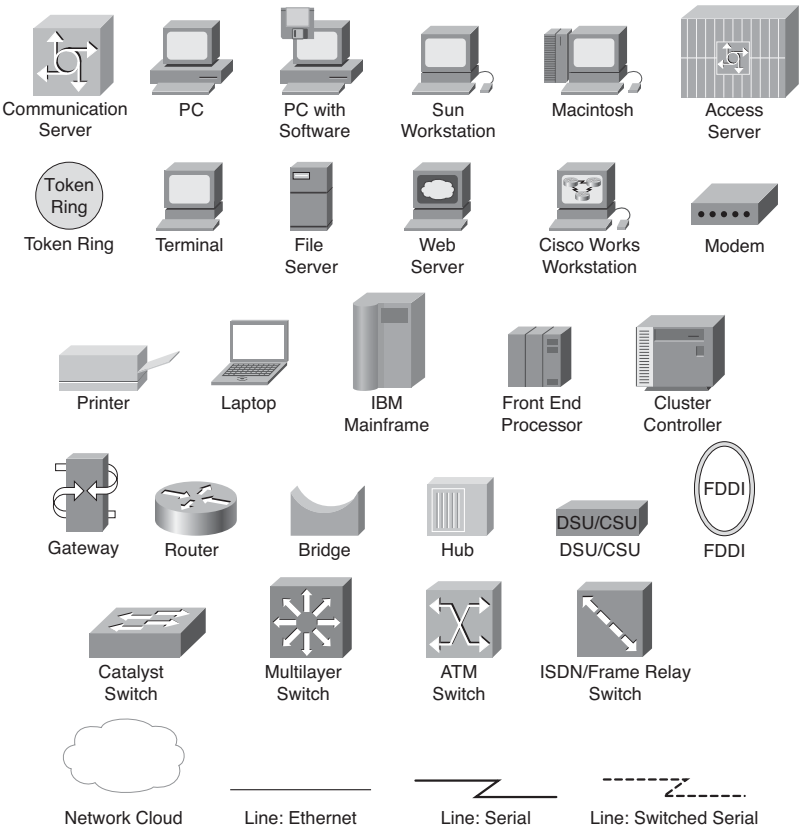
Part III Leveraging the Power of Communications Manager and Unity

Chapter 12 Maximizing CUCM and Unity/Connection 627
Advanced Communications Manager Features 627
Configuring Administrative Rights 627
Time-of-Day Routing 631
Creating a Time Period 632
Creating a Time Schedule 633
Assigning a Time Schedule to a Partition 634
Hunt List 635
Creating a Line Group 635
Creating a Hunt List 637
Creating Hunt Pilots 639
Advanced Unity/Unity Connection Features 642
Enabling Call Queuing 642
Configuring Destination Call Screening 643
Unique Solutions 644
Enhanced Vacation Schedules 644
Configuring Unity/Connection as a Meet-Me Conference Manager 647
Managing Multilocation Overlapping Extensions 648
Summary 649

Appendix Additional Reference Resources 651

Index 657

Icons Used in This Book



Command Syntax Conventions

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

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

Introduction

On March 10, 1876, Alexander Graham Bell made the first successful telephone call. As with many things, the test was purely accidental. Graham spilled acid on his leg, and Watson, his assistant, heard his call for help through the telephone. So, what has changed over the last 129 years? It would be easier to discuss what hasn't changed. The world of telephony has undergone some significant changes but none as exciting as Voice over IP (VoIP) solutions from Cisco. There are still those who believe we were all a lot better off in an analog world, but you can't stop progress, and the Cisco Unified Communications solutions are starting to grow faster than many had believed.

This new technology brings with it the need for individuals to learn how it works. Although there are many fine Cisco Press books on this technology, I noticed many of my students requesting a task-oriented book. They were looking for a book in which they could look up a specific task and be walked through it. This was the initial goal of the book. Through the writing process, the book evolved from offering only a step-by-step guide into also offering easy-to-understand explanations for many of the Cisco Unified Communications concepts and components.

Goals and Methods

New technologies bring new opportunities and challenges. One of the challenges that we are faced with in the Cisco Unified Communications world is the capability to easily understand the many facets of the configuration and integration process. Because this platform can be deployed in so many different configurations and environments, system administrators and system engineers need a resource that offers quick access to step-by-step solutions. In an environment such as this, it is nearly impossible to keep track of the exact steps for each configuration task. Those tasks that you do on a daily basis are easy to perform, but when you are called upon to perform unfamiliar tasks, you don't always have the time to learn the proper steps. *Configuring Communication Manager and Unity Connection* shows readers how to complete many of the common tasks, and some not-so-common tasks, performed within a Cisco Unified Communications solution.

Who Should Read This Book

The book is aimed at individuals who are required to configure Communications Manager and Unity and Unity Connection solutions as a primary part of their jobs. The book is unique because it covers Communications Manager, Unity, and Unity Connection.

Although this book focuses on the tasks that must be performed, it also offers easy-to-understand explanations for many of the technologies that are commonly found with Cisco Unified Communications environments, which makes it an excellent resource for individuals who are new to this technology.

How This Book Is Organized

Within the book, tasks are organized in the same order in which they would naturally be performed. Some tasks include cross-references to prerequisite tasks. Whenever possible, however, all tasks are presented within the same section.

Different people, depending on their knowledge and background, will use this book in different ways. Many will find it a useful reference tool when completing an unfamiliar task, and those new to this technology will find that reading this book from cover to cover will help them gain a solid understanding of this technology. Although the step-by-step guides were written with the assumption that you have access to a Communications Manager while reading the steps, this is not required. This book includes numerous screen shots, which enable you to see what is happening in the administration interface even if you do not have access to a Communications Manager.

Chapter 1 offers you a high-level overview of most of the concepts and components that are found within Communications Manager and Unity. Basically, the information found in two weeks of classes has been compressed to quickly bring you up to speed. This by no means is a replacement for these classes—just a quick overview.

Chapters 2 through 6 cover Communications Manager configuration, whereas Chapters 7 through 11 discuss Unity and Unity Connection configuration. The last chapter speaks to more advanced features of both technologies and offers a few ways to leverage the strengths of both to create a more feature-rich environment.

The following is a brief description of each chapter.

Chapter 1: CUCM and Unity Connection Overview

This chapter offers a broad overview of the Cisco Unified Communications solutions to ensure that you are comfortable with what follows in the book. The intent of this chapter is to offer you an overview of the various components of a Cisco Voice over IP solution. You are strongly encouraged to refer to suggested reference material for additional information on any topic with which you might be unfamiliar. You can find this material in the appendix.

Chapter 2: Preparing CUCM for Deployment

To ensure a smooth deployment, tasks must be performed in a certain order. In this chapter, you learn what tasks must be completed before adding devices. As with most things, if you fail to create a solid foundation, you will encounter problems in the future. This chapter ensures that the proper foundation is created and future problems are avoided. Topics covered include services configuration, enterprise parameters, and device registration tasks. Additionally, this chapter includes step-by-step instructions for each task.

Chapter 3: Deploying Devices

After the predeployment tasks are completed, you are ready to add devices. This chapter focuses on the tasks required to add various devices to your Communications Manager environment. Devices have been divided into two major categories: clients (IP phones, softphones, and so on) and gateways. The chapter includes step-by-step instructions for adding each device.

Chapter 4: Implementing a Route Plan

Before you can place calls to destinations that are not directly connected to your Communications Manager environment, you must configure a route plan. This chapter discusses all the components of a route plan, such as route patterns, route lists, and route groups and the tasks that are needed to implement an efficient dial plan. The step-by-step tasks show how to create and configure route patterns, route lists, and route groups and more advanced components, such as CTI route points, translation patterns, and route filters.

Chapter 5: Configuring Class of Service and Call Admission Control

After a dial plan is created, you might want to limit what destinations certain devices can reach. This chapter discusses how to do this by configuring Calling Search Spaces and partitions. It is also necessary that some types of Call Admission Control be deployed on WAN links so that the quality of voice is maintained. To this end, Call Admission Control features are covered. Finally, this chapter discusses the importance of special services, such as 911, and describes how to properly configure the dial plan to handle these types of calls.

Chapter 6: Configuring CUCM Features and Services

After basic call-processing functions are configured and working properly, you need to add new features and monitor the health of the system. This chapter explores a number of the features that can be implemented, including IP phone service, media resources, and Extension Mobility. The need for, and the functions of, SRST is also covered in this chapter. Furthermore, this chapter examines some of the monitoring services that are included in Communications Manager. Step-by-step instructions that explain how to add each feature and service are included.

Chapter 7: Unity Predeployment Tasks

The first step to proper configuration is verifying that the integration is correct and that all predeployment tasks are complete. This chapter includes step-by-step instructions for completing predeployment tasks, such as verifying integration, defining system parameters, and creating templates, distribution lists, and CoS.

Chapter 8: User Reference

After a proper integration between Unity/Connection and Communications Manager is achieved and the predeployment tasks discussed in the previous chapter are completed, the user can be added. In this chapter, the different types of users are examined. Then, the process for adding, importing, and managing users is explored. Within the "Managing Users" section, various administrative tasks are discussed, which range from "How to reset a user's password" to "How to properly remove users." Each task includes step-by-step instructions.

Chapter 9: Call Management

One of the system's most useful and often underutilized features is call management. This chapter ensures that the reader understands the way that the system processes a call. The most basic object of the call management system is a call handler. A brief review of how

call handlers work is included in the beginning of this chapter. Additionally, a common use of the system's call management feature is to deploy a basic auto-attendant, which is described within this text. The chapter also addresses some of the more advanced call management features, such as call routing rules and audio-text applications. Complete step-by-step instructions are included within this chapter.

Chapter 10: Implementing Unity Networking

Because many organizations are migrating to Unity/Connection from a voicemail system or have other voicemail systems deployed at other locations, Unity/Connection must communicate with them. Unity can be integrated with these systems through a number of industry-standard protocols. This chapter discusses the different types of networking that can be deployed and looks at how to determine the proper one to use.

Chapter 11: Exploring Additional Tools

Although most day-to-day tasks can be accomplished using the system administrative interface, it is often more efficient to use one of the many tools that are included with Unity/Connection. The tools help accomplish tasks that range from making bulk user changes to migrating users to another server. This chapter introduces the reader to these tools and includes step-by-step details on how to use each of them.

Chapter 12: Maximizing CUCM and Unity Connection Capabilities

As Communications Manager and Unity/Connection evolve, more and more advanced features are added. This chapter looks at a few of these more advanced features, such time-of-day routing and call queuing. In addition, the chapter offers a few examples of features that can be created by taking existing features of each application and adding a new twist to them, such as using Unity as a conference manager.

Target Version

This book was written for Communications Manager, Unity, and Unity Connection versions 8.0 and 8.5. This is not to say that you must run any of these versions for this book to be of value to you. It does, however, mean that some of the step-by-step guides might be slightly different. With each new version, the menus are sometimes moved or slightly changed, or there might be an additional field in the new version. However, none of these issues should cause you great concern. If the field isn't there, don't worry about it. If a menu isn't exactly where you expect it, just look above or below, and you are sure to find it. Including the exact steps for every version of these applications would have made the book larger than you would care to lift, let alone read. Remember that the value of this book goes beyond the step-by-step guides, because it also provides easy-to-understand explanations of many Cisco Unified Communications concepts.

Chapter 5

Configuring Class of Service and Call Admission Control

Now that you have created a basic dial plan, it is time to build on that and create a more complete dial plan. Often you want to allow and disallow access to certain destinations. For example, you might want only a certain group of callers to dial international numbers. This is done by creating a telephony class of service (CoS). In addition, if there are calls traversing limited-bandwidth links, some type of Call Admission Control (CAC) should be deployed to help ensure voice quality. This chapter examines the various concepts associated with CoS and CAC and describes how to configure the required components for each.

Rights and Restrictions

After the dial plan is created and users can place calls to destinations outside the cluster, you might think that you are all set and can sit back and relax. Not quite. After the system is configured to enable calls to be placed outside of the system, you need to start working on how to prevent certain calls from being placed. This chapter touches on how you can use route patterns to block certain destinations, and now you need to move beyond that and discuss how certain destinations can be reachable by some devices, but not by others. To accomplish this, you need to configure Calling Search Spaces (CSS) and partitions. The following sections explain what these are and how they work.

Understanding Call Search Spaces and Partitions

Of all the concepts within a Communications Manager environment, it is believed that the CSS and partitions cause the most confusion. This is rather odd because they are not complex. Simply put, the partition assigned to the destination affects what devices can reach it, and the CSS determines which destinations can be reached. Locks and key rings are good analogies. Think of the partition as a lock and the CSS as the key ring. To place a call to a destination, you must have a key that matches the device's lock. The key ring contains all the keys and therefore determines which destinations you can reach.

Of course, there is more to it than just locks and keys, but by using this analogy, you begin to understand how they work. You take a closer look at this analogy. Figure 5-1 shows five phones. The first four phones have partitions (locks). It is important to point out that the partitions (locks) are not assigned to devices, but rather to patterns and directory numbers (DN). For this example, assume that each phone has only a single line and that the partition (lock) is assigned to that line. Below each phone is a CSS (key ring) that shows to which partitions (locks) the phone has access. CSS (key rings) can be assigned to the device or the line. In this example, assume that they are assigned to the device.

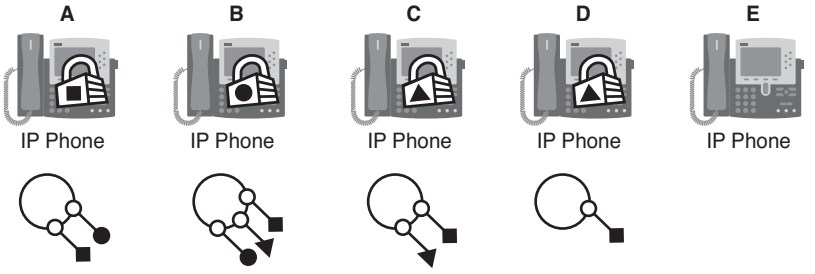


Figure 5-1 *Calling Search Spaces and Partitions Analogy*

The locks in this figure have different-shaped keyholes, which means that to open a lock, you must have a key ring that has the correct-shape key. Keeping in mind that the locks represent partitions and that the key rings represent CSS, answer the following questions:

- What phones can phone A reach?
- What phones can phone D reach?
- What phone can reach all other phones?
- What phones can reach phone E?
- What phones can phone E reach?

The answers to these questions are as follows:

Q. What phones can phone A reach?

A. To determine what phones phone A can reach, you need to look at its CSS (key ring). Phone A has a circular key and a square key on its key ring, which means that it can call itself and phone B. However, because phone E has no lock (partition) assigned to it, any phone can reach it, just as a door with no lock can be opened by anyone.

Q. What phones can phone D reach?

A. Because phone D has only a square key, it can dial phone A and, of course, phone E because it has no lock (partition).

Q. What phone can reach all other phones?

A. Because phone B has a key ring (CSS) that contains all the keys, it can reach all the devices.

Q. What phones can reach phone E?

A. Because phone E has no lock (partition), all phones can reach it.

Q. What phones can phone E reach?

A. Because phone E has no keys, it can only reach devices that have no locks. In this example, phone E can only dial itself.

Figure 5-1, along with these questions and answers, should help you begin to understand how partitions and CSS work. Of course, as with any simple concept, it has the potential to become more complicated as the number of CSS and partitions grows. This is where some people begin to become confused, because of an inaccurate base understanding of the concepts. Now look at some of the more interesting aspects of CSS and partitions.

The first misconception that should be dispelled is this: If two devices have the same partition, they can call each other. Having the same partition alone is not enough. Going back to the lock and key ring analogy, if two people have the same locks, keyed the same way on their houses, but they have no keys, can they access each other's houses? Of course they can't, and they cannot even access their own houses. This demonstrates that a device's partition (lock) has no effect on where the device can call. However, if two devices that have the same partition also have a CSS that enables them access to their partitions, they can dial each other.

The next important point is the order of CSS. As demonstrated in the earlier example, CSS can enable access to more than one partition. Now, imagine that a device has a CSS that enables it to match two devices with the same number, but in different partitions. Figure 5-2 offers an example of this situation.

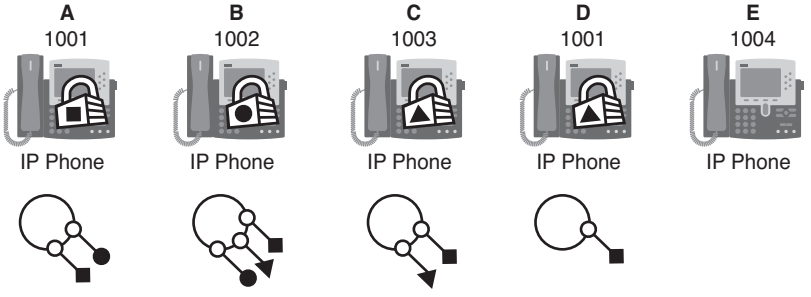


Figure 5-2 *CSS Matches Multiple Destinations*

In this example, phones A and D have the same extension of 1001. Phones B and C can reach both phones because their CSS enables access to both the square and triangle partition. So the question is, which phone rings when phone C dials 1001? Often people answer this question with, "It takes the closer match." Because 1001 matches 1001 exactly, both phones are the closest matches. Others assume that both phones ring because

phone C has access to both partitions. What actually happens is that when a search for a match is conducted, multiple closest matches are found. Because there are multiple closest matches, the order in which objects appear in the CSS comes into play. When you create a CSS, you prioritize the order in which partitions should be searched. This order determines which partition is used if there are two closest matches. In the example, Figure 5-2 shows that the order of the keys for phone C is square followed by triangle, meaning that when phone C dials 1001, it would first match the 1001 that has the square partition, which is phone A.

To add a little more complexity to this, it is possible to have a CSS on both the device and the line. For example, the phone can have a CSS that grants access to the square partition, and a line on the phone can have a CSS that grants access to the triangle partition. In such a case, the line CSS takes priority. Figure 5-3 shows an example of this. This example moves away from the locks and keys analogy to focus more on the actual terms.

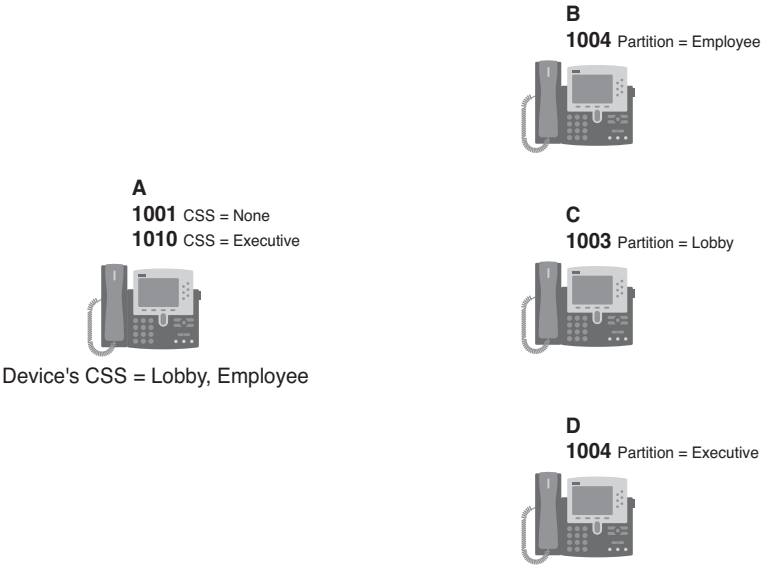


Figure 5-3 *Line/Device CSS Example*

In Figure 5-3, phone A has two lines, 1001 and 1010. 1001 has no CSS, and line 1010 has a CSS that grants access to devices in the executive partition. Phone A also has a CSS at the device level, which enables access to devices in the lobby and employee partitions. Because the 1001 line does not have a CSS of its own, it has access only to devices that can be reached using the device's CSS. Because line 1010 has a CSS of its own, it has access to devices that can be reached using its CSS and the device's CSS. This means that when dialing from line 1001, only devices in the lobby and employee partitions are accessible; but when dialing from line 1010, devices in the lobby, employee, and exec partitions are accessible.

Now, take a look at the other three phones. Phone B has the extension of 1004, and that line is in the employee partition. Phone C has the extension of 1003, and that line is in the lobby partition. Phone D has the extension of 1004, and that line is in the exec partition.

Using what you have learned, answer the following three questions:

- What is the result if 1004 is dialed from line 1001?
- What is the result if 1004 is dialed from line 1010?
- Can line 1010 reach line 1003?

The answers to these questions are as follows:

Q. What is the result if 1004 is dialed from line 1001?

A. Because line 1001 has no CSS of its own, it relies solely on the device's CSS. The device's CSS has access to the employee and lobby partitions, so line 1001 can reach only the 1004 on phone B because it is in the employee partition.

Q. What is the result if 1004 is dialed from line 1010?

A. Because line 1010 has a CSS, it has access to all devices to which the line and device's CSS grants access. Because it can reach phones B and D and both of them match 1004, the line's CSS takes priority and phone D rings.

Q. Can line 1010 reach line 1003?

A. Line 1010 can reach any device to which the line and/or the device's CSS grants access. Because the device's CSS has access to the lobby partition, which is the partition that 1003 is in, it can reach it.

At this point, you should have a good idea of how partitions and CSS work. We now take a look at a real-world, practical example of how CSS and partitions can be used.

The BGD Company has deployed a Communications Manager solution and has configured the route patterns that are shown in Table 5-1. As you can see, the route patterns enable callers to reach anywhere they need to dial with the exception of 1-900 numbers, which are blocked. The problem is that these patterns also enable some callers to make unauthorized calls that the company disapproves of. For example, if a person's job does not require the placement of international calls, the dial plan should not enable the employee's phone to place them.

In this example, BGD has decided that it actually has four classes of users. The first class, the executives, can make any calls they want, other than 1-900 calls. The second class, the administrative assistants, are not allowed to make 1-900 calls or international calls. The third class, standard users, can only reach internal extensions, local numbers, and emergency services. The fourth class, lobby phones, for example, can only make calls internally and to emergency services. To accomplish this, partitions and CSS must be configured and assigned to patterns and devices.

Table 5-1 *BGD's Route Patterns*

Pattern	Notes	Matches
9.[2-9]XXXXXX 9.810[2-9]XXXXXX	PreDot Discard PreDot Discard	Local 7- and 10-digit calls
9.810586XXXX 9.810587XXXX	PreDot Discard PreDot Discard	10-digit calls that are not local
9.1[2-9]XX[2-9]XXXXXX	PreDot Discard	Long-distance calls
9.011! 9.011!#	PreDot Discard PreDot Trailing-# Discard	International calls
9.1900[2-9]XXXXXX	Block Pattern	1-900 numbers
911 9.911	Urgent Priority PreDot Discard and Urgent Priority	Emergency service calls

When creating partitions, a common practice is to name them so that the name describes to what the partition is assigned. For example, a partition that is going to be assigned to a pattern that matches a local number can be called Local PT.

Tip The PT at the end of the name helps identify this object as a partition. Because it is possible to have partitions and CSS with the same name, it is recommended that you add a PT to the end of partition names and CSS to the end of CSS names.

In this example, five types of calls are allowed: internal, local, long-distance, international, and emergency. The following is the list of partitions that are needed, and to which patterns they are assigned:

- **Internal_PT:** Patterns that match internal numbers
- **Local_PT:** Patterns that match local numbers
- **LD_PT:** Patterns that match long-distance numbers
- **International_PT:** Patterns that match international numbers
- **Emergency_PT:** Patterns that match emergency service numbers

After the partitions are created, CSS are needed. Because BGD has defined four classes of users, four CSS are needed. Just as with partitions, it is recommended that CSS are named so that the name helps identify to which partitions the CSS have access. Table 5-2 shows the CSS and the partitions to which each has access and that are needed for BGD.

Now that partitions and CSS are defined, take a look at what each is assigned to. First, examine the partitions. You need to understand that partitions are assigned to patterns of DNs, not devices. This means that if you want to prevent a device from making long-distance calls, you assign a partition to the patterns that match long-distance numbers,

and make sure that the device's CSS does not have access to the partition. Table 5-3 shows the five partitions that have been created and the patterns to which each is assigned.

Table 5-2 *CSS and Associated Partitions*

CSS	Partitions
Internal_CSS	Internal_PT Emergency_PT
Internal_Local_LD_CSS	Internal_PT Local_PT Emergency_PT
Internal_CSS	Internal_PT Local_PT LD_PT Emergency_PT
Unlimited_CSS	Internal_PT Local_PT LD_PT International_PT Emergency_PT

Table 5-3 *Partitions and Patterns*

Partitions	Patterns
Internal_PT	DNs of the phones
Local_PT	9.[2-9]XXXXXX 9.810[2-9]XXXXXX
LD_PT	9.810586XXXX 9.810587XXXX 9.1[2-9]XX[2-9]XXXXXX
International_PT	9.011! 9.011!#
Emergency_PT	911 9.911

You might notice that the 9.1900[2-9]XXXXXX pattern has not been assigned to a partition but will still work. Remember, if a pattern does not have a partition explicitly assigned, it falls into the null partition, and all devices have access to the null partition. Because the 9.1900[2-9]XXXXXX pattern is set up so that it blocks all calls that match it, you want all devices to have access to it so that no one can place these types of calls. However, it is recommended to apply partitions to all patterns to ensure that no calls can be placed by phones that do not have the proper CSS. With this is mind, the Internal_PT partition can be applied to the 9.1900[2-9]XXXXXX pattern because all devices can reach that partition.

Now look at how the CSS should be assigned. Remember that CSS can be assigned at both the device and line. For this example, they are assigned at the device level only. Table 5-4 shows the CSS and the types of device to which each is assigned.

Table 5-4 *CSS and Assigned Devices*

CSS	Devices
Unlimited_CSS	Executive phones
Internal_Local_LD_CSS	Administrative assistant phones
Internal_Local_CSS	Standard users
Internal_CSS	Lobby phones

Now that you understand which CSS and partitions are needed for BGD, and where each is applied, take a look at the big picture. Table 5-5 shows which CSS is assigned to each of the four different classes of phones. Under the CSS heading is a list of the partitions that can be accessed. Under the partitions is a list of patterns. Using this table, it is easy to see what destinations various phones can reach.

Table 5-5 *CSS Assigned to Phones and the Patterns They Can Reach*

Device	CSS>Partition>Patterns
Executive phones	Unlimited_CSS Internal_PT
	All Internal Phones
	Local_PT
	9.[2-9]XXXXXX
	9.810[2-9]XXXXXX
	LD_PT
	9.810586XXXX
	9.810587XXXX
	9.1[2-9]XX[2-9]XXXXXX
	International_PT
	9.011!
	9.011!#
	Emergency_PT
	911
	9.911

Table 5-5 *CSS Assigned to Phones and the Patterns They Can Reach*

Device	CSS>Partition>Patterns
Administrative assistant phones	Internal_Local_LD_CSS Internal_PT
	All Internal Phones
	Local_PT
	9.[2-9]XXXXXX
	9.810[2-9]XXXXXX
	LD_PT
	9.810586XXXX
	9.810587XXXX
	9.1[2-9]XX[2-9]XXXXXX
	Emergency_PT
	911
	9.911
Standard user phones	Internal_Local_CSS Internal_PT
	All Internal Phones
	Local_PT
	9.[2-9]XXXXXX
	9.810[2-9]XXXXXX
	Emergency_PT
	911
	9.911
Lobby phones	Internal_CSS Internal_PT
	All Internal Phones
	Emergency_PT
	911
	9.911

Up to this point, only the assigning of CSS to phones and lines has been discussed. CSS are assigned to devices, which include gateways. A CSS is assigned to a gateway so that inbound calls can reach internal destinations. In the example of BGD, all the internal phones are placed in the Internal_PT partition. If the gateways do not have access to this partition, no incoming calls are allowed. So you can see that not only must phones have CSS, but gateways require them as well. In the case of BGD, the Internal_CSS can be assigned to the gateways, which would grant outside calls access to all internal phones.

Note CSS and partitions are only locally significant. This means, for all intents and purposes, that after a call leaves the local system, the CSS and partitions no longer exist.

In the BGD example, all internal phones were in the Internal_PT partition, meaning that because all devices had a CSS that granted access to the Internal_PT partition, all phones could be reached. In some cases, this is undesirable. Sometimes there are certain numbers that should be reached only by certain devices. An example often used is that of an executive's phone. Often it is desired that only the executive's assistant be able to reach the executive. To accomplish this, the executive's phone is placed in a separate partition, to which only the assistant's phone has access.

Now that you have a good idea of what CSS and partitions are, move on to discussing how they are created and configured.

Creating Calling Search Spaces and Partitions

Creating CSS and partitions is much easier than understanding and properly applying them. Before you move on to the process of creating them, you should make sure that you have taken the time to determine the different classes of users your environment has, and what destinations each user will be allowed to call. After you have done this, create a list of the partitions that are required. Next, create a CSS that defines what partitions are accessible. After you have created this, you can begin to create the partitions and CSS. Because CSS are created by choosing partitions to which they will have access, the partitions must be created first. The following steps show how to create partitions:

Step 1. From within CCMAdmin, select **Call Routing > Class of Control > Partition**.

Step 2. Click the **Add New** link.

Step 3. A screen displays that offers an area in which you can enter the name of the partition followed by a description. You must place a comma (,) between the name and description. If you do not enter a description, the name of the partition will be used as the description. You can create up to 75 partitions at a time on this screen by placing each on a new line. Figure 5-4 shows an example of adding five partitions at one time.

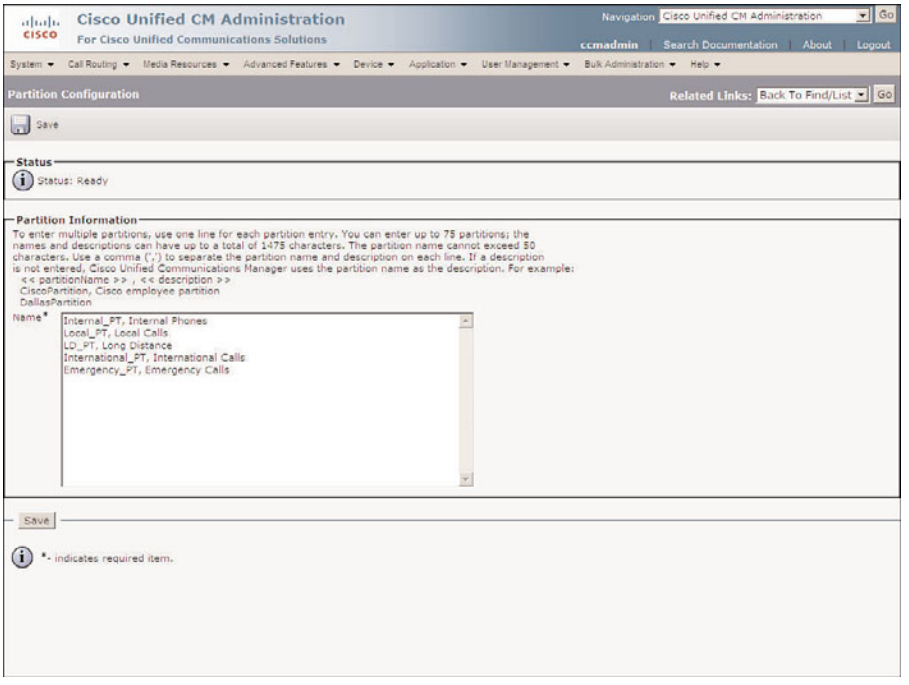


Figure 5-4 *Creating Partition Configurations*

Step 4. After you enter all the desired partitions, click **Save**.

As you can see, the creation of partitions is a simple task. Now that partitions are added, you can start to create CSS by working through the following steps:

Step 1. From within CCMAdmin, select **Call Routing > Class of Control > Calling Search Space**.

Step 2. Click the **Add New** link.

Step 3. A screen similar to that shown in Figure 5-5 displays.

Step 4. Enter a name in the **Calling Search Space Name** field. Remember that the name should help identify the purpose of this CSS.

Step 5. Enter a description in the **Description** field.

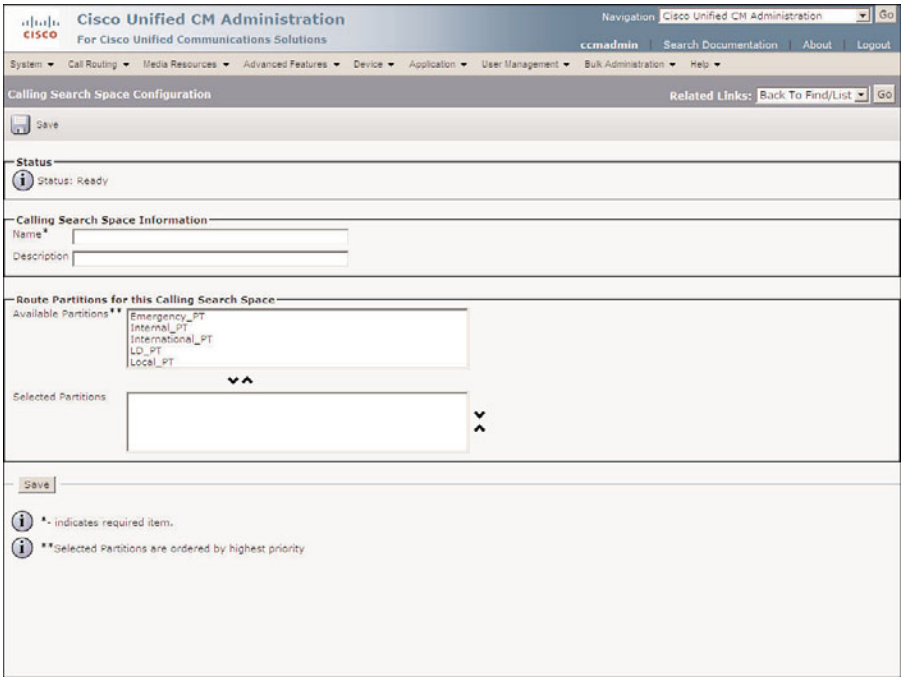


Figure 5-5 *Creating CSS*

Step 6. A list of partitions displays in the **Available Partitions** box. If you have a large number of partitions, you can limit the partitions that display in this list by entering the appropriate search criteria in the Find Partitions Where fields and clicking **Find**.

Step 7. Highlight the first partition to which you want the CSS to have access, and click the Down Arrow below this box. This causes that partition to display in the **Selected Partitions** box.

Step 8. Repeat Step 7 for each partition to which you want the CSS to have access. These should be added in the order you want to have them searched.

Step 9. After all the partitions have been added, you can change the order in which they display. Remember, the order in which they display determines which partition is used if multiple partitions within the same CSS contain exact matches for a dialed number. To change the order, highlight the partition you want to move, and click the Up or Down Arrow to the right of the box. Figure 5-6 shows what the screen looks like when adding the Internal_Local_CSS, which was used in the previous example.

Step 10. After all desired partitions are listed in the correct order in the Selected Partitions box, click **Save**.

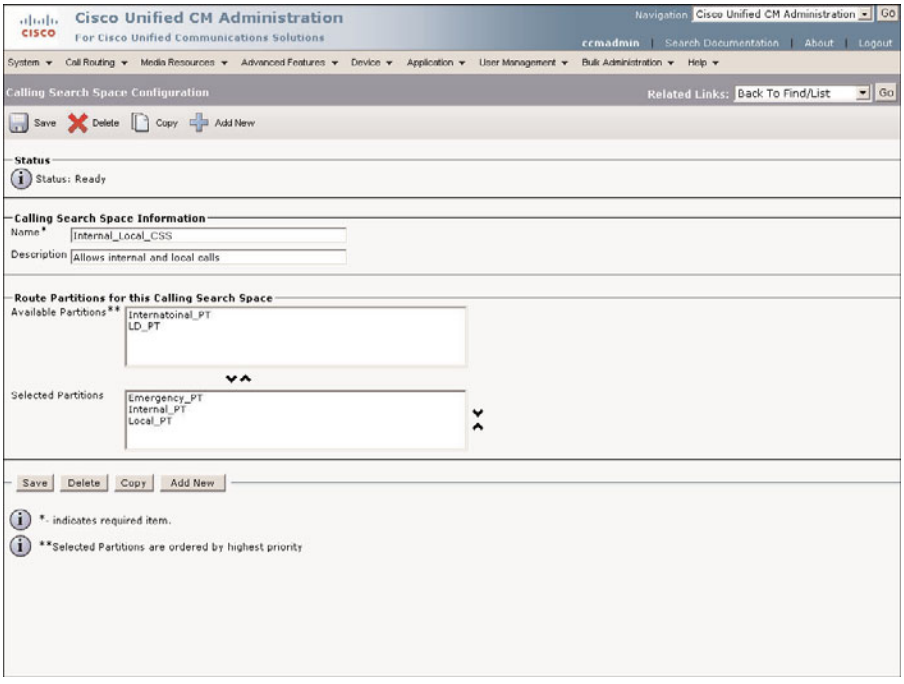


Figure 5-6 *Example CSS*

You need to repeat these steps to add all the CSS that your environment requires. After all the partitions and CSS are added, it is time to apply them. Adding partitions and CSS have absolutely no effect on call processing until they are applied to patterns and devices.

Applying Calling Search Spaces and Partitions

You are now ready to start applying the partitions and CSS to devices and patterns. After a partition is added to a pattern, only devices that have the correct CSS can reach that pattern. For this reason, you might want to assign CSS to the devices before assigning partitions. Assigning partitions before assigning CSS is similar to putting a lock on a door and not giving anyone a key. Until the keys are handed out, no one can get in.

Note When adding partitions and CSS to a system, it is best to apply them during non-production times. After they are added, thorough testing should be done. If it is not possible to add them off-hours, be certain to apply CSS before applying partitions. A good tool that can be used to verify the results is called the Dialed Number Analyzer. This tool can be installed from the Install Plugins page. This tool enables you to enter an origination and destination number and shows you how the call will be handled, based on the current dial plan. For more information on this tool, refer to the Dialed Number Analyzer guide, which can be found at Cisco.com by searching for Dialed Number Analyzer.

CSS are applied to devices and lines. When applied to both, the line's CSS has priority but does not nullify the devices. This means a line that has its own CSS has access to partitions that both the line's CSS and the device's CSS allow.

Note Often people want their assistants to answer their lines for them. To do this, you must put the directory number on the assistant's phone. The CSS assigned to the line stays with the line, no matter which phone the line is on. This means that if the boss's line has the rights to call international numbers, the assistant can do so as well, if the boss's line is on the assistant's phone. To deal with this, it is recommended that the more generous CSS be applied to the device, not the line.

Now take a look at how a CSS is assigned to a phone, a line on the phone, and a gateway.

Assigning a CSS to a Phone

The steps that follow show how to assign a CSS to a phone:

Step 1. From within CCMAdmin, Select **Device > Phone**.

Step 2. Enter search criteria in the search field to limit the results and click **Find**.

Step 3. Select the phone to which you want to assign a CSS from the list that is generated.

Step 4. The Phone Configuration screen displays. To assign a CSS to the phone, select a CSS from the **Calling Search Space** drop-down list, as shown in Figure 5-7.

Step 5. Click **Save**.

Step 6. A window displays to inform you that you must click the **Apply Config** button for the change to take affect. Click **OK**.

Step 7. Click **Apply Config**.

Step 8. A window displays to warn you that when you apply the configuration, the device might go through a restart. Click **OK**.

Assigning a CSS to a Line

The steps that follow show how to assign a CSS to a line on a phone:

Step 1. From within CCMAdmin, select **Device > Phone**.

Step 2. Enter search criteria in the search field to limit the results and click **Find**.

Step 3. Select the phone that contains the desired line from the list of phones that is generated.

Step 4. Click the desired line on the left side of the screen.

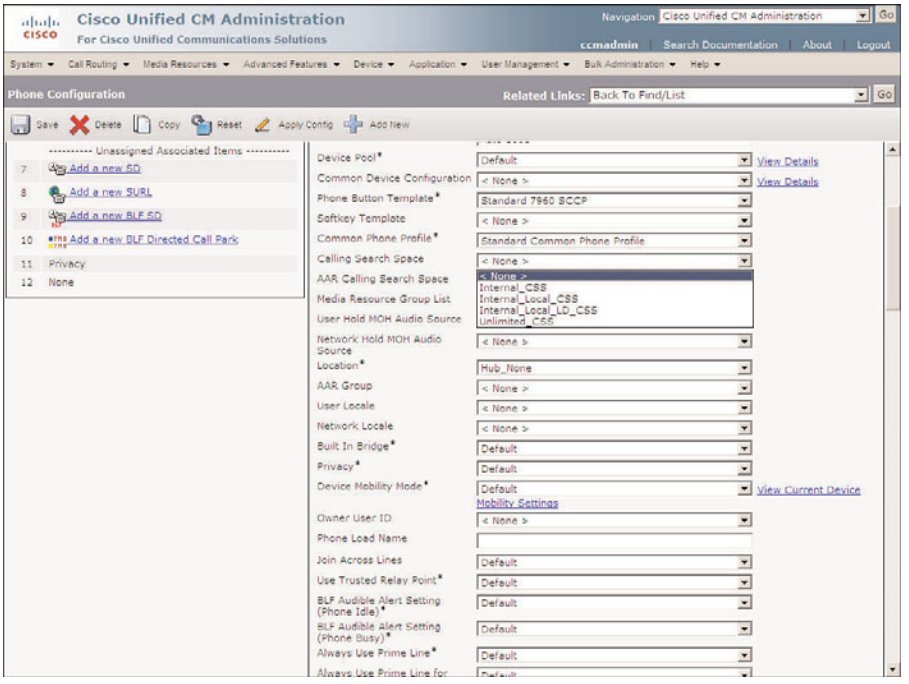


Figure 5-7 *Assigning a CSS to a Phone*

Step 5. On the Directory Number Configuration page, select the desired CSS from the **Calling Search Space** drop-down list, as shown in Figure 5-8.

Step 6. Click **Save**.

Note When you make a change to the directory number configuration and click Update, the line will be reset on all the phones that appear on this line. If a caller is currently on a call, the line resets after the call is ended.

Assigning a CSS to a Gateway or Trunk

The steps that follow show how to assign a CSS to a gateway or a trunk. Because the steps are so similar for both components, they have been combined.

Step 1. From within CCMAdmin, select **Device > Gateway or Device > Trunk**.

Step 2. Enter search criteria in the search field to limit the results, and click **Find**.

Step 3. From the list that is generated, select the gateway/trunk to which you want to assign a CSS.

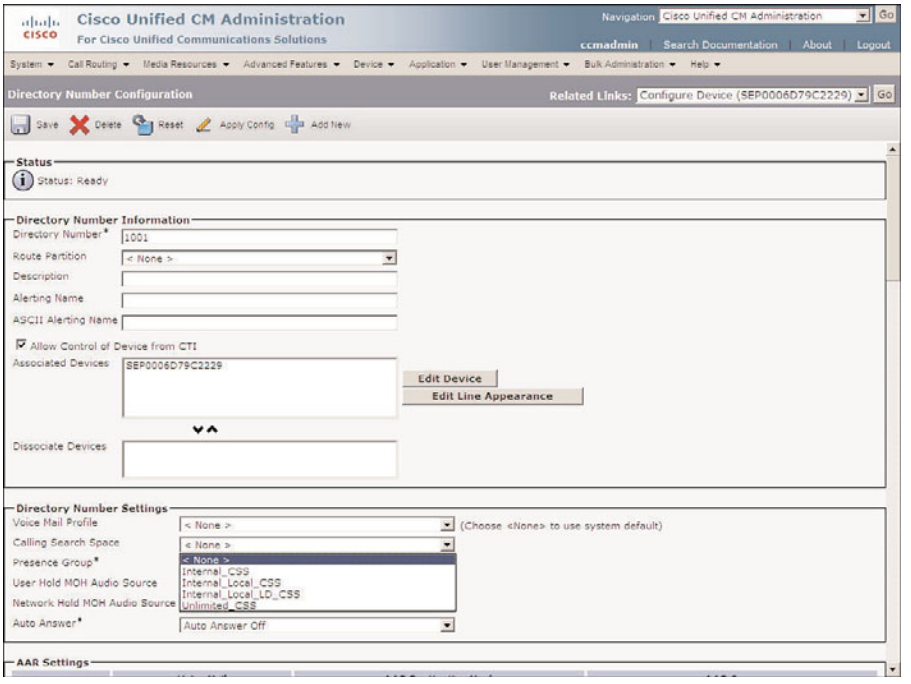


Figure 5-8 *Assigning a CSS to a Line*

Note When configuring CSS for Session Initiation Protocol (SIP) trunks, additional CSSs are configured. In the Inbound Call section, select the desired AAR CSS from the AAR Calling Search Space drop-down list. Under the Outbound Calls section, select the desired CSS from the Called Party Transformation CSS and Calling Party Transformation CSS drop-down lists. Under the SIP Information section, there are additional CSSs that should be configured. These included the Rerouting Calling Search Space, Out-Of-Dialog Refer Calling Search Space, and SUBSCRIBE Calling Search Space.

Step 4. Select the CSS from the **Calling Search Space** drop-down list.

Note For some gateways such as Media Gateway Control Protocol (MGCP), you need to navigate to the subunit configuration page to assign a CSS.

Step 5. Click **Save**.

Step 6. A window displays informing you that you must click **Apply Config** for the change to take affect. Click **OK**.

Step 7. Click **Apply Config**.

Step 8. A window displays warning you that when you apply the configuration, the device might go through a restart. Click **OK**.

Now that you have assigned CSS, you can assign partitions. Partitions are assigned to patterns of directory numbers. Examples of how to assign them to CSS and partitions follow.

Assigning a Partition to a Line (Directory Number)

The following steps show how to assign a partition to a line:

Step 1. From within CCMAdmin, select **Device > Phone**.

Step 2. Enter search criteria in the search field to limit the results and click **Find**.

Step 3. Select the phone that contains the desired line from the list of phones that is generated.

Step 4. Click the desired line on the left side of the screen.

Step 5. On the Directory Number Configuration page, select the desired partition from the **Route Partition** drop-down list, as shown in Figure 5-9.

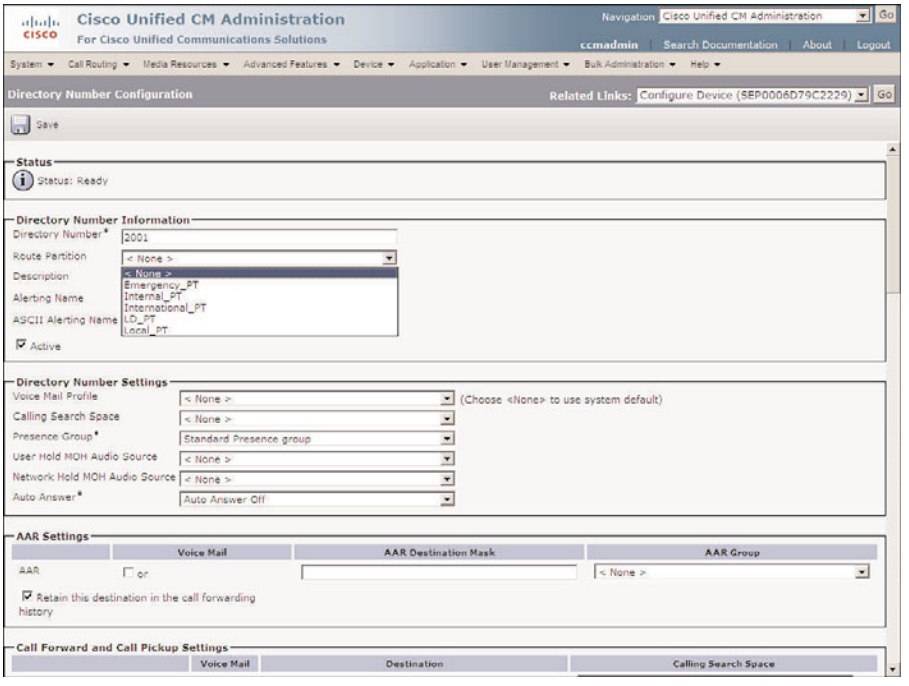


Figure 5-9 *Assigning a Partition to a Line*

Step 6. Click **Save**.

Assigning a Partition to a Pattern

Step 1. From within CCMAdmin, select **Call Routing > Route/Hunt > Route Pattern.**

Step 2. To limit the results, enter search criteria in the search field and click **Find.**

Step 3. Select the route pattern from the list that displays.

Step 4. Select the partition from the **Route Partition** drop-down list, as shown in Figure 5-10.

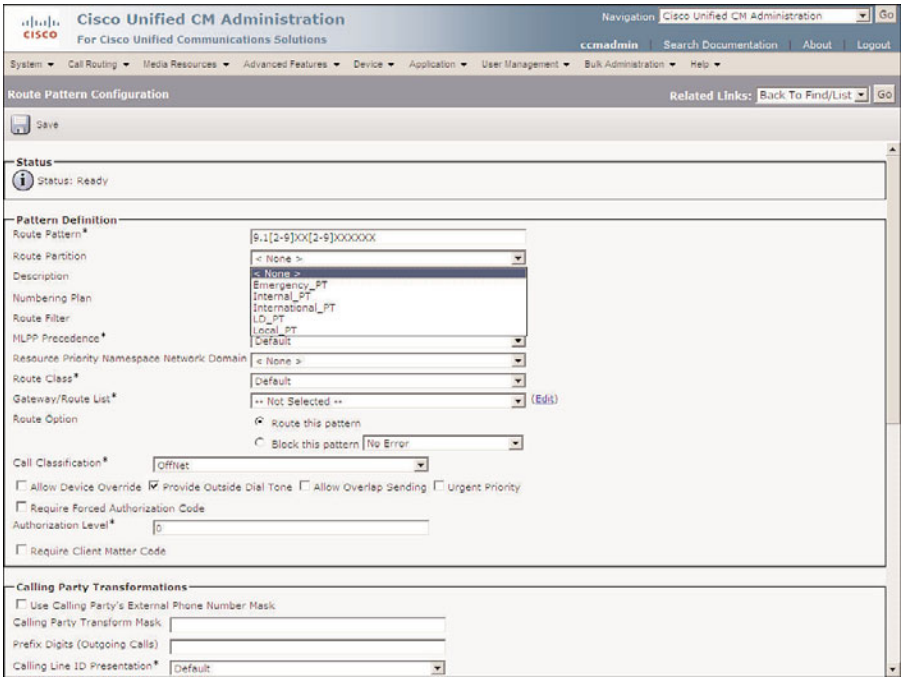


Figure 5-10 *Assigning a Partition to a Route Pattern*

Step 5. Click **Save.**

Note Two alert windows can appear. If you have not assigned authorization codes to this pattern, an alert will inform you of this. You can click OK. The other alert informs you that any update to a route pattern automatically resets the route list or gateway; click OK.

After the partitions are applied, you can begin testing the system to ensure that allowed calls can be placed, and those that are not allowed cannot be placed.

Adding CSS and partitions after the system is in place can require a lot of work. Remember that you can use the the Bulk Admin Tool (BAT) to quickly apply or change a CSS or partition on a large number of objects.

Implementing Call Admission Control

After you have set up your system to allow calls to be placed to outside destinations and have applied CSS and partitions to restrict access, you need to configure the system to ensure the quality of the calls. Although there are many things that can affect the quality of the call, this book deals only with things that can be configured directly in Communications Manager. The following sections discuss what must be configured to ensure that the Voice over Internet Protocol (VoIP) link is not over subscribed.

When calls are placed between sites using an IP link as the transport, the quality of the call can be affected if more calls are allowed than what the link can support. To prevent this, some type of Call Admission Control must be deployed. How this is accomplished depends on the environment. If the calls are being sent across intercluster trunks, a gatekeeper is required. If calls are being placed to remote sites that are part of the same cluster, locations are used. If both types of calls are taking place, both solutions must be deployed.

Locations are objects that are configured within Communications Manager. A location for each site is created that contains available bandwidth for calls. A closer look at the configuration of locations is offered later in this chapter. Before looking at locations, gatekeepers are examined.

Configuring CAC for a Distributed Deployment

A gatekeeper is a process that runs on a Cisco IOS router. It keeps track of the active calls between clusters and determines whether a call can be placed across an intercluster trunk. In most cases, only one gatekeeper is needed because each can support more than a 100 sites. It is recommended, however, to have a redundant gatekeeper. This can be accomplished by having a second router running Hot Standby Routing Protocol (HSRP) or by implementing gatekeeper clustering. The only requirement for the physical location of a gatekeeper is that all clusters must reach it through an IP path.

When a call is placed across a gatekeeper-controlled H.225 or intercluster trunk, the Communications Manager on the originating side asks the gatekeeper whether the call can be placed. If there is enough bandwidth, the gatekeeper grants admission. If admission is granted, call setup begins, and the Communications Manager on the other side of the call must request admission. If the gatekeeper determines that there is enough bandwidth, admission is granted and the call setup is complete.

A gatekeeper grants admission based upon availability of configured bandwidth. The gatekeeper is configured with the amount of bandwidth that can be used for calls. Each time a call is placed, the gatekeeper removes a certain amount from the available bandwidth. When the call is over, it returns the bandwidth to the available pool.

The amount of bandwidth required for each call depends on which codec is being used. The gatekeeper has the preconfigured amount of bandwidth that each codec requires, and this number cannot be changed. This figure might not be the actual bandwidth the call needs, but is used to ensure that enough bandwidth is available. A gatekeeper

running IOS 12.2(2)XA or later assumes that 128 kbps is needed for G7.11 calls and 16 kbps is required for G.729 calls. Although it might seem odd that the gatekeeper might request more or less bandwidth than it needs, it isn't a problem because the amount of available bandwidth is a setting that you configure in the gatekeeper. The gatekeeper does not have the ability to monitor the link and decide whether there is available bandwidth. It relies totally on the number that is configured. It is best to determine the amount of calls you want to allow on the link and the codec that will be used. Then simply multiply the amount of bandwidth the gatekeeper uses for that codec by the number of calls. The result is the amount of bandwidth that should be configured. For example, if the gatekeeper is running IOS version 12.2(2)XA or later and you want to allow ten calls all using the G.729 codec, the formula is 10 x 16 (10 calls x 16 kbps), which means that 160 kbps will be needed.

The gatekeeper can also be configured to provide the destination IP address to which the call should be sent. This feature is sometimes referred to as an *anonymous device*. An anonymous device is preferred in many environments, especially those with multiple intercluster trunks. When more than two clusters are connected, an intercluster trunk must be created between each cluster if an anonymous device is not used. Figure 5-11 shows that when connecting four clusters, 12 intercluster trunks are required.

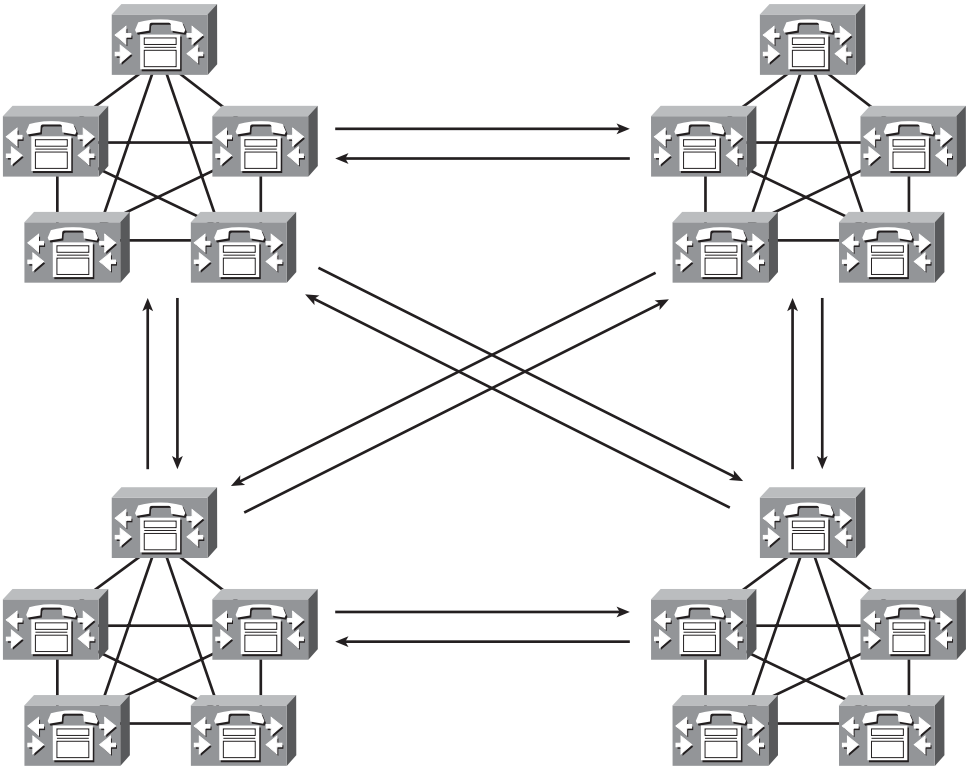


Figure 5-11 *Intercluster Trunks*

The formula used to determine how many intercluster trunks are required is N x (N–1). That is the number of clusters times the number of clusters minus 1. In Figure 5-11, there are four clusters. This means that the total number of intercluster trunks is 4 x (4–1) or 4 x 3, which equals 12. As the number of clusters increases so does the number of required trunks. For example, with four clusters, 12 intercluster trunks are needed, but with eight clusters, 56 intercluster trunks are needed. This is where an anonymous device becomes extremely useful. Instead of creating all the intercluster trunks, just one gatekeeper-controlled intercluster trunk is created, and all calls destined to any of the other clusters are sent to this trunk. When the gatekeeper responds to an admission request, it also provides the IP address of the destination.

Because the gatekeeper is going to provide destination information, it must know the destination IP address. This is part of the configuration that must be done on the gatekeeper itself. The bandwidth allowed for calls must also be configured in the gatekeeper to give you an idea of what needs to be configured. The following example shows a partial configuration:

```
gatekeeper
zone local DTW bgd.com 10.10.12.28
zone prefix DTW 4...
gw-type-prefix 1#* default-technology
bandwidth total zone DTW 256
no shutdown
```

A complete explanation of this configuration can be found in the article "Configuring H.323 Gatekeepers and Proxies" on Cisco.com. However, to give you an idea of what this configuration is achieving, the third command, "zone prefix DTW 4...," denotes that calls in the 4000 range can be handled by the DTW gatekeeper. The fifth command, "bandwidth total zone DTW 256," means that the total amount of bandwidth available for calls to and from DTW is 256 kbps.

Warning The gatekeeper should be configured only by an individual who is extremely knowledgeable of IOS configurations and commands and who thoroughly understands VoIP technologies. Because the gatekeeper might also be serving other routing functions, incorrect configuration could negatively affect the network as a whole.

Configuring a Gatekeeper

In addition to the required configuration on the gatekeeper itself, the gatekeeper must also be configured in the Communications Manager. Adding a gatekeeper in Communications Manager is quite simple. The following steps show how this is done:

Step 1. From within CCMAdmin, select **Device > Gatekeeper**.

Step 2. Click the **Add New** link.

Step 3. A screen similar to that shown in Figure 5-12 displays. Enter the IP address of the gatekeeper in the **Host Name/IP Address** field.

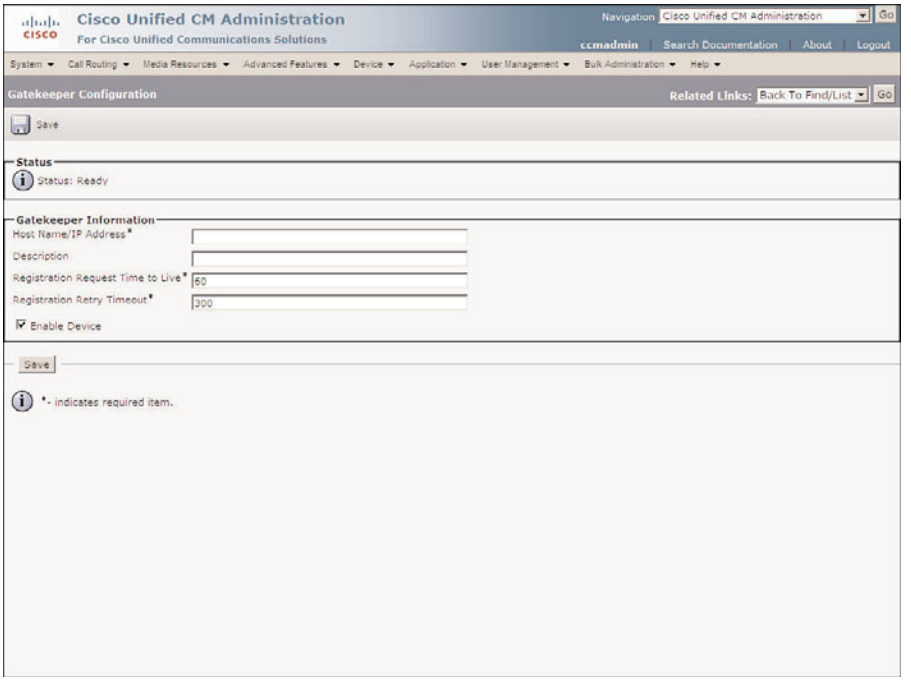


Figure 5-12 *Gatekeeper Configuration*

Step 4. In the **Description** field, enter a description that helps to identify this gatekeeper.

Step 5. The **Registration Request Time to Live** field should be left at the default. Change this field only if the Cisco Technical Assistance Center (TAC) tells you to do so. This field determines how often the Communications Manager must send a registration keepalive to the gatekeeper.

Step 6. The **Registration Retry Timeout** field should be left at the default. Change this field only if TAC tells you to do so. This value determines how long Communications Manager waits before trying to register after a registration attempt fails.

Step 7. Typically, the **Enable Device** check box should be left selected. This allows the gatekeeper to register with Communications Manager. When you need to gracefully unregister the gatekeeper, deselect this box.

Step 8. Click **Save**.

After a gatekeeper is configured, you must create a gatekeeper-controlled intercluster trunk so that the calls placed across the intercluster trunk request admission from the gatekeeper. This also allows you to take advantage of the anonymous device features if the gatekeeper is configured to provide call-routing information. Creating a

gatekeeper-controlled intercluster trunk is similar to creating a nongatekeeper-controlled intercluster trunk.

Configuring a Gatekeeper-Controlled Trunk

The steps required to configure a gatekeeper-controlled H.225 trunk and a gatekeeper-controlled intercluster trunk are similar. The following steps show how to configure a gatekeeper-controlled intercluster trunk and explain its various settings:

Step 1. From within CCMAdmin, select **Device > Trunk**

Step 2. Click the **Add New** link.

Step 3. On the next page, select Inter-Cluster Trunk (Gatekeeper Controlled) from the **Trunk Type** drop-down list.

Step 4. The Device Protocol field can be left at Inter-Cluster Trunk. No other option is available. Click the **Next** button.

Step 5. The Trunk Configuration screen, as shown in Figure 5-13, displays. Enter a functional name for the gateway in the **Device Name** field.

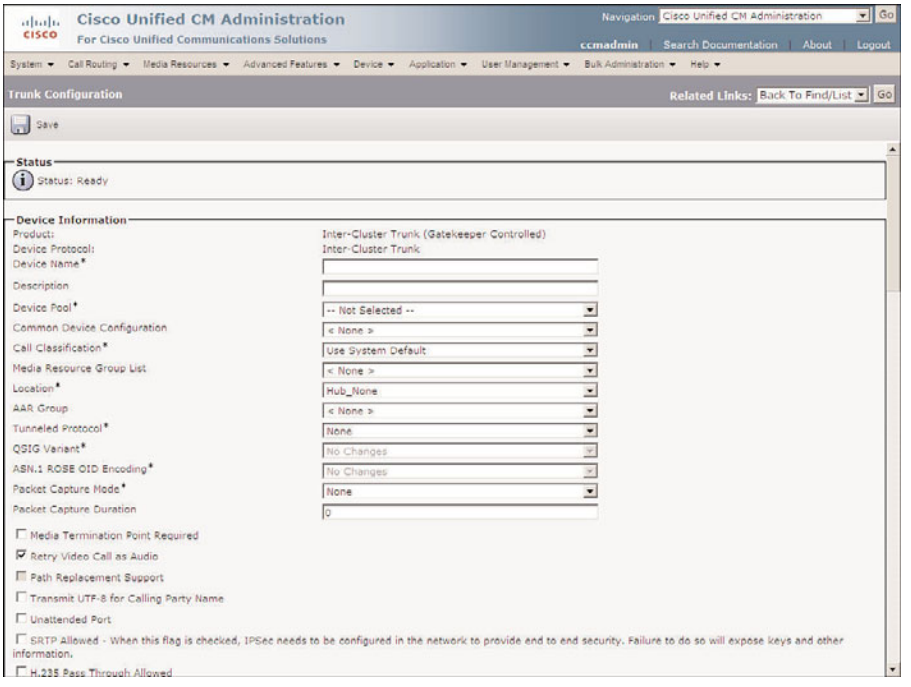


Figure 5-13 *Trunk Configuration*

Step 6. In the **Description** field, enter a description that makes this device easily identifiable.

Step 7. From the **Device Pool** drop-down list, select the desired device pool for this gateway.

Step 8. From the **Common Device Configuration** drop-down list, select the common device configuration that the trunk will use.

Step 9. From the **Call Classification** drop-down list, select whether incoming calls on this device should be considered OnNet or OffNet. This parameter is used to determine whether calls can be transferred and forwarded. This is to help prevent fraud.

Step 10. The next field is the **Media Resource Group List**. It determines the accessibility of media resources to a device. These are discussed further in Chapter 6, "Configuring CUCM Features and Services."

Step 11. Information entered in the **Location** field is used to prevent WAN links from becoming oversubscribed in centralized deployments. If you have defined locations, select the appropriate one for this device from the drop-down list.

Step 12. The **AAR Group** field determines the appropriate association of this device with an AAR group. An AAR group provides the prefix that is assigned when a call fails because of insufficient bandwidth. AAR is discussed in further detail in Chapter 6. Select an AAR group if AAR is being used. If this field is set to None, AAR is, in effect, disabled on this device.

Step 13. The **Tunneled Protocol** drop-down list allows you to select Q Signaling (QSIG), which enables intercluster trunk (ICT) to transport non-H.323 protocol information by tunneling it through H.323. Leave this set to None, unless you know that this type of tunneling is required.

Step 14. The **QSIG Variant** parameter is only configurable if QSIG is selected as the tunnel protocol. Leave this parameter alone unless Cisco TAC instructs you to change it.

Step 15. The **ASN.1 ROSE OID Encoding** parameter is only configurable if QSIG is selected as the tunnel protocol and is beyond the scope of this book.

Step 16. The next two fields, **Packet Capture Mode** and **Packet Capture Duration**, are for troubleshooting purposes only and should not be configured when adding a new trunk.

Step 17. The **Media Termination Point Required** check box needs to be selected if the H.323 device does not support features such as hold and transfers.

Step 18. If the **Retry Video Call as Audio box** is selected, Communications Manager sets up a voice call if a video calls fails to set up.

Step 19. The **Path Replacement Support** check box is automatically selected if you select QSIG from the Tunneled Protocol drop-down list. Otherwise it is left deselected.

Step 20. If the **Transmit UTF-8 for Calling Party Name** check box is left deselected, the user locale setting in the device pool will be used to determine whether Unicode information is sent and translated. Typically this can be left at the default.

Step 21. The **Unattended Port** check box is used to indicate that the device has unattended ports. This is normally used if the port is used to send calls to an application such as a voicemail server. In most cases, this box should be left deselected.

Step 22. If you want to allow both secure and nonsecure calls on this gateway, you must select the **SRTP Allowed** check box. If this is not selected, only nonsecure calls are allowed.

Step 23. If the **H.235 Pass Through Allowed** check box is selected, the shared-secret key can pass through a CM, allowing H.323 endpoints to set up a secure connection.

Step 24. The **Use Trusted Relay Point** field determines whether a relay point such as a Media Termination Point (MTP) or a transcoder must be labeled *trusted* to be used by this device. This field is typically only changed in virtualized environments.

Step 25. If the **Cisco Intercompany Media Engine** feature is being used and calls through this trunk might reach the PSTN, make sure the that PSTN Access check box is selected.

Intercompany Media Engine

Step 26. E.164 transformation profiles are used when Intercompany Media Engine (IME) is used. IME enables different companies to automatically learn routes, which enables calls to travel across the Internet instead of the PSTN.

Incoming Calling/Called Party Settings

Step 27. The **Incoming Calling Party Settings** and **Incoming Called Party Settings** are used to globalize numbers. Each calling and called party number has a number type assigned to it. The incoming calling/called part settings are based on the number type assigned. There are four number types: national, international, unknown, and subscriber. The four settings for each of these number types are

- **Prefix:** Digit enters are added to the beginning of the number after the specified number of strip digits are removed.
- **Strip Digits:** This is the number of digits that should be stripped from the number before the prefix is applied.
- **Calling Search Space:** This is the CSS that is used after transformation has occurred.

- **Use Device Pool CSS:** When this box is selected, the device pool CSS is used.

If your environment requires the manipulation of incoming called and calling numbers, configure the appropriate settings for each of these fields.

Step 28. The next two fields define the Multilevel Precedence and Preemption (MLPP) characteristics of this gateway. If these fields are left blank or set to default, the values set in the device pool are used. The first MLPP field is the **MLPP Domain**. MLPP grants higher priority only from calls with the same MLPP domain. If MLPP is used, an MLPP domain is needed; otherwise, this field can be left at None.

Step 29. The second field in this category, **MLPP Indication**, determines whether tones and indications will be presented when a precedence call is made. If the is field set to Off, no precedence indication is presented. If this field is set to On, indication is used for a precedence call.

Call Routing Information—Inbound Calls

Step 30. The next set of fields refers to inbound calls. The **Significant Digits** field determines the number of digits of an incoming dialed number that Communications Manager uses. Communications Manager counts from right to left. So if the number entered in this field is 4 and the digits received are 8105559090, 810555 would be removed. Only 9090 would be used to determine the destination of this call.

Step 31. A Calling Search Space (CSS) determines the accessible destinations of inbound calls. Choose a CSS from the **Calling Search Space** drop-down list. If this field is left at None, the dialing privileges of this gateway could be limited.

Step 32. Automated Alternate Routing (AAR) is used to provide an alternate route if a call fails because of insufficient bandwidth. The AAR CSS can be used to limit the paths a call can use when it is rerouted. Select an AAR CSS from the **AAR Calling Search Space** drop-down list.

Step 33. The **Prefix DN** field defines what digits are added to the front of an incoming destination number. This is applied to the number, after Communications Manager truncates the number, based on the Significant Digits setting.

Step 34. The **Redirecting Number IE Delivery–Inbound** check box should be selected if your voicemail system supports redirecting number IE. Otherwise, leave this box deselected.

Step 35. If the **Enable Inbound FastStart** check box is selected, FastStart will be used. H.323 FastStart requires only two message exchanges to open logical channels, whereas normal setup requires 12. However, if FastStart is selected, both ends must support and be configured for FastStart.

Call Routing Information—Outbound Calls

Step 36. Called party transformation enables you to change the number that is dialed. Select the **Called Party Transformation CSS** that contains the called party transformation patterns that should be applied to calls routed through the trunk. You can also leave this set to None and use the Called Party Transformation CSS assigned to the device pool by selecting the **Use Device Pool Called Party Transformation CSS** check box.

Step 37. Calling party transformation enables you to change the caller ID. Select a **Calling Party Transformation CSS** that contains the calling party transformation pattern that is assigned to the device. You can also leave this set to None and use the Calling Party Transformation CSS assigned to the device pool by selecting the Use Device Pool Calling Party Transformation CSS check box.

Step 38. The **Calling Party Selection** field determines what number is sent for outbound calls. The choices are

- **Originator:** The directory number of the device that placed the call.
- **First Redirect Number:** The directory number of the first device to redirect the call.
- **Last Redirect Number:** The directory number of the last device to redirect the call.
- **First Redirect Number (External):** The external directory number of the first device to redirect the call.
- **Last Redirect Number (External):** The external directory number of the last device to redirect the call. Select the desired value for this field.

Step 39. The **Calling Line ID Presentation** field determines whether Communications Manager sends caller ID information. To send caller ID information, select Allowed from the drop-down list. To block caller ID, select Restricted from the drop-down list.

Step 40. Cisco recommends that the next four fields remain set to the default of Cisco CallManager. The four fields are

- Called party IE number type unknown
- Calling party IE number type unknown
- Called Numbering Plan
- Calling Numbering Plan

These fields deal with dial plan issues and should be changed only when advised to do so by Cisco or an experienced dial plan expert. The need to change these usually occurs when installing Communications Manager internationally.

Step 41. The **Caller ID DN** field is used to determine what caller ID is sent out of this gateway. A mask or a complete number can be entered in this field. For example, if the mask 55536XX is entered in this field, Communications Manager sends 55536 and the last two digits of the calling number.

Step 42. If the **Display IE Delivery** check box is selected, the calling and called party name information is included in messages.

Step 43. The **Redirecting Number IE Delivery-Outbound** check box should be selected when integrating with a voicemail system that supports redirecting number IE. Otherwise, leave it deselected.

Step 44. If the **Enable Outbound FastStart** check box is selected, FastStart will be used. H.323 FastStart requires only two message exchanges to open logical channels, whereas normal setup requires 12. However, if FastStart is selected, both ends must support and be configured for FastStart.

Step 45. If the Enable Outbound FastStart check box is selected, you must select the codec that is to be used. This is selected from the **Codec for Outbound FastStart** drop-down list.

Gatekeeper Information

Step 46. From the **Gatekeeper Name** drop-down list, select the desired gatekeeper.

Step 47. The **Terminal Type** field specifies the type of devices this trunk controls. Choose Gateway for normal trunks.

Step 48. The **Technology Prefix** field enables you to assign a prefix that matches the prefix in the gatekeeper. By assigning a matching prefix, you can avoid having to add the IP address of each Communications Manager in the gatekeeper on the gw-type-prefix line. It is recommended that you use 1#* in both this field and the gatekeeper configuration. The value entered in this field must exactly match what is configured in the gatekeeper.

Step 49. The **Zone** field determines which zone this Communications Manager registers with on the gatekeeper. If this field is left blank, the gatekeeper's zone subnet command is used to determine to what zone the Communications Manager registers. If you enter a zone name in this field, it must match exactly with what is configured in the gatekeeper (this includes capitalization).

Geolocation Configuration

Step 50. The geolocation information can be used to determine the logical partition of a device. If you are using the geolocation feature, select the appropriate geolocation from the **Geolocation** drop-down list.

Step 51. There are 17 configurable geolocation fields. Geolocation filters enable you to choose which fields are used to create a geolocation identifier. If you use the geolocation feature, select the appropriate geolocation filter from the **Geolocation Filter** drop-down list.

Step 52. Click **Save**.

After the gatekeeper-controlled intercluster trunk is configured, you can add it to a route group. Then configure a pattern that matches calls that should be routed over this trunk. The pattern should point to a route list that contains the route group of which this trunk is a member.

Configuring CAC for a Centralized Deployment

To accomplish CAC for environments that have remote sites, locations are configured in Communications Manager. Locations define the amount of bandwidth that can be used to place calls to and from the remote sites. After locations are configured, they must be assigned to devices such as phones, trunks, and gateways. You can accomplish this by assigning them to a device pool. This process enables the phones, trunks, and gateways' device pool to determine the location. When a call is placed across the IP WAN, Communications Manager uses the location information to determine whether there is enough available bandwidth for the call. By deducting available bandwidth for each call that is active on the WAN, Communications Manager can determine availability. When using locations, Communications Manager assumes that the following bandwidth is required for each codec:

- A G.711 call uses 80 kbps.
- A G.722 call uses 80 kbps.
- A G.723 call uses 24 kbps.
- A G.728 call uses 16 kbps.
- A G.729 call uses 24 kbps.
- A GSM call uses 29 kbps.
- A wideband call uses 272 kbps.

To better understand locations, now look at the steps required to create and apply them.

Creating Locations

The following steps show how to create a location:

Step 1. From within CCMAdmin, select **System > Location**.

Step 2. Click the **Add New** link.

Step 3. A screen similar to that shown in Figure 5-14 displays. Enter the name of the location in the **Name** field.

Step 4. In the **Audio Bandwidth** field, enter the amount of bandwidth available for voice calls to and from this location. If you select the **Unlimited** radio button, no limit is placed on voice calls. To determine the value to enter here, take the bandwidth that Communications Manager used for each call based on the

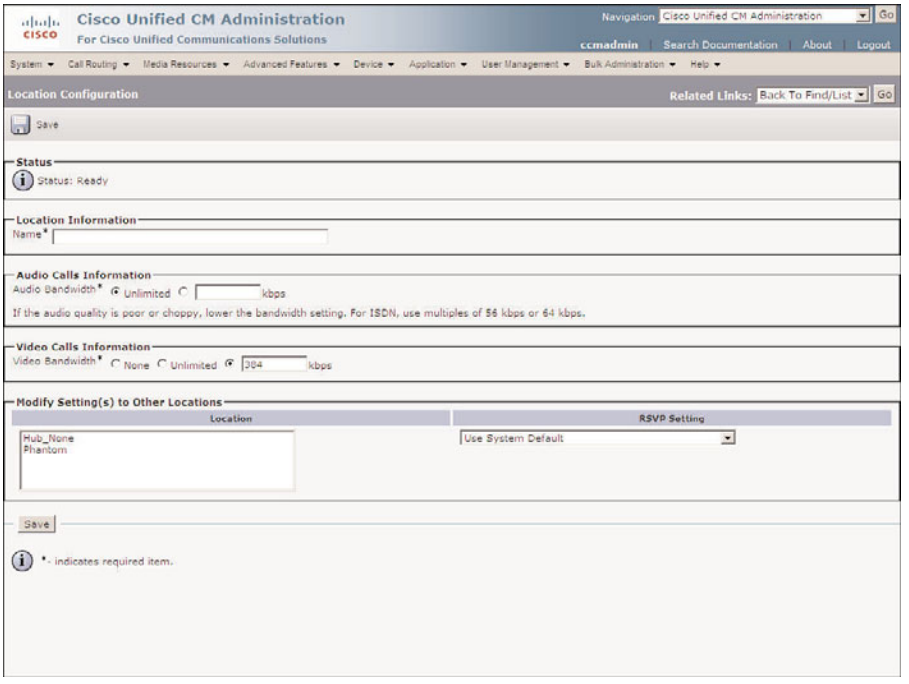


Figure 5-14 *Location Configuration*

codec that is being employed, and multiply it by the number of calls that you know can safely traverse the link. For example, if you use G.729 and you know that ten calls can traverse the link, multiply 24 kbps by 10. This tells you that 240 should be entered in this field. The bandwidth that Communications Manager assumes for each codec is listed earlier in this section.

Step 5. In the **Video Bandwidth** field, enter the amount of bandwidth available for video calls to and from this location. If you select the **Unlimited** radio button, no limit is placed on video calls. You can also select the **None** radio button, which prohibits video calls.

Note Video bandwidth is in increments of the video codec. If video codec is 384 and two video calls are allowed, the bandwidth should be set to 768.

Step 6. Resource Reservation Protocol (RSVP) can be used to reserve bandwidth for calls. The RSVP settings can be determined by highlighting a location in the Modify Setting(s) to Other Locations section and selecting the desired RSVP setting from the **RSVP Setting** drop-down list.

Step 7. Click the **Save**. The location has been added when the status line reads Insert Completed.

Assigning a Location to Devices

After locations are added, you must assign them to devices. As stated earlier, it is recommended that the location information be assigned to the device pool. The following steps show how to assign a location to a device pool:

Step 1. From within CCMAdmin, navigate to **System > Device Pool**.

Step 2. To limit the results, enter search criteria in the search field, and click **Find**.

Step 3. Select the device pool to which you want to assign a location from the list that is generated.

Step 4. Select a location from the **Location** drop-down list.

Step 5. Click **Save**.

Step 6. The device pool must be reset. Click **Reset**.

Step 7. A new window will appear; click **Reset** in the new window.

Step 8. Close the Device Reset window.

If you want to assign the location at the device level, follow these steps. The steps to add a location to a phone, trunk, or gateway are all similar. The following steps can be used to add a location to any of these devices:

Step 1. The path you select from within CCMAdmin depends on which type of device you are assigning a location. To assign a location to a phone, select **Device > Phone**. To assign a location to an ICT, select **Device > Trunk**. To assign a location to a gateway, select **Device > Gateway**.

Step 2. To limit the results, enter search criteria in the search field, and click **Find**.

Step 3. Select the device to which you want to assign a location from the list that is generated.

Step 4. If configuring an MGCP gateway, select the endpoint to which you want to assign a location. If you are not configuring an MGCP gateway, skip this step.

Step 5. The Device Configuration screen displays. Select a location from the **Location** drop-down list, as shown in Figure 5-15. Figure 5-15 shows a phone configuration screen, but the screen should be similar regardless of the device that you are configuring.

Step 6. Click **Save**.

Step 7. A window displays informing you that you must click the **Apply Config** button for the change to take affect. Click **OK**.

Step 8. Click **Apply Config**.

Step 9. A window displays warning you that when you apply the configuration, the device might go through a restart. Click **OK**.

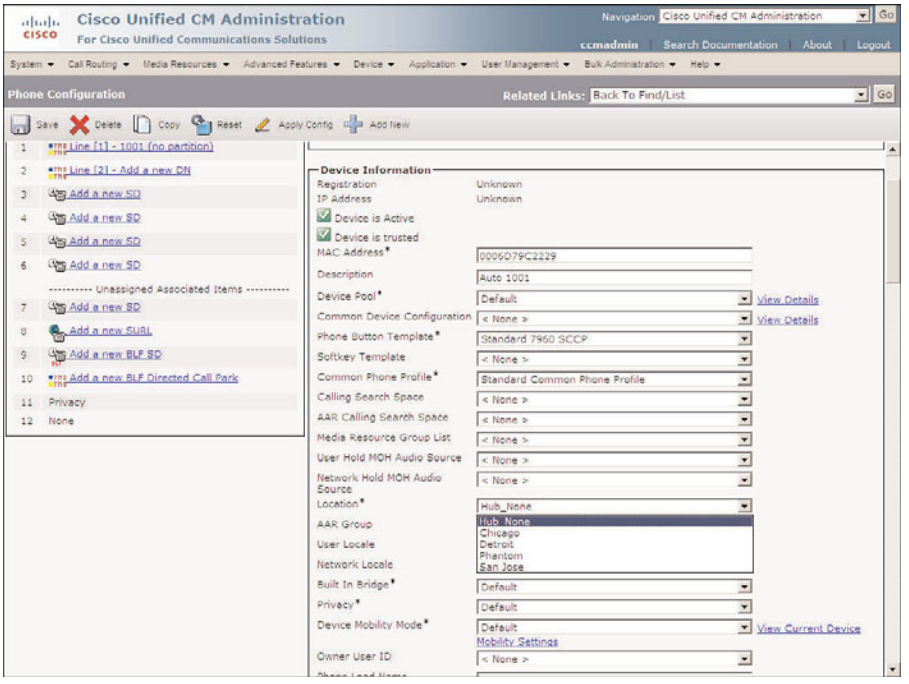


Figure 5-15 *Assigning a Location to a Device*

That's all there is to it. Unlike gatekeeper, no additional configuration is required outside of Communications Manager. Communications Manager handles all the CAC functions itself when locations are used for remote sites.

Special Services Configuration

There are certain types of calls that should always be given priority and availability to be dialed from all phones. The first call of this type is 911. When a 911 call is placed, it is important that the call gets through. Not only is it necessary to make the call possible, but you also need to ensure that it goes to the right destination. The following sections discuss some of the issues that can arise with these services.

Special Services Overview

Depending on your local service, various special services might be available. For example, the following is a list of special service numbers that are commonly available in North America. Check with your local phone company to see which of these are valid in your area.

- **311:** Nonemergency police services
- **411:** Directory assistance

- **511:** Travel information
- **611:** Phone equipment repair
- **711:** Telecommunications Device for the Deaf (TDD) operator
- **911:** Emergency

After you determine which services are available, you must configure route patterns that will match these calls. The most important of these calls is 911. Because in an emergency, a person might not think to dial 9 before dialing 911; patterns should be created that enable the call to go out regardless of whether 9 is dialed first. This means that two patterns need to be created, 911 and 9.911. PreDot discard instructions must be applied to the 9.911 pattern so that only 911 is sent out the public switched telephone network (PSTN).

When there are remote locations, things become a little more complicated. Imagine that you have an office in San Jose and a remote office in San Francisco. When callers dial 911 from San Francisco, the call must be routed to the local emergency service, not the service in San Jose. Although this seems obvious, it is sometimes overlooked. To accomplish this, multiple 911 and 9.911 patterns must be created. Partitions and CSS are used to allow phones in each location to match only the pattern that routes the call to the correct location.

For all other special services, the 9.X11 pattern should be sufficient. Once again, be sure to create patterns for each remote location so that the call is routed to the local PSTN.

Another concern when dealing with 911 calls is that some local legislation requires that more detailed location information be sent than just the street address. These laws normally apply to buildings that are over a certain size. Typically the floor and room number are required in addition to the street address. This requirement is referred to as an E911 or enhanced 911. Imagine that someone dialed 911 from a 20-story building and all that was sent was the street address. This would make it difficult to determine which floor, let alone which office, it came from. The solution is to have a database that contains the detailed address information for each phone number in your company. This database is typically maintained by an outside company and is accessible by the emergency service.

Another issue that arises with Communications Manager is that because a phone can be moved so easily, the information in the database can become outdated rather quickly. In addition to this, a feature known as extension mobility makes the Communications Manager system even more nomadic. To deal with these issues, Cisco offers an Emergency Responder product. This product ensures that the correct detailed information is sent when a 911 call is placed. For more details on this product, refer to the "Cisco Emergency Responder Administration Guide" on Cisco.com.

Configuring Special Services Route Patterns

To ensure that special services numbers are accessible, you must create route patterns for them. As mentioned previously, it is recommended that you create at least three patterns for each location. The first two are for 911 services and should be 911 and 9.911. If your

location does not use a leading 9 for PSTN access, the first 9 in the 9.911 pattern should be replaced with whatever number is used for PSTN access. The third pattern is 9.X11. This pattern will match all other special services numbers.

The 9.911 and 911 patterns should be marked Urgent Priority so that as soon as the number is dialed, it is sent. If this pattern is not marked Urgent Priority, delays could occur before the call is sent, and this should never happen.

As often happens, one solution creates another problem. I have heard people say that they do not use the 911 pattern because people often dial it by mistake. What happens is that a person dials 9 for an outside line, then presses one to begin a long distance call, and then mistakenly presses one again. This, of course, matches 911 and routes the call to emergency services. It is *never* recommended that you not include the 911 pattern. Although people misdialing 911 is problematic, it is gravely problematic if 911 cannot be dialed during an emergency. I have heard of many ways people have fixed this problem, but I would not recommend any of them because they all result in either the failure or delay of the call.

An overview of the tasks required to create patterns to allow access to special services numbers follows. Refer to Chapter 4, "Implementing a Route Plan," for detailed steps on how to create route patterns.

Step 1. Create a 911 route pattern.

Step 2. Assign a partition to this pattern that all phones in the location can dial. If there are remote locations, a separate pattern must be created and placed in a partition that only phones in that location can reach. This pattern must then point to a route list that will send the call out the local PSTN. Figure 5-16 shows an example of this.

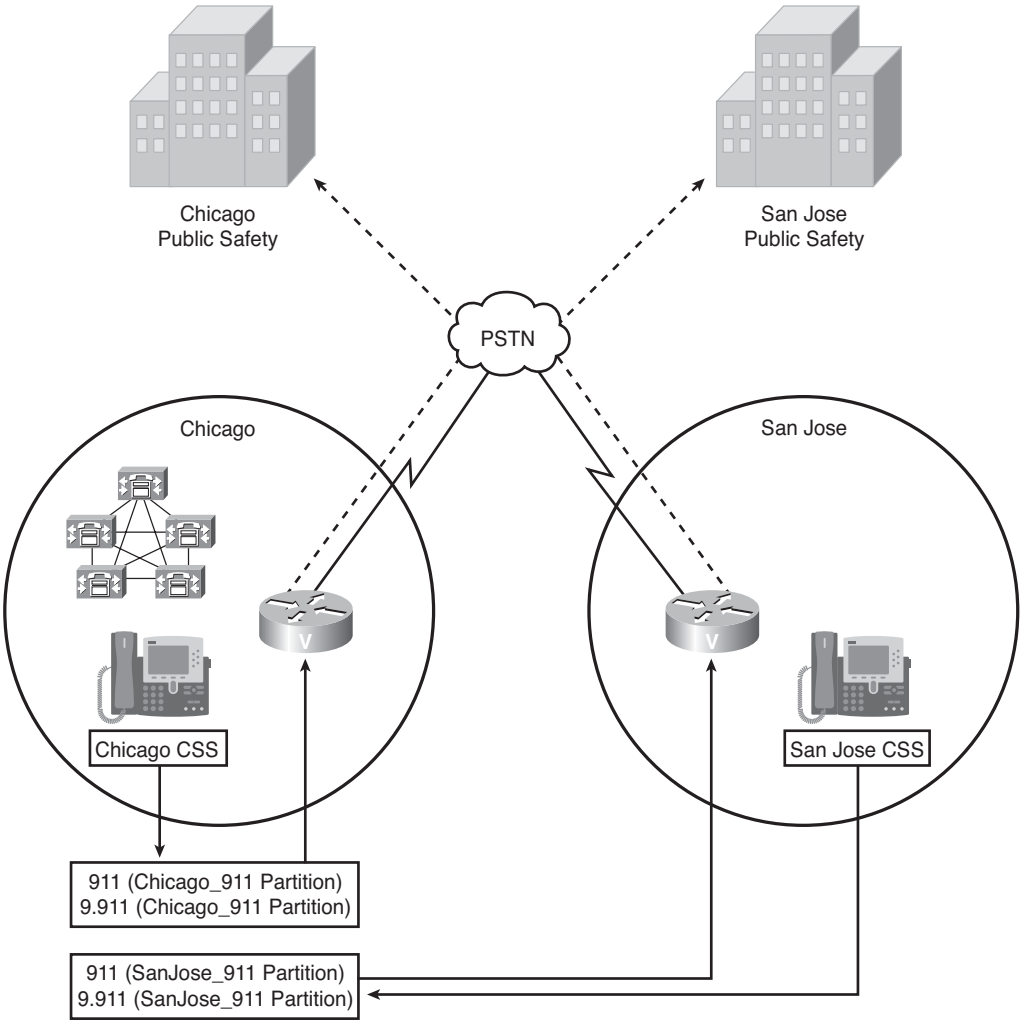


Figure 5-16 *Routing 911 Calls for Multiple Locations*

Warning When configuring 911 patterns in environments that include remote locations, it is imperative that you create a route plan that will send the call to the proper 911 operator. For example, if the Communications Manager cluster is in Chicago and a remote location is in San Jose, you must make certain that when a user in San Jose dials 911, the call reaches the San Jose 911 operator, not the Chicago 911 operator. The responsibility to ensure that this works properly is solely upon you. If you are uncertain how to properly implement this, you should seek additional help from an individual with proven experience in this field.

Step 3. Select a gateway or route list that will send this pattern out the local PSTN gateway.

Step 4. Select the Urgent Priority and OffNet Pattern (and Outside Dial Tone) check boxes.

Note Although it is not necessary to provide an outside dial tone for this pattern, if you do not, the outside dial tone will not be played for any number that begins with 9, until enough digits are dialed so that the number does not match 911. That means, in most cases, when dialing a long-distance number, the outside dial tone is not heard until three digits are dialed. For this reason, it is recommended that you select the OffNet Pattern (and Outside Dial Tone) check box.

Step 5. Create a 9.911 route pattern. If your location does not use a leading 9 for PSTN access, the first 9 in the 9.911 pattern should be replaced with whatever number is used for PSTN access.

Step 6. Assign a partition to this pattern that all phones in the location can dial. If there are remote locations, a separate pattern must be created and placed in a partition that only phones in that location can reach. The pattern must then point to a route list that will send the call out the local PSTN. Figure 5-16 shows an example of this.

Warning When configuring 9.911 patterns in environments that include remote locations, it is imperative that you properly create a route plan that will send the call to the proper 911 operator. For example, if the Communications Manager cluster is in Chicago and a remote location is in San Jose, you must make certain that when a user in San Jose dials 9.911, the call reaches the San Jose 911 operator, not the Chicago 911 operator. The responsibility to ensure that this works properly is solely upon you. If you are uncertain as to how to properly implement this, you should seek additional help from an individual with proven experience in this field.

Warning Special emergency call routing considerations must be made when deploying device mobility or extension mobility. Since device mobility and extension mobility allow the user to change physical locations you must ensure that the call will be routed based on the physical location of the user. The techniques used to ensure this are beyond the scope of this book. If you are unsure as to how this should be configured you should enlist the assistance of a experienced Cisco voice engineer. The responsibility to ensure all call routing, which includes emergency call routing, works properly is solely upon you.

Step 7. Select a gateway or route list that will send the pattern out the local PSTN gateway.

Step 8. Select the Urgent Priority and OffNet Pattern (and Outside Dial Tone) check boxes.

Step 9. Set the discard digits to PreDot.

Step 10. Create a 9.X11 route pattern.

Step 11. Assign a partition to the pattern that all phones in the location can dial. If there are remote locations, a separate pattern must be created and placed in a partition that only phones in that location can reach. The pattern must then point to a route list that can send the call out the local PSTN.

Step 12. Select a gateway or route list that will send the pattern out the local PSTN gateway.

Step 13. Set the discard digits to PreDot.

Step 14. Select the OffNet Pattern (and Outside Dial Tone) check box.

It is essential that after you have created patterns for these services, you make test calls to ensure that the call is routed properly. The steps provided previously are only general practices; additional configuration might be required. There is no guarantee that the previous steps will work in each situation. It is your responsibility to make sure that you test these services thoroughly before the system goes live.

Summary

This chapter explored how certain calls can be restricted by applying CSS and partitions to devices and patterns. Because it is often required that different devices have access to various destinations, the steps for creating and applying CSS and partitions are provided.

When deploying VoIP solutions, ensuring the quality of the call is essential. To accomplish this, CAC was discussed. Detailed steps were provided that show how to configure a gatekeeper that provides CAC for calls between clusters. Steps were also included to show how to configure locations for CAC, for calls to and from remote sites.

Finally, special services, such as 911, were discussed in this chapter. An overview of the required steps for the proper configuration of these services was given.

This page intentionally left blank

Index

A

AAR (Automated Alternate Routing), 187
  configuring, 290-292
access, granting to licensed features, 463-464
accessing
  Unity Administrator, 296-300
  Unity Connection administrative interface, 301-303
account policies (Unity), defining, 334-337
activating Communications Manager services, 42-43
AD (Active Directory), schema extensions, 569
adding
  gateways, 119-149
    H.323, 119-126
    ICTs, 143-149
    MGCP, 126-138
  holidays in Unity, 321-322
  phones
    autoregistration, 86-89
    with BAT, 106-118
    call forwarding settings, 102-103
    CAPF information, 96
    device information, 89-95
    directory numbers, 100-102
    extension information, 98
    external data locations, 97
    manually adding phones, 89
    MLPP information, 98
    Park Monitoring, 103
    with TAPS, 118-119
administration tools
  Unity, 600-608
  Unity Connection, 614-619

administrative rights, configuring Communications Manager, 627-631
Administrator parameters (Communications Manager), 52-53
advanced call-routing systems, 542-565
AMIS-a (Audio Messaging Interchange Specification-Analog)
networking, 577-578
subscribers, 31
annunciators, 16
configuring, 281-282
antivirus software, Windows OS, 36
assigning
audio source to MoH, 276
CSS
to gateways, 207-209
to lines, 206-207
to phones, 206
FACs to route patterns, 245-246
MRGLs
to device pools, 286
to phones, 285
partitions to patterns, 210
audio management tools (Unity), 608-609
audio sources, assigning to MoH, 276
audio text applications, configuring, 549-551
authentication rules (Unity Connection), configuring, 363-365
authentication settings (Unity), configuring, 331-332
auto-attendant
call flow architecture, 496-497
call handlers, 497-499
configuring, 540-542
autoregistration, 37, 86-89
availability, 15-16
five 9s, 2

B

basic call-routing systems, creating with call handlers, 500-527
BAT (Bulk Administration Tool), 616-618
phones, adding, 106-118
bridge networking, 580-581
brief menus (Unity/Connection), configuring, 487-488
building device pools, 72-74

C

CAC (Call Admission Control)
centralized deployments, configuring, 221-224
distributed deployments, configuring, 211-221
call flow, 152-154
architecture, 496-497
Unity, 25-26
Unity Connection, 25-26
call forwarding, 102-103, 187-189
call handlers, 26-29, 497-499
basic settings, configuring, 517-518
caller input, configuring, 510-512, 520-522
directory handlers, 28
greetings, configuring, 507-510, 522-525

interview call handlers, 27
Unity, configuring, 543-546
Unity Connection, configuring, 546-549
messages, configuring, 513-514, 525-527
owners, configuring, 526-527
profile settings, configuring, 502-506
remote management, 551-552
system call handlers, 27
transfer rules, configuring, 518-520
for Unity Connection, configuring, 514-516

call park numbers, configuring, 237-239

call pickup groups, configuring, 231-235

call queuing, configuring, 642-643

call routing
advanced call-routing systems, 542-565
configuring, 552-560

call screening, configuring, 643-644

call transfer, screening options, 466-467

caller input options
call handlers, configuring, 510-512
modifying, 469-473

calling privileges, 21-22

CAPF (Certificate Authority Proxy Function), 96

CCM Web Services parameters, Communications Manager, 59

CCMUser parameters (Communications Manager), 53-54

CDP (Cisco Discovery Protocol), support for in VoIP infrastructure, 4

CDR parameters, Communications Manager, 55

centralized deployment environments, configuring CAC, 221-224

Cisco Syslog Agent parameters, Communications Manager, 61

Cisco Unity Digital Networking, 571-577

class of control, 21

Cluster Domain Configuration parameter, Communications Manager, 60

CMBE (Communications Manager Business Edition), 10

CMCs (client matter codes), configuring, 246-248

common device configuration, Communications Manager, 66

Communications Manager, 7
administrative rights, configuring, 627-631
annunciators, configuring, 281-282
call park numbers, configuring, 237-239
call pickup groups, configuring, 231-235
CMC, configuring, 246-248
components, 8-10
publisher, 9
conference bridges, configuring, 276-278
deployment models
multisite WAN with centralized call processing, 17
multisite WAN with distributed call processing deployment model, 17-18
single-site, 17

device control, 9
device pools, 62-65
building, 72-74
devices, 10-16
common device configuration, 66
gatekeepers, 14-15
gateways, 12-13
media resources, 15-16
phones, 11-12
directed call park numbers, configuring, 239-240
DNS dependencies, removing, 48-50
enterprise parameters
Administrator parameters, 52-53
CCM Web Services parameters, 59
CCMUser parameters, 53-54
CDR parameters, 55
general parameters, 50-52
localization parameters, 55
Logical Partitioning Configuration parameters, 61-62
MLPP parameters, 55-56
phone URL parameters, 57-58
security parameters, 56-57
trace parameters, 59
user search parameters, 58
extension mobility, configuring, 265-272
FACs, configuring, 244-246
groups
creating, 66-69
date/time groups, 69-70
H.323 gateways, adding, 119-126
hunt lists, configuring, 635-642
ICTs, adding, 143-149
integration, verifying, 305-310
intercoms, configuring, 240-244
IP Phone services, configuring, 263-265
media resources, managing, 282-285
meet-me patterns, configuring, 235-237
MGCP gateways, adding, 126-138
MTPs, configuring, 279
phones
adding, 84-119
device settings, defining, 78-84
regions, configuring, 70-72
route plans, 18-22
call flow, 19-20
calling privileges, 21-22
wildcards, 20
security, 36-37
services, activating, 42-43
SRST, configuring, 287-290
time-of-day routing, configuring, 631-634
transcoders, configuring, 279-281
Unity Connection integration, verifying, 351-357
users, creating, 259-262
voice ports, configuring, 248-259
components
of Communications Manager
publisher, 9
components of Communications Manager, 8-10
conference bridges, configuring, 276-278
configuration settings, defining in Unity, 322-330
configuring
audio text applications, 549-551

auto-attendant, 540-542
brief menus (Unity/Connection), 487-488
CAC
for centralized deployments, 221-224
for distributed deployments, 211-221
call handlers, 502-506
basic settings, 517-518
caller input, 520-522
caller input settings, 510-512
greetings, 522-525
greetings settings, 507-510
message settings, 513-514
messages, 525-527
owners, 526-527
profile settings, 502-506
transfer rules, 518-520
for Unity Connection, 514-516
call routing, 552-560
call screening, 643-644
Communications Manager
AAR, 290-292
administrative rights, 627-631
annunciators, 281-282
call park numbers, 237-239
call pickup groups, 231-235
CMCs, 246-248
conference bridges, 276-278
directed call park numbers, 239-240
extension mobility, 265-272
FACs, 244-246
hunt lists, 635-642
intercoms, 240-244
IP Phone services, 263-265
meet-me patterns, 235-237
MTPs, 279
regions, 70-72
SRST, 287-290
time-of-day routing, 631-634
transcoders, 279-281
voice ports, 248-259
CTI route points, 183-191
directory handlers
for Unity, 528-534
for Unity Connection, 534-540
gatekeeper-controlled trunks, 215-217
gatekeepers, 213-215
hold options, 466-467
hunt lists, 252-253
hunt pilots, 253-256
message notification, 476-481
messages, playback, 489-493
MoH servers, 273-275
MWI, 256-258
route filters, 174-179
route groups, 157-158
route lists, 158-163
route patterns, 166-170
special services, 225-229
translation patterns, 179-183
Unity
authentication settings, 331-332
CoS, 337-347
networking, 571-577
ports, 332-334
restriction tables, 561-563

Unity Connection
authentication rules, 363-365
CoS, 368-371
dial plans, 372-375
interview call handlers, 543-546
message aging policy, 359-361
restriction tables, 366-367, 563-565
user search parameters, 488-489
voicemail pilots, 258-259

contacts (Unity Connection), 456-460

CoS (class of service), 21
changing for subscribers, 463
configuring, 337-347
Unity Connection, configuring, 368-371

creating
Communications Manager groups, 66-69
CSS, 202-205
CTI route points, 183-191
dial plans, 171-173
hunt pilots, 639-642
partitions, 202-205
PDLs, 349
private lists, 475-476
reliability in VoIP infrastructure, 5-7
route filters, 174-179
route groups, 157-158
route lists, 158-163
route patterns, 166-170
schedules
Unity, 318-322
vacation schedules, 644-647
subscriber templates, Unity subscribers, 381-414
templates, Unity Connection users, 420-450
translation patterns, 179-183
Unity Connection users, 451-454
Unity subscribers, 414-417
users, 259-262, 378

CRS Application parameters, Communications Manager, 60

CSS (Calling Search Spaces), 193-202
assigning
to gateways, 207-209
to lines, 206-207
to phones, 206
creating, 202-205
intercom CSS, creating, 241

CTI route points
creating, 183-191
lines, adding, 185-191

Custom Keypad Mapping tool (Unity Connection), 617-618

D

date/time groups (Communications Manager), defining, 69-70

defining
account policies in Unity, 334-337
configuration settings in Unity, 322-330
date/time groups (Communications Manager), 69-70
mailbox quotas (Unity Connection), 358-359
phone settings, 78-84

deployment models, Communications Manager
multisite WAN with centralized call processing, 17
multisite WAN with distributed call processing, 17-18
single-site, 17
destination call screening, configuring, 643-644
device control (Communications Manager), 9
device pools, 62-65
building, 72-74
MRGLs, assigning, 286
devices
Communications Manager, 10-16
common device configuration, 66
gatekeepers, 14-15
gateways, 12-13
media resources, 15-16
phones, 11-12
CSS, applying, 205-210
diagnostic tools (Unity), 609-612
dial plans
creating, 171-173
CTI route points
creating, 183-191
lines, adding, 185-191
route filters, creating, 174-179
translation patterns, creating, 179-183
Unity Connection, configuring, 372-375
digit manipulation, 154-157
configuring, 159-163
Digital Networking, 571-577
directed call park numbers, configuring, 239-240
directory handlers, 28, 527-540
for Unity, configuring, 528-534
for Unity Connection, configuring, 534-540
disabling greetings, 468-469
distributed deployment environments (CAC), configuring, 211-221
Domino subscribers, 30
DoS Protection parameter, Communications Manager, 60

E

enabling
call queuing, 642-643
greetings, 468-469
Live Reply feature, 474-475
enterprise parameters (Communications Manager)
Administrator parameters, 52-53
CCM Web Services parameters, 59
CCMUser parameters, 53-54
CDR parameters, 55
Communications Manager, 48-50
general parameters, 50-52
localization parameters, 55
Logical Partitioning Configuration parameters, 61-62
MLPP parameters, 55-56
phone URL parameters, 57-58
security parameters, 56-57
trace parameters, 59
user search parameters, 58
Exchange servers, subscribers, 30, 378

extension mobility, configuring, 265-272
extensions (subscribers), changing, 462
external data locations, adding phones, 97

F

FACs (forced authorization codes), configuring, 244-246
fields (device pools), 62-64
five 9s, 2

G

gatekeeper-controlled trunks, configuring, 215-217
gatekeepers, 14-15
configuring, 213-215
gateways, 12-13
adding, 119-149
CSS, assigning, 207-209
H.323, adding, 119-126
ICTs, adding, 143-149
interoperability gateway, 569-570
MGCP, adding, 126-138
general configuration settings (Unity Connection), 355-358
general parameters (Communications Manager), 50-52
Grammar Statistics tool (Unity Connection), 618
granting
access to licensed features, 463-464
system access rights, 465
greetings
call handlers, configuring, 507-510, 522-525
enabling, 468-469
maximum length of, changing, 467
groups (Communications Manager)
creating, 66-69
date/time groups, 69-70

H

H.323 gateways, adding, 119-126
hold options, configuring, 466-467
holidays, adding in Unity, 321-322
hunt lists
configuring, 252-253, 635-642
hunt pilots, creating, 639-642
hunt pilots, 252
configuring, 253-256
creating, 639-642

I-K

ICT (intercluster trunk), 13
adding, 143-149
IME (Intercompany Media Engine), 217
importing
Unity Connection users, 454-456
Unity subscribers, 417-420
infrastructure, 3-5
CPD support, 4
inline power, 4
voice VLANs, 4
VoIP
reliability, 5-7
voice gateways, 4-5

inline power, VoIP infrastructure, 4
intercoms
configuring, 240-244
CSS, creating, 241
partitions, creating, 241
Internet, subscribers, 31
interoperability gateway, 569-570
interview call handlers, 27
for Unity, configuring, 543-546
for Unity Connection, configuring, 546-549
IP Phone services, configuring, 263-265

L

licensed features, granting access to, 463-464
lines
adding to CTI route points, 185-191
CSS, assigning, 206-207
Live Reply feature, enabling, 474-475
localization parameters, Communications Manager, 55
locations, 568
Logical Partitioning Configuration parameters, Communications Manager, 61-62

M

mailbox quotas (Unity Connection), defining, 358-359
managing
media resources, 282-285
multilocation overlapping extensions, 648
PDL members, 350-351
user access, unlocking accounts, 460-461
manually adding phones, 89
maximum greeting length, changing, 467
MCS (media convergence server), 7
media resources, 15-16
meet-me patterns, configuring, 235-237
message aging policy (Unity Connection), configuring, 359-361
messages
call handlers, configuring, 513-514, 525-527
managing, 472-487
playback, configuring, 489-493
MGCP (Media Gateway Control Protocol), 12
gateways, adding, 126-138
MLPP parameters, Communications Manager, 55-56
modifying caller input options, 469-473
MoH (Music on Hold), 16
audio source, assigning to phones, 276
servers, configuring, 273-275
monitoring capabilities of Status Monitor (HTML), 588-591
MRGLs (media resource group lists), assigning
to device pools, 286
to phones, 285
MTPs (Media Termination Points), configuring, 279
multilocation overlapping extensions, managing, 648

multisite WAN with centralized call processing deployment model, 17
multisite WAN with distributed call processing deployment model, 17-18
MWI (Message Waiting Indicator), configuring, 256-258

N

navigating
Unity Administrator, 296-300
Unity Connection administrative interface, 301-303
networked subscribers, 378
networking
AMIS networking, 577-578
bridge networking, 580-581
Unity
components, 568-569
configuring, 571-577
VPIM, 585-586
Unity Connection, 581-582
Unity Connection-to-Unity, 583-585
Unity Connection-to-Unity Connection, 582-583
Unity-to-legacy voicemail networking, 570
Unity-to-Unity, 569-570
VPIM networking, 578-580

O

one-to-one redundancy, 9
owners (call handlers), configuring, 526-527

P-Q

parameters, Unity Connection users, 31-33
partitions, 193-202
assigning to patterns, 210
creating, 202-205
intercom partitions, creating, 241
passwords, resetting, 461-462
PBXs, verifying Unity integration
Communications Manager integration, 305-310
PIMG/TIMG integration, 315-317
SIP integration, 311-315
PDLs (public distribution lists)
creating, 349
member management, 350-351
phone URL parameters, Communications Manager, 57-58
phones, 11-12
adding
autoregistration, 86-89
with BAT, 106-118
call forwarding settings, 102-103
CAPF information, 96
device information, 89-95
directory numbers, 100-102
extension information, 98
external data locations, 97
manually adding phones, 89
MLPP information, 98
Park Monitoring, 103
with TAPS, 118-119
autoregistration, 37
CSS, assigning, 206
device settings, defining, 78-84
MRGLs, assigning, 285

playback of messages, configuring, 489-493
ports, configuring, 332-334
private lists, creating, 475-476
profile settings, configuring call handlers, 502-506
publisher (Communications Manager), 9

R

redundancy
one-to-one, 9
in VoIP infrastructure, 6-7
regions, configuring, 70-72
reliability in VoIP infrastructure, creating, 5-7
remote management, call handlers, 551-552
remote site failover
AAR, configuring, 290-292
SRST, configuring, 287-290
removing Communications Manager DNS dependencies, 48-50
reporting tools (Unity), 612-613
reports (Status Monitor), 592-593
subscriber reports, 593-595
system reports, 595-598
reports, Unity Connection, 619-625
resetting passwords, 461-462
restriction tables
for Unity, configuring, 561-563
for Unity Connection, configuring, 366-367, 563-565
roles (Unity Connection), 371-372
route filters, creating, 174-179
route groups, 19
creating, 157-158
digit manipulation, 154-157
route lists, 19
creating, 158-163
digit manipulation, 154-157
route patterns, 19, 163-173
creating, 166-170
FACs, assigning, 245-246
meet-me patterns, configuring, 235-237
special services, configuring, 225-229
wildcards, 165
dial plans, creating, 171-173
route plans, 18-22
call flow, 19-20, 152-154
calling privileges, 21-22
wildcards, 20

S

SA (System Administrator), accessing, 296-300
schedules
Unity
creating, 318-322
vacation schedules, 644-647
Unity Connection, creating, 361-363
schema extensions, 569
screening options, 466-467
security
authentication settings (Unity), configuring, 331-332
Communications Manager, 36-37
Unity, 38-39
Windows OS, antivirus software, 36

security parameters, Communications Manager, 56-57
servers (MoH), configuring, 273-275
services
Communications Manager, activating, 42-43
special services, 224-225
Show Dependencies tool (Unity Connection), 619
single-site deployment model, 17
SIP (Session Initiation Protocol), 12
integration, verifying, 311-315
SMTP Address Search tool (Unity Connection), 619
SMTP notification fields, 480
software architecture
Unity, 23-25
Unity Connection, 25
special services, 224-225
route patterns, configuring, 225-229
SRST (Survivable Remote Site Telephony), configuring, 287-290
Status Monitor (HTML)
monitoring capabilities, 588-591
reports, 592-593
subscriber reports, 593-595
system reports, 595-598
subscriber reports, 593-595
subscribers
AMIS-a, 31
CoS, changing, 463
Domino, 30
Exchange servers, 30
Exchange subscribers, 378
extension, changing, 462
Live Reply feature, enabling, 474-475
networked subscribers, 378
search parameters, configuring, 488-489
Unity, 30
creating, 414-417
importing, 417-420
templates, creating, 381-414
Unity/Connection, managing, 472-487
VPIM, 31
switch integration tools (Unity), 613-614
system access rights, granting, 465
system call handlers, 27
system reports (Status Monitor), 595-598

T

TAPS (Tool for Auto-registered Phone Support), adding phones, 118-119
Task Management tool (Unity Connection), 615
templates, 379-460
Unity Connection users, creating, 420-450
Unity subscribers, creating, 381-414
time-of-day routing, configuring Communications Manager, 631-634
TLS Handshake Timer parameter, Communications Manager, 60
trace parameters, Communications Manager, 59
transcoders, 16
configuring, 279-281

transfer rules, configuring call handlers, 518-520
translation patterns, creating, 179-183
trunks, gatekeeper-controlled, configuring, 215-217

U

Unity
account policies, defining, 334-337
administration tools, 600-608
audio management tools, 608-609
authentication settings, configuring, 331-332
call flow, 25-26
call handlers, 26-29
interview call handlers, configuring, 543-546
call queuing, enabling, 642-643
call screening, configuring, 643-644
configuration settings, defining, 322-330
CoS, configuring, 337-347
directory handlers, configuring, 528-534
holidays, adding, 321-322
meet-me conference manager, configuring, 647-648
networking
components, 568-569
configuring, 571-577
PDLs, creating, 349
ports, configuring, 332-334
reporting tools, 612-613
restriction tables, configuring, 561-563
schedules, creating, 318-322
security, 38-39
software architecture, 23-25
Status Monitor (HTML)
monitoring capabilities, 588-591
reports, 592-593
subscribers, 30
creating, 414-417
templates, creating, 381-414
supported networking, 33-35
switch integration tools, 613-614
Unity Administrator
accessing, 296-300
navigating, 296-300
Unity Connection
administration tools, 614-619
administrative interface, accessing, 301-303
authentication rules, configuring, 363-365
call flow, 25-26
call handlers, 26-29
configuring, 514-516
call queuing, enabling, 642-643
call screening, configuring, 643-644
CoS, configuring, 368-371
diagnostic tools, 609-612
dial plans, defining, 372-375
directory handlers, configuring, 534-540
general configuration settings, 355-358
integration, verifying for Communications Manager integration, 351-357
interview call handlers, configuring, 546-549

mailbox quotas, defining, 358-359
meet-me conference manager, configuring, 647-648
message aging policy, configuring, 359-361
messages
managing, 472-487
messages, managing, 472-487
networking, 581-582
reports, 619-625
restriction tables
configuring, 563-565
restriction tables, configuring, 366-367
roles, 371-372
schedules, creating, 361-363
software architecture, 25
subscribers, importing, 417-420
supported networking, 33-35
users, 29-30, 378
contacts, 456-460
creating, 451-454
importing, 454-456
parameters, 31-33
templates, creating, 420-450
VPIM networking, 585-586

Unity Connection-to-Unity Connection networking, 582-583

Unity Connection-to-Unity networking, 583-585

Unity-to-legacy voicemail networking, 570

Unity-to-Unity networking, 569-570

unlocking user accounts, 460-461

user management parameters, Communications Manager, 60

user search parameters, Communications Manager, 58

users
acounts, unlocking, 460-461
Communications Manager, creating, 259-262
creating, 378
passwords, resetting, 461-462
templates, 379-460
Unity Connection, 29-30, 378
contacts, 456-460
creating, 451-454
importing, 454-456
parameters, 31-33
templates, creating, 420-450

V

vacation schedules, creating, 644-647

VC (Voice Connector), 568-569

verifying
Unity Connection integration, Communications Manager integration, 351-357
Unity integration
Communications Manager integration, 305-310
PIMG/TIMG integration, 315-317
SIP integration, 311-315

voice gateways, VoIP infrastructure, 4-5

voice ports, configuring, 248-259

voice VLANs, VoIP infrastructure, 4

voicemail
Unity
call flow, 25-26
call handlers, 26-29
security, 38-39
software architecture, 23-25
subscribers, 30
supported networking, 33-35
Unity Connection
call flow, 25-26
call handlers, 26-29
software architecture, 25
supported networking, 33-35
user parameters, 31-33
users, 29-30
voicemail pilots, configuring, 258-259
VoIP
infrastructure, 3-5
VoIP infrastructure
CPD support, 4
inline power, 4
reliability, 5-7
voice gateways, 4-5
VPIM (Voice Profile for Internet Mail)
networking, 578-580
subscribers, 31
Unity networking, 585-586

W-Z

wildcards, 165
dial plans, creating, 171-173
Windows OS security, antivirus software, 36