IP COMMUNICATIONS

Cisco Unity Connection

ciscopress.com

David Schulz

www.it-ebooks.info

Cisco Unity Connection

David Schulz

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

www.it-ebooks.info

Cisco Unity Connection

David Schulz

Copyright © 2012 Cisco Systems, Inc.

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

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

Printed in the United States of America

First Printing June 2011

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

ISBN-13: 978-1-58714-281-9

ISBN-10: 1-58714-281-3

Warning and Disclaimer

This book is designed to provide information about Cisco Unity Connection. 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

www.it-ebooks.info

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Senior Development Editor: Christopher Cleveland

Project Editor: Seth Kerney

Editorial Assistant: Vanessa Evans

Book Designer: Louisa Adair

Cisco Representative: Erik Ullanderson

Cisco Press Program Manager: Anand Sundaram

Technical Editors: Alex Hannah, Toby Sauer

Copy Editor: Apostrophe Editing Services

Proofreader: Sheri Cain

Indexer: Heather McNeill

Composition: Mark Shirar

Cover Designer: Gary Adair

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0609R)

www.it-ebooks.info

About the Author

Dave Schulz has more than 27 years of experience with various technologies, ranging from routing and switching to security and voice technologies. Before joining Skyline Advanced Technology Services, he was involved in network engineering and consulting, project management, and oversight of engineering and maintenance activities for a reseller in the Midwest. Dave has also been involved in teaching various technologies to customers and engineers and creating various process and procedure methodologies, service pricing, and documentation. Dave has been involved with designing a Technical Assistance Center, while being a manager and director of professional services and performing installation, support, and consulting in various customer environments. He also had contracting responsibilities at a large global enterprise-level corporation, where duties varied from routing, switching, security, wireless, and project management.

Dave has three daughters, Amy, Ericka, and Tiffany, and resides in Cincinnati, Ohio, with his wife, Peggy.

Dave's current focus is in writing and developing courseware and teaching voice technology classes for Skyline Advanced Technology Services. He currently holds various Cisco certifications, including CCSI, CCNP-Voice, CCSP, and CCDP.

www.it-ebooks.info

About the Technical Reviewers

Alex Hannah (CCIE Voice #25853) is a Cisco Certified Systems Instructor, specializing in teaching the Cisco Advanced IP Communications product line. He has more than 7 years consulting experience in Cisco Unified Communications for SMB through Enterprise spaces. Alex is president of Hannah Technologies LLC, a Richmond, Virginia, based Cisco consulting firm specializing in Cisco Advanced IP Communications and application development using Microsoft technologies. He holds a bachelor's degree in information systems from Virginia Commonwealth University with a minor in business. Additionally Alex is the founder of UCCX.net, a video-based training website for the Cisco UC product line. In his spare time, you can find Alex on his boat wakeboarding with his family and friends.

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

Toby became a Cisco voice instructor in 2000. As the Communications Manager product continued to grow and develop, Toby 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. Toby teaches all the Cisco Standard Voice courses and many custom variations of these courses.

www.it-ebooks.info

Dedications

This book is dedicated to my wife, Peggy, whose support, love, and patience have truly made this possible. Peg, you are the best and the love of my life!

Acknowledgments

I would like to thank the following individuals that helped me through the various stages of this book and my career. Specifically, I would like to thank Toby Sauer, Wendell Odom, and Dave Bateman for their input, encouragement, help, support, and friendship.

Throughout my career, there have been many individuals that have had an impact on my life and career. I would like to acknowledge these individuals. A special thanks to Art Juarez, Tom Malkus, Kurt Loock, Ron Smith, and Pete Kurtz. Also I want to acknowledge my mom and dad who have since passed on but gave so much of their lives to me and others. I am extremely grateful and will always remember.

I would like to also acknowledge Brett Bartow, Chris Cleveland, and the editors for all their hard work and contributions to the final product.

www.it-ebooks.info

Contents at a Glance

Foreword xx

Introduction xxi

Chapter 1 Cisco Unity Connection Overview 1

Chapter 2 Designing Voicemail Systems with Cisco Unity Connection 13

Chapter 3 Installing and Upgrading Cisco Unity Connection 43

Chapter 4 Integrating Cisco Unity Connection 101

Chapter 5 Cisco Unity Connection Users and Contacts 157

Chapter 6 Providing Users Access to Voice Messaging 211

Chapter 7 Understanding User Features and Applications 255

Chapter 8 Understanding Call Handlers and System Features 319

Chapter 9 Understanding Cisco Unity Connection Networking 359

Chapter 10 Implementing Voice Profile for Internet Mail (VPIM) 417

Chapter 11 Using Cisco Unity Connection Tools and Reports 445

Chapter 12 Maintaining Cisco Unity Connection 487

Chapter 13 Advanced Features in Cisco Unity Connection 513

Chapter 14 Troubleshooting Cisco Unity Connection: Case Studies 535

Index 557

www.it-ebooks.info

Contents

Foreword xx
Introduction xxi

Chapter 1 Cisco Unity Connection Overview 1
Introduction to Cisco Unity Connection 2
Cisco Messaging Solutions 4
Cisco Unity Express 5
Cisco Unity 5
Cisco Unity Connection 5
Cisco Unified Messaging Gateway 6
Planning for Voice Messaging 6
Current Network Status and Design 7
Current Users and Requirement 8
Scalability 9
Redundancy 10
Feature Requirements 10
Summary 11
Case Study 12

Chapter 2 Designing Voicemail Systems with Cisco Unity Connection 13
Determining Server Sizing 14
Understanding Codecs and Voicemail Storage 15
G.711 Codec 16
G.729 Codec 16
G.722 Codec 16
G.726 Codec 17
iLBC 17
PCM Linear Codec 17
Transcoding in Cisco Unity Connection 17
Users, Codecs, and Message Storage Considerations 20
IMAP Clients and Voice Ports 21
Determining Voicemail Port Requirements 22
High-Availability and Redundancy 24
Server Sizing and Platform Overlays 25
Virtualization 26
User Location, Geography, and Digital Networking 27

www.it-ebooks.info

Case Study: Voicemail Design 27
Introduction to Integration 28
Introduction to Voicemail Networking 28
Intrasite Networking 29
Introduction to Intersite Networking 32
Intrasite Versus Intersite Networking 34
Case Study: Voicemail Network Design 35
Other Voicemail Networking Options 36
Case Study: VPIM Voicemail Design 36
Intersite Links and VPIM Networking 37
Case Study: Multisite Voicemail Design 38
Summary 40

Chapter 3 Installing and Upgrading Cisco Unity Connection 43
Cisco Unity Connection Installation Procedures 44
Installing Cisco Unity Connection Software 45
Pre-Installation Tasks 45
Cisco Unity Connection Software Installation 47
Installation Processes 47
Basic Installation 48
System Installer and Platform Checks 48
Product Deployment Selection 50
Platform Installation Wizard 52
Basic Installation Dialogue 54
Cisco Unity Connection Server Verification 71
Cisco Unity Connection Login Verification 73
Installation Log Files 76
Active-Active Cluster Pair Configuration 76
Publisher Installation 77
Subscriber Installation 77
Subscriber Server Installation 78
Subscriber Software Installation 81
First Node Configuration 81
Subscriber Node Installation Dialogue 81
First Node Access Configuration 83
Active-Active Cluster Pair Verification 83
Unattended Installation Using the Answer File 86

www.it-ebooks.info

Performing Software Updates 88
Upgrade During Install 89
Upgrade Using Cisco Unified OS Administration 91
Upgrades from Unity and Unity Connection 1.2 92
Virtual Installation Overview 92
Open Virtual Machine Format (OVA) Extension 93
Understanding Licensing in Cisco Unity Connection 94
Top-Level Software License 95
Server License 96
User License 96
HA License 96
Speech Connect 96
License Ordering Procedures 96
Case Study 98
Summary 99

Chapter 4 Integrating Cisco Unity Connection 101
Attributes of an Integration 103
Integration with Cisco Unified CM Overview 104
Integration with CME Overview 106
Integration with PIMG and TIMG Overview 106
Bandwidth Considerations Using PIMG and TIMG 109
Understanding Multiple Integrations 109
Messaging Deployment Models 110
Single-Site Messaging 110
Centralized Messaging 111
Distributed Deployment Model 112
Case Study: Messaging Deployment Design 113
Cisco Unity Connection Integration 114
Understanding Phone Systems, Port Groups, and Ports 114
Integrating with Cisco Unified CM 116
Cisco Unified CM Voicemail Configuration 116
Cisco Unity Connection Integration Configurations 128
Voicemail Integration Verification 135
Voicemail Port Verification 135
Voicemail Pilot and Profile Verification 136

www.it-ebooks.info

Integration Troubleshooting 136
SIP Integrations with Cisco Unified CM 140
SIP Trunk Configuration in Cisco Unified CM 140
Cisco Unity Connection SIP Integration 144
Integrating with Cisco Unified CM Express 145
Cisco Unified CME Integration Configuration 145
Integrating with Cisco PIMG/TIMG 151
Call Flow and Routing Rules 152
Understanding Direct and Forwarded Routing Rules 152
Case Study: Cisco Unity Connection Integration with Legacy Systems 154
Summary 155

Chapter 5 Cisco Unity Connection Users and Contacts 157
Introduction to Users and Contacts 158
Understanding Users and Contacts 159
Users Without Mailboxes 159
User With Mailboxes 159
Contacts 160
Default Users 160
Configuring Users 161
Authentication Rules 162
Schedules and Holidays 165
Class of Service 169
Templates 172
Configuring Users 176
Configuring Users Without Mailboxes 177
Configuring Users With Mailboxes 179
Roles 181
Bulk Administration Tool 183
LDAP Synchronization and Authentication 190
Case Study: Four-Digit to Six-Digit Phone Number Conversion 199
Administrative XML Integration with Cisco Unified CM 202
Case Study: Importing Users 205
Summary 208

www.it-ebooks.info

Chapter 6 Providing Users Access to Voice Messaging 211

Voice-Message Features and Applications Overview 212

Phone Access to Voice Messaging 213

Transfer Rules 214

Message Waiting Indicators 216

Alternate Extensions 219

Phone Menu Options 220

Message Settings Options 223

Web Application Access to Voice Messaging 226

Personal Communications Assistant 226

Using Really Simple Syndication (RSS) Feeds for Voice Messaging 233

Phone View and Visual Voicemail 238

Mobility and Unified Communications 250

Case Study: Mobility 252

Summary 252

Chapter 7 Understanding User Features and Applications 255

Understanding User Features 256

Message Storage Settings and Administration 256

System Configuration Directory 258

Mailbox Store 258

Mailbox Stores Membership 263

Voice-Message Directory 267

Creating Users in a Mailbox Stores 268

Message Aging Policy 268

Aging Alert Text 273

Message Recording Expiration 275

Mailbox Quotas 276

Case Study: Message Aging and Archiving 279

Greetings and Caller Input 280

Greetings 280

Caller Input 287

Case Study: Alternate Greetings 290

Post-Greeting Recordings 290

Message Notification 292

Alternative Extension Features and Restriction Tables 296

www.it-ebooks.info

Distribution Lists: System and Private 300
System Distribution Lists 300
Case Study: Configuring System Distribution List Access Lists 306
Private Distribution Lists 308
External Service Accounts 311
Unified Messaging Service 313
Using ViewMail for Outlook with Single Inbox 314
Configuring Single Inbox 314
User Configuration for Single Inbox 315
SMTP Proxy Addresses 316
Summary 317

Chapter 8 Understanding Call Handlers and System Features 319
Call Handler Components 320
Understanding System Call Handlers 321
Default System Call Handlers 321
Configuring Call Handlers 322
Transfer Rules 325
Greetings 325
Caller Input 328
Post Greeting Recordings 329
Message Settings 330
Call Handler Owners 331
Configuring New Call Handlers 332
Call Handler Templates 333
Understanding Directory Handlers 334
Understanding Interview Handlers 335
Configuring Interview Handlers 337
Building an Audiotext Application 339
Audiotext Application Design 339
Cisco Unity Connection Dial Plan Components 341
Partitions 341
Search Spaces 342
Case Study: Configuring The Dial Plan 344
Configuring Partitions 345
Configuring Search Spaces 346
Assigning Partitions to Search Spaces 346
Applying Partitions and Search Spaces 348

www.it-ebooks.info

Changing the Default Search Space and Partition 350
Removing Search Spaces and Partitions 350
Case Study: Troubleshooting Dial Plan Issues 354
Case Study: Configuring The Greeting Administrator 356
Summary 358

Chapter 9 Understanding Cisco Unity Connection Networking 359
Simple Mail Transfer Protocol 360
Cisco Unity Connection Networking 361
Locations, Sites, and Intrasite Links 362
Intersite Links and Cisco Voicemail Organization 363
Preparations for Networking Cisco Unity Connection Servers 365
Review the Current Network Design and Software 365
Ensure Connectivity Between Locations 365
Configure Display Names and SMTP Domains 365
Case Study: Configuring Display Names 367
Changing the SMTP Domain 367
Case Study: Configuring SMTP Domains 369
Cluster Management 371
Review the Naming Conventions of System Objects 373
Case Study: Managing Distribution Lists 375
Configuring Intrasite Links 377
Automatic Versus Manual 377
Networking Verification 385
Case Study: Performing Post-Networking Tasks (Dial Plan) 392
Voice Network Map 393
SMTP Smart Host Function and Configuration 397
Configuring Intersite Links 399
Interlocation Options and Features 401
Cross-Server Sign-In 403
Cross-Server Transfer 405
Cross-Server Live Reply 405
Cross-Server Feature Configuration 406
Case Study: Configuring Cross-Server Features 408
Configuring Users for Live Reply 410
Transfer Using Phone System Trunks 411
Other Post-Networking Considerations 414
Summary 415

www.it-ebooks.info

Chapter 10 Implementing Voice Profile for Internet Mail (VPIM) 417

Voice Profile for Internet Mail 418

Preparing for Configuring VPIM Networking 419

License Considerations 419

Determine the Number Scheme for Dial IDs 419

Determine the Dial Plan 419

VPIM Contact Creation 420

Blind Addressing 420

Distribution List Considerations 420

Domain Name Considerations 421

SMTP Smart Host and DNS Considerations 421

Networking and Connectivity Considerations 421

Configuring VPIM in Cisco Unity Connection 421

Case Study: Controlling Directory Synchronization 422

Configuring the SMTP Domain Name 422

Verify VPIM Licenses 425

Configuring VPIM Locations 425

Creating VPIM Contacts 429

Automatic Directory Updates 431

Automatic Directory Update Options 433

Case Study: Directory Updates and Blind Addressing 433

Blind Addressing Using Cisco Unity Connection Inbox 434

Automatically Create Contacts 435

Automatically Delete Contacts 437

VPIM Features 440

Case Study: VPIM Features 440

Summary 444

Chapter 11 Using Cisco Unity Connection Tools and Reports 445

Cisco Unity Connection Tools 446

Using the Real-Time Monitoring Tool 447

Accessing RTMT 447

System Summary 449

Server-CPU and Memory 451

Server-Process 451

Server-Disk Usage 451

Critical Services 453

Cisco Unified Serviceability 456

www.it-ebooks.info

Cisco Unity Connection Services—RTMT—Critical Services 457
Cisco Unity Connection Serviceability 459
Case Study 460
Performance 460
Tools 468
Cisco Object Backup and Restore Application Suite (COBRAS) 472
Cisco Unity Connection Migrate Utilities 477
Cisco Unity Connection Task Management Tool 478
Understanding Reports 479
Summary 484

Chapter 12 Maintaining Cisco Unity Connection 487
Disaster Recovery System 488
Certificate Management Overview 489
Performing a Backup 490
Backup Device Configuration 492
Backup Components 494
Case Study: Backing Up Mailbox Stores 496
Manual Backup 497
Backup Scheduler 499
Performing a Restore 501
Using the Restore Wizard 501
Warm Standby Server 503
Cluster Management 506
Overview of Survivable Remote Site Voicemail 508
Cisco Voice Technology Group Subscription Tool 509
Cisco Unity Connection Tools Online 509
Configuring Simple Network Management Protocol 509
Summary 512

Chapter 13 Advanced Features in Cisco Unity Connection 513
Fax Integration 514
Preparation for Fax Integration 515
Faxable Document Types and Fax Reports 515
Configuring Cisco Unity Connection Fax Integration 516
Cisco Unity Connection User Account Fax Configuration 518

www.it-ebooks.info

Fax Integration Testing and Verification 520
Gateway Configuration for Voice and Fax Integration 520
SpeechView 522
SpeechView Configuration 522
SpeechView Licensing 523
Smart Host Configuration for SpeechView 524
Access List Configuration the Email Server for SpeechView 525
Preparation for SpeechView Configuration 525
SpeechView Configuration in Cisco Unity Connection Administration 525
User Configuration for SpeechView 527
Configuring Notification 529
Configuring SMTP and SMS Notification 529
Summary 533

Chapter 14 Troubleshooting Cisco Unity Connection: Case Studies 535
Basic Troubleshooting Techniques 536
Stay the Course 537
Assess the Situation 537
Develop the Plan and Strategy 538
Use Good Troubleshooting Procedures 538
Provide Reporting, Resolution, Documentation, and Lessons Learned 539
Troubleshooting MWI Issues 539
Scenario 539
Resolution 540
Troubleshooting Call Transfer Rules 542
Scenario 542
Resolution 543
Troubleshooting Partitions and Search Scopes 545
Scenario 545
Resolution 545
Troubleshooting Dial Plan Issues in Digital Networks 547
Scenario 547
Resolution 547
Troubleshooting Access to Features 549
Scenario 549
Resolution 549

www.it-ebooks.info

Troubleshooting Audiotext Applications 550
Scenario 550
Resolution 550
Troubleshooting Digital Networking Issues 552
Scenario 552
Resolution 552
Troubleshooting VPIM Networking Issues 555
Scenario 555
Resolution 555
Summary 556

Index 557

www.it-ebooks.info

Icons Used in This Book

www.it-ebooks.info

Foreword

This book, *Cisco Unity Connection*, by Dave Schulz, hits the bull's-eye of its intended topic: Cisco Unity Connection. This book zeroes in on the target with clarity and depth. Anyone that uses or considers using the Cisco Unity Connection product needs a copy of this book to read when planning a deployment, administering the features, or troubleshooting problems. Simply put, it's the kind of desk reference you should have when working with Unity Connection.

Dave Schulz has a lot of experience with implementing networking solutions, managing groups that implement those same technologies, plus many years as an expert instructor of Cisco authorized Unified Communications courses. He brings this varied experience to bear in this new book that focuses on Cisco Unity Connection, from initial installation, integration with other products, administration, tools, and troubleshooting.

The Cisco Press imprint, under which this book is published, has a long and outstanding reputation as the best source for books and other content related to Cisco technologies and certifications. This and all others from Cisco Press have been developed through an agreement between Cisco and the publisher. As such, the Cisco Press series of books are the only Cisco-authorized books on Cisco technology.

Cisco Press publishes a variety of products across the spectrum of Cisco technologies, with much focus on the Unified Communications product line. The Cisco Press titles include topics such as Unified Communications Manager, Unified Communications Manager Express, Unity Express, QoS, Gateways and Gatekeepers, Telepresence, VoIP technologies and protocols, planning, troubleshooting, and other topics as well.

Dave is a good friend, wonderful instructor of voice topics, and now the primary author on a book related to voice technology. I hope you find his book both useful and enjoyable, and I hope to see more such titles from Dave in the future.

Wendell Odom
Certskills, LLC
December 2010

www.it-ebooks.info

Introduction

This book focuses on Cisco Unity Connection as a voice messaging solution. It is designed for both implementation engineers and administrators involved in the implementation, upgrade, or expansion of their voice-mail deployments. Through the text you explore the Cisco Unity Connection product, its design, implementation, and configuration. Even though you might be familiar with voice technology and networking systems, many of the terms and concepts used throughout the text are explained in depth, to facilitate this understanding.

For organizations at the beginning stages of designing, building, or migrating to Cisco Unity Connection, this text provides the necessary information required to make an informed decision on the proper design and configuration of their specific voice messaging solution. Throughout the book, you explore design considerations via specific case studies to assist you in understanding the architecture of a messaging solution in your organization.

Cumulatively, the chapters in this book provide a comprehensive guide to designing networks using Cisco Unity Connection and implementing and configuring the various features that users require. You learn about the new features of Cisco Unity Connection v8.5 software, along with a detailed approach for their configuration and application.

The organization of this book is designed into three parts. Part I begins with the design of Cisco Unity Connection, its operating system, database, and server requirements followed by configuration procedures on how to implement this in a Cisco Unified Communication Manager (CUCM) network and Cisco Unified Communications Manager Express (CME) network using the Session Initiation Protocol (SIP). Digital and Voice Profile for Internet Mail (VPIM) networking is discussed in detail, along with case studies to enforce your understanding of both technologies. For non-Cisco integrations, PBX IP Media Gateway (PIMG) and T1 IP Media Gateway (TIMG) integration is discussed. This section also includes a number of case studies and design considerations that need to be considered for users looking to implement Cisco Unity Connection. Specifically, Chapter 2 focuses on design and planning of the Cisco Unity Connection implementation. Finally, this part concludes with a discussion of upgrades in Cisco Unity Connection from previous versions of Cisco Unity Connection and Cisco Unity using the Cisco Objected Backup and Restore Application Suite (COBRAS).

Part II of this book focuses on the configuration of the various options in Cisco Unity Connection, such as users and contact, call routing, dial plan, class of service, and templates. This section also covers the various features and applications available to the users in Cisco Unity Connection, and the various methods in which they can access voicemail, such as Personal Communications Assistant, Internet Message Access Protocol (IMAP) clients, ViewMail, and PhoneView. This section covers the necessary knowledge and understanding a Cisco Unity Connection administrator should possess for maintaining and supporting users' needs and requirements. This section includes case studies to assist you in understanding the application of the various features and options learned in this section. Many of the new features released with version 8.5 software are also addressed throughout the text.

www.it-ebooks.info

Part III addresses the various tools and reports available to system engineers and administrators. This section also covers the ongoing troubleshooting and maintenance of Cisco Unity Connection. It is imperative for personnel involved in this product to understand the basics of troubleshooting the various issues that arise in the implementation and configuration phases. This section is a requirement for the engineers and administrators involved in the ongoing support of Cisco Unity Connection.

Goals and Methods

The goal of this book is that you get a comprehensive understanding of the Cisco Unity Connection product as a voice messaging solution and how it might better serve their organization, provide users with cohesive solution, and enable engineers and administrators to properly design, implement, and administer the Cisco Unity Connection system.

Who Should Read This Book?

This book is designed to provide an understanding of Cisco Unity Connection from planning, design, and implementation to maintenance of the voice messaging system. Network designers, engineers, and administrators can benefit from the explanations, examples, and case studies included in the text, which are meant to help direct you to possible issues and solutions that might be encountered in your organization.

How This Book Is Organized

This book is designed to be read from beginning to end and provides a complete understanding of the Cisco Unity Connection software. However, each chapter can be selected seperately enabling you to place your focus on the specific subject or element.

Chapter 1, "Cisco Unity Connection Overview" provides an overview of Cisco Unity Connection and its features and capabilities. This chapter also includes a description of the other various Cisco voice messaging product offerings and a descripiton of the Cisco Unity Connection database, operating system, and software components.

The core chapters, Chapters 2 through 13, cover the following topics, whereas Chapter 14 includes an overview of troubleshooting and discussion of various case studies:

Chapter 2, "Designing Voice-Mail Systems with Cisco Unity Connection": This chapter discusses the design considerations required before installing Cisco Unity Connection in today's business environments. This chapter addresses the voice-messaging design using the active-active cluster pair and single server configurations, designs, and considerations including server sizing, equipment, codecs, networking, features, and capabilities.

www.it-ebooks.info

Chapter 3, "Installing and Upgrading Cisco Unity Connection": This chapter examines the details of Cisco Unity Connnection software installation and upgrade procedures for various implementations, including single server and active-active cluster pair implementation. Also, this chapter discusses the various considerations for licensing and upgrade procedures.

Chapter 4, "Integrating Cisco Unity Connection": This chapter covers the various integration types between Cisco Unity Connection and the phone system. This chapter includes an explanation of the various protocols used, SCCP, and SIP and a detailed step-by-step explanation of the integration elements and procedures. You are also provided an understanding of the basic call flow for direct and forwarded calls to Cisco Unity Connection.

Chapter 5, "Cisco Unity Connection Users and Contacts": This chapter begins the administration section of the text, starting with an understanding of users and contacts in Cisco Unity Connection Administration. The discussion consists of the various means to create users through the use of Cisco Unity Connection Administration, Bulk Administration Tool, Administrative XML (AXL), and LDAP integration and authentication. This chapter also includes a step-by-step configuration of the various elements required to configure users and contacts.

Chapter 6, "Providing Users Access to Voice Messaging": This chapter examines the various methods that users can use to access their voice messaging using the phone interface and various web and mobile applications.

Chapter 7, "Understanding User Features and Applications": This chapter examines the various user features and application available and the various elements that control access to these features. Specific case studies increase your understanding of these features.

Chapter 8, "Understanding Call Handlers and System Features": This chapter explores the basic concepts and configuration of the various call handlers, directory handlers, interview handlers, and dial plan components, including partitions and search scopes. These concepts are discussed along with the configuration of a basic audiotext application.

Chapter 9, "Understanding Cisco Unity Connection Networking": This chapter examines the various components and configuration elements of networking Cisco Unity Connection servers and cluster pairs including intrasite and intersite links, trunks, and cross-server features. Also, included in this chapter is an overview of Simple Mail Transport Protocol (SMTP) parameters and SMTP Smart Host configuration in Cisco Unity Connection.

Chapter 10, "Implementing Voice Profile for Internet Mail (VPIM)": This chapter discusses the Voice Profile for Internet Mail (VPIM) protocol, design, licensing, configuration, and implementation parameters in Cisco Unity Connection. Included in this discussion is an exploration of the various features, addressing, and contact creation parameters.

Chapter 11, "Using Cisco Unity Connection Tools and Reports": This chapter covers the various tools and reports necessary to provide the proper administration tasks within Cisco Unity Connection. These tools consist of the Real-Time Monitoring Tool (RTMT), Cisco Object Backup and Restore Application Suite (COBRAS), Migrate Utilities, Task Management, and reports available in Cisco Unity Connection.

www.it-ebooks.info

Chapter 12, "Maintaining Cisco Unity Connection": This chapter covers the fundamental maintenace of Cisco Unity Connection and resources and tools required for this task. Also included in this chapter is a discussion of the provision for redundancy and backup including use of the Disaster Recovery System (DRS), Certificate Management, Licensing and Warm Standby Server, SNMP configuration, Survivable Remote Site Voicemail (SRSV), and various tools available on the Cisco website.

Chapter 13, "Advanced Features in Cisco Unity Connection": This chapter explores a few of the advanced features available in Cisco Unity Connection, which includes fax integration, SpeechView, and SMS notification.

Chapter 14, "Troubleshooting Cisco Unity Connection: Case Studies": This chapter is designed to provide an understanding of basic troubleshooting concepts and procedures and various case studies that you might encounter with Cisco Unity Connection voice messaging within the various deployments. This is the culmination of the knowledge learned within the various chapters in the text and geared to encourage you to think through specific issues.

www.it-ebooks.info

Chapter 1

Cisco Unity Connection Overview

This chapter covers the following subjects:

- **Cisco Unity Connection Overview:** Provides an overview of the Cisco Unity Connection product and its capabilities, features, and components.
- **Cisco Messaging Products:** Describe the various Cisco Unified messaging products and the comparison of these products to the current Cisco Unity Connection version 8.x product offering.
- **Cisco Unity Connection Software Overview:** Describes the Cisco Unity Connection database and operating system software components of Cisco Unity Connection version 8.x.

This chapter begins with an overview of the Cisco Unity Connection (CUC) messaging solution. Some of the features and distinguishing characteristics of the CUC product are explored, along with the various components. In this chapter, you can achieve the following:

- Gain a general understanding of the CUC product as a voice-messaging solution.
- Understand the various Cisco voice-messaging solutions.
- Understand the planning necessary to make a proper product choice for your organization's voice-messaging solution.
- Understand the foundations of the Cisco Unity Connection software and database design.

www.it-ebooks.info

Introduction to Cisco Unity Connection

Cisco Unity Connection (CUC) provides an integrated messaging solution for the enterprise-level businesses, offering many features required by business organizations. These features enable users to interact with their voicemail in the most practical way as defined by their job responsibilities. Users can retrieve voice messages by using their phone, voice recognition, mobility devices, or various client applications. Described as a feature-rich application, Cisco Unity Connection also provides a highly customizable audiotext application. With a flexible interface, administrators can easily design and configure an audiotext application to meet the needs of their specific organization.

Connection continues to be a highly scalable solution enabling the configuration of up to 20,000 users per server. If more users are required, you can also use digital networking to extend this limitation up to 100,000 users. In this case, you can network up to 10 servers or cluster pairs together to form a single cohesive voicemail network.

Cisco Unity Connection version 8.5 introduces Unified Messaging features enabling users to synchronize their voicemail with Exchange. This provides users with the appearance of a single inbox synchronized by Cisco Unity Connection.

As of version 7.x, Cisco Unity Connection enables an active-active cluster-pair design, which provides redundancy and scalability beyond a single server solution. Cluster pairs are explored in depth in later chapters. However, a cluster-pair enables for two servers to be paired together using a single database, to provide redundancy in case of server failure and to increase the number of ports to 500 under normal operation.

Also, Cisco Unity Connection supports the Voice Profile for Internet Mail (VPIM) protocol. VPIM is an industry-standard protocol defined in RFC 2423 (VPIM) and RFC 3801 (VPIM2) that you can use to network different voice-messaging platforms, such as Cisco Unity, or other disparate systems that support the VPIM protocol specification, such as Nortel or Avaya voicemail systems.

For organizations that require a smaller system, you can install Cisco Unity Connection as part of the Cisco Unified Communications Manager Business Edition solution. Business Edition combines Cisco Unified Communications Manager and Cisco Unity Connection into a single server solution with up to 500 phones, 500 voicemail users, and 24 voicemail ports. Designed for smaller businesses, this product does not enable redundancy and is limited in its scalability; however, the Business Edition can be a cost-effective and easy to administer voice-messaging solution, requiring only a single server.

Administrators currently using Cisco Unified Communications Manager (CUCM) systems can appreciate the design of the Cisco Unity Connection interface. Connection uses the same Linux-based operating system and IBM Informix database design employed by the CUCM product. Therefore, the interface is similar to what administrators already understand, enabling them to quickly adapt to the new system. Also, many of the tools and features in Cisco Unity Connection support the integrations with CUCM, such as PhoneView and Live Record.

www.it-ebooks.info

Along with these similarities, the administration interface in Cisco Unity Connection uses some of the same tools and configurations as those used to manage CUCM. For example, the Lightweight Directory Access Protocol (LDAP) configuration is configured similarly in both products, even though the database has some marked differences. The method used to create a backup and perform a restore is also the same, using the Disaster Recovery System (DRS) user interface. This capability aids in the ease of administration and maintenance of the system.

The database design of CUCM and Cisco Unity Connection uses the concept of active and inactive partitions. This feature affords the ability of engineers and administrators to upgrade easily to newer releases of software with minimum downtime. CUC also enables other tools to accomplish upgrades from Cisco Unity and Cisco Unity Connection 1.0 systems using the Cisco Objected Backup and Restore Application Suite (COBRAS). This tool works with Cisco Unity and some past releases of CUC to achieve an upgrade to the new Cisco Unity Connection v8.x software.

When using CUCM, the installer can quickly design and build an integration using either Session Initiation Protocol (SIP) or Skinny Client Control Protocol (SCCP). SCCP, or Skinny for short, is the lightweight client-server protocol currently used as the signaling protocol for most Cisco IP Phones. SCCP was originally created by Selsius Systems in the early 1990s, that designed and developed early IP telephony technology used in CUCM. Cisco acquired Selsius in the late 1990s. SCCP is now a proprietary protocol currently owned by Cisco.

The design of CUC enables multiple integrations to be created and maintained. This feature makes it easier for organizations to adopt a phase-in migration approach, without having to do a flash cut or forklift upgrade to the new system. The flash cut method of migration is defined as an immediate change from the older system to the new system without a phase-in approach.

A phase-in approach means that both systems, existing and new, coexist for a defined period of time. Users are then migrated (according to a schedule) to the new system using a phase-in approach. This can be done by department, location, or division. Issues that occur during the implementation phase can be addressed and resolved without affecting the entire company's voice-messaging systems. Also, there might be configuration parameters and details that need to be addressed that are specific to a certain department.

The decision as to whether to employ a flash cut or phase-in approach depends on the company. The phase-in approach is slower in the final deployment providing a more defined installation methodology and defined schedule. This approach provides for better management of existing systems, troubleshooting efforts, and problem resolution because only some users are migrated during each phase of the migration. The flash cut method, on the other hand, is a faster approach in the final deployment but provides the higher risk. Because all users are migrated to the new system, proper planning is imperative to ensure a successful deployment. Most companies will adopt the phase-in approach to minimize risks and system outages for existing systems. The phase-in approach provides for the coexistence of multiple systems. Users can be migrated as wanted to the new Cisco Unity Connection voice-messaging system according to a defined schedule.

www.it-ebooks.info

Many enterprise organizations require the coexistence of multiple integrations with different phone systems. This can be easily accomplished and maintained providing cohesiveness to users, who can send, reply, and forward messages regardless of the phone system used by the sender or receiver. In this case, both systems continue to operate and provide services to their respective users, as shown in Figure 1-1.

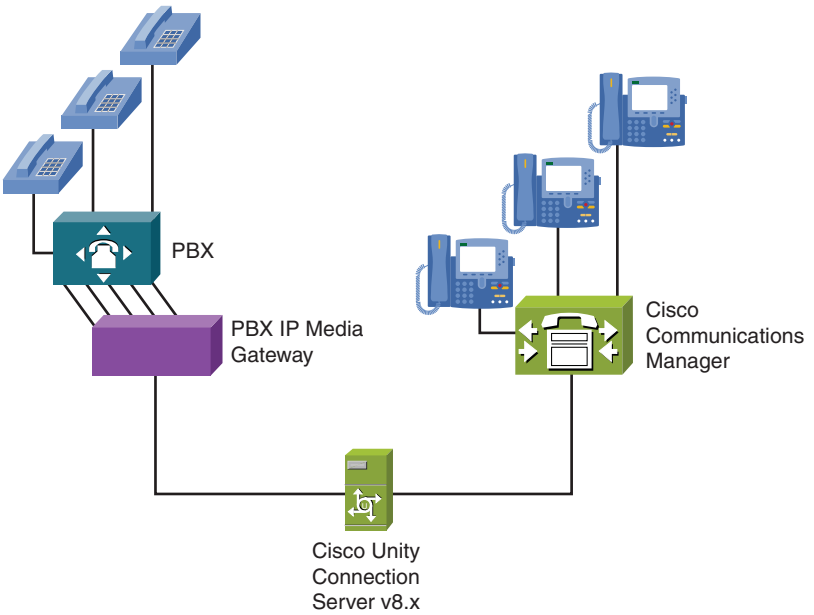

Figure 1-1 *Multiple Systems Integrated with Cisco Unity Connection*

The next section explores the various voice-messaging solutions available from Cisco and investigates their capabilities and features.

Cisco Messaging Solutions

Cisco provides a number of voice-messaging solutions with capabilities designed to meet the needs of any size organization. Cisco Unity Connection, being the newest product, began as a mid-range solution for small-and-medium businesses (SMB) and has since grown to meet the demands of large enterprise environments.

The current Cisco voice-messaging system offerings consist of the following products:

- Cisco Unity Express (CUE)
- Cisco Unity
- Cisco Unity Connection (CUC)
- Cisco Unified Messaging Gateway

www.it-ebooks.info

The following sections investigate these products from a higher level; however, the focus of the discussion is on Cisco Unity Connection.

Cisco Unity Express

Cisco Unity Express (CUE) is a router-based voicemail solution for the small-to-medium size branch office. CUE provides up to 500 mailboxes, 32 voice-messaging ports, and 600 hours of voicemail storage. Cisco Unified Communications Manager Express can be integrated with Cisco Unity Express on the Integrated Services Router (ISR) to provide a cost-effective, router-based voicemail solution for IP phones using a single platform. Cisco Unity Express gives users an affordable solution for small businesses or branch locations offering voicemail, fax, integrated voice response, and automated attendant features. CUE can also be integrated with the Cisco Voice Messaging Gateway. The Messaging Gateway enables users to send, forward, and reply to users on other CUE systems, creating a voice-messaging network between locations. For redundancy, Cisco Unity Express v8.x supports Cisco Unified Survivable Remote Site Voicemail (SRSV). This feature uses the Cisco Voice Messaging Gateway and Cisco Unity Connection version 8.x to provide redundancy for voicemail at the remote locations using Cisco Unity Express v8.x. Cisco Unified SRSV is discussed in Part III.

Cisco Unity

The Cisco Unity product was the first enterprise-level voice-messaging product offered by Cisco. The technology was originally acquired by Cisco from Active Voice in November 2000. Unity can integrate and unify messaging in both Exchange and Domino environments. Unity continues to be an enterprise-level product offering and is scalable up to 15,000 users and 200 ports per server. Redundancy is achieved through the use of a standby server configured for failover. Cisco Unity offers users many of the features required in a voice-messaging system including phone, client, and mobile access to voice messages. Cisco Unity supports both digital networking and VPIM to extend the capabilities of voice messaging beyond the limitations of a single server. Different from the other voice-messaging platforms, Unity is installed on a supported platform using the Microsoft operating system and having SQL as the data store, which is installed directly from the Unity installation media.

Cisco Unity Connection

Cisco Unity Connection is the first voice-messaging platform released by Cisco that uses the Linux Red Hat operating system using the IBM Informix database. In the earliest version of Cisco Unity Connection, the software was originally installed using the Microsoft Windows-based operating system (version 1.1 and 1.2) and supported a maximum of 1500 users and 72 ports, depending on the server model or type deployed. The first Linux-based version of Cisco Unity Connection (v2.0) supported up to 7500 users and up to 72 ports. Because these earlier versions did not provide any redundancy or

www.it-ebooks.info

failure, they were limited in their scalability. Therefore, the product was suited more to small-to-medium business environments.

Since the release of Cisco Unity Connection v7.x, however, Connection has proved itself to be an effective solution for enterprise-level businesses. Based on the Linux Red Hat Enterprise Linux version 4 operating system using IBM Informix database services, Cisco Unity Connection v8.x continues to qualify as a premier, feature-rich voice-messaging solution for the enterprise business environment.

Cisco Unified Messaging Gateway

The Cisco Unified Messaging Gateway product is a router-based solution that supports Cisco Unity Express, Cisco Unity, and Cisco Unity Connection. The Cisco Unified Messaging Gateway functions as a centralized gateway for voice messaging between various systems. Cisco Unified Messaging Gateway is highly scalable, supporting up to 500,000 users and 1000 messaging systems, consisting of Cisco Unity Express, Cisco Unity Connection, and Cisco Unity. The gateway also provides backup capabilities to the Cisco Unity Express branch office through the Cisco Unified SRSV feature. The features for the Cisco Unified Messaging Gateway include support for Voice Profile for Internet Mail (VPIM) with Cisco Unity Express, Cisco Unity Connection, Cisco Unity, and Avaya Interchange.

Now that you have a basic understanding of the various messaging products offered by Cisco, each organization must make an informed and calculated decision on its product choice for voice messaging, the design, and finally the implementation approach applied to the new voice-messaging solution. The next section investigates these choices by addressing the basics of planning and design for new voice-messaging systems and the various business considerations that need to be addressed.

Planning for Voice Messaging

Project management includes planning, design, implementation, and operate (PDIO) as a model for a successful project, as illustrated in Figure 1-2. Cisco has expanded this model to Plan, Prepare, Design, Implement, Operate, and Optimize (PPDIOO). This text is by no means meant to be an exhaustive study of project management and the PDIO and PPDIOO models; however, some mention and discussion of good planning, design, and project management is necessary. Good planning makes for a successful implementation and profitable companies. Poor planning, on the other hand, makes a good product look bad.

Just as an architect creates a well-researched, detailed plan for any building project, the voice-messaging design must proceed with thorough planning. This planning could proceed in many different forms; however, any form should begin with a high-level design that accounts for the following factors:

www.it-ebooks.info

- Current network status and design
- Current users and requirements
- Scalability
- Redundancy
- Feature requirements

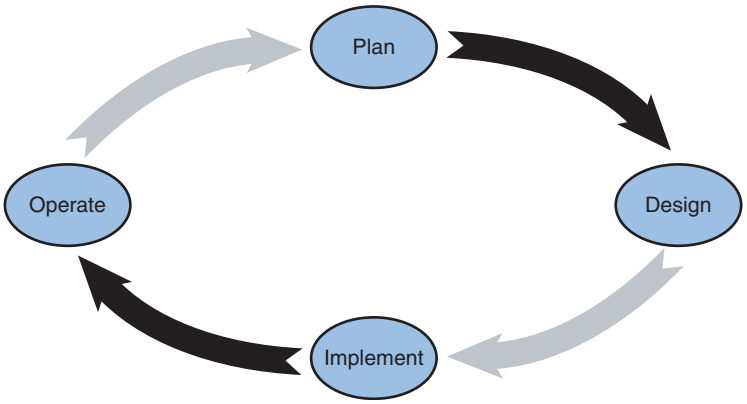

Figure 1-2 *PDIO Model*

This can simply be called *information gathering and research*. A well-documented and organized network might have most of this information readily available. Nevertheless, many organizations might be less prepared because of staffing, dynamic operations, and little or no change in management.

High-level design requires a number of design meetings that can vary from company to company and depend on the size of the organization. Larger enterprise organizations might require multiple meetings with department heads and managers to gain an understanding of the information required in this phase. The following discussion is a representation of a model for planning, not a rule. Each topic within this phase is different according to the size, type, and needs of each business. What is similar, however, is an understanding of your current network and future growth. Therefore, the questions asked might take on many different forms. Again, the following information is meant to act as a guide to your specific business plan.

Current Network Status and Design

Organizations that have an engineering staff that can perform network services and that is proactive with network assessment and monitoring might already be familiar with its current network performance. You can assemble this information from network diagrams, network management workstation logs, network analysis, and the like.

www.it-ebooks.info

In the past, I worked at a large, global enterprise company, where every project was planned, designed, and approved before any equipment was purchased or any configuration was completed. All configurations, right down to the last subnet and interface were discussed, detailed, and documented. Also, nothing in the network could be changed without the proper process and procedures for change management. No exceptions! This method of documentation and change management afforded accurate information. The services and support team appreciated this. When a user had an issue, the current configuration could be quickly located, and the resolution came quickly with little downtime. This occurred because troubleshooting was facilitated with good and accurate documentation.

Of course, these procedures create more work and increase the time involvement with each project; however, most projects stayed on track with few delays and fewer unforeseen circumstances when the project entered the configuration stage. This extra time spent in planning is well worth the effort to not only reduce delays, but to also avoid unexpected costs and eliminate *scope creep*, which occurs when something new is introduced to a project already underway or implemented—usually, something that was not thought about and addressed. This happens when those responsible for the planning and design make the statement, "I didn't think about that." All questions about the design should be addressed and answered during the planning and design phase. Scope creep happens when these questions occur after the implementation begins. The affect of scope creep creates delays, unexpected costs, and leaves management and users with a bad feeling about the project, the technology, and the outcome. Proper planning takes time, but it is necessary. A close friend of mine made the statement regarding poor planning. He said, "We never have time to do it right the first time, but always have time to do it over and over again."

In the early days of IP telephony, I worked at a company where the engineering staff was responsible for implementing a complete IP telephony and voice-messaging system for a large law firm. Designs were completed, equipment ordered, and configurations were done. The firm decided to make a few unexpected changes, which were allowed to proceed without further discussion. These changes caused the "I didn't think about that" syndrome. The implementation went to production and, eventually, the users experienced a number of problems and issues. This caused delays and some heated discussion with the firm. And you don't want to get on the bad side of a law firm. After a lot of time involvement from engineers and designers, they recovered from near disaster; however, the lessons learned were invaluable. If I could communicate one of the greatest lessons I learned in project management, it would be to never take shortcuts on planning and design.

The next section addresses some of the specific questions that need to be addressed about the new voice-messaging planning and design.

Current Users and Requirement

The first group of information to be gathered will be information about users and their requirements. This information should include more than just the quantity of users in the

www.it-ebooks.info

company, but their locations, functions, features, and expectations. The expectations focus on how they work and what tools and devices are required to access voice messaging. These expectations might vary from department to department, and even within any specific department. The expectations and features might also vary based on user functions and job responsibilities. The questions in this section can take the following form:

- What is the total number of users that require voice messaging?
- What are the total number of locations and number of users at each location?
- What is the current voice-messaging solution for these users?
- Are these users currently integrated on the same or different systems?
- Are these users required to have unified messaging or integrated messaging?
- How do users expect to get their voice messages? Phone, IMAP client, or Outlook client? Will voice recognition be required for any users?
- What features are required for users (beyond retrieving, forwarding, and replying to messages)?
- Must the new voice-messaging system closely match how users currently operate on the old system for ease of user adoptability?

Scalability

Scalability addresses current and future growth. This is a requirement for any dynamic, growing company that plans to upgrade or change to a new system. Corporations of any size don't like to hear that they need to replace equipment as their business expands. Cisco has engineered its products to be highly scalable. Even though the future cannot be predicted with 100 percent accuracy, there needs to be an element of forecasting in the planning equation. Decision making based on the predictive information can help the organization to make calculated decisions and planning for the voice-messaging design, server sizing, and product deployment. The following two factors need to be included:

- Geography and locations
- Number of users per location

Some questions that need to be addressed related to scalability follow:

- How many users (with voicemail) are currently deployed?
- How many users (with voicemail) will be projected to be added to the network?
- How many locations are currently deployed? What is the total number of voicemail users dispersed at each location?
- What is the projected growth in locations/sites to be deployed with voicemail users?

www.it-ebooks.info

Redundancy

The details included in the redundancy conversation might be solely business-model driven. What this boils down to is that certain types of businesses must experience little or no downtime. For example, this might entail businesses involved in healthcare and finance. In these cases, the redundancy of equipment and configuration must be factored into the design. This type of business must adopt a high availability model for networking, computing, telephony, and voice messaging.

Some businesses might not be required to use this same high availability in their businesses. This might be because of the type of business and extra cost involved with redundancy. However, if there is not going to be redundancy built into the network, the planning must include a network restoration plan. In other words, what procedures are taken if a system failure occurs? Some of the questions about redundancy that need to be discussed include the following:

- Does the company need to adopt a high availability model with no downtime?
- What is the current/planned network restoration/resolution procedure?
- Does the company plan to purchase extra equipment (spares) to be used if an outage occurs?
- What are the maintenance process and procedures that will be implemented?

Feature Requirements

The final area of discussion involves two items: current features required by users and future projected features. This might seem like a minor aspect of project planning but can prove to be vital in the final planning stage and the project outcome. Based on the features required by users, these issues might influence your overall product decision. Companies should not use a specific feature because users like something they saw on a website or it appears to be something they like. The decision to enable and configure specific features should be reached through discussion with management and business-driven requirements. The questions offered in this area can be lengthy; therefore, the following questions are definitely not exhaustive, and others should be added to this list as the business requirements demand. The questions asked about features should include the following:

- Are voice-=mail users going to be created manually, imported from another application, or synchronized with a third-party LDAP?
- How will users retrieve messages? Phone, Outlook, voice response, PhoneView, RSS, or mobile devices?
- What other features may be required?
    - Live Record
    - IMAP

www.it-ebooks.info

- Text-to-Speech
- Fax Integration
- SpeechView (transcription of messages)

Another area that you need to address involving feature requirements revolves around currently installed systems. Is another voicemail system going to continue in production, or is there another related company that is to be networked with this new system? The amount of networked users and contacts should be projected. Upcoming chapters cover digital networking and VPIM. This issue must be addressed when there are to be multiple voicemail systems involved in the equation. Therefore, some questions that need to be covered in this area include the following:

- Will the current voicemail system remain after the new system is installed? If so, do users need to send, reply, and forward messages between systems?
- What are other requirements that need to be addressed regarding third-party decisions, such as third-party firms, related divisions, or various branch offices?

All information must be assembled, researched, and discussed within the organization to address current and future needs for voice messaging. Again, good planning upfront can reap the benefits in the long run by allowing for a voice-messaging implementation that meets the current business requirements and fulfills future demands.

The next chapter focuses on the next stage of implementing a voice-messaging solution. In this stage, the project entails the delivery of designs based on the information assembled from the planning phase.

Summary

This chapter overviewed Cisco Unity Connection and various Cisco voice-messaging solutions. This discussion also included the planning required based on the current and future business needs of the organization. More precisely, you learned how

- Cisco Unity Connection features can provide voice messaging to up to 20,000 users per server.
- Cisco Unity Connection can use digital networking and VPIM to increase the number of voice-messaging users beyond the 20,000 user limitation.
- Cisco Unity Connection operates using the Linux operating system using the IBM Informix database for configuration and message storage.
- The various Cisco voice-messaging products, including Cisco Unity Express, Cisco Unity, Cisco Unity Connection, and Cisco Unified Messaging Gateway, each have different capabilities and limitations.
- Planning and design are key elements to address before deploying a new voice-messaging solution.

www.it-ebooks.info

- The planning phase helps the organization understand its current and future business requirements.

Case Study

Tiferam Corporation is in need of a new voice-messaging solution as it is at the point of outgrowing its existing legacy system. The headquarters is located in the Midwest, with two branch offices located in the same city. The company is unclear of the product deployment. Therefore, before making a product decision, a network designer was brought in to help define the requirements. The designer met with all the department heads within the organization and assembled the following information:

- Current requirements: 1200 users (with voicemail) with a projected growth to 2000.
- Location requirements: 1000 users at headquarters, with 100 users at each remote location. All projected growth (users) will be located at the headquarters location.
- Users will be required to have voicemail access at all times (high availability).
- Users will be using their phone and Outlook to retrieve voicemails.
- No other requirements are needed at this time.

Based on this information, the network designer was able to submit a preliminary design that would meet these current business requirements. This design included two Cisco Unity Connection servers configured as an active-active cluster pair to provide redundancy, scalability and the feature requirements desired. From these preliminary designs, a finalized design, scope of work, and implementation plan can be devised to meet Tiferam's business needs.

This company and others will be used as case studies throughout the text to assist in your understanding of the various concepts and features. These companies are purely fictitious and any resemblance to valid organizations is coincidental.

www.it-ebooks.info

Chapter 2

Designing Voicemail Systems with Cisco Unity Connection

This chapter covers the following subjects:

- **Design Considerations:** Understand the capability of Cisco Unity Connection as it pertains to current users, network design, codecs, voicemail ports, and projected growth.
- **Active-Active Cluster Pair:** Explore the high availability and redundancy feature of Cisco Unity Connection using the active-active cluster pair configuration.
- **Voice-Messaging Design:** Design the voice-messaging system using Cisco Unity Connection platform overlays by determining the proper server sizing, equipment, codec, feature, and capabilities.
- **Voice-Messaging Networking:** Understand the various networking options available in Cisco Unity Connection version 8.x software.

After you understand your current voice-messaging environment, users' needs, and projected growth within the planning stages, you can develop a preliminary design based on this information. This preliminary design can help the business to understand and review the designed solution that meets the needs defined during the planning stage. Good communication within the organization is vital for all stages of the deployment, but especially important for the design. After the preliminary design has been reviewed, modified, and adjusted according to the business model, you can develop the final design and scope of work.

This procedure must be completed before any product is ordered and the implementation begins. The planning and design phase determines the actual product and implementation, and ensures that the user requirements are met. As stated previously, good planning and design that closely matches the final implementation helps to avoid unforeseen project delays and over-budget issues.

www.it-ebooks.info

This chapter takes your project plan to the next phase of the Planning, Design, Implementation, and Operation (PDIO) model, the design phase. You need to collect all information assembled from the planning phase and determine a preliminary design. A properly crafted preliminary design can consist of input from reviewers, management, and users to allow for modifications and collaboration. The end result in this phase will be a final design that will be ready for implementation. Part of this phase also involves features, capabilities, and configurations to ensure that all requirements are met as determined according to the project plan. Therefore, you need to understand the interworking, features, and capabilities of Cisco Unity Connection.

The focus in this chapter is on the Cisco Unity Connection product design and capabilities as they pertain to its various systems, database, and networking. You need to understand the following:

- How to determine the server sizing to be used when implementing Cisco Unity Connection version 8.x software.
- Understand codecs, users, Internet Message Access Protocol (IMAP) client, voicemail storage, and ports. Explore how this information can influence your server sizing and voice-messaging design.
- Understand the various IMAP clients that can be used with Cisco Unity Connection and investigate the differences between IMAP non-Idle and Idle mode.
- Learn the Cisco Unity Connection database design and how active-active cluster pairs deliver redundancy and high availability.
- Determine the preliminary design based on geography, function, and client types to be used for voice messaging.
- Create a finalized design from the elements of the planning phase and the discussions and feedback from the design phase.

Determining Server Sizing

Cisco Unity Connection enables organizations to build and configure their voice-messaging system according to their business needs. These needs can involve the decisions based on the number of users, voicemail ports, codec, and even what type of clients will be used to retrieve voice messages. At this point in the process, many of these needs should have been identified and determined in the earlier planning phase.

The first goal is to determine the proper server sizing to meet the current user requirements and future growth. Server sizing refers to the proper platform hardware to be purchased. It is important for not only budgets, but also user requirements to purchase the correct server platform to meet the users' current and future requirements.

Scalability defines the capability of an organization to adapt to growth and changes. The voice-messaging design needs to include considerations for scalability in providing the required operations and services as the organization continues to grow and expand over time. Cisco Unity Connection enables this scalability with its current software and the

www.it-ebooks.info

capabilities provided with digital and Voice Profile for Internet Mail (VPIM) networking services.

You must identify a number of elements in this stage about the server sizing because these decisions can influence an organization's choice of hardware. These elements consist of the following:

- Audio codecs
- Voice-messaging storage capacity
- Voicemail ports
- Current and future users
- Voicemail users
- IMAP clients

The next sections review these requirements and the best practices related to server sizing.

Understanding Codecs and Voicemail Storage

You must understand the basic differences of the various codecs before understanding how Cisco Unity Connection handles these codecs. This discussion is not meant to be an in-depth study of codecs, but a general overview to provide a proper understanding of codecs as they are implemented in Cisco Unity Connection.

Codecs are defined as the encoding and decoding of the audio signal. An audio signal needs to be converted to a digital format before it can be sent over the IP network. This is referred to as *encoding*. This digitally encoded signal takes the form of a real-time transport protocol (RTP), which uses User Datagram Protocol (UDP) as the transport layer. Likewise, at the remote location, this encoded digital signal needs to be converted back into an audio stream. This process is called *decoding*. Together, the encoding and decoding determines the codec used to send an audio signal across the IP network.

The process of encoding an audio signal into a digital signal use is referred to as *sampling*. The sampling rate is determined by the amount of samples per second. Each sample is analogous to a snapshot in time. The accepted sampling rate was determined from work performed by Harry Nyquist and Claude Shannon in the 1920s surrounding the telegraph. Their research determined that the amount of information sent into a telegraph channel should be twice the amount of its highest frequency. In actuality, the theorem determines that a sampled analog signal can be correctly reconstructed if the sampling rate exceeds twice the highest frequency of the original signal. This theory referred to as Nyquist-Shannon Theorem, or simply Nyquist's sampling theorem. Since this time, the basic theory of telegraphs has been applied to digital networking.

The human voice can produce sound from approximately 300 Hz to 4000 Hz. Keeping with the same logic that Nyquist used for the telegraph, you can determine a sampling rate for voice communications to be 8000 Hz (4000 Hz * 2), or 8000 samples per second.

www.it-ebooks.info

Each sample would consist of a single byte. Therefore, the information consisting of this sample would be 8 bits * 8000 samples, or 64,000 bits per second. This is the basis for an uncompressed digitized audio signal in IP telephony, which is called the G.711 codec. This is also the calculation used for a DS-0 or voice channel within a T1/PRI digital circuit. This bandwidth is defined as the payload, not including Layer 2 and Layer 3 overhead. This overhead on an Ethernet network accounts for approximately 25 percent of the overhead of an uncompressed voice payload, or 16 k (or 80 k). This includes IP, RTP, and UDP headers.

Cisco Unity Connection supports a number of different codecs, as described in the following sections.

G.711 Codec

The G.711 codec is the most used and supported codec in IP telephony. It is produced using pulse code modulation at an uncompressed sampling rate of 8000 samples per second. The bandwidth required for the G.711 codec is 64,000 bits per second. This is the bandwidth of the payload (not including IP, RTP, and UDP headers). As stated in the previous section, on an Ethernet network, this accounts for approximately 25 percent of the overhead of an uncompressed voice payload, or 16 k (or 80 k).

There are two versions or formats of the G.711 codec. G.711 µ-Law is the codec used in North America. The G.711 a-Law is used outside North America. Even though both codecs have the same bit rate of 64,000 bits per second, they perform a completely different sampling of pulse code modulation to arrive at their respective digitized samples. Therefore, the codecs are not directly compatible and require transcoding between G.711 µ-Law and G.711 a-Law. However, both of these codecs produce a high-quality audio steam.

G.729 Codec

The G.729 codec is also used extensively in IP telephony and also widely supported. This codec uses a compression algorithm to attain a payload bandwidth of 8000 bits per second. Because of bandwidth conservation, this codec is used for remote IP telephony communications and where bandwidth oversubscription is a concern. A number of versions of the G.729 codec exist. Two of these codecs, G.729a and G.729b, incorporate additional options and features. The sound quality produced using G.729 is not as high quality as G.711 but is still considered to be toll quality (similar to a residential phone service or traditional landline services). These lower bandwidth codecs are used primarily to save the bandwidth for lower speed WAN circuits. In these cases, the overhead calculation is still approximately 16 k, providing a total bandwidth calculation of 24 k.

G.722 Codec

The G.722 codec produces is a high quality audio signal and is supported on many of the newer IP telephony devices and IP phones. G.722 uses its own compression algorithm called Sub-Band Adaptive Differential Pulse Code Modulation (SB-ADPCM) and can

www.it-ebooks.info

produce a digital signal using a number of bandwidths (48 k, 56 k, and 64 k). The G.722 codec requires 64,000 bits per second as the payload bandwidth for this codec; although it can adapt the compression algorithm based on changes in the network. This codec is used with the newer Cisco 79X2 and 79X5 IP Phones.

G.726 Codec

The G.726 codec uses Adaptive Differential Pulse Code Modulation (ADPCM) to produce a payload bandwidth of 16 k, 24 k, 32 k, or 40 k bits per second, although the most widely supported codec used is 32 kbps. Using half the bandwidth of G.711, this codec is used for many phone service providers, VPIM networking, and Simple Mail Transfer Protocol (SMTP) communications. You examine the use of this codec in Chapter 5, "Cisco Unity Connection Users and Contacts," in the discussion of VPIM and SMTP protocols.

iLBC

Internet Low Bitrate Codec (iLBC) is defined in RFC 3951 as a narrowband speech codec, suitable for Voip application and streaming audio. This algorithm used for iLBC is much more resilient to the lost frames when degraded networks are encountered. iLBC uses a bandwidth of 13.3kbps, with a slightly higher quality than G.729.

PCM Linear Codec

The PCM Linear codec uses pulse code modulation (PCM) to digitize samples based on a variable sampling rate of 8 k to 48 k. This format is used in DVD technology to encode WAV and AU type sound files because this codec produces the highest quality audio; however, this quality is produced as the expense of increased bandwidth. For example, a sampling rate of 8 k for a 16-bit samples requires 128 kbps for the payload bandwidth (16 bits * 8000 samples / sec = 128 kbps).

Transcoding in Cisco Unity Connection

Voice calls arriving to Cisco Unity Connection enter the system using a negotiated line codec. The administrator can choose to support a certain codec based on its advertisement.

When callers leaves message for users with a mailbox, they reach Cisco Unity Connection via an available voicemail port. The audio stream is received as a digitized signal in one codec (called the line codec). This digitized signal needs to be converted before it is recorded to the users' voice mail. *Transcoding* is the process to convert a digitized signal from one codec to another codec. Cisco Unity Connection performs transcoding with every call as it is received and recorded in the users' voice mailbox.

Cisco Unity Connection supports a number of codecs on the line side. These codecs are used on the line side, as the digitized signal is received by Cisco Unity Connection. Also,

www.it-ebooks.info

as stated previously, the administrator can influence which codecs are used, or not used, by changing the advertising of these codecs to external devices. The codecs supported on the line side follows:

- G.711 µ-Law
- G.711 a-Law
- G.722
- G.729
- iLBC

The audio stream received on one of these line codecs is then transcoded to the system codec, which is always PCM Linear. As per the discussion of codecs, this codec produces the highest quality audio and is therefore the system codec. The system codec cannot be changed and is always used with every call and recording. The system codec receives the call from the line codec. The recording codec receives the call from the system coded (PCM Linear).

Finally, the PCM Linear stream (system codec) is then transcoded to the system recording codec. The supported system recording codecs in Cisco Unity Connection follows:

- PCM Linear
- G.711 µ-Law (default)
- G.711 a-Law
- G.729a
- G.726
- GSM 6.10

The default recording codec is G.711 µ-Law. It is advisable to keep the system recording codec at this default because this produces a good quality audio signal with acceptable disk space utilization (8 KB/sec).

All transcoding here is done directly within the Cisco Unity Connection system. If calls and recorded messages are transferred to the integrated phone system or Cisco Unity Connection, transcoding resources might be required.

Figure 2-1 illustrates the relationship between the line, system, and recording codec as they are implemented in Cisco Unity Connection.

www.it-ebooks.info

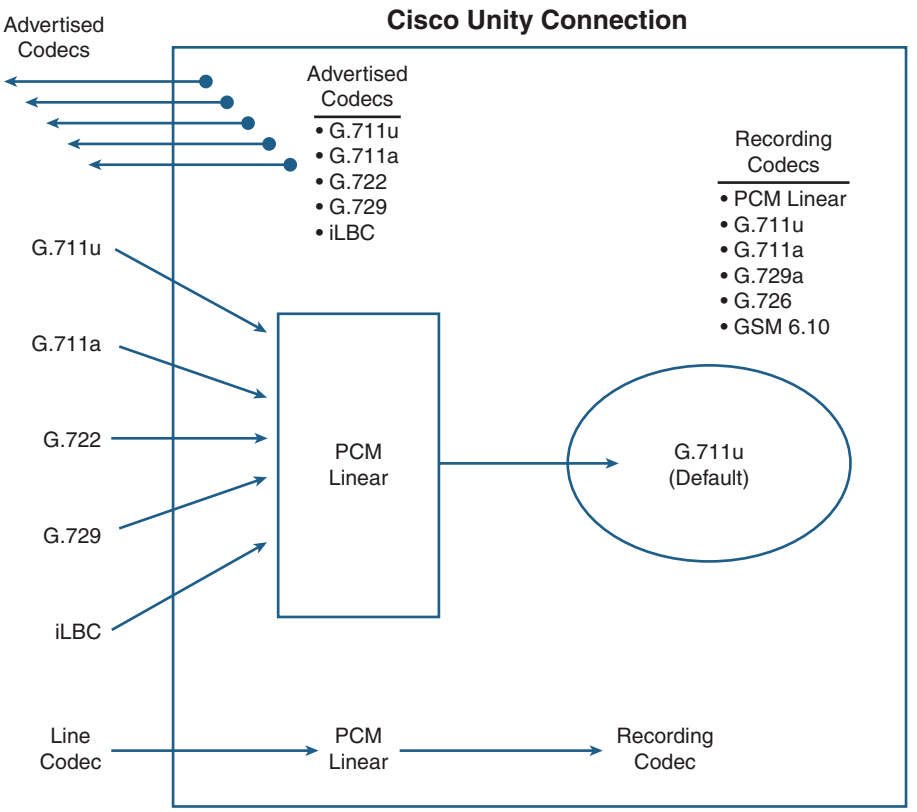

Figure 2-1 *Codec Implementation in Cisco Unity Connection*

The System recording codec can be changed to G.729a, G.726, or GSM 6.10 to conserve disk space for message storage. These codecs require from 1 KB/sec to 4 KB/sec, half the amount of disk space required for the same recording using the default system recording codec of G.711. However, the audio quality produced with these codecs will be much lower. Changing the system recording codec to one of these codecs should be done only if there is a real need to conserve disk space. You must understand and decide if this should be done to sacrifice recording quality. Also, changing the default system recording codec can affect playback of messages on specific mobile devices and cell phones that might not support the specific codec using IMAP.

On the other hand, you can use the PCM Linear codec for the system recording codec to increase the audio quality. This codec produces the highest quality of audio stream, but at the expense of disk space. The PCM Linear codec uses twice the bandwidth required by the G.711 default recording codec. This should be done only if there is no consideration to conserve disk spaces, and when G.722 is used as the line codec. Using PCM Linear as the system recording codec when the line codec is G.711 cannot increase the quality of the audio stream and only use more disk space. For most installations, Cisco

www.it-ebooks.info

Unity Connection uses G.711 as the line codec. Therefore, it is best to leave the system recording codec at the default, G.711.

You need to keep the system level recording at G.711 because most endpoints use this codec as their audio format to Cisco Unity Connection. This determination is made only to preserve the audio quality, not avoid transcoding. As Figure 2-1 illustrates, transcoding is done for every call received by Cisco Unity Connection. There is little system performance impact from a different codec on the line, as compared to using a specific recording codec. Certain codecs do require additional resources and computation because of their complexity. The codecs defined here that require more resources to transcode are the line codecs, G.722 and iLBC. Limit the use of these codecs for this reason. Because of these resource requirements, Cisco Unity Connection can support only half the amount of simultaneous connections using these line codecs, as compared with the other line codecs. You must consider this calculation when determining the platform sizing and the number of voicemail ports.

Table 2-1 provides an overview of the various codecs supported by Cisco Unity Connection for their audio quality, sample size, bandwidth, and disk space using an 8 kHz/sec sampling rate.

Table 2-1 *Recording Codecs Relationship and Limitations (Based on 8 KHz/sec Sampling Rate)*

Recording Codec	Characteristics
PCM Linear	Excellent Audio Quality Requires 16 KB/sec disk space 16 bit samples * Used for system codec
G.711 u-Law * G.711 a-Law	Good Audio Quality Requires 8 KB/sec disk space 8 bit samples * Default Recording Codec
G.726	Good Audio Quality Requires 4 KB/sec disk space 16 bit samples
G.729a	Fair Audio Quality (Toll Quality) Requires 1 KB/sec disk space
GSM 6.10	Good Audio Quality Requires 1.6 KB/sec disk space

Users, Codecs, and Message Storage Considerations

Now that you understand the implications of the codecs as they apply to system performance, audio quality, and disk storage space, you must use this information along with the current and future projected users to determine the server sizing. The message storage

www.it-ebooks.info

is designed to handle between 20 minutes to 30 minutes of message storage (using the G.711 system recording codec) for each user configured according to the supported message platform. In most cases, this might be more than sufficient for most organizations. You need to consider emails sent to the users' voice mailbox for replies, forwards, and faxes in the message storage calculation.

The server sizing should be based on projected growth of users to ensure scalability; the codecs to be used; and the total amount of voice mails, replies, forwards, and faxes that need to be available per user. If this is a new installation, it would be advisable to investigate the current voice message stores to gain a benchmark to determine the Cisco Unity Connection server sizing for the message stores.

Finally, you must also understand the clients that might be used to retrieve voice messages and emails because this might influence the number of users supported. The type of clients supported in Cisco Unity Connection can be any of the following types:

- Telephone user interface (phone users)
- Voice user interface (voice recognition users)
- IMAP clients
- Messaging inbox clients using Personal Communications Assistant (PCA)
- IBM Lotus Sametime clients
- RSS reader clients

IMAP Clients and Voice Ports

Cisco has made some marked improvements in the latest 8.x software release of Cisco Unity Connection for its handling of IMAP clients. If users are using clients that support IMAP Idle, there is no increased impact on the load to Cisco Unity Connection. This was not the case in previous versions; however, the clients must be IMAP Idle-mode instead of non-Idle. IMAP Idle is defined as the ability of the client to indicate to the server that is ready to accept messages, without having to click a refresh button or repeatedly make requests to the server. In this case, the same amount of users and ports are supported, whether the users use their phone or IMAP Idle clients. Most IMAP clients support Idle-mode, with a few exceptions.

The Internet Message Access Protocol (IMAP), formerly called Internet Mail Access Protocol, supports both online (non-Idle) and offline (Idle) modes. The mode used depends entirely on the specific client. Cisco Unity Connection supports both non-Idle and Idle-mode clients. However, non-Idle-mode places a significant load on the server and the number of total clients supported is reduced significantly. A single non-Idle IMAP client is counted as four Idle IMAP clients.

www.it-ebooks.info

The products that support the IMAP Idle-mode consist of the following:

- Microsoft Outlook
- Microsoft Outlook Express
- Microsoft Windows Mail
- Lotus Notes
- Cisco Unified Personal Communicator (CUPC) version 8.x and later
- IBM Lotus Sametime version 7.xx and later

The following Cisco products support only Non-Idle mode:

- Cisco Unified Personal Communicator version 7.x and earlier
- Cisco Unified Mobile Communicator
- Cisco Unified Mobility Advantage
- IBM Lotus Sametime plugin

If you use other clients not listed here, consult the documentation for your specific product or software. Of course, you can use non-Idle clients with Cisco Unity Connection, but the amount of users supported is reduced. As stated previously, a single non-Idle IMAP client should be considered as four IMAP Idle clients when calculating users to determine the server sizing.

Cisco Unity Connection version 8.x software enables organizations to mix non-Idle and Idle IMAP clients on the same server. However, for accounting purposes, it might be advisable to put them on separate servers, or at least create a completely different class of service to account for the number of each type of client on each server. Whether the clients are on separate servers or the same server, the calculations are still the same—meaning, a non-Idle IMAP client still counts as four IMAP Idle clients.

The IMAP non-Idle clients are the only clients that affect the amount of the users in the Cisco Unity Connection version 8.x software. This must be accounted for with current and future users when considering server sizing to allow for scalability.

Determining Voicemail Port Requirements

The number of voicemail ports required is another factor you need to consider in server sizing calculations. To ensure that callers get their calls answered by Cisco Unity Connection and never receive a fast busy, it is imperative that ports are available at all times. The information collected to make the initial calculation can be gathered from the current voice-messaging system to gather traffic volume statistics during the specific busy hours.

www.it-ebooks.info

The main purpose of a voicemail port in Cisco Unity Connection is to answer calls to Cisco Unity Connection, enabling callers to leave voice messages and for users to retrieve these messages. If you look at only the current voicemail traffic and volume, however, you will be missing many vital factors that must be determined to calculate the correct number of ports. To understand voicemail ports, you must first explore their functions, beyond leaving and retrieving messages. Voicemail ports supply the following functions to Cisco Unity Connection:

- Answer calls for incoming callers
- Recording messages
- Retrieving messages
- Message notification
- Telephony Record and Playback (TRaP)
- Message waiting indicator (MWI)

To determine the actual number of ports to install, the designer must research answers to the following questions:

- How many users need to be configured on the server for voice messaging?
- What is the expected and projected message activity for these users?
- How can the users retrieve messages?
- Can the organization use call handlers within an audiotext application that to answer all or some of the calls to the organization?
- What features are required for voice-messaging users? Voice recognition? SpeechView? TRaP?
- Is message notification required?
- Is high availability a requirement?

The number of users can help the designer to clearly understand the server sizing. Likewise, the amount of voice messages received and retrieved can help clarify the voicemail port requirements. If users use the phone to retrieve their voicemails, a port is required; however, if they use an IMAP client, a port is not required. Users retrieving their messages using the Cisco Messaging Inbox and Microsoft Outlook with the ViewMail have the ability to listen their message through the PC speakers or their IP Phone. The clients themselves do not require a voicemail, but if the users decide to direct their messages to the IP Phone, a port is required. This is referred to as *Telephony Record and Playback (TRaP)*. Users might decide to use their IP Phone if they do not have a workstation capable of audio, or to maintain a level of privacy in the workplace.

www.it-ebooks.info

When a user receives a message, Cisco Unity Connection notifies the user by sending specific digits to the phone to turn on the message waiting indicator (MWI) light on the user's phone. When the last message is retrieved by the user, Cisco Unity Connection then sends a different set of digits to the phone to turn the MWI light off.

Other than voice messaging, Cisco Unity Connection enables an organization to create call-handlers to be used within custom audiotext applications. Part II explores call-handlers and audiotext applications in depth. Many companies choose to use this application as an auto-attendant for incoming calls, thereby allowing callers to be quickly directed to the proper person, department, or application, thereby decreasing the length of time that users use a specific port. If the audiotext application is used in this means, the call volume to Cisco Unity Connection can greatly increase because a voicemail port is used for every incoming call.

Certain other features employed by users can increase the port usage. For example, if users are configured for message notification, an outgoing call is made from Cisco Unity Connection for every configured message notification attempt, which uses an existing voicemail port. Also, users can choose to be notified of urgent, some, or all messages according to a defined time period. After they receive a notification, the user can choose to listen to the message. The message notification and message retrieval uses an available voicemail port.

Finally, if high availability is a requirement, two servers are required to be configured in a cluster-pair. A single server uses the IBM Informix database for the configuration database and message store. This single server can support up to 250 ports, depending on the server platform, with Cisco Unity Connection version 8.x software. The issue with having the single server configuration is that there is no redundancy if a server failure occurs and no available load sharing, meaning that a single server is responsible for database configuration, message stores and voicemail port activity. The loss of the server can cause a voice-messaging outage until the server is restored.

High-Availability and Redundancy

As of version 7.x software, Cisco Unity Connection supports the active-active cluster pair configuration. This configuration is defined as active-active because both servers actively process calls. In the active-active cluster pair configuration, the active-active cluster pair can support up to 500 ports (250 ports/server) simultaneously, depending on the server platform. If one server in a cluster pair is unavailable, the other server can handle all voice messaging, but with a decreased number of ports (maximum of 250 ports). Therefore, if high availability is a requirement, the total number of ports considered in the design should be kept at a maximum of 250 ports to ensure port availability during an outage. In this way, a server failure can still maintain the required number of ports.

The active-active cluster pair requires two servers with the same software level. The two servers are actively processing calls, even though a single database is still actively performing load sharing and providing redundancy in case of server failure. You can explore the active-active cluster pair design and configuration in the next chapter. At this time,

www.it-ebooks.info

you need to consider this model in your design if high availability is a requirement in tour voice-messaging solution.

Figure 2-2 illustrates the single server and active-active cluster pair design.

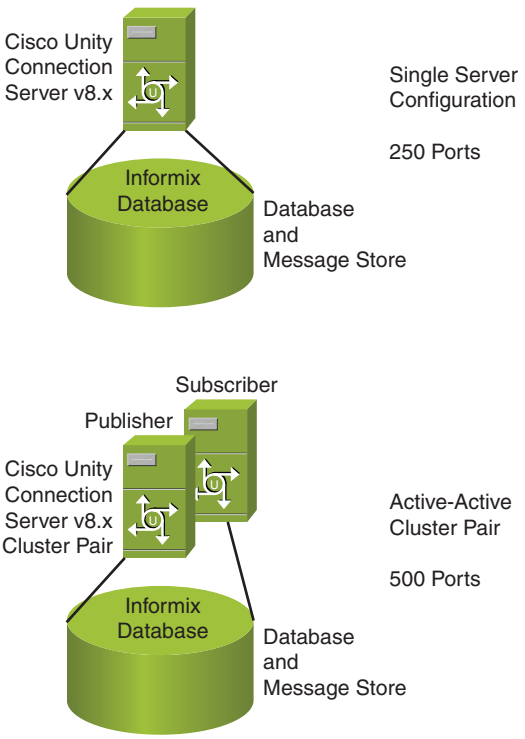

Figure 2-2 *Single Server and Active-Active Cluster-Pair Design*

Server Sizing and Platform Overlays

When you understand the business requirements within your specific organization, you can decide on the specific platform overlay to meet these design requirements. This decision should be carefully considered given the design requirements and need for scalability. Then, you can determine the proper platform overlay and procure the correct product for implementation. Considerations should also be given to product lead times in the ordering process.

Cisco System enables users to use a number of physical platforms according to their needs and business requirements. As of Cisco Unity Connection version 8.x, virtualization is now supported according to two specific overlays.

Table 2-2 and Table 2-3 (covered in the next section) provide an overview of these overlays, whether you use physical or virtual platforms in the voice-messaging solution. For

www.it-ebooks.info

the latest information regarding product models, consult Cisco.com. The following tables are provided here to demonstrate only an overview of these overlays. The supported platforms are based on the IBM equivalents.

Table 2-2 *Physical Platform Overlay Overview*

Option	Platform Overlay 1	Platform Overlay 2	Platform Overlay 3
Processors	1	2	2
Hard disk	2–250 GB	2–300 GB	4–300 GB
Total ports/server	48	150	250
Total ports/cluster	96	300	500
Total users	2000	4000	20,000
Platform	MCS7825-I4	MCS7835-I3	MCS7845-I3

The Cisco MCS 7828 series platform can be deployed for the Cisco Unified Communication Manager Business Edition to support up to 500 users and phones and 24 voicemail ports providing for Cisco Unity Connection voicemail and CUCM integrated within a single platform.

Virtualization

Virtualization has gained greater acceptance for business applications throughout the past number of years and is now supported using VMware with specific platform overlays. Some types of virtualization include memory, data, storage, and software. From the perspective of Cisco Unity Connection and the platform overlays, you can refer to operating system-level virtualization, in which a single OS can host a number of different operating systems and applications concurrently, which are referred to as *guests*. Virtualization provides a cost savings to companies and assists in energy efficiency.

Years ago, I worked at an enterprise company that had a large room filled with servers, each of which performed a specific application that was vital to its business operations. Virtualization was introduced in the company, and over the course of a couple months; they virtualized all existing applications from approximately 50 to 60 servers down to 4 servers, using a single rack. This provided for easier administration, centralized management, and greater efficiency at an extraordinary cost savings to its business.

Cisco now supports implementations using virtualization. Two platform overlays are currently supported. Table 2-3 lists the supported overlays for virtualization (at press time). Again, this is provided as an overview. Therefore, consult Cisco.com for further details and updates to these overlays.

www.it-ebooks.info

Table 2-3 *Overview of Virtual Platform Overlay*

Option	Platform Overlay (500 Users)	Platform Overlay 2 (1000 Users)	Platform Overlay (5000 Users)	Platform Overlay (10,000 Users)	Platform Overlay (20,000 Users)
vCPU	1	1	2	4	7
vRAM	2 Gig	4 Gig	4 Gig	4 Gig	8 Gig
vDisk	1–160 GB	1–160 GB	1–200 GB	2–146 GB	2–300 GB 2–500 GB
Total ports/server	16	24	100	150	250
Total ports/cluster	32	48	200	300	500
Total users	500	1000	5000	10,000	20,000

For both the physical and virtual platform overlays, you need to consult the current documentation and release notes for your specific release of Cisco Unity Connection version 8.x software because this information might vary with future releases and updates.

User Location, Geography, and Digital Networking

The next area to consider in the voice-messaging design has to do with the location of users and current network design. You must understand the current location of users, how users need to access their voice messages, and the current network topology for IP telephony and voice messaging. An organization might have one or two locations with a single phone system in which all users have IP Phones and access emails directly from Cisco Unity Connection using its phone, IMAP client, or Microsoft Outlook with ViewMail. In these cases, you can consider a design that is either a single server or an active-active cluster-pair to supply load balancing and high-availability (refer to Figure 2-2).

Some organizations might have remote users and a number of remote locations with multiple phone systems. This being the case, the decisions might be a bit more complex concerning server sizing, multiple servers, and server placement within the design equation.

Case Study: Voicemail Design

Tamicka-Peg Corporation is looking to implement a voicemail solution. This company is a large service corporation with 7000 users located at its corporate office on the east coast and another 5000 users located at a single regional branch office on the west coast. Each location has its own Cisco Unified Communications Manager 8.x cluster to support the required number of IP phones. Given this scenario, some design questions need to be

www.it-ebooks.info

considered. The questions discussed earlier concerning voice-messaging traffic and voicemail ports must first be answered. Then, additional questions concerning location and geography must be answered before a preliminary design can be considered. These questions consist of the following:

- Do users need to send, forward, and reply to users at the remote location?
- Do users need to log in to their voicemail from the remote location?
- What voice messaging currently exists at the remote location?
- Where is the call processing equipment (CUCM or PBX) located?
- Concerning call processing and PBXs: Are there multiple PBX/Cisco Unified Communications Manager servers existing in the organization? At remote locations?
- What capabilities exist with any non-Cisco call processing equipment? IP, Analog, or digital ports?

In the next section, you discover the answers to these questions concerning the integration of Cisco Unity Connection.

Introduction to Integration

In most cases, Cisco Unity Connection needs to be integrated with a new or existing PBX or Cisco Unified Communications Manager (CUCM) server or cluster. This is what is referred to as integration. For integrations with CUCM, the IP integrations can be accomplished using Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP). For legacy PBXs that support only analog or digital integrations, another device is required depending on the support provided by the PBX. There are currently two solutions for legacy integrations: PBX IP Media Gateway (PIMG) and T1 IP Media Gateway (TIMG). Both products use SIP for communications between the PIMG/TIMG unit and Cisco Unity Connection. Dialogic Corporation is a key manufacturer of PIMG/TIMG units, though some of the PIMG/TIMG products might be End of Sale (EOS).

As an integration is defined as the communications from the voice-messaging system to the call processing system (Cisco Unity Connection to CUCM), voicemail networking describes communications between voice-messaging systems.

Introduction to Voicemail Networking

Within most organizations, users need to send, forward, and reply to users at the remote locations. Also, as more users travel, they need access to their voicemail from other locations. If this is the case, networking between voicemail systems need to be considered. This can be easily done with Cisco Unity Connection version 7.x and 8.x. However, if a

www.it-ebooks.info

different non-Cisco voice-messaging system is to remain, a different networking method needs to be investigated, depending on the support provided by the existing voice-messaging system. You explore these various networking technologies and configuration in the next chapter. However, you first need to understand the networking concepts, terminology, and fundamental mechanics of each option to create a voice-messaging design that meets the business requirements.

Intrasite Networking

Each server platform overlay has limitations on the number of users supported. If an organization has user requirements beyond these limitations, or if users are located at remote locations with a different call processing system, intrasite networking is required. In previous versions of Cisco Unity Connection, this was referred to as digital networking. With the current version of Cisco Unity Connection, up to ten servers can be joined together to form single voice-messaging network. This network is referred to as a *connection site*. Each server or cluster-pair in the connection site is called a *location*. Up to ten locations, consisting of single servers or active-active cluster pairs can connect via intrasite links to form a single connection site.

Note To help clarify Cisco terminology, intrasite links are used within a connection site to join locations, where an intersite link joins two connection sites to form a Cisco Voicemail Organization.

As you learned earlier, a server or cluster pair using Cisco Unity Connection version 8.x software can provide voice messaging for up to 20,000 users. Using intrasite links to form a connection site, this limitation can be exceeded to provide voice messaging for up 200,000 users—though the global directory is limited to 100,000 users and contacts.

Users can have IP phones registered to a single CUCM or PBX. Cisco Unity Connection system can support multiple integrations while being part of a connection site with multiple intrasite links. An organization might decide to keep its existing PBX along with CUCM and transition users and phones to the new system over a period of time. This feature affords the flexibility to use intrasite networking to meet current business needs and transition to the new system using a phased approach.

Figure 2-3 illustrates this option using a single or multiple call processing systems within a connection site.

Intrasite links can be formed using active-active cluster-pairs if load sharing and high availability is a requirement. Figure 2-4 depicts the intrasite links used in a cluster-pair configuration. As displayed, single server configuration and active-active cluster-pair configuration can be combined with the connection site.

www.it-ebooks.info

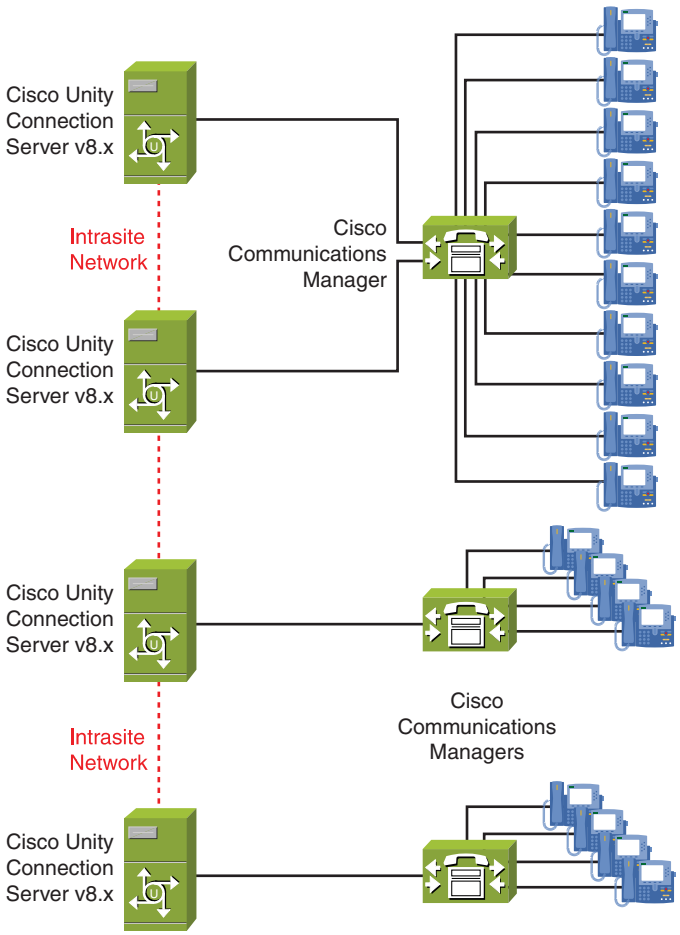

Figure 2-3 *Single and Multiple Call Processing Within a Connection Site*

The important aspect of intrasite links between servers is that all communication, transfer, and sending of messages is accomplished using Multipurpose Internet Mail Extensions (MIME) over Simple Mail Transfer Protocol (SMTP). Both protocols are Internet standards, so the transfer and sending of voicemail can be easily accomplished over the WAN or Internet. In this way, each remote location can have a Cisco Unity Connection server along with its own CUCM or PBX. The Cisco Unity Connection servers can then be joined together using intrasite links to form a single connection site, allowing users the ability to send, forward, and reply to messages from users at the other locations.

Now that you know the various implications of intrasite network, refer to the case study and the voice-messaging solution for Tamicka-Peg Corporation. Tamicka-Peg Corporation

www.it-ebooks.info

has 7000 users at the east coast location and 5000 users at the west coast location. Each site has its own Cisco Unified Communications Manager cluster to support the required phones. After further discussion, it was determined that the organization required high availability at both locations, and users need to have the ability to send, forward, and reply to messages at the other remote location, regardless of their locale.

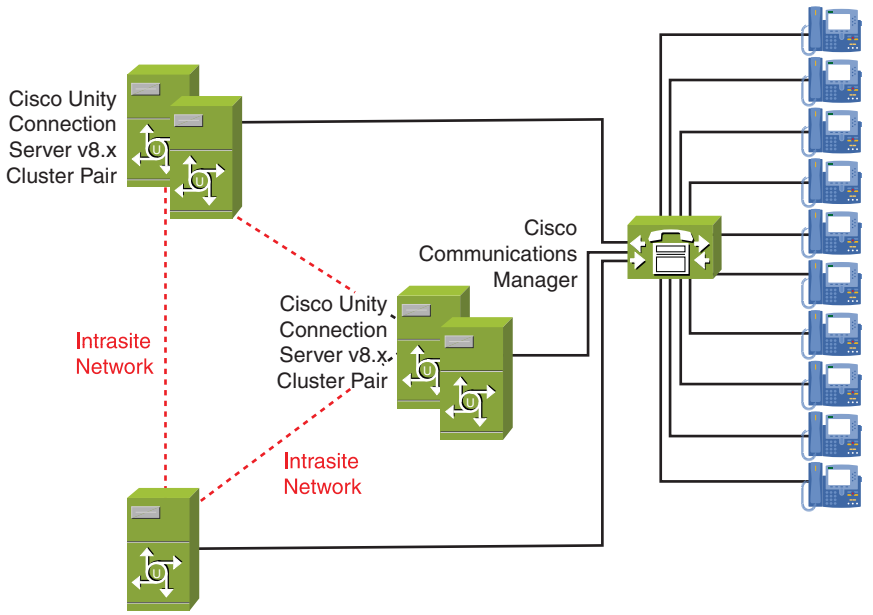

Figure 2-4 *Single Server and Active-Active Cluster-Pairs Used Within a Connection Site*

Given the voice-messaging requirements, the decision was made to create a preliminary design based on active-active cluster pairs integrated to the CUCM cluster at each location and create an intrasite link between each active-active cluster pair to form a connection site.

Figure 2-5 illustrates this preliminary design. The single connection site with intrasite links using cluster-pairs provides high availability and load sharing using the cluster pair. In this case, an intrasite link creates a single connection site between the two locations. The design enables users to send, forward, and reply to messages at either location. If a user travels to either remote location, they can access their voicemail by logging through the local Cisco Unity Connection system. This is accomplished by using what the *cross-server login feature*. Additionally, callers at one location can address messages and be transferred to users who have a mailbox at the remote location. This is attained through the use of the cross-server transfer feature. The cross-server login and transfer features and configuration are explored in the next section.

www.it-ebooks.info

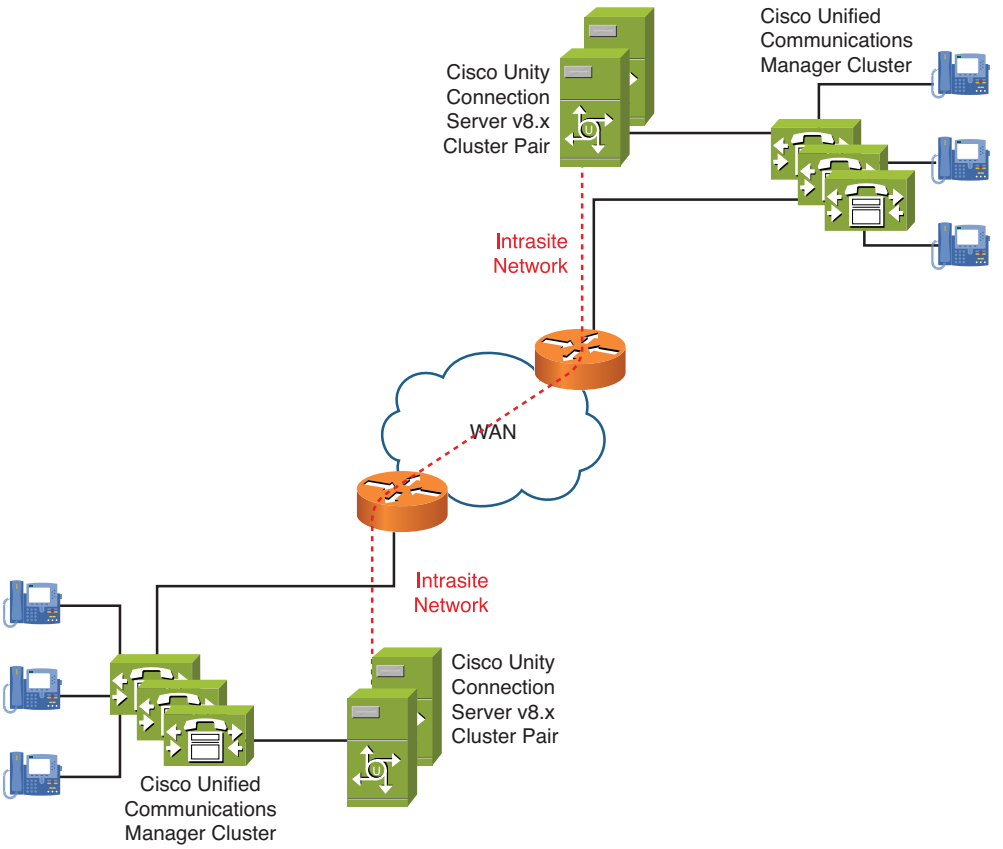

Figure 2-5 *Intrasite Links over the WAN Form a Connection Site*

Another feature available in Cisco Unity Connection version 8.x enables users to perform a Live Reply between locations within a connection site. The Live Reply feature enables users to reply directly to a user located on another Cisco Unity Connection version 8.x server by transferring directly to a caller who left the message as they are in the process of listening to the voice message. Users can also use live reply to callers that leave messages from external phones through a gateway.

These features combine to provide the connectivity required from most voicemail users within a Cisco Unity Connection network.

Introduction to Intersite Networking

Intrasite links connect Cisco Unity Connection locations to form a single connection site for voice messaging. Up to ten locations can be connected using intrasite links. Additionally, two connection sites can be linked together using an *intersite link*. An intersite link extends the networking limitation of 10 servers to enable up to 20 servers to form a *voicemail organization*. A voicemail organization is two connection sites interconnected with a single intersite link between a pair of Cisco Unity Connection servers

www.it-ebooks.info

acting as the gateway to the remote connection site. This design has the limitation of allowing only one intersite link per connection site.

All voice-messaging and directory-synchronization traffic can directly pass between the Cisco Unity Connection servers configured with the intersite link, and therefore, act as the gateway to the remote connection site.

The advantage of the intersite link provides an organization with the capability to limit traffic, updates, and message transfer to a single intersite link between the two Cisco Unity Connection servers acting as the gateways for the voicemail organization. Only two connection sites can be linked together using the intersite link. When these two connection sites are linked together to form a voicemail organization, SMTP is used for message transfer between connection site gateway, and HTTP/HTTPS is used for directory synchronization. Therefore, the designer must ensure that a connectivity between connection site gateways exists. For SMTP connectivity, a SMTP smart host can be employed if this connectivity is not possible. Chapter 3, "Installing and Upgrading Cisco Unity Connection," explores this scenario and its configuration in more depth.

Figure 2-6 illustrates the use of an intersite link between connection sites to form a voicemail organization.

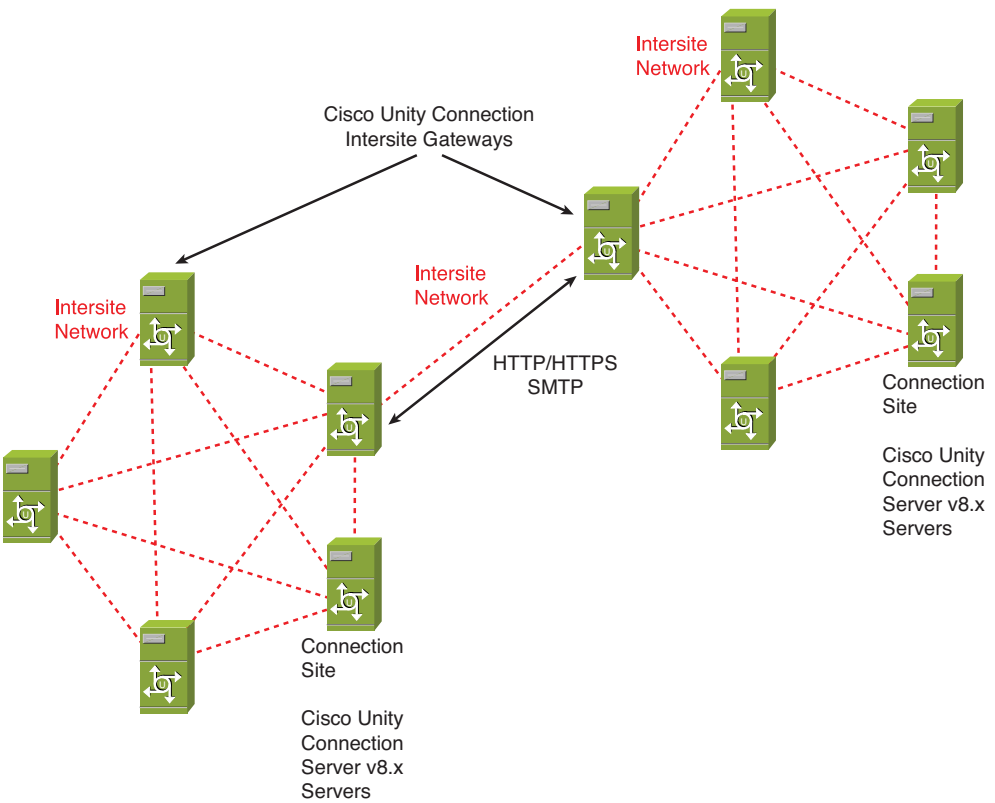

Figure 2-6 *Intersite Link Used to Network Two Connection Sites to Form a Single Voicemail Organization*

www.it-ebooks.info

Intrasite Versus Intersite Networking

Intrasite and intersite links each have their advantages and disadvantages; however, they both provide networking between Cisco Unity Connection voice-messaging servers within the organization. For example, if an organization has a combination of existing Cisco Unity Connection version 7.x servers to be networked with Cisco Unity Connection version 8.x servers, they are limited to intrasite links. Only Cisco Unity Connection version 8.x software can support the intersite links. Intrasite links are limited to 10 locations. However, an intersite link extends the network to support up to 20 locations.

The replication and synchronization is different between the intrasite and intersite links. Within a connection site, locations connect with intrasite links. In this case, all system information (users, contacts, distribution lists, and so on) is replicated throughout the connection site, including membership of all system distribution lists.

Replication across intersite links is performed only once and is scheduled. This replication takes place only between the gateways that have the configured intersite link. Also, the system distribution lists are replicated to the remote gateway across this intersite link, but distribution list membership is not replicated. Because all information is replicated and synchronized to all other location in a connection site using intrasite links, the bandwidth requirement is greater. With intersite links, replication and synchronization takes place only between the gateways, thereby reducing the required bandwidth.

Administratively, the intrasite links are easier to manage than intersite site links and affords the flexibility to add locations to the connection site as the organization experiences growth. Intersite links are limited in scalability because only a single intersite link can be configured to network two connection sites.

Intrasite links enable the configuration of a Cisco Unity Connection version 8.x server to be networked to Cisco Unity Connection version 7.x servers, as long as the intersite link is not used. (Version 7.x does not support intersite links.) The use of intersite links forbids this and requires only Cisco Unity Connection version 8.x servers throughout both connection sites that use an intersite link; however, a Cisco Unity Connection version 8.x site can be networked with a Cisco Unity version 8.x server using an intersite link.

Intersite links can connect a Cisco Unity Connection site with a Cisco Unity site; however, all Cisco Unity Connection servers must be version 8.x. Also, the gateway server on the Cisco Unity site must be version 8.x software. All other Cisco Unity servers must be a minimum of version 5.x software. When the intersite link is used in this manner, a user is added to the Cisco Unity Connection site directory for all Cisco Unity subscribers. Likewise, an Internet subscriber is added to Cisco Unity for every Cisco Unity Connection user. However, VPIM, AMIS, Bridge, and Internet subscribers from Cisco Unity are not replicated across the intersite link to the Cisco Unity Connection site gateway.

Cisco Unity Connection does not support AMIS and Bridge networking; however, VPIM is supported and you must explore a number of considerations if intersite links are employed in the network. Chapter 5 looks at these considerations in more detail.

www.it-ebooks.info

Case Study: Voicemail Network Design

After the preliminary design was presented to Tamicka-Peg Corporation, it was discovered that management was in the process of buying a division of Tiferam Corporation in the Midwest, which has a growing connection site consisting of five Cisco Unity Connection servers. Management of both organizations determined that they require voice-messaging connectivity between the two companies. It was determined that most of the voice messaging will occur between the Tiferam and the management team at Tamicka-Peg Corporation, which is located in their east coast location. Both companies decided that conserving bandwidth on the link between their two companies was an important consideration in the final design.

After further review, the finalized design (based on the original preliminary design) was approved to provide the proper voice messaging between Tamicka-Peg's east and west locations and with the newly acquired division of Tiferam Corporation in the Midwest.

Figure 2-7 illustrates this final design, in which an intersite link is used between the two companies to create a voicemail organization between connection sites located at each company.

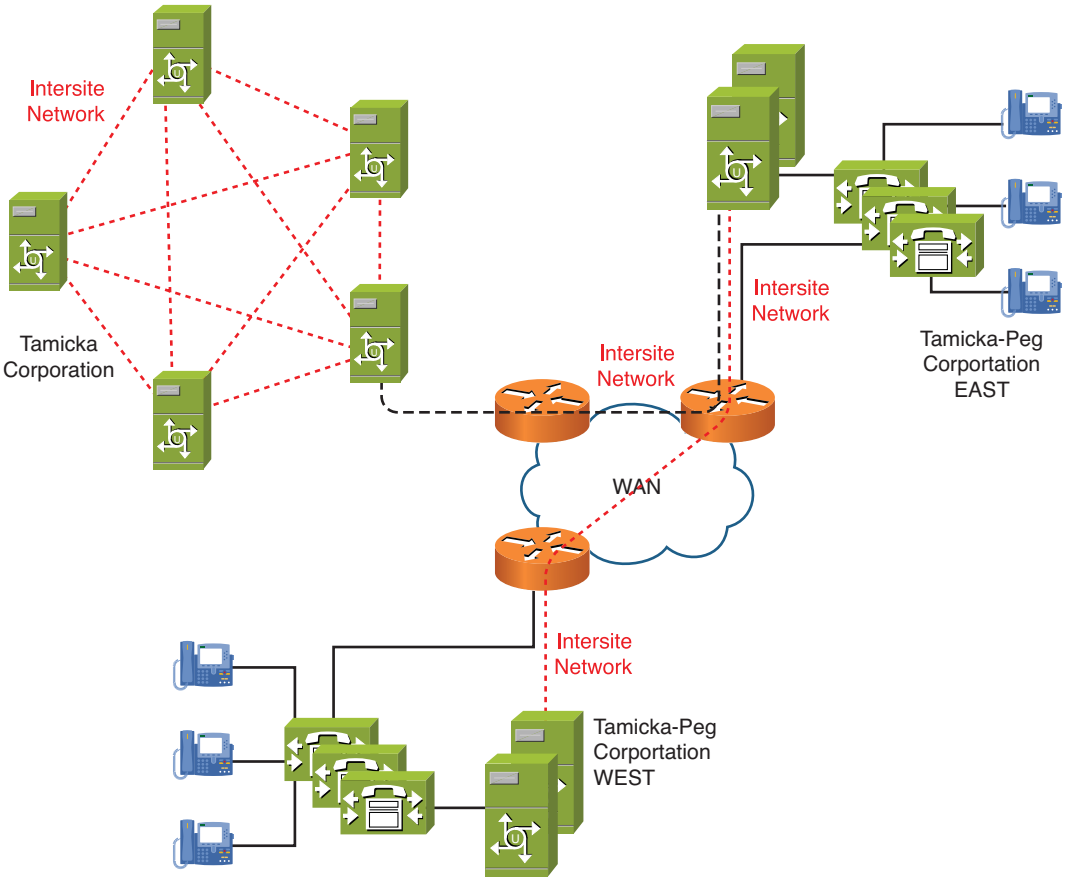

Figure 2-7 *Final Design of Tiferam and Tamicka-Peg Using an Intersite Link*

www.it-ebooks.info

Other Voicemail Networking Options

Intrasite and intersite links are excellent networking options for multiple Cisco Unity Connection version 8.x servers to network connection sites together forming a single voicemail organization. However, there might be cases in which a company does not have the capability to replace existing voice-messaging systems entirely because of technical, organizational, or budget reasons. In this case, Cisco Unity Connection might need to coexist with a completely different, disparate voice-messaging system. Even though this system might be a different system, there is another option that exists to enable networking with Cisco Unity Connection. This solution uses an industry-standard protocol called Voice Profile for Internet Mail (VPIM).

VPIM is an Internet-standard protocol for transfer of voice messages between voice processing systems. The VPIM specification defines the encoding of the voice messages using a MIME-type message and sending to a remote VPIM location using an SMTP transport. This procedure is similar to what is accomplished using the intrasite links but is mainly used when networking dissimilar voice-messaging systems. The VPIM protocol was defined in RFC 3801 as the VPIMv2 standard and dictates the use of a similar addressing format to that used with email system (myEmailAddress@myDomain.com). The main purpose of the VPIM is to enable voice messaging between disparate systems. These systems could be similar or dissimilar between the same or different manufacturers, as long as they support the VPIM standards. VPIM is also supported between Cisco Unity, Cisco Unity Connection, Cisco Unity Express, and various other non-Cisco voice-messaging systems that support the VPIM protocol.

Case Study: VPIM Voicemail Design

Jensen Industries, a mid-sized manufacturing firm in North America, has an existing Cisco Unity version 5.x server and Cisco Unity Express voicemail system in two different locations. These systems need to be networked with their new Cisco Unity Connection version 8.x server, which will be located in their main headquarters. Also, Andres Consultants is a contract service company that provides networking service to Jensen. There is also a requirement to enable addressing of messages between the Jensen and Andres Consultants.

Because you will be networking completely dissimilar systems, VPIM might be the perfect solution to provide networking between all three Jensen Industries sites and Andres Consultants. Figure 2-8 depicts this solution using VPIM networking.

www.it-ebooks.info

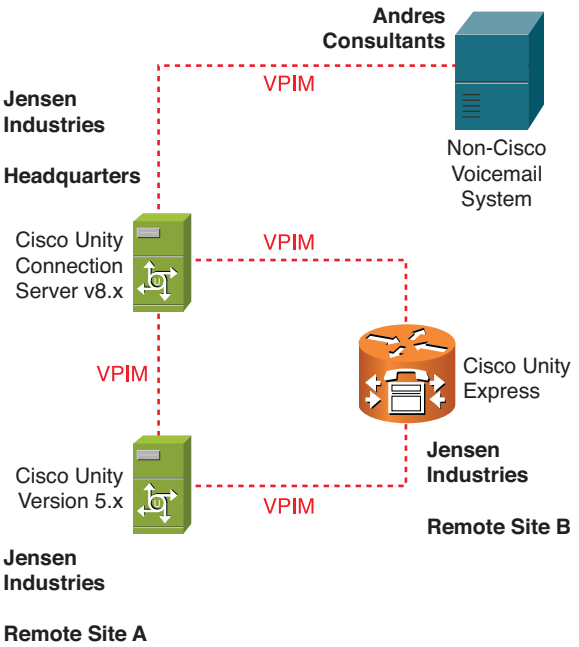

Figure 2-8 *VPIM Networking Solution to Provide Networking Between Disparate Voice-Messaging Solutions*

VPIM networking enables various addressing methods between locations. In the next chapter, you investigate the in-depth details and configuration of VPIM networking, contact creation, and addressing.

Intersite Links and VPIM Networking

As was pointed out in the discussion of intersite links, VPIM, AMIS, Bridge, and Internet subscribers are not replicated across an intersite link to the Cisco Unity Connection site gateway. Therefore, if VPM networking is a requirement, each connection site gateway needs to include a VPIM connection. The site gateway for the intersite link can also act as the VPIM connection gateway, or bridgehead server. Or the VPIM connection can be hosted on another server in the connection site.

Figure 2-9 illustrates the use of multiple VPIM connections to a server to enable connectivity between multiple connection sites with an intersite link.

www.it-ebooks.info

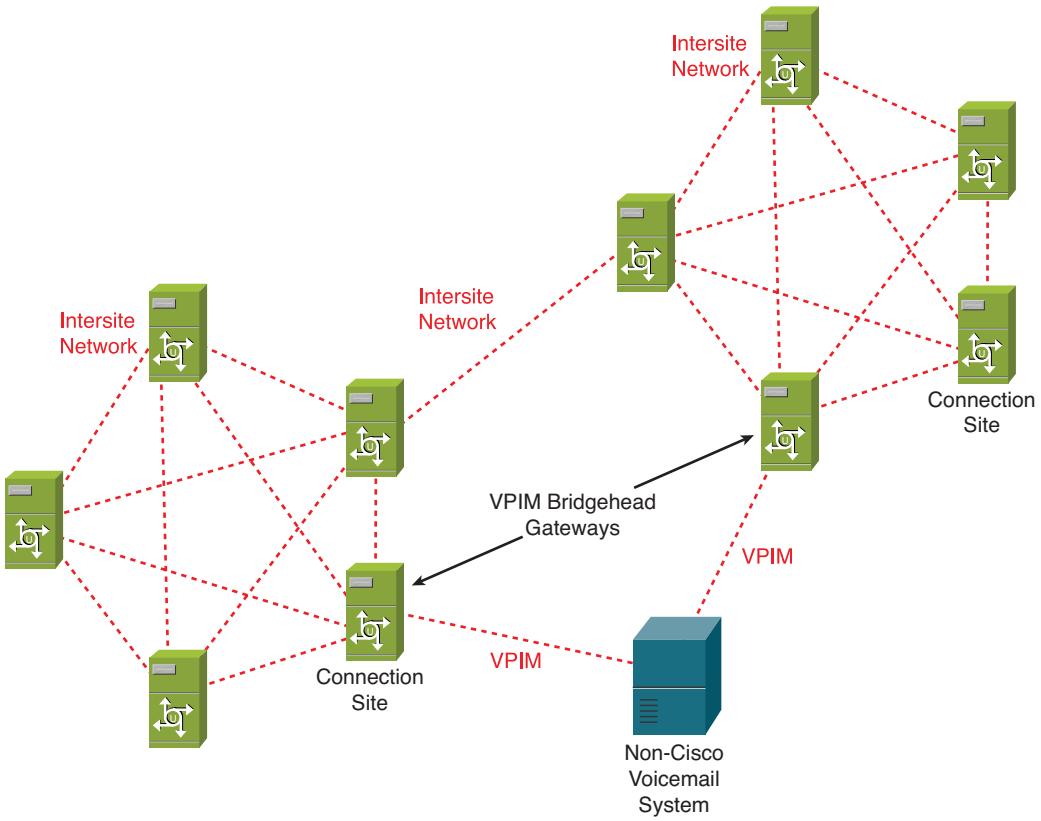

Figure 2-9 *Multiple VPIM Connections Using an Intersite Link Between Connection Sites*

In Chapters 3 and 4, you investigate the installation, integration, networking of Cisco Unity Connection. The discussion also includes important features required to provide users with the necessary options and connectivity to perform voice messaging according their business needs.

Case Study: Multisite Voicemail Design

LMN Corporation, a large enterprise in Dallas and Orlando is in need of a new voice-messaging solution. It has a subsidiary in London that has an existing legacy voicemail and phone system supporting 100 users at that location. Dallas is its main headquarters with 3500 users. The Orlando location is a smaller division with 150 users. All IP Phones in the U.S. network need to be supported using a CUCM at the Dallas location.

www.it-ebooks.info

London plans to upgrade to Cisco Unity Connection in the future but because of budget constraints, this has been postponed to a future date. However, users still need the ability to send and forward messages between the U.S. locations and its London office. After researching the currently network design and meeting with management and users at all locations, the following information was determined from the planning stage:

- In Dallas, there are 3500 users (with voicemail) with a projected growth to 5000 over the next 2 years.
- The Orlando location is a sales division, where users will be using a variety of mobile clients that are capable of only the IMAP Non-Idle mode. Projected growth at this division might increase to 200 users over the next couple years.
- The London location will eventually migrate to Cisco Unity Connection but at a later time. The current voice messaging is a legacy system, but further documentation research discovered that this system does support the VPIM protocol.
- Users within the U.S. offices will be required to have access to voicemail at all times (high availability) and will use their phone and Outlook to retrieve voicemails.
- During the peak hours, there have been measurements indicating up to 90 concurrent voicemail sessions at any particular time within all U.S. locations combined.

From the information discovered in the planning phase, a preliminary design was constructed using the centralized IP telephony design already in place between Dallas and Orlando. It was decided that an active-active cluster pair would be located in the Dallas headquarters because the CUCM cluster is located at this location to support all IP Phones at both U.S. offices, and high availability is a design requirement.

The voice-message implementation needs to support 5200 users between Dallas and Orlando; however, because the Orlando division is going to use IMAP non-Idle clients, you need to allow for the additional requirements of IMAP non-Idle. As you learned in this chapter, an IMAP non-Idle client counts as four IMAP Idle clients. Therefore, the calculation for Orlando will be (based on the projected growth) 200 clients * 4 = 800 users. Therefore, the total calculation should be 800 users (Orlando) + 5000 users (Dallas) for a total user count of 5800 users.

Based on these calculations, a physical platform has been decided on using the MCS7845 platform with a minimum of 96 ports purchased initially. This means that two servers with identical software can be configured as an active-active cluster pair to provide high availability for the U.S. locations. VPIM networking will be configured between the Dallas and London locations to support the sending, forwarding, replies to messages between the London, Dallas, and Orlando locations, as illustrated in Figure 2-10.

www.it-ebooks.info

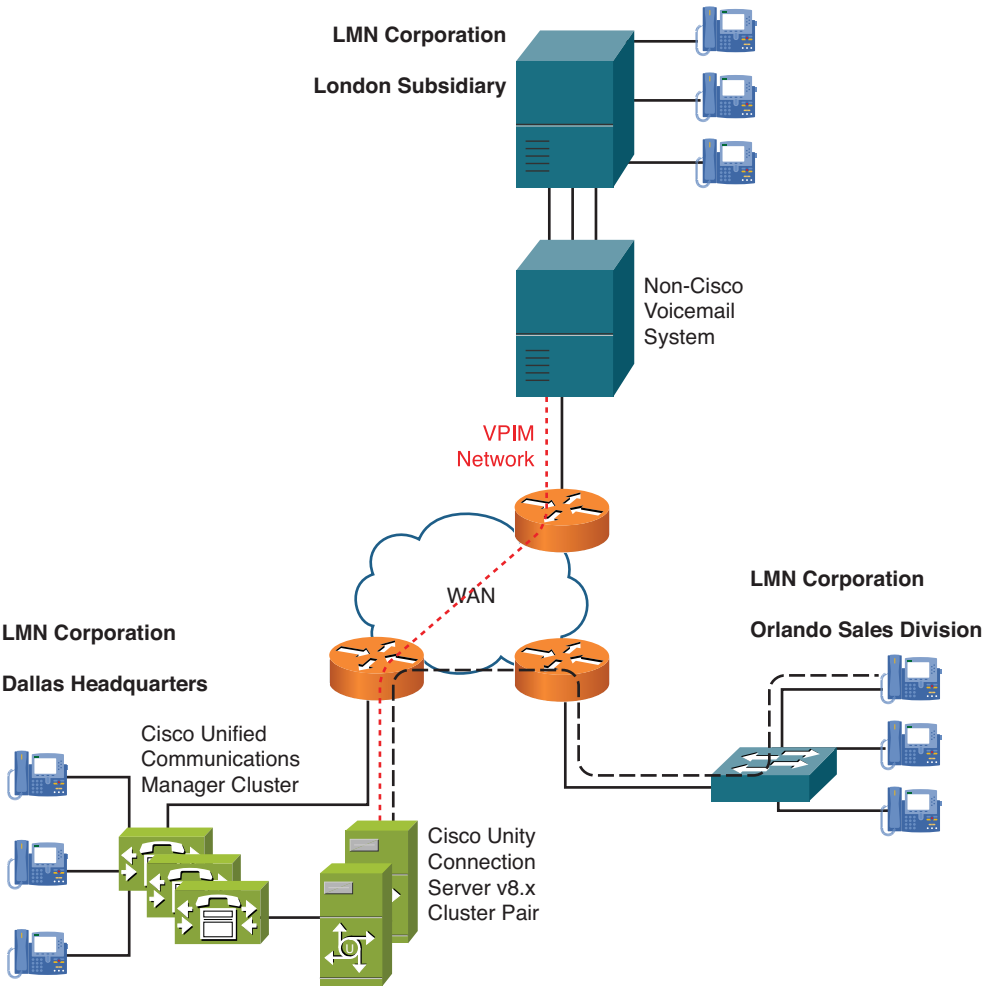

Figure 2-10 *LMN Corporation Voice-Messaging Solution*

Summary

This chapter provided an overview of Cisco Unity Connection software and the necessary elements to consider when designing a voice-messaging system. You learned how to

- Determine the specific server sizing based on users, codec, ports, and client applications.
- Understand the basics of how Cisco Unity Connections version 8.x handles codecs and transcoding for voice messaging.
- Understand the differences between IMAP Idle and IMAP non-Idle and how the amount of users is affected in the design considerations.

www.it-ebooks.info

- Describe how high-availability and redundancy is accomplished using the active-active cluster-pair model with Cisco Unity Connection version 8.x servers.
- Determine the server sizing based on the physical or virtual platform overlays and the amount of ports and users supported.
- Understand intrasite and intersite networking using Cisco Unity Connection and describe the protocols, advantages, and limitations.
- Describe VPIM networking and how it is used with Cisco Unity Connection and other Cisco voice-messaging products.
- Determine the specific technology requirements based on the voice-messaging system and assemble information collected in the planning phase to create a preliminary design based on the users, location, and geography of the organization.

www.it-ebooks.info

This page intentionally left blank

www.it-ebooks.info

Chapter 3

Installing and Upgrading Cisco Unity Connection

This chapter covers the following subjects:

- **Cisco Unity Connection Software Installation:** Provides detailed instructions on installing Cisco Unity Connection version 8.x software in a standalone environment using the basic installation, upgrade during installation, and the unattended installation using the answer file.
- **Active-Active Cluster Pair Installation:** Illustrates the configuration and installation of Cisco Unity Connection active-active cluster pairs using version 8.x software to understand the differences between the publisher and subscriber implementation.
- **Cisco Unity Connection Upgrade Procedures:** Explores the various upgrade procedures required when upgrading from an earlier version of Cisco Unity Connection and Cisco Unity.
- **Cisco Unity Connection Licensing:** Covers the licensing requirement for the Cisco Unity Connection server, active-active cluster pair, ports, users, and features.

You have now completed the planning and design phase for the voice-messaging implementation and are ready to enter the next phase of building a new voice-messaging system. The planning and subsequent designs have been created, discussed, and adjusted to enable the current and future business requirements as they pertains to voice messaging. Allowances have been made for scalability, Internet Message Access Protocol (IMAP) clients, and the various port usage considerations. Throughout the meetings, discussions, and designs, the decision has been made to implement the Cisco Unity Connection product as the voice-messaging solution. Based on these elements of the planning and design phases, a final platform overlay has been selected, and the correct product has been ordered and delivered to support the new Cisco Unity Connection installation. You have now entered the implementation phase.

The implementation of Cisco Unity Connection software and installation procedure for single server and cluster pair configurations are discussed first. For a new installation, the

www.it-ebooks.info

planning and design phase needs to consider the software installation process, based on a physical or virtual implementation.

As discussed in Chapter 1, "Cisco Unity Connection Overview," the installation might be completed as a phased approach or a flash cut. A phased approach occurs when the installation occurs over a period of time, by department, users, or some other corporate delimiter. A flash cut implementation defines an immediate migration to the new software for all users.

This chapter focuses on the implementation and upgrading of Cisco Unity Connection version 8.x software. The knowledge gained in this chapter enables you to understand the implementation of Cisco Unity Connection in a standalone and active-active cluster pair environment. You need to know a number of important elements before each installation can be completed. Even though this chapter includes a step-by-step approach to the implementation, you should read this chapter in its entirety before attempting an install or upgrade.

Throughout this chapter, you gain an understanding of the following:

- How to install Cisco Unity Connection software as a standalone server.
- How to install a Cisco Unity Connection active-active cluster pair, designating a publisher and subscriber and understand the configuration elements required for each type of implementation.
- The differences and purpose between the various installation methods, including the basic installation, upgrade during install, and unattended installation using an answer file.
- The methods to upgrade to Cisco Unity Connection 8.x from previous versions of Cisco Unity Connection and Cisco Unity implementations.
- The elements of licensing in Cisco Unity Connection.

Cisco Unity Connection Installation Procedures

The installation phase for the software implementation consists of a number of tasks discussed within this chapter. These tasks consist of the following:

- Software installation and configuration
  - Single server installation
  - Active-active cluster pair
- Testing administrator workstation functionality
- Configuration phone system integration
- Understanding call flow: direct and forwarded routing rules
- Performing a backup using the disaster recovery system
- Post installation and administrative tasks

www.it-ebooks.info

This chapter examines each of these tasks, with the exception of the post installation and administrative tasks, which Part II extensively covers.

Installing Cisco Unity Connection Software

Cisco Unity Connection will be installed on the physical or virtual platform according to the specific overlay, which was decided during the design phase. This chapter explores physical platform overlay, followed by the virtual considerations. After the installation process begins, slight differences exist between each of these installation methods relative to the software installation. This chapter reviews the various configuration options and elements for each type of implementation, whether you perform a single server or cluster pair installation. This chapter also discusses the physical platform installation, the single server installation, and the active-active cluster pair implementation.

Pre-Installation Tasks

Before beginning the software installation, the installer needs to acquire the configuration information necessary to complete the implementation. This information should already have been determined and documented during the design phase and will be entered within the installation dialogue phase of the installation. This information that pertains to the Cisco Unity Connection server installation follows:

- **Time zone configuration:** Applies to the time zone in which the physical server is to be located.
- **Interface speed and duplex:** The switchport for the server must agree with the port configuration if you are statically configuring the speed and duplex on both devices. Auto-negotiation using the 802.3u/ab standards enables the switchport and server to automatically negotiate the fastest transmission (speed and duplex) between the two interconnected devices. If auto-negotiation fails or is not supported on a specific device in the network, speed and duplex mismatches might occur causing packet loss and directly affecting the network and voice quality.
- **Maximum Transmission Unit (MTU):** The largest packet or protocol data unit (PDU). By standards, an Ethernet PDU is designated as an MTU of 1500 bytes. Various systems might fix the MTU, whereas others might negotiate the MTU at the time of connection, as is the case with serial point-to-point links. For Cisco Unity Connection, the MTU can be configured as needed through the Cisco Unity Connection installation dialogue.
- **Server name, IP address, subnet, and default gateway or Dynamic Host Control Protocol (DHCP) selection** Must be determined before beginning the installation.
- **Domain Name System (DNS) configurations:** (Optional) If using DNS, a DNS server is required and must be configured and installed before the Cisco Unity Connection installation can be performed. If possible, it is recommended to eliminate the reliance on DNS for voice networking to eliminate this added element. However, in some larger enterprise environments, this might not always be the case. If DNS is to

www.it-ebooks.info

be configured, it will be necessary that redundancy and backup services are properly configured for the DNS implementation.

- **Administrator login (username/password):** Designated username/password combinations used for logging into the following applications:
  - Cisco Unified OS Administration
  - Command-line interface (CLI)
  - Disaster Recovery System

Note The Administrator login is referred to as the Platform Administrator account, which is used to access the command-line interface and the various web pages for the server operating system and backup and restore configuration. This login is different from the Application Administrator account, which is used specifically for the Cisco Unity Connection Administration and Serviceability web pages.

- NTP Configurations: A protocol commonly used to synchronize clocks/time between network devices. NTP designates a series of 16 different stratums, levels, or hierarchies. The purpose of stratums is to avoid synchronization loops with different NTP sources. In this case, any device prefers the source with the lowest stratum number, unless statically configured. Cisco Unity Connection must be statically configured during the installation dialogue.

Following are two ways to synchronize clocks for Cisco Unity Connection:

- With a corporate head-end router synchronized with a Public NTP time server
- Directly with an external Public NTP time server

The Cisco Unity Connection server or publisher requires an external NTP source. Cisco Unity Connection version 8.x requires NTP services to be accessible for a successful installation. During normal operations, the NTP service ensures that the time synchronized is accurate for date/timestamps of messages, reports, and various tools, such as logs and traces.

The Cisco Unity Connection subscriber acquires NTP synchronization from the publisher when configuring an active-active cluster pair.

- **Security Password:** Used specifically by the subscriber to allow access to the database and join the cluster. It is entered in the publisher configuration dialogue. When using the cluster pair, the security password is included in the subscriber configuration, along with the publisher hostname and IP address to allow the subscriber to join the cluster and subscribe to the database.
- **SMTP host configuration:** Indicates the SMTP domain name to be used for this server. If this option is not configured, the server name is used for SMTP host configuration.

www.it-ebooks.info

Note The SMTP domain name is different from the DNS domain name. The SMTP domain is used for organization and delivery of messages.

- Application user configuration (username/password): Designated username/password combinations used for logging into the following applications:
  - Cisco Unity Connection Administration
  - Cisco Unified Serviceability
  - Cisco Unity Connection Serviceability

Cisco Unity Connection Software Installation

To begin, ensure that the server is located in the proper environment, with sufficient air flow, cooling, networking, switchports, and a proper, uninterruptible power source (UPS). Of course, this consideration should be part of any server installation to ensure that the server or servers continue to provide continued service through a power outage. NIC teaming, or network fault tolerance, can be configured on the same servers, depending on the specific server platform. The lower-end servers do not support this feature.

When the server is properly located, power up the server and insert the Cisco Unity Connection installation DVD purchased from Cisco. You need to ensure that the server boots from the DVD to begin the installation process. There are a number of installations that can be performed with Cisco Unity Connection. You can perform one of the following:

- Basic installation
- Installation and upgrade
- Unattended installation using the answer file

The basic installation is examined first because this is common to all installations. After the basic installation, the chapter covers each of the other configuration procedures.

Installation Processes

A number of processes run as you begin the installation of Cisco Unity Connection. Depending on the type of installation you perform, these processes might vary; although many will be identical. The processes that run in the course of an installation when configuring a single server deployment follows:

- System Installer (includes media and platform checks)
- Product Deployment Selection
- Platform Installation Wizard

www.it-ebooks.info

- Installation dialogue
- First Node Configuration
- First Node Installation dialogue
- Software installation:
  - Formatting drive system
  - Platform installation: Installing the operating system
  - Post install: Performing Post-install configuration
  - Application installation: Installation, backup, and security checks
- Server Restart
- Application Pre-install
- Configuring network and host files
- Network connectivity check
- License and Cryptographic Informational page
- Application Post-Install: Cisco Unity Connection
- Installation Complete: Login Prompt

Basic Installation

To begin, ensure that the server platform is powered on and booting from the DVD, by making sure that the DVD software media is properly inserted in the drive. The basic installation will usually be completed for a new installation, especially where the software media has been purchased separately from the server platform. This would be the case if you acquired the server from an authorized supplier, such as IBM or HP, and then later purchased the Cisco Unified Communications software from Cisco or an authorized Cisco partner.

The installation process is examined in a step-by-step procedure to provide complete understanding and to ensure all options have been properly configured.

System Installer and Platform Checks

After the installation process begins, the system installer process automatically performs the media and platform checks. The console screen displays with the following message during this phase of the installation:

Running the Cisco Unified Communications 8.0 System Installer.

Please Wait....

Detecting Server Hardware - This Can Take Several Minutes

www.it-ebooks.info

At the beginning of the software installation, the administrator can choose to perform the media check, which would then check the platform, disk, memory, RAID, and platform BIOS. Therefore, the software needs to be installed on the correct server platform. Figure 3-1 shows the media check.

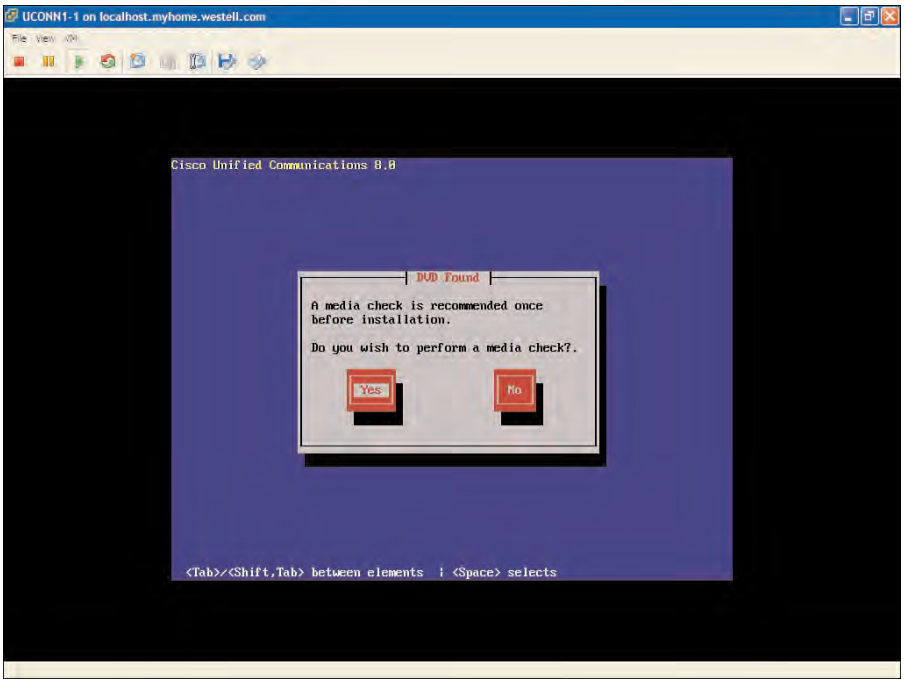

Figure 3-1 *Media Check*

All installations of Cisco Unity Connection should follow the designated platform overlays as discussed in the previous chapter. This should be the case whether using physical or virtual platforms. After the media check completes, the installation determines the server platform compatibility. If you try to install the software on an unsupported platform, the installation will end with a critical error. The only option at this point is to cancel the install and correct the issue by reinstalling the software on the correct platform. The same critical error can occur for virtual installations when the memory, hard disk, or host OS is not selected properly.

In Figure 3-2, an error was purposely caused in the virtual installation for illustration purposes. In this case, the amount of memory and disk space allocated for the installation did not meet the minimum requirements.

After the media check completes, the media check results display with either a Pass or Fail designation. All media check failures need to be corrected before the installation proceeds. When the result displays a pass, select the **OK** button to proceed with the Product Deployment Selection.

www.it-ebooks.info

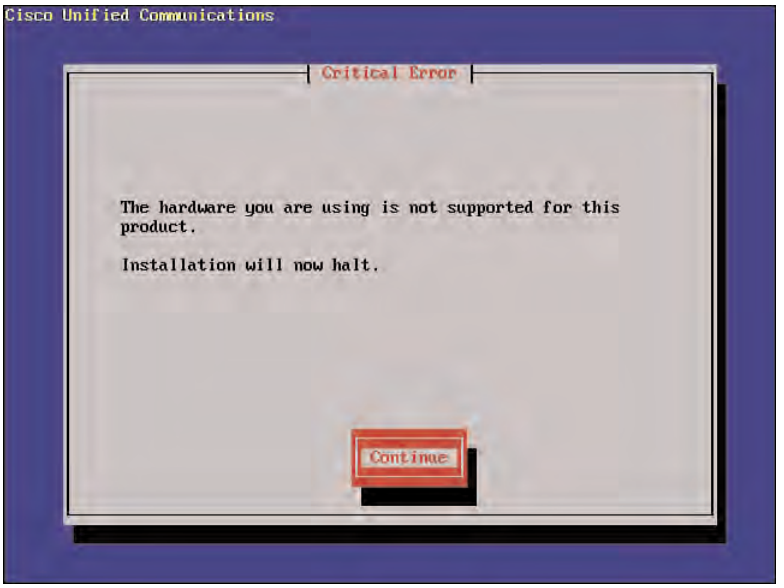

Figure 3-2 *Critical Error Caused by Server Platform Incompatibilities*

Product Deployment Selection

After the System Installer and Platform Check phase is complete, a number of screens are presented to the installer. The first screen is the Product Deployment Selection.

The Cisco Unified Communications 8.x media enables the user to install one of three products:

- Cisco Unified Communications Manager (CUCM)
- Cisco Unity Connection
- Cisco Unified Communications Manager Business Edition

Press the Tab key and Alt+Tab key combination to move between the various options. Press Space to make a selection.

In Figure 3-3, Cisco Unity Connection was selected by using the Tab key to move the cursor to the Cisco Unity Connection selection and pressing Space. Then, select the Tab key two more times to highlight the OK button. Press **Enter** to complete the configuration of the options.

After the Product Deployment Selection is complete, the installation process enables the installer to verify the correct software level. Select **Yes** by using the Enter key to proceed with the installation, as illustrated in Figure 3-4.

www.it-ebooks.info

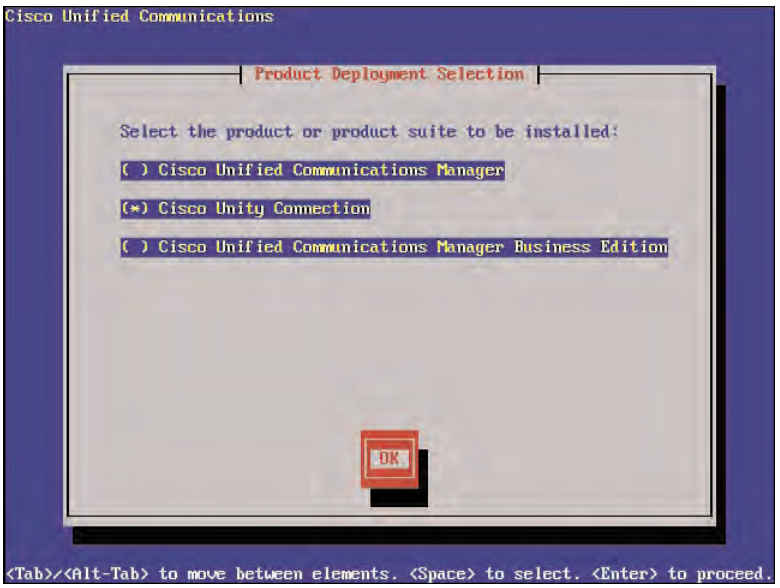

Figure 3-3 *Product Deployment Selection*

Figure 3-4 *Verify Software Level and Proceed with Install*

Note The Cisco Unity Connection server is created with an active and inactive partition. The initial software installation will be performed to the active partition on the

www.it-ebooks.info

server. Future software upgrades to the original installation will be performed to the inactive partition.

Platform Installation Wizard

The next phase of the installation process is composed of a number of important selections depending on the type of installation performed. The installation might be a basic installation where you supply all the necessary configuration information as determined in the design phase; however, the installation might also require a software upgrade or patch to be applied during the installation process. On the other hand, you might want to perform a software only installation, or an unattended installation. In this case, the software installation will complete, but the configuration information will be supplied at a later time using an answer file.

The Platform Installation Wizard enables the installer to make the necessary selection based on the type of installation. Figure 3-5 shows the first Platform Installation Wizard page that displays.

Figure 3-5 *Platform Installation Wizard Selection*

The installer has three possible options based on the type of installation. The basic installation will be the most common, where the user enters the required configuration parameters. For this type of installation, press the **Tab** key to highlight the **Proceed** selection and press **Enter**. If you want to perform the software installation without entering the configuration information (unattended installation), press the **Tab** key to highlight the

www.it-ebooks.info

Skip selection and press **Enter**. For this type of installation, you need to use the Cisco Unified Communications Answer File Generator at Cisco.com. If you decide to cancel the installation, press the **Tab** key to highlight the **Cancel** option and press **Enter**.

After the first Platform Installation Wizard selections are complete, the Apply Patch page displays. This option enables the installer to apply a software patch, release, or update during the software installation. In this case, the installation can take on a different format, meaning that you need to have the specific software patch available. Then, the software installation and updates will be completed prior to the installation dialogue. With the basic installation, the installation dialogue is completed prior to the software installation.

To apply a patch, press the **Tab** key to highlight the **Yes** option, and press **Enter**. The initial software release proceeds from the local DVD, followed by the applicable software patch or update. The software patch can be accessed from a file share or server capable of Secure File Transfer Protocol (SFTP) or File Transfer Protocol (FTP). This method requires the proper configuration and availability to an external server. SFTP provides a faster method for upgrades and patches, compared with using the DVD.

If using the DVD, the update must be available on media, where the DVD needs to be inserted into the drive at the proper time. The installer will be prompted for the location of the patch after the initial software installation has been completed.

If you want to continue with the installation without applying a software patch, press **Enter** for the **No** option. This is the default selection, as displayed in Figure 3-6. From this page, the installer also has the option to select **Back** to return to the previous screen.

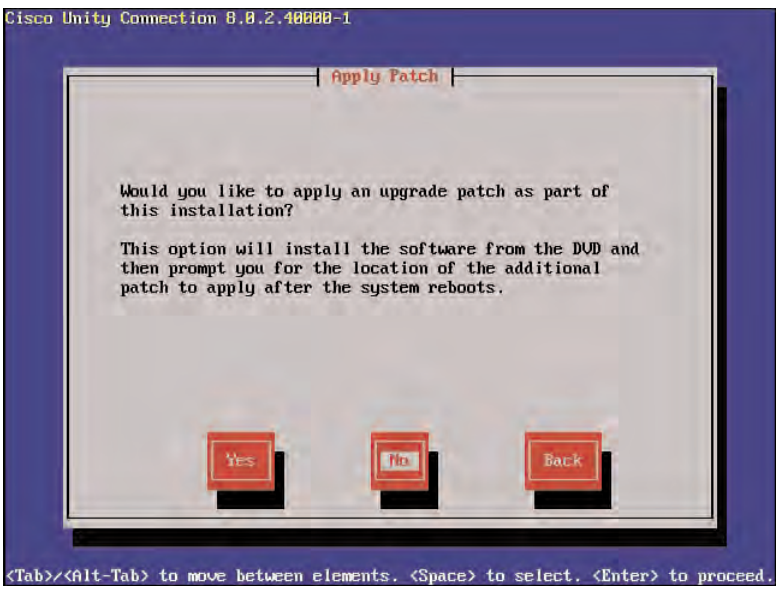

Figure 3-6 *Apply Patch During Software Installation*

www.it-ebooks.info

After the apply patch selection is made using the **No** option, the user is presented with the summary of the installation that will be performed. In this case, the basic installation is selected, where the installer is prompted to enter the configuration information. The only option at this point is to press **Enter** to select the **Continue** option, as displayed in Figure 3-7.

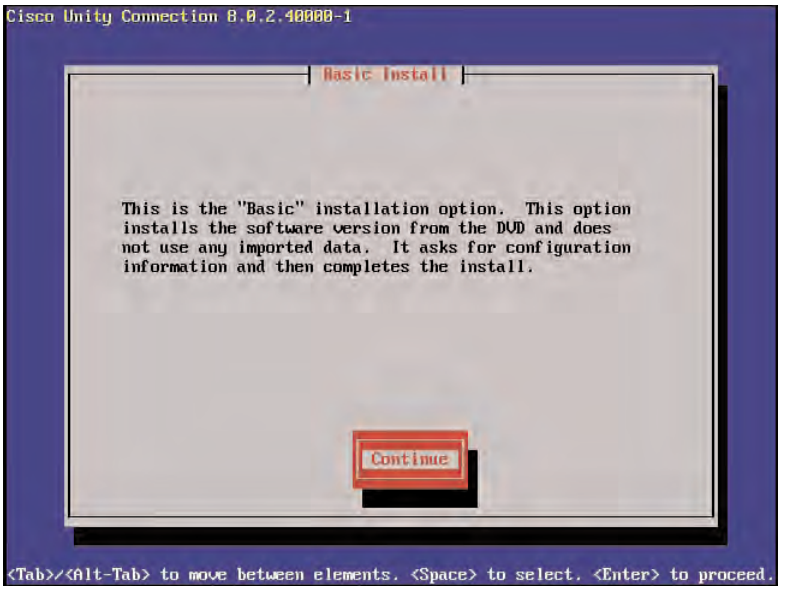

Figure 3-7 *Basic Installation*

Basic Installation Dialogue

The next few screens present the installer with the various configuration options to be selected to complete the software installation. This information was reviewed in the pre-installation section at the beginning of this chapter.

Time Zone Configuration

The time zone configuration page enables the installer to select the correct time zone for the server location. This configuration designates the time zone in which the physical server is to be located, not the location of users or contacts. This configuration is used by the server (along with the NTP configuration) for all voicemail timestamp, traces, SMTP traffic, and log information. Select the applicable time zone based on the applicable city/location, and press **Tab** to highlight the **OK** option; press **Enter** as displayed in Figure 3-8. The **Back** and **Help** options are also available on this page. If your specific city is not reflected in the options, select the closest city within your specific time zone.

www.it-ebooks.info

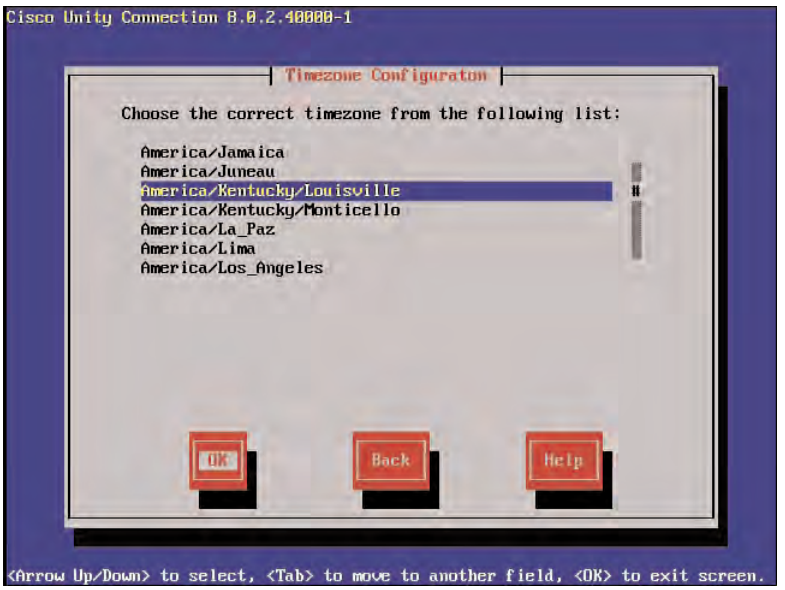

Figure 3-8 *Time Zone Configuration*

Auto-Negotiation Configuration

The next selection will be to select auto-negotiation or statically configure the network interface speed and duplex. Figure 3-9 displays the auto-negotiation screen.

Figure 3-9 *Auto-Negotiation Configuration*

www.it-ebooks.info

If you select **Yes**, the network interface attempts to auto-negotiate the speed and duplex setting with the switchport. If you select **No**, you then are presented with the next screen, as shown in Figure 3-10, to statically set the interface speed and duplex settings. In this case, the default settings display.

Figure 3-10 *NIC Speed and Duplex Configuration*

You should always hard code the switchport and server. For example, set the switchport and server for 100 Meg/full duplex, or set to the server to Auto for Gigabit Ethernet (GigE). If you use GigE, set the server and switchport to Auto/Auto. Auto-negotiation enable the fastest possible transmission mode for speed and duplex to be automatically configured. Mismatches with speed and duplex can cause network and voice-related issues because of packet loss.

Note You can use the space and Tab keys to navigate the installation pages. See the information located in the lower portion of the page.

MTU Configuration

The Maximum Transmission Unit (MTU) defines the largest packet that can be forwarded through the network. The standard Ethernet packet is 1500 bytes. In most cases, this will not be changed; however, if there is a configuration specific to your network that requires a different MTU, select **Yes** on the MTU Configuration screen. The next screen enables the installer to select a different packet size. If you are in doubt of your packet size, it is advisable to leave this option at the default of 1500 bytes.

www.it-ebooks.info

Selecting a different packet size would be more prevalent where a VPN or IPsec tunnel is used with a custom packet size. Web access over VPN can cause web pages not to load because of an improper MTU configuration. Figure 3-11 depicts the MTU Configuration page. Select **No** to keep the default MTU size of 1500 bytes.

Figure 3-11 *MTU Configuration*

DHCP Configuration

The next configuration is to select Dynamic Host Control Protocol (DHCP) or use a static configuration for the IP address, subnet mask, and default gateway.

DHCP enables a network device to request its network configuration information (IP address, subnet mask, default gateway, and other various configurations) from a DHCP server. A DHCP server can run as an application on a network server or directly on a Cisco router. If you do not use DHCP, the network information must be statically configured. It is advisable to statically configure these settings, rather than using DHCP. This ensures that the correct address is always set to the proper options; however, if you require DHCP, static DHCP host configuration is recommended. Static DHCP ensures that the DHCP server always provides the same IP address settings to the server. It is always a best practice to statically configure the network settings; however, in some dynamic environments, this might not always be the case.

Figure 3-12 displays the initial DHCP Configuration page.

If you select **Yes** on the DHCP Configuration page, the server sends DHCP Discover frames to acquire its network information. If you select **No**, you will be presented with the Static Network Configuration page, as displayed in Figure 3-13. From this page, you

www.it-ebooks.info

need to enter the host name, IP address, subnet mask, and default gateway. Static configuration is recommended for the Cisco Unity Connection server.

Figure 3-12 *DHCP Configuration*

Figure 3-13 *Static Network Configuration*

www.it-ebooks.info

Note The server must be connected to the properly configured switchport and have access to the default gateway. The server installation might take up to 20 minutes to test network connectivity and gateway availability before timing out.

DNS Client Configuration

Domain Name System (DNS) enables a device to request the location of another device through a domain name server, whereby the domain name server returns the correct IP address for the requested server name. Cisco Unity Connection enables the use of a domain name server to locate other Cisco Unity servers and devices. This is necessary when configuring digital networking and active-active cluster pairs. DNS is commonly used in enterprise networks where the network addressing might tend to be more dynamic. In environments where DNS is required, it is advisable to configure a redundant DNS server to avoid any loss of connectivity or service.

Figure 3-14 displays the DNS client configuration screen. Selecting **Yes** requires the installer to enter the domain name for this server. Select **No** to skip the DNS client configuration. You can also configure the DNS settings after the configuration is complete through the command-line interface (CLI).

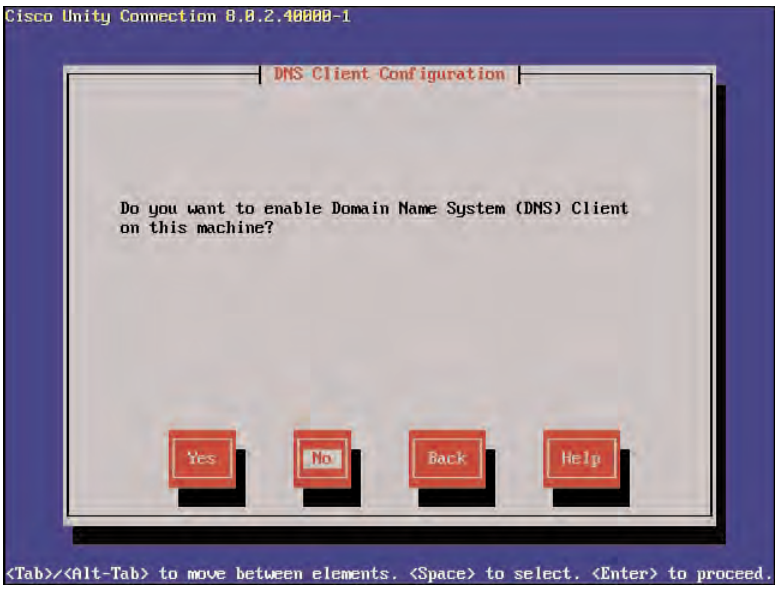

Figure 3-14 *DNS Client Configuration*

www.it-ebooks.info

Administrator Login Configuration

The next option required in the installation process is configuring the administrator login. This is sometimes referred to as the platform administrator login. This username/password combination can be used for logging into the Cisco Unified OS Administration, CLI, and Disaster Recovery System applications.

It is advisable to document the chosen username and password, and ensure that this selection follows the company security policies for login information. Additional username/password combinations can be entered through the CLI.

As displayed in Figure 3-15, enter the selected username and password. Re-enter the password a second time to confirm. Finally, press the **Tab** key to highlight the **OK** button, followed by **Enter**.

Figure 3-15 *Administrator Login Information*

The administrator username is case-sensitive and must begin with an alphabetic character and be at least six characters in length. You can use alphanumeric characters, hyphens, and underscores as part of this username.

Certificate Information

The next screen affords the configuration of the certificate information. This page might appear to be simply informational but is required by the server to create a self-signed certificate. This information can be displayed after the installation finishes in Cisco Unified Operation System Administration.

Figure 3-16 displays the certificate information consisting of the organization, unit, location, state, and country.

www.it-ebooks.info

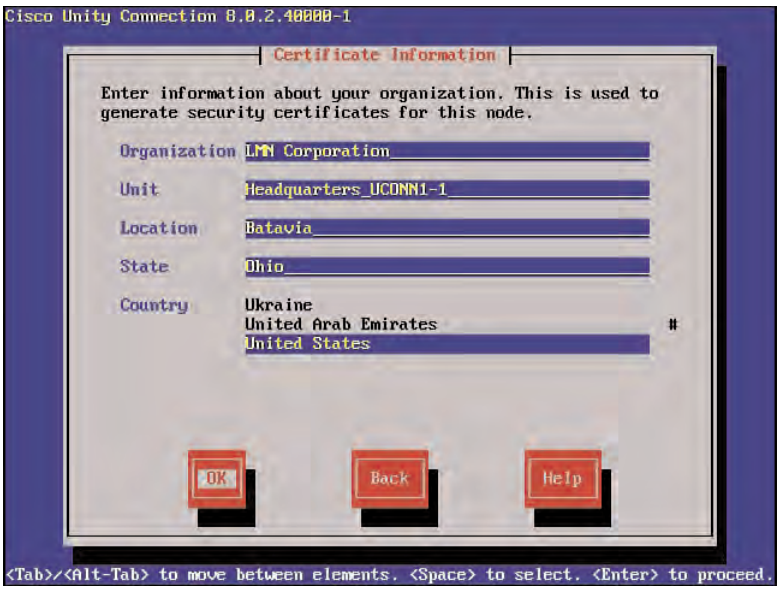

Figure 3-16 *Certificate Information*

First Node Configuration

The installation now proceeds to the first node configuration. Figure 3-17 depicts the First Node Configuration page. This page is a vital decision point based on the function of the Cisco Unity Connection server in the network. Because you install the server in a single server deployment, you need to configure this server as the first node, or publisher. Press the **Tab** key to highlight the **Yes** option and press **Enter**. The only instance in which you need to select **No** on this page is when configuring a server to be the subscriber in an active-active cluster pair. The function of the publisher and subscriber is discussed later in the "Active-Active Cluster Pair Configuration" section.

Network Time Protocol Client Configuration

In previous versions of Cisco Unity Connection, NTP configuration was optional. As of version 8.x, NTP is required to complete the installation. The first node (publisher), as discussed previously, needs to be configured to use an NTP server configured on a network head-end router or a public NTP time server.

Figure 3-18 illustrates the NTP client configuration page. The installer can select up to five NTP servers for redundancy and as few as one NTP source. It is advisable to configure at least three sources for redundancy.

NTP is a hierarchy of levels, called *stratums*. Therefore, the server can synchronize with any accessible server but can select the server with the highest stratum available (the lowest number stratum). To ensure synchronization with an external NTP source, ensure that the configured sources have a stratum nine or better (1–9). In most cases, the server

www.it-ebooks.info

stratum will be at a Stratum 2 (synced directly with an NTP server) or Stratum 3 (synced with a network router, which is already synced with an NTP server).

Figure 3-17 *First Node Configuration*

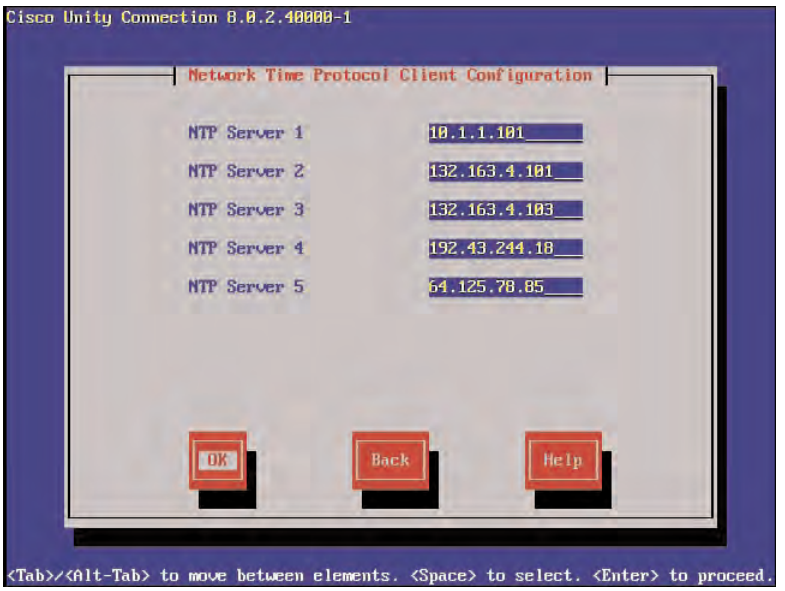

Figure 3-18 *Network Time Protocol Client Configuration*

www.it-ebooks.info

Security Configuration

The security configuration page is now presented to enable the installer to add a security password. This password should be documented and kept secretive. This password is used by a subscriber server in an active-active cluster pair to subscribe to the database. This password, along with the configuration of the subscriber server in the publisher, provides the authentication required for the subscriber to join the cluster and provide the replication of the database from the publisher to the subscriber. This password can also be changed through the CLI after the installation is complete.

The subscriber uses the hostname, IP address, and security password to join the publisher as a cluster pair. Figure 3-19 illustrates the security configuration. Enter the security password and confirm it by entering it a second time. Select the **Tab** key to highlight the **OK** option, and press **Enter**.

Figure 3-19 *Security Configuration*

SMTP Host Configuration

Simple Mail Transport Protocol (SMTP) enables the sending and forwarding of the messages using port 25. You need to configure SMTP when using intrasite links and Voice Profile for Internet Mail (VPIM) networking. SMTP configuration can be performed after the installation is complete by using the Cisco Unified OS Administration or the CLI.

To configure SMTP for this server, highlight the **Yes** option and press **Enter.** To skip the SMTP configuration, highlight the **No** option and press **Enter,** as displayed in Figure 3-20. SMTP configuration is required when networking with intrasite and intersite links

www.it-ebooks.info

with SMTP smart hosts. This configuration is discussed in Chapter 9, "Understanding Cisco Unity Connection Networking."

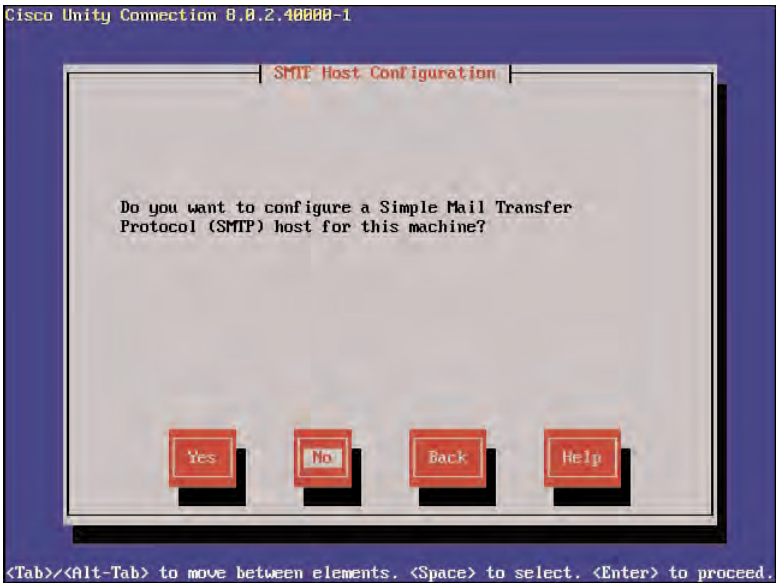

Figure 3-20 *SMTP Host Configuration*

Application User Configuration

The application username and password configuration is the next configuration information that you need to enter, as displayed in Figure 3-21. Enter the username and password, and confirm it in the proper option fields. This username/password combination is used for various administrative web pages, such as Cisco Unity Connection Administration, Cisco Unity Connection Serviceability, and Cisco Unified Serviceability. The application administrator username is not case-sensitive, which is different from the platform administrator username. You need to configure additional username/passwords for administration through the Cisco Unity Connection Administration pages. These application username/password combinations will be created for the individuals that will be the administrators for the system. The various administrative features and options are discussed throughout Part II; however, this specific username/password should be documented and kept secretive.

Platform Configuration Confirmation

The platform configuration confirmation page indicates the end of the first node installation dialogue. This is the final selection before the actually software installation begins and the last chance for the installer to go back and make changes.

To confirm the platform configuration and begin the software installation, select the **Tab** key to highlight the **OK** option, and press **Enter**, as illustrated in Figure 3-22.

www.it-ebooks.info

Figure 3-21 *Application User Configuration*

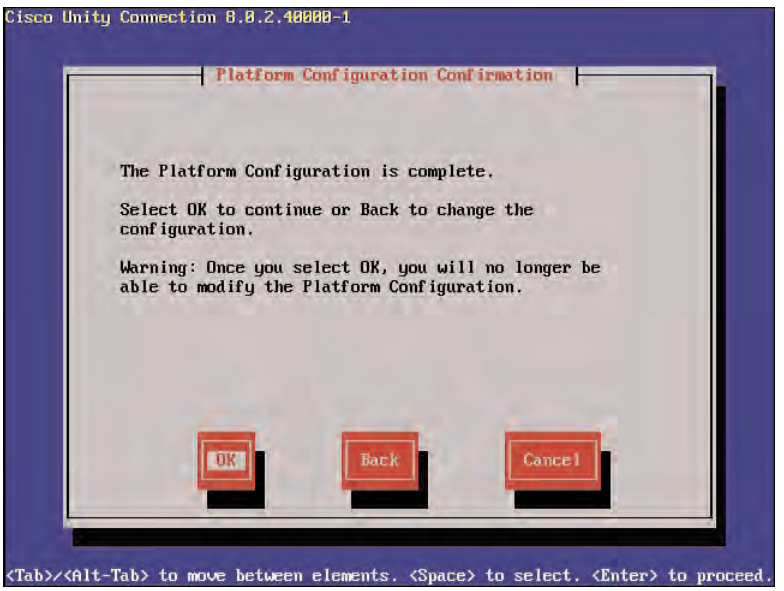

Figure 3-22 *Platform Configuration Confirmation*

www.it-ebooks.info

Software Installation

After the platform configuration confirmation page has been completed, the software installation begins. At this point, the installation might take close to an hour or more, depending on your specific platform. The following procedures occur as the software installation proceeds and consist of the following steps:

Step 1. Format the drive system.

Step 2. Install the platform and the operating system.

Step 3. Install the platform and the post-installation configuration.

Formatting the Drive System

The hard drive is prepared and formatted to enable the installation of Cisco Unity Connection software, as displayed in Figure 3-23. During this time, the active and inactive partitions are configured on the drive space and the partitions required for database, system information, and support.

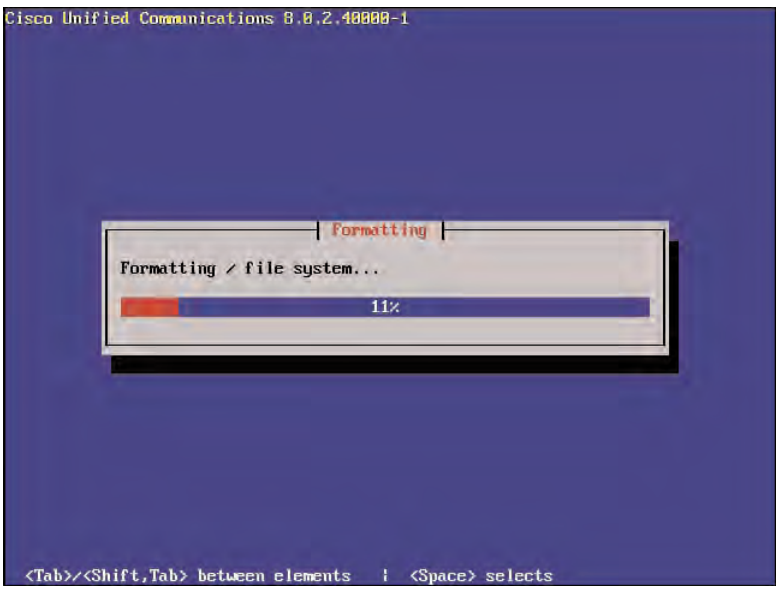

Figure 3-23 *Formatting the Drive System*

Platform Installation: Installing the Operating System

Following the formatting of the drive, the installation of Linux Red Hat version 4.x operating system installation occurs automatically. This is the operating system used for all three products, Cisco Unified Communications Manager, Cisco Unity Connection, and Cisco Unified Communications Manager Business Edition, and is installed as part of the software installation. Third-party software cannot be installed on any Cisco version 8.x applications.

www.it-ebooks.info

Post Install: Performing Post-Install Configuration

Post-installation configuration tasks prepare the operating system and IBM Informix database for the installation of Cisco Unity Connection. The screens displayed during the remainder of the installation tasks can be similar to those listed in Figure 3-24.

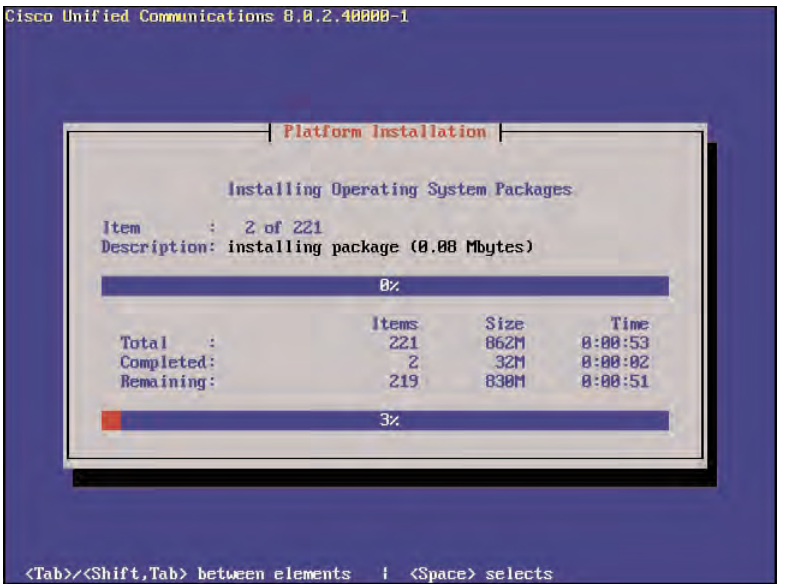

Figure 3-24 *Platform Installation*

Application Installation: Installation, Backup, and Security Checks

The application installation proceeds with the installation of the Cisco Unity Connection software packages and performs the required security checks. As an installer and administrator, you have no access to the root system of the server, except those offered by the CLI and Cisco Unified OS Administration web pages. The Cisco OS Administration web pages provide for the configuration of access by Cisco TAC. This is used specifically for troubleshooting by Cisco TAC and cannot be used for user access to the root of the Cisco Unity Connection system.

Server Restart

Installer is informed about the server restart. The server then continues with the installation, post-installation, and configuration of Cisco Unity Connection software.

Application Pre-Install

After the server starts with the new operating system and database, the Cisco Unity Connection software continues with the installation and post-installation tasks.

www.it-ebooks.info

Configuring Network and Host Files

The final phase of the installation process can commence with the network and host configuration, the DNS, DHCP, or static configuration option.

Network Connectivity Check

After the network configuration has completed, the network configuration of the server and connectivity check is performed. It is imperative that the server connects to the proper switchport, VLAN, and has access to the configured default gateway and NTP servers. Problems that occur with any of these during this connectivity check can cause the installation to pause. The installer must correct the issue before the installation can complete.

In Figure 3-25, an error was purposely caused with the installation by disallowing connectivity between the server and the default gateway during the network connectivity check, as the network connectivity check failure screen displays. At this point, the installer has the option to retry, halt the install, ignore the error and continue, or review the current configuration and make the necessary changes.

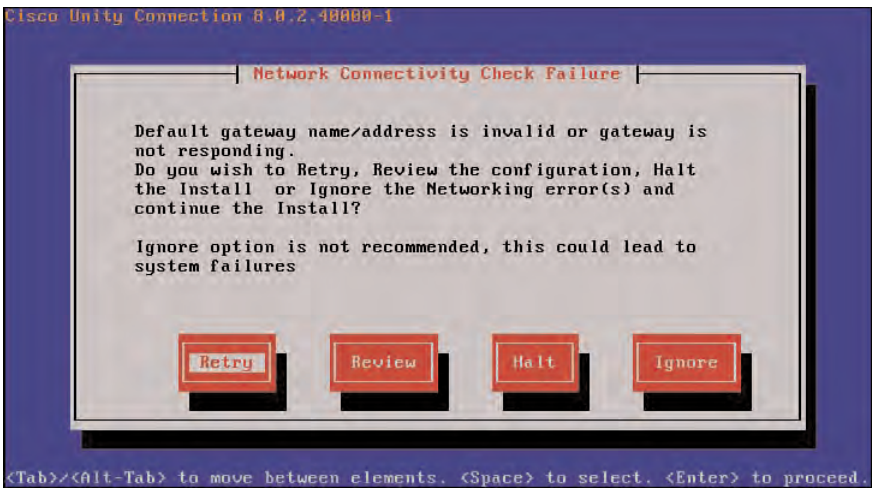

Figure 3-25 *Network Connectivity Check Failure*

License and Cryptographic Informational Page

The final display on the console provides information to the installer about the licensing and cryptography.

Figure 3-26 displays information about the product licensing. When the Cisco Unity Connection server initially is installed, a demo license enables the initial configuration of Cisco Unity Connection users and features. A proper implementation necessitates including the purchase of licenses. The exact licenses are based on the number of users, features, servers, and deployment. This information would have been determined in the planning and design phase.

www.it-ebooks.info

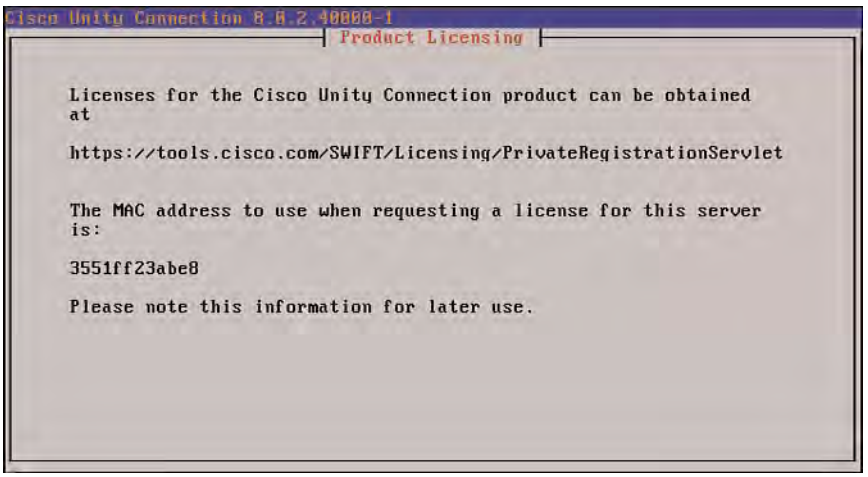

Figure 3-26 *Product Licensing Page*

The license file is based on the purchased Product Authorization Key (PAK) and the MAC address of the server; therefore, this is a good location to make a note of the specific MAC address for your server. The Product Authorization Key (PAK) can be obtained from Cisco or an authorized Cisco partner. The licensing of Cisco Unity Connection is discussed at the end of this chapter.

The cryptography information page displays after the licensing page, as shown in Figure 3-27. This page displays information based on the cryptography of the server.

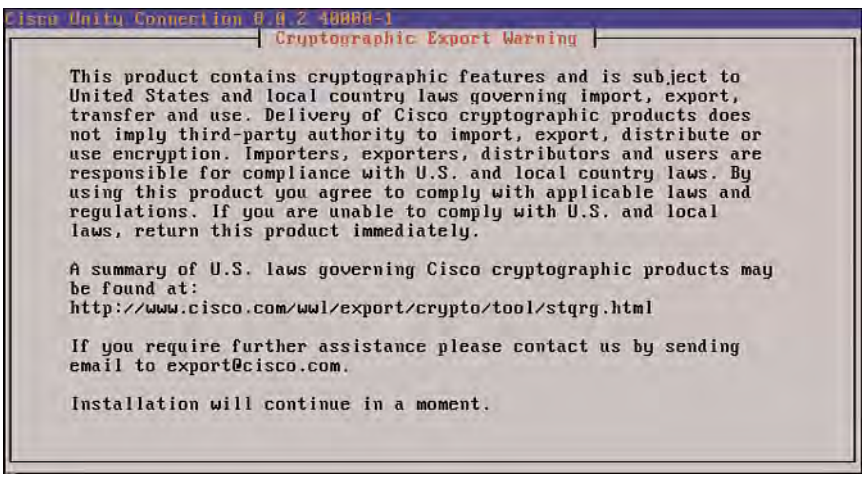

Figure 3-27 *Cryptography Information Page*

www.it-ebooks.info

Application Post-Install: Cisco Unity Connection

The application post-installation automatically completes. This is the final process that occurs as part of the installation procedure. Any final installation scripts required by the installation processes are completed during this final phase.

Installation Complete: Login Prompt

When the installation completes, the login prompt displays, as shown in Figure 3-28. The CLI is the only access directly to the server (console or SSH). The prompt displays the server name, where the installer can login using the platform administration username and password. The CLI is explored further in the next section about installation verification.

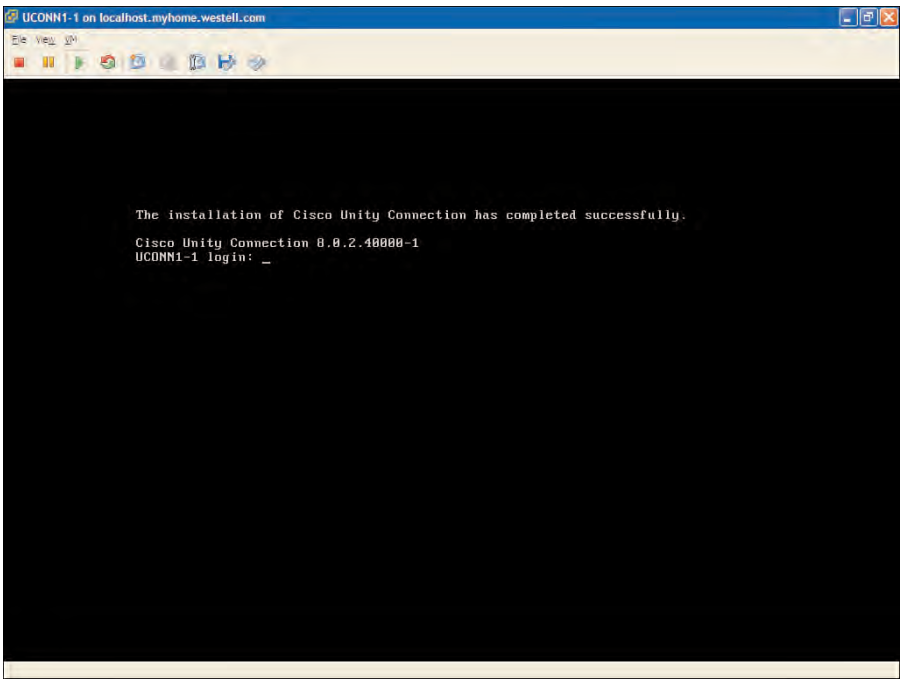

Figure 3-28 *Console Login Prompt (Installation Complete)*

This completes the installation of the single server configuration. This same configuration procedure must be completed for the subscriber in the cluster pair.

The subscriber software installation for a Cisco Unity Connection cluster pair is also the same up to the point of the First Node Configuration screen. The active-active cluster pair configuration is discussed in the “Active-Active Cluster Pair Configuration” section.

www.it-ebooks.info

Cisco Unity Connection Server Verification

After you complete the installation of the Cisco Unity Connection server, you need to verify its operations and services. This verification requires familiarity with and access to the various available interfaces. To begin, you need to understand the various logins available in Cisco Unity Connection.

The administrator and application user login information was entered during the installation process. These two username/password combinations can sometimes be confusing to know which to use for each interface login. To assist your understanding, the administrator login can be viewed as the platform administrator login. This login configures the server or server administration specific features, such as IP addresses, gateways, network time protocol, and so forth. Therefore, this login is used to log in to the Cisco Unified OS Administration, CLI, and Disaster Recovery System. The administrator account should be shared only with installers and engineers that have a thorough understanding and are responsible for platform administration and upgrades and backup and restore operations. Additional platform administrator login credentials can be configured directly through the CLI.

Figure 3-29 illustrates the use of the platform administrator login.

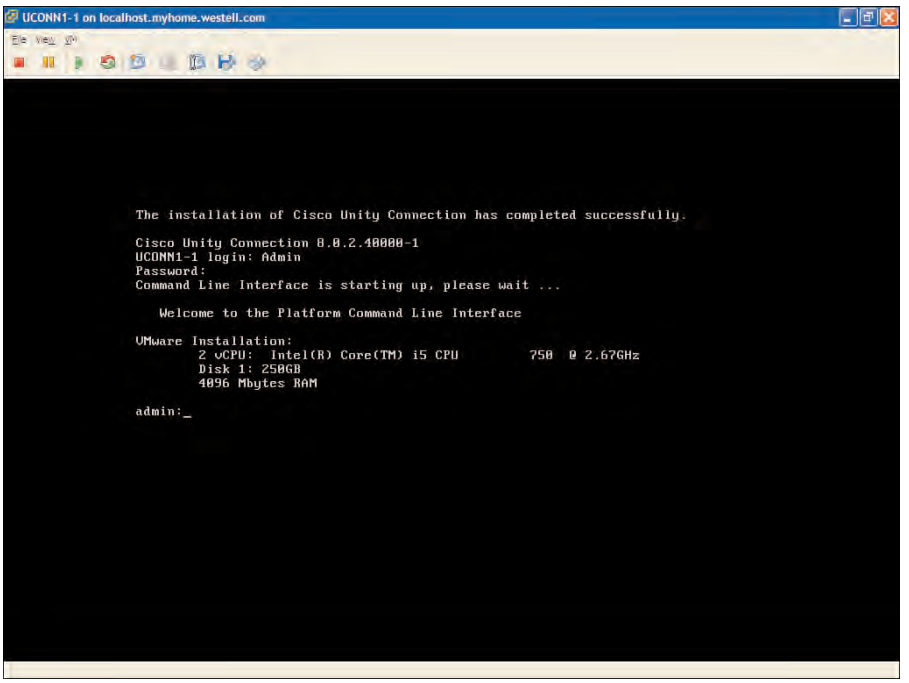

Figure 3-29 *Administrator Login*

www.it-ebooks.info

You need to begin the verification procedure with the CLI. The console displays the hostname of the server followed by the login prompt. As the installer, log in to the console and verify the services and proper operation. Figure 3-30 displays the console, where the user has logged in using the administrator login credentials. When logged in, you can use the **?** to list the available commands. To create additional platform administrator login credentials, use the **set account** command.

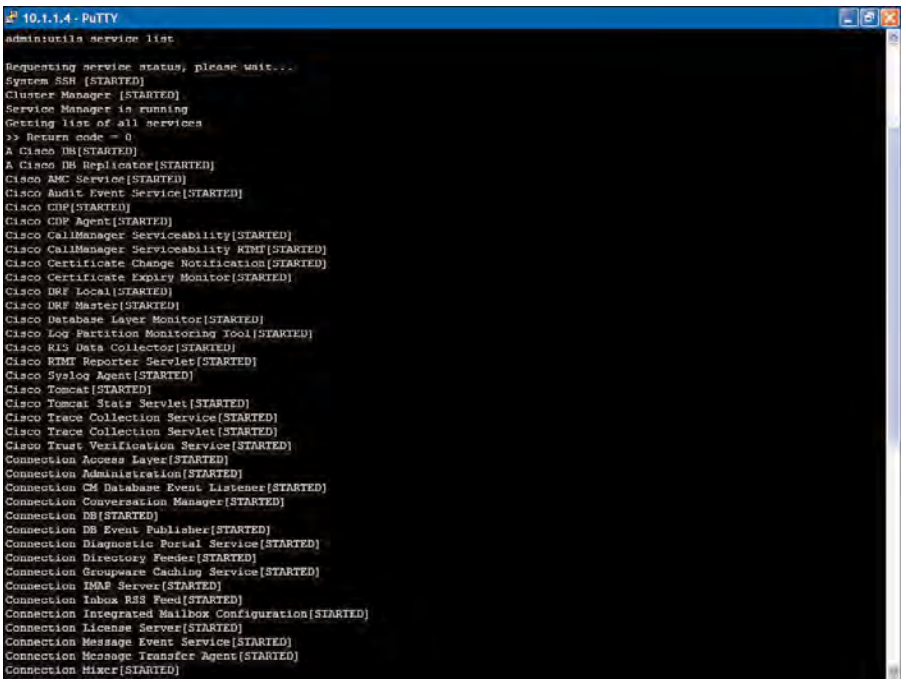

Figure 3-30 *CLI Verification*

To verify the services, type in the **utils service list command**. It might take a few minutes for all services to start completely. During this time, you might notice that services might be listed as **[Starting]**. Repeat the **utils service list** command to ensure that all network services are listed as **[Started]**. Services can be activated through the Cisco Unified Serviceability or Cisco Unity Connection Serviceability web pages. Services that must be activated from these pages are listed as **[Stopped]** in the service list display. You activate the various services as they are needed.

Note Services might take a few minutes to be fully activated. Therefore, allow sufficient time for all services to complete activation.

You want to verify that the Cisco Tomcat service displays as started. This is the service that provides service for all web pages, which are used in the next verification.

www.it-ebooks.info

Cisco Unity Connection Login Verification

You have now verified that all services are operational, especially the Cisco Tomcat service. You need to test the login to the various web pages. Most important, you must verify that all applications are available and the authentication (username/password) is operating correctly.

This is the first time that you have accessed the publisher server, so you need to ensure that your workstation has a supported browser available. Cisco Unity Connection supports the following browsers:

- Microsoft Internet Explorer 8.0 and 7.0
- Mozilla Firefox 3.0 and 2.0

Note In most cases, the default setting should be sufficient; however, you might also need to ensure that Java and Java Scripting is enabled and you accept cookies. If you experience issues accessing the various web pages on your workstation, you might need to reinstall or update Java. Ensure that you use the current version of Java.

Consult Cisco.com for any changes or updates to this information.

Point your web browser to https://<*publisher_ip_address*>/cuadmin. Then, log in to Cisco Unity Connection Administration by entering the application user credentials and selecting the **Login** button, as displayed in Figure 3-31. Ensure that you accept or import the self-signed certificates.

Note You could simply enter the IP address of the server without the extension. In this case, you will be provided a server page to redirect you to the Cisco Unity Connection Administration application.

In the next verification, you need to access the Cisco Unified OS Administration and verify the server status. Point your web browser to https://<*publisher_ip_address*>/cmplatform.

You need to log in to Cisco Unified OS Administration, by entering the administrator user credentials and selecting the **Login** button, as displayed in Figure 3-32.

Note The platform administrator credentials are used to log in to the Cisco Unified OS Administration. These credentials are different from the application administrator credentials used to log in to Cisco Unity Connection Administration.

www.it-ebooks.info

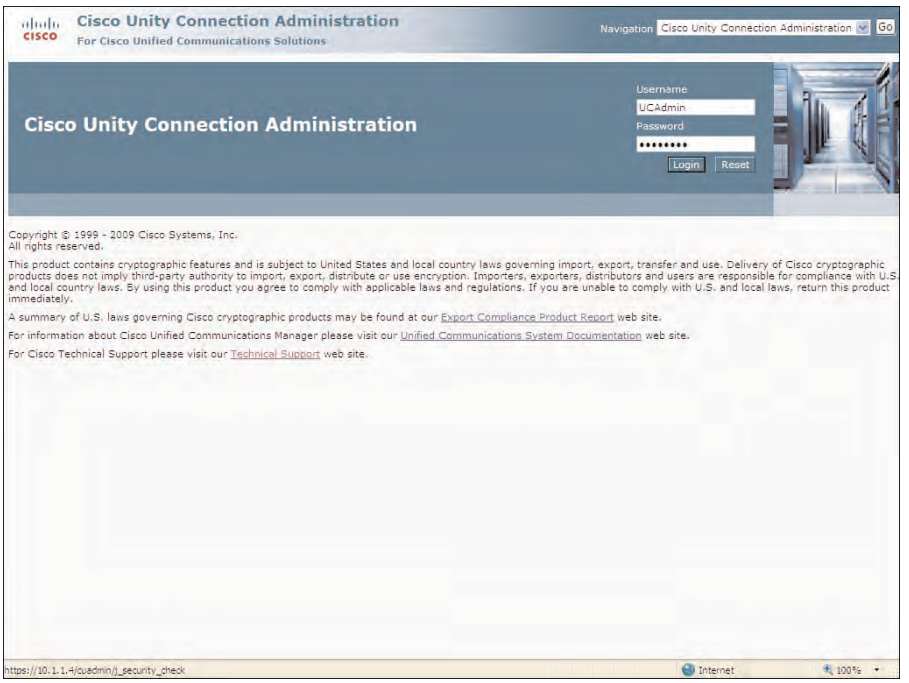

Figure 3-31 *Cisco Unity Connection Administration Login*

From the Cisco Unified OS Administration web pages, you can perform the following functions:

- Show the various network, hardware, cluster, and system settings.
- Configure NTP servers, SMTP configurations, restart, and shut down the server.
- Perform certificate management, IPsec configuration, TFTP file management, and software upgrades.
- Customize the login messages for the various web interfaces and CLI.
- Ping support services such as ping and remote support (to allow Cisco TAC use).

From the Cisco Unified Operating System Administration page, select **Show > System** from the toolbar to display the System Status. The system status displays the current date, uptime, software level, along with the CPU and memory usage, as displayed in Figure 3-33.

www.it-ebooks.info

Figure 3-32 *Cisco Unified OS Administration Login*

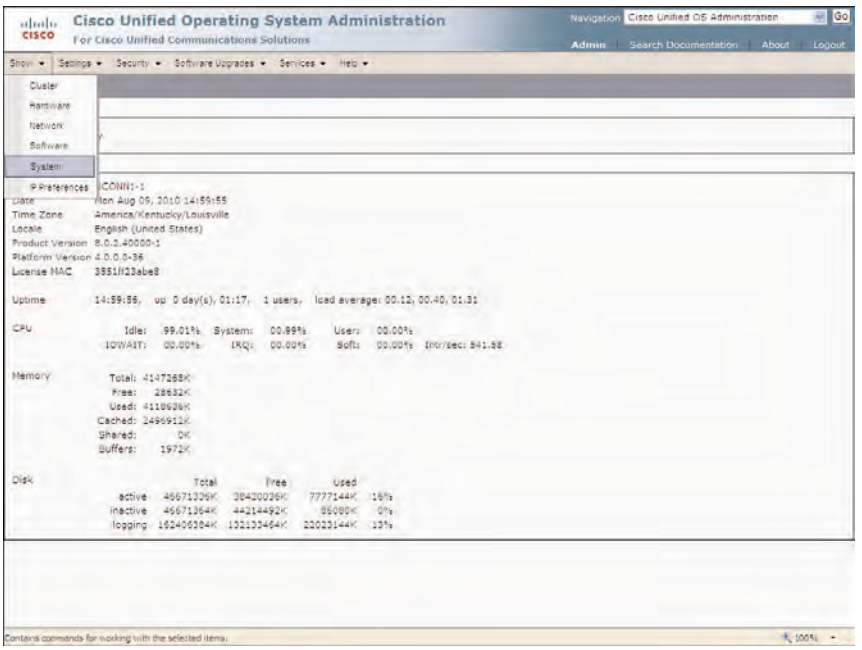

Figure 3-33 *System Status Display*

www.it-ebooks.info

This is a good time to become familiar with the other options available in Cisco Unified Operating System Administration. You need to test these other options as part of the server verification:

- **Show > Hardware:** Checks the hardware platform type, serial number, hardware, and other options related to hardware
- **Show > Network:** Displays the current network interface configuration, status, and packets
- **Show > Software:** Displays the current active and inactive software partitions

You can explore other features in the Cisco Unified Operating System interface throughout this book.

Installation Log Files

If a problem with the installation occurs, you can view the installation log files. From the console or CLI, enter the following command to display a list of available log files:

```
file list install *
```

To view a specific log file from the CLI, enter the following command:

```
file view install log_file
```

Part III discusses the Real-Time Monitoring Tool, which has the capability to view system history, log, and trace files.

Active-Active Cluster Pair Configuration

The active-active cluster pair configuration was first available with version 7.x and is composed of two Cisco Unity Connection servers using the same software level and revision. Only two servers can be used in the cluster, unlike Cisco Unified Communications Manager (CUCM) that can contain up to 20 servers in a cluster. The first server to be installed is the publisher, which is responsible for publishing the database. The second installed server is the subscriber, which subscribes to this database. Therefore, there is still only one database that exists for configuration information and the message store between the two servers.

The cluster pair is considered active-active because both servers are responsible for call handling, IMAP traffic, and HTTP requests for administrative web pages and the Cisco Unified Personal Communications Assistant. Similar to the single server deployment, the cluster pair can still handle traffic for up to 20,000 users and IMAP Idle clients; however, the port capacity is now doubled when using a cluster pair. A single server deployment can support up to 250 ports. The active-active cluster pair can handle up to 500 ports concurrently (250 ports/server).

The active-active cluster provides redundancy and load-sharing to the voice-message environment. If a server fails, the other server continues to provide voice-messaging services

www.it-ebooks.info

for all users; however, there will be half as many ports available until the failed server is restored. For complete redundancy, it is best to ensure that you have configured enough ports on a single server to handle the total amount of voicemail traffic. For load sharing, the active-active capability of the cluster enables the installer to direct traffic to either server as needed. The recommended integration dictates sending the majority of call traffic to the subscriber, while sending client traffic (IMAP, HTTP, Outlook, and so on) to the publisher server. Of course, both servers (publisher or subscriber) can handle both types of traffic.

Publisher Installation

The publisher in a Cisco Unity Connection cluster pair is considered to be the first node and is always the first server to be installed. As the term implies, the publisher is responsible for publishing the database and message store to the subscriber. If you use a single server deployment, this server is actually a publisher without a subscriber server configured and installed.

Subscriber Installation

The subscriber in the active-active cluster pair is the second (and last) server installed. During the installation of the subscriber, the publisher server must be available and have the subscriber configured to enable the subscriber to join the cluster. During the subscriber installation, the installer is required to provide the following information configured on the publisher server:

- Publisher's hostname
- Publisher's IP address
- Security password (originally configured on the publisher server)

If these three elements are not configured, or are entered incorrectly, the subscriber server cannot be allowed to join the cluster. This provides the needed security for the voice-messaging system by preventing any rogue servers from joining the cluster. If the hostname and IP address of the publisher are correct, the subscriber uses the configured security password to subscribe to the configuration database and message store. The security password was configured in the installation dialogue of the publisher server and can be changed only through the CLI of the publisher server. The subscriber installation does not include an NTP configuration because it synchronizes its time from the publisher server.

The following pages illustrate the configuration of the subscriber server in an active-active cluster pair from the point forward of the First Node Configuration screen display. Previous to this, the installation is identical.

www.it-ebooks.info

Subscriber Server Installation

As stated earlier, the installation of the subscriber node up to the first node configuration screen is exactly the same. From this point forward, the subscriber installation is markedly different. Therefore, the configuration procedure from the First Node Configuration page is discussed as it applies to the subscriber. The processes that occur for a subscriber installation follows:

- System Installer (includes media and platform checks)
- Product Deployment Selection
- Platform Installation Wizard
- Installation Dialogue
- First Node Configuration
- Subscriber Node Installation Dialogue
- Software Installation
- Formatting Drive System
- Platform Installation: Installing the Operating System
- Post Install: Performing Post-Install Configuration
- Application Installation: installation, backup, and security checks
- Server Restart
- Application Pre-Install
- Configuring Network and Host files
- Network Connectivity Check
- License and Cryptographic Informational page
- Application Post-Install: Cisco Unity Connection
- Installation Complete: Login Prompt

The following section discusses the publisher and subscriber configuration from the perspective of creating an active-active cluster pair.

Before configuring the subscriber server, you need to access the publisher server and configure the IP address of the subscriber in Cisco Unity Connection Administration. Also, this can verify access to the various web pages within the server configuration.

First Node Configuration

Before configuring the subscriber server, you must first log in to the Cisco Unity Connection Administration web pages on the publisher server or first node using the application user credentials. Then, you need to add the IP address of the subscriber server under the cluster configuration.

www.it-ebooks.info

To complete this task, select **System Settings > Cluster** from the navigation pane on the left portion of the page in Cisco Unity Connection Administration. The Find and List Servers page displays on the right portion of the screen. The name of the publisher server is listed. Select the publisher server name. The Server Configuration page for the publisher displays, as shown in Figure 3-34.

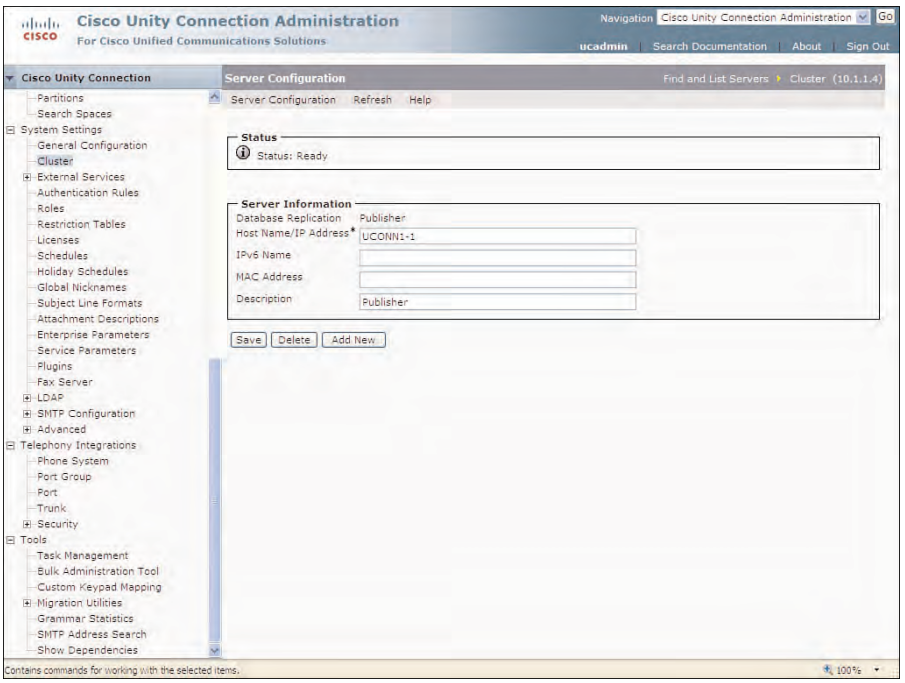

Figure 3-34 *Server Configuration*

If you are not using DNS, change the name of the server here to the correct IP address of the server and add a description, if wanted. Click the **Save** button to ensure that all changes are written to the database.

Note IPv6 and MAC address configuration are optional fields on the Server Configuration page. However, changing the server name to its respective IP address is optimal to eliminate the reliance on DNS.

Note You must select the Save button whenever changes are made to any of the web pages. If you exit the page without saving, all changes will be discarded.

www.it-ebooks.info

Select **Server Configuration > Find and List Servers** from the toolbar. Then, click the **Add New** button to add the subscriber server to the cluster. The server configuration page displays.

Enter the IP address of the subscriber along with a description, if wanted, as displayed in Figure 3-35. Click the **Save** button to complete the operation.

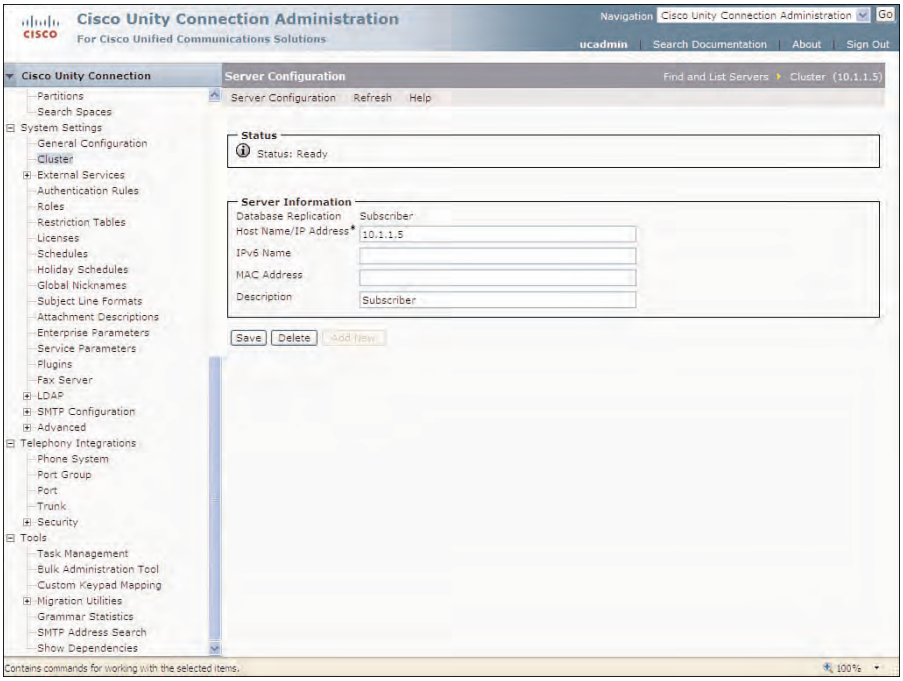

Figure 3-35 *Subscriber Server Configuration on the Publisher*

Select **Server Configuration > Find and List Servers** from the toolbar again. The Find and List Servers page displays the publisher, and subscriber IP addresses are listed, as shown in Figure 3-36. Also notice that the **Add New** button is no longer available because you cannot add more than one subscriber to an active-active cluster pair.

Note Adding a subscriber to the cluster pair can take up to five minutes to complete.

You are now finished with the publisher configuration. Make sure that the publisher server is online and has connectivity to the subscriber server before beginning the subscriber software installation. You might want to verify the server connectivity and ensure that the proper licensing is purchased and installed on the publisher server.

www.it-ebooks.info

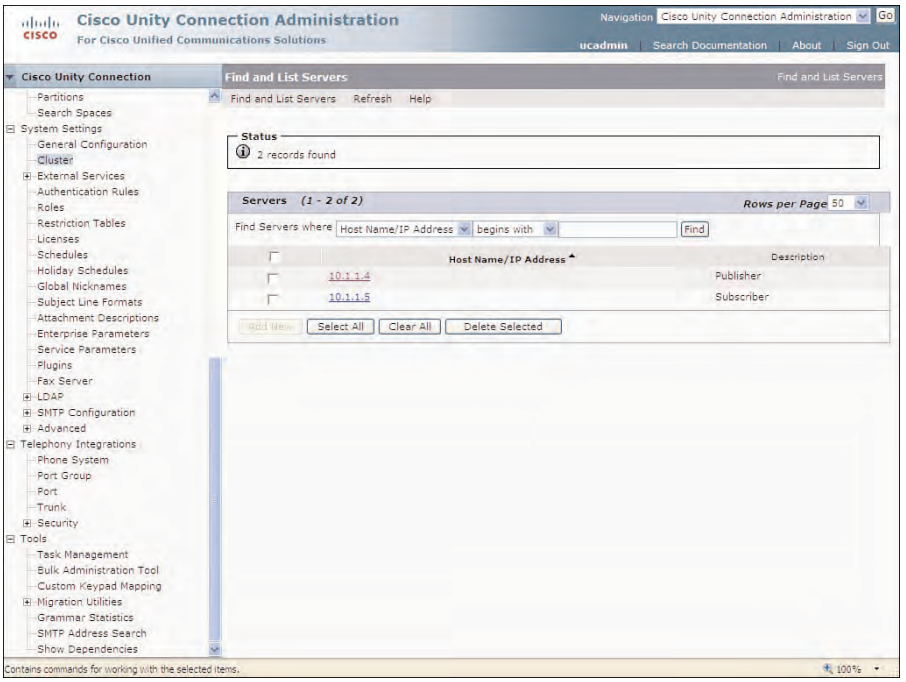

Figure 3-36 *Find and List Server Page Displaying an Active-Active Cluster Pair*

Subscriber Software Installation

To begin, all the options that were discussed pertaining to the publisher also apply to the subscriber. Perform the software installation exactly the same up to the First Node Configuration screen. Therefore, the subscriber installation discussion begins from this point.

First Node Configuration

On the First Node Configuration page of the subscriber, select the **No** option to indicate that this server is to be installed as the subscriber, as shown in Figure 3-37.

Subscriber Node Installation Dialogue

The next few screens will begin the Subscriber Node Installation Dialogue. The warning message indicates that the publisher should be available and configured with the subscriber IP address before beginning the installation. Because you have already completed this step, select **OK** to begin the installation dialogue, as shown in Figure 3-38.

At this point, the Network Connectivity Test Configuration page displays. On this page, you have the option to perform the installation immediately after the validation by selecting **No**, or to pause the installation after verification. In some cases, such as in a

www.it-ebooks.info

production network, it might be beneficial to perform the installation at a later time. This screen is shown in Figure 3-39.

Figure 3-37 *First Node Configuration Page for the Subscriber Server*

Figure 3-38 *First Node Configuration Options Page*

www.it-ebooks.info

Figure 3-39 *Network Connectivity Test Configuration Page*

First Node Access Configuration

Figure 3-40 illustrates the first node access configuration page selections. The installer must supply the correct publisher hostname, IP address, and security password. Confirm the security password, and select **OK** to complete the subscriber dialogue.

This information is verified during the installation process. Any incorrect entries on this page disallow the subscriber server from joining the cluster. In some cases, this verification might require multiple retries to complete the verification process.

After the First Node Access Configuration page finishes, the only other selection that needs to be made is for the SMTP Host Configuration, followed by the Platform Configuration Confirmation, which are both similar to what was completed during the publisher installation. After this point, the software configuration begins and completes through to the login prompt.

Active-Active Cluster Pair Verification

After the installation completes and the console displays the CLI login prompt, the service takes a few moments to start completely and a little longer for the subscriber to subscribe to the database that will be published by the first node, or the publisher. You can view this status in Cluster Management, which is included in the Cisco Unity Connection Serviceability web pages.

From a web browser, you need to access the Cisco Unity Connection Serviceability and verify the server status. Point your web browser to *publisher_ip_address*/cuservice.

www.it-ebooks.info

Figure 3-40 *First Node Access Configuration Page for the Subscriber Server*

You need to log in using the application user credentials and select the Login button. Then, select **Tools > Cluster Management** from the toolbar. The Cluster Management page displays, as shown in Figure 3-41.

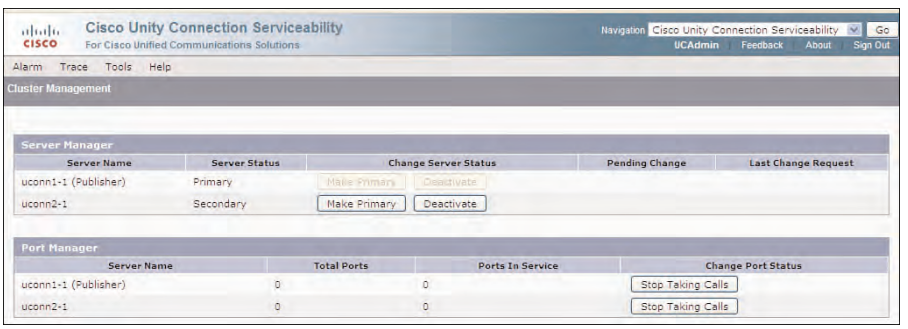

Figure 3-41 *Cluster Management Verification*

You need to review a number of items as part of the verification procedures. First, you want to ensure that both the publisher and subscriber are listed. Then, review the Server Status column and ensure that the publisher server is listed as Primary and the subscriber is listed as Secondary.

When a subscriber first attempts to join the cluster and subscribe to the database, both servers might attempt to contend for the Primary status. In this case, a **Split Brain**

www.it-ebooks.info

Recovery condition might exist. However, this condition should last for a only few moments until the servers detect that the cluster exists. At this point, the publisher is assigned the Primary status, while the subscriber will be assigned the Secondary status, as shown in Figure 3-41. This is the normal operating condition of the cluster pair.

You can also notice that the Change Server Status column enables the user to force a change of Primary to the subscriber. You can also deactivate the subscriber operating in Secondary mode from this section. A publisher can never be deactivated; neither can a subscriber server operating as Primary be deactivated. To deactivate a subscriber, you must ensure that the server operates with secondary server status.

The differences between Primary and Secondary can sometimes be confusing because both servers are actively processing voice-message traffic. The Primary server is responsible for publishing the database information and message store to the other server. It is also the server that is responsible to initiate message notifications, MWI requests, and SMTP and VPIM messages, and processes IMAP traffic, email applications, and Cisco PCA applications. The Secondary server can receive the database and message data that is replicated from the Primary. Any traffic and changes processed by the Primary (message notification, MWI, and so on) will be replicated by the Primary to the Secondary server. The Connection Server Role Manager service can run on both publisher and subscriber and is responsible for detecting this server status and initiating role changes (Primary and Secondary) between servers and for sending alarms and notifications about role change events.

As was stated in the design discussion of ports, the majority of call traffic should be directed to the subscriber, while the client traffic (IMAP, Cisco PCA, and so on) should be directed to the publisher. Because the publisher can automatically be established as the Primary, it makes sense that it should be responsible for the bulk of client traffic.

When the cluster is correctly operating, the Cluster Management display indicates the publisher as Primary and the subscriber as Secondary status. The publisher assumes Primary responsibilities, which is to publish the database and message store. If the publisher server fails, the subscriber can assume this responsibility of publishing the database and message store until service is restored to the publisher. This is a completely different concept from the publisher and subscriber servers in CUCM, in which a publisher will be responsible for replication, and the subscribers cannot assume this responsibility.

A couple of other conditions might occur under the Server Status of the Cluster Management page. A server might temporarily display the status of **Replicating Data**, Starting, or **Split Brain Recovery** during the startup initiation phase, when the subscriber is joining the cluster. **Split Brain Recovery** might also occur if the subscriber loses contact with the publisher. This condition occurs when both servers attempt to assume the Primary server status.

If a server has been manually deactivated, the status displays as **Deactivated**. This is different if a server has been shut down or becomes unavailable, in which case the server status displays as **Not Reachable**.

www.it-ebooks.info

In Figure 3-42, the publisher server has failed. The Server Status for the publisher indicates **Not Reachable**. On the Subscriber server, the Connection Server Role Manager has lost connectivity to the publisher and therefore has assumed the server role of Primary.

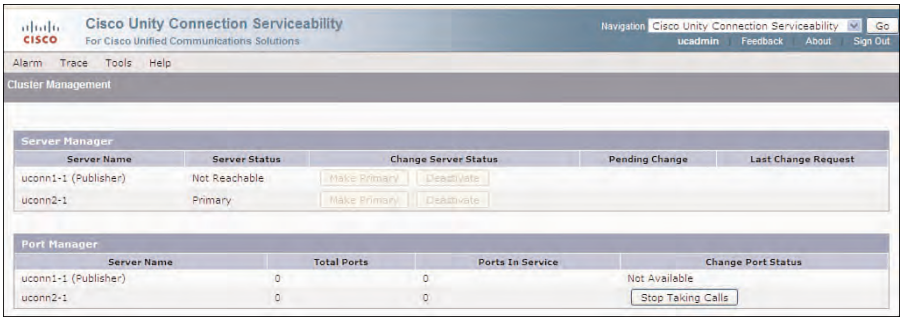

Figure 3-42 *Cluster Management: Publisher Failure*

Unattended Installation Using the Answer File

The last method to perform an installation is the unattended installation using an *answer file*. This method enables the installer to supply a configuration file on a USB or floppy drive for the installation and thereby skips the installation dialogue. This method is useful when you ship the product to a remote location and someone else is connecting and powering up the server. In this case, they do not need to respond to the various questions about the configuration. The answer file is automatically accessed to supply this configuration information.

To begin, you need to access the Answer File Generator on Cisco.com at **www.cisco.com/web/cuc_afg/index.html**.

Complete the information and choose to generate by the answer file by clicking the button near the bottom of the page. Figure 3-43 illustrates the Answer File Generator website on Cisco.com.

After generating the answer file, the option is presented to enable the download of the answer file. Select the **Download File** button to begin the download procedure, as illustrated in Figure 3-44.

Follow the direction to download the file. Ensure that the answer file is saved as *platformConfig.xml*.

After you download the answer file, save the file to the root directory of a USB drive or floppy disk. You need to have access to this file during the final installation process.

Note Some servers might not read larger USB drives. If problems are encountered, try using a smaller USB, which should accommodate the size of the required configuration file.

www.it-ebooks.info

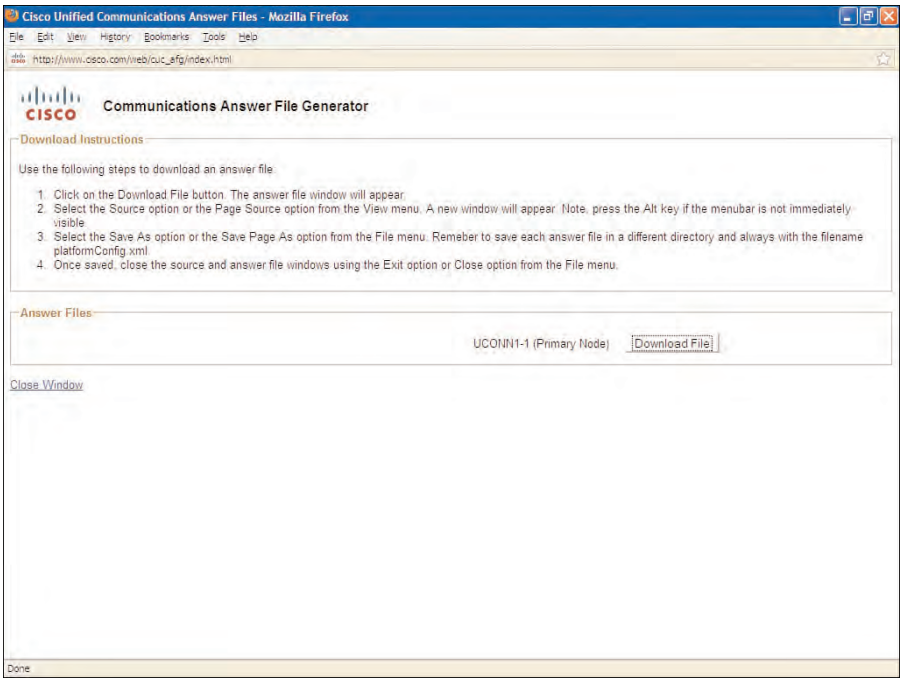

Figure 3-43 *Answer File Generator*

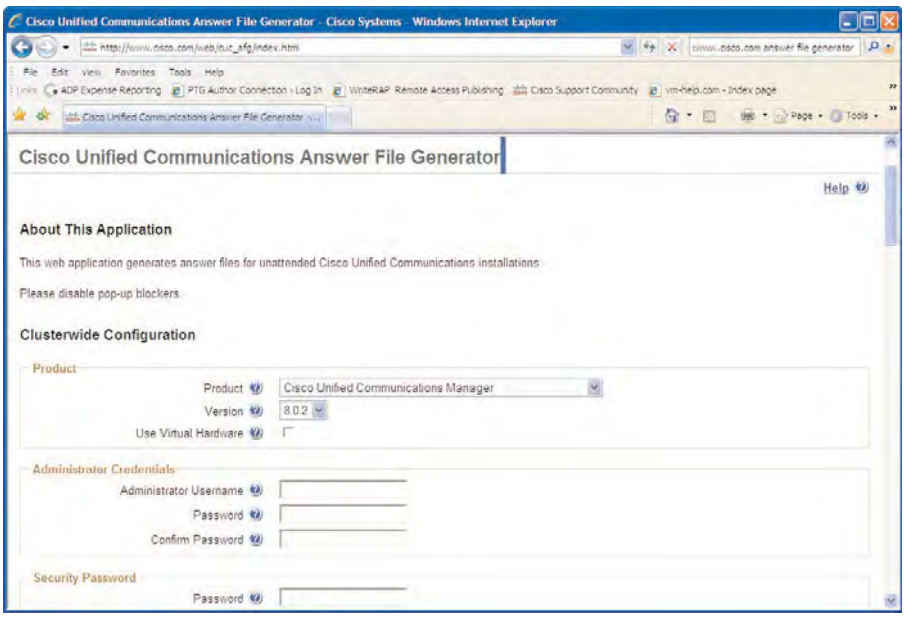

Figure 3-44 *Download Instructions Page*

www.it-ebooks.info

During the Platform Installation Wizard, you want to choose **Skip** to complete the unattended installation, as shown in Figure 3-45.

Figure 3-45 *Platform Installation Wizard: Unattended Installation*

After **Skip** is chosen from the Platform Installation Wizard page, the software installation proceeds followed by the prompt for the configuration answer file. The Pre-Existing Configuration Information page displays, as illustrated in Figure 3-46. The installer is prompted to insert the USB or floppy drive to complete the installation. If the USB or floppy drive is not located when the installer selects **Continue**, the installation proceeds to the Platform Installation Wizard. At this point, the installer could enter the specific configuration information as previously discussed to complete the installation.

Performing Software Updates

You can use a number of different methods to perform software updates. You can perform software updates during the installation or by using the Cisco Unified OS Administration. The first method is normally done when you apply a software update to a software release performed as part of the original install. In some cases, the DVD might be out-of-date when media is received. This method is the fastest way to get to the latest software level. The installation process using the Cisco Unified OS Administration is usually performed on a production server to update to a new release, software patch, or update. In this case, the initial software install is already complete, and the system is in operation.

www.it-ebooks.info

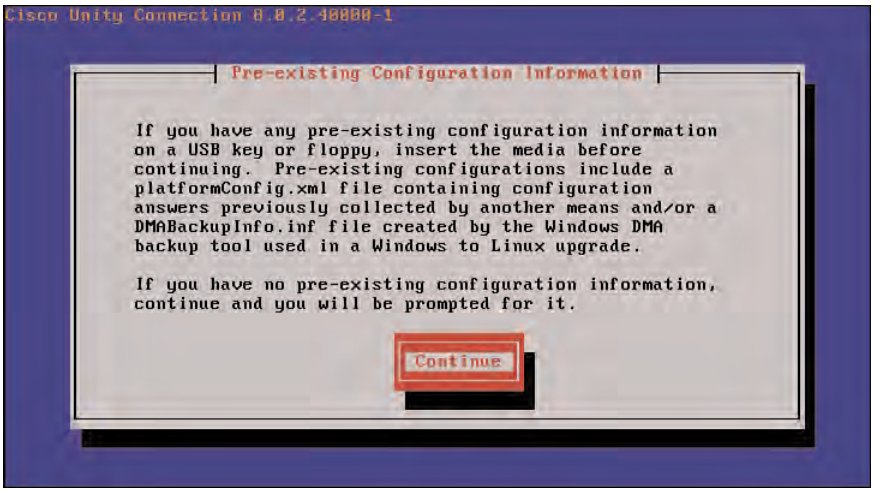

Figure 3-46 *Pre-Existing Configuration Information*

Note The restore operation cannot be used as a method to upgrade. When rebuilding a server to be restored from backup, the version level must match the backup version to successfully complete the restore operation.

Upgrade During Install

To perform the upgrade during the installation, you need to select **Yes** to the Apply Patch question after the Platform Installation Wizard, as displayed in Figure 3-47.

When the Apply Patch option is answered as **Yes**, the software installation begins. This is different from the basic installation, where the installer is presented with the installation dialogue configuration. In this case, the process is reversed, meaning that the initial software installation will be completed first, followed by the installation dialogue configuration.

After the software installation procedure completes, the server reboots and continues the installation followed by the Install Retrieval Mechanism Configuration.

At this time, the installation procedures automatically prompts for the location of the upgrade. This needs to be available on a network server via SFTP or FTP, or on a DVD media inserted in the local drive. Figure 3-48 illustrates the Install Upgrade Retrieval Mechanism Configuration page. After selecting the option for SFTP or FTP, the installer is prompted for the file and location after the network configuration. Selecting **LOCAL** automatically searches for the image on the appliance DVD drive. The use of SFTP and FTP requires the proper configuration and availability to an external server. SFTP provides a faster method for upgrades and patches, compared with using the DVD.

www.it-ebooks.info

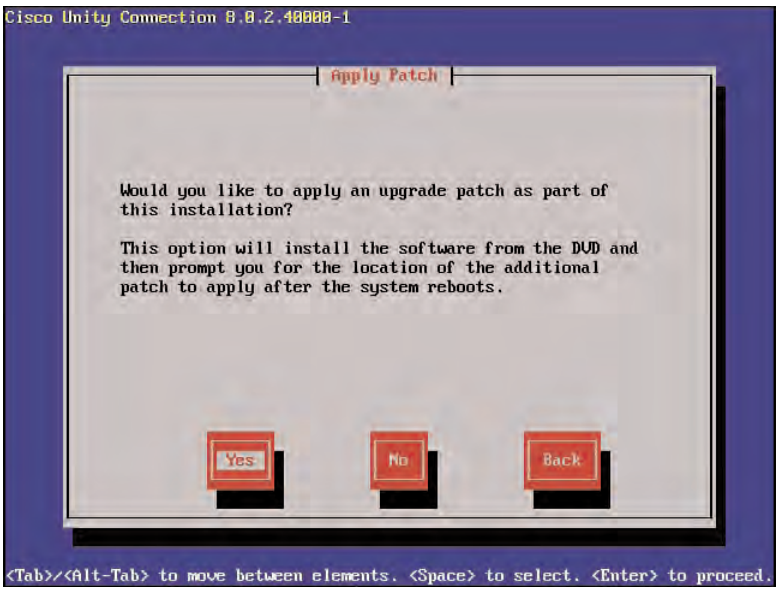

Figure 3-47 *Apply Patch: Perform an Upgrade During Install*

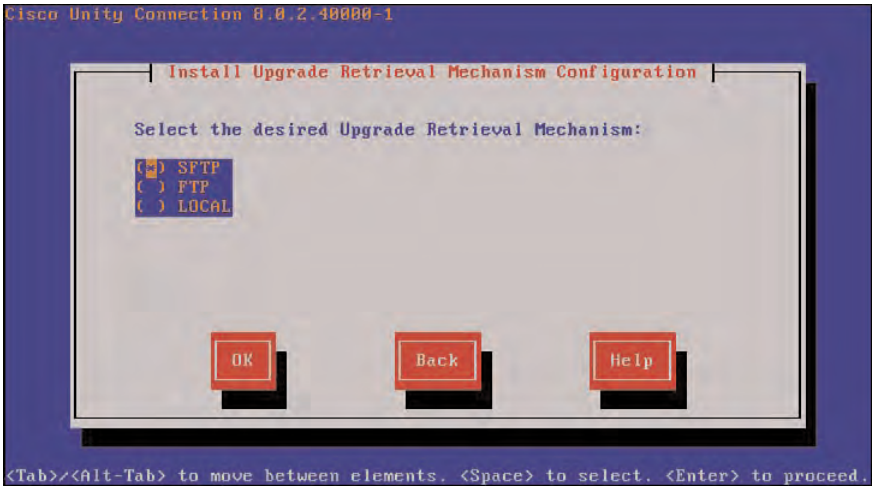

Figure 3-48 *Install Upgrade Retrieval Mechanism Configuration*

The upgrade during install then proceeds based on the software patch or update. The installation again prompts for a reboot a second time, followed by the installation dialogue configuration.

www.it-ebooks.info

Upgrade Using Cisco Unified OS Administration

If the Cisco Unity Connection server is already in production and needs to be upgraded to a new release, the Cisco Unified OS Administration provides the necessary tools to complete this upgrade operation. You can perform a direct upgrade from Cisco Unity Connection version 7.1(3) to the current shipping version of Cisco Unity Connection version 8.x. Some versions of Cisco Unity Connection 2.x can be directly upgraded to version 8.x; although some releases might require an intermediate upgrade to version 7.1(3). In these cases, you need to check the specific release note on Cisco.com for your version.

The Cisco Unity Connection database is designed with two valid partitions of which only one can be active at any point in time. The active partition is the current version that is operational. When you perform an upgrade, the software uploads to the inactive partition. In this way, the server continues to operate, while the software is uploaded. To perform the upgrade, you need to initiate the **switch version** command from the CLI or Cisco Unified OS Administration.

To begin the upgrade process, you need to log in to the Cisco Unified OS Administration web pages using the administrator login credentials. Select **Software Upgrades > Install/Upgrade** from the toolbar. The Software Installation/Upgrade page displays, as illustrated in Figure 3-49.

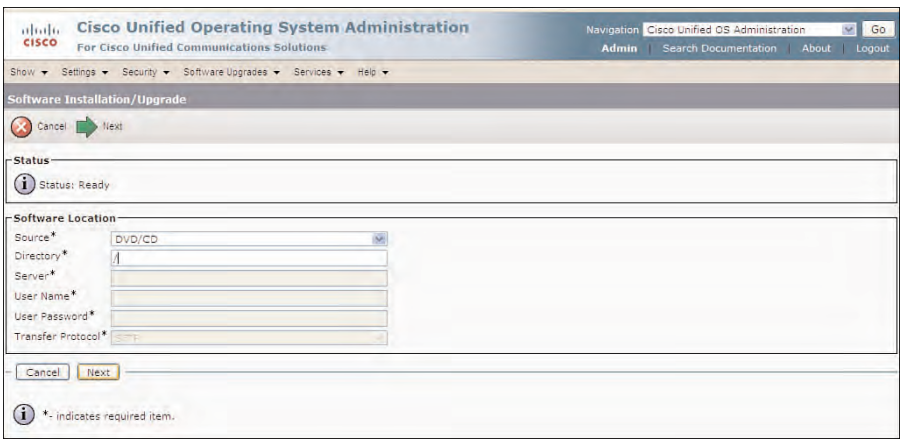

Figure 3-49 *Software Installation/Upgrade*

Select either DVD/CD or Remote File System from the Source drop-down. If using the Remote File System, select the proper directory, username, password, and transfer protocol (SFTP or FTP). Ensure that the upgrade file is available on the selected location along with the proper credentials.

If using the DVD/CD option, ensure that the DVD is inserted in the local drive and select **/** for the Directory option and click **Next**. The upgrade version displays and enables the installer to proceed with the upgrade. During the software installation process, the server

www.it-ebooks.info

continues to process calls and voice messaging because the new software will be installed on the inactive partition.

To upgrade to the new version of software from Cisco Unified OS Administration, select **Settings > Version** from the toolbar. Review the versions available for the active and inactive partitions. Select the **Switch Version** options to begin the upgrade to the new version. At this point, the server restarts with the new version, so you need to perform this operation during off-hours or a maintenance window.

If using the CLI, use the **utils system switch-version** command to switch from the active to the inactive partition. Using the CLI or Cisco Unified OS Administration performs the same operations.

To accomplish the upgrade of a cluster pair, you need to upgrade the publisher first and then the subscriber. The subscriber continues to provide voice-messaging service during the version switching on the publisher server. After upgrades have completed, you need to check the database replication and server status using the CLI and Server Management in Cisco Unity Connection Serviceability pages.

Upgrades from Unity and Unity Connection 1.2

There might be cases in which an upgrade to Cisco Unity Connection is not supported by using the previously mentioned methods. In this case, you can use an available tool for this purpose, specifically for upgrades from Cisco Unity and Cisco Unity Connection 1.2. This tool is the Cisco Objected Backup and Restore Application Suite (COBRAS) and is available for download at **www.ciscounitytools.com. This website is referenced throughout this text because it has many useful tools, updates, and training information available to installer, administrators, and users.**

The COBRAS tools are a suite of applications that enable partial backups and restore between different versions of Unity to the current version of Cisco Unity Connection. This tool is discussed in its entirety in Part III.

Virtual Installation Overview

Cisco supports the installation of Cisco Unity Connection version 8.x software on a virtual machine; however, specific restrictions and specifications must be adhered to. Currently, you must use VMware ESXi v4 Update1 or later on the host server supporting Cisco Unity Connection. The number of users supported on the virtual machine can vary depending on the number of CPUs, RAM, and virtual disk space allocated, and depending if you deploy templates. However, the maximum number of users supported for virtual implementations is currently 20,000 users.

When performing an installation, the virtual machine parameters must be correct for the installation to complete successfully. Cisco provides two different templates that you can deploy for installation up to 20,000 users. These templates assist the installer and ensure that the correct settings are configured for the virtual installation.

www.it-ebooks.info

Open Virtual Machine Format (OVA) Extension

OVA is the extension for the Open Virtualization Format (OVF). OVF is a standard method to package, create, and distribute virtual machines. This helps simplify the installation of Cisco Unity Connection. For example, the installer can download the desired template from Cisco.com and deploy this template in ESXi to assist with the Cisco Unity Connection installation. Of course, the use of the template is optional. However, the template ensures that all configuration settings are correct and applicable to the desired installation and number of users. At press time, the latest templates available for download are listed as follows (see Cisco.com for currently available options):

- **CUC_1000_user_v1.0_vmv7.ova:** Supports 1000 users.
- **CUC_20000_user_300GB_v1.0_vmv7.ova:** Supports 20,000 users
- **CUC_20000_user_500GB_v1.0_vmv7.ova:** Supports 20,000 users

Changing the virtual machine setting is not supported and can cause the virtual machine to pause during the boot up processes. Figure 3-50 and Figure 3-51 illustrate the console messages that display (in that order) when the installer changed the memory allocation for the Cisco Unity Connection virtual machine. The installer must respond to these messages before the startup procedure can continue. For the second screen, the installer must select **Agree** to choose to continue with the startup with an unsupported platform. Therefore, changing the virtual machine setting is not recommended, except in lab testing, pilot, or other nonproduction environments.

Figure 3-50 *Hardware Configuration Error (Screen 1)*

www.it-ebooks.info

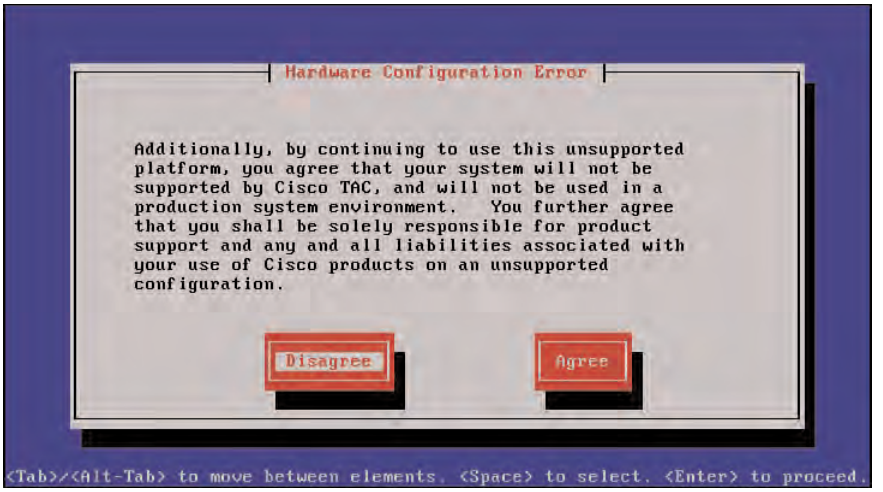

Figure 3-51 *Hardware Configuration Error (Screen 2)*

The use of virtual machines can support the active-active cluster feature; however, the publisher and subscriber must be installed on different host machines to ensure high availability.

If performing an unattended installation, you must have access to a floppy drive because USB is not supported for virtual installations. For the basic installation, similar to the physical platform installation method, you must have an NTP server available and accessible to the server to complete the installation.

The first supported version for virtual installations is release 8.0(2). The complete discussion of the virtual installation is not covered in this text. Therefore, it is advisable to consult the release notes about the specific level and type of installation for your implementation.

Understanding Licensing in Cisco Unity Connection

Cisco Unity Connection ships with a demo license that is automatically configured during the installation process. The available licenses can be viewed in Cisco Unity Connection Administration.

You need to log in to Cisco Unity Connection Administration and select **System Settings > Licenses**. The License page displays, as illustrated in Figure 3-52. Notice that the Status section mentions the filename as ***CUCdemo.lic***. This is the demo license file, where all license files will end with the ***.lic*** extension.

www.it-ebooks.info

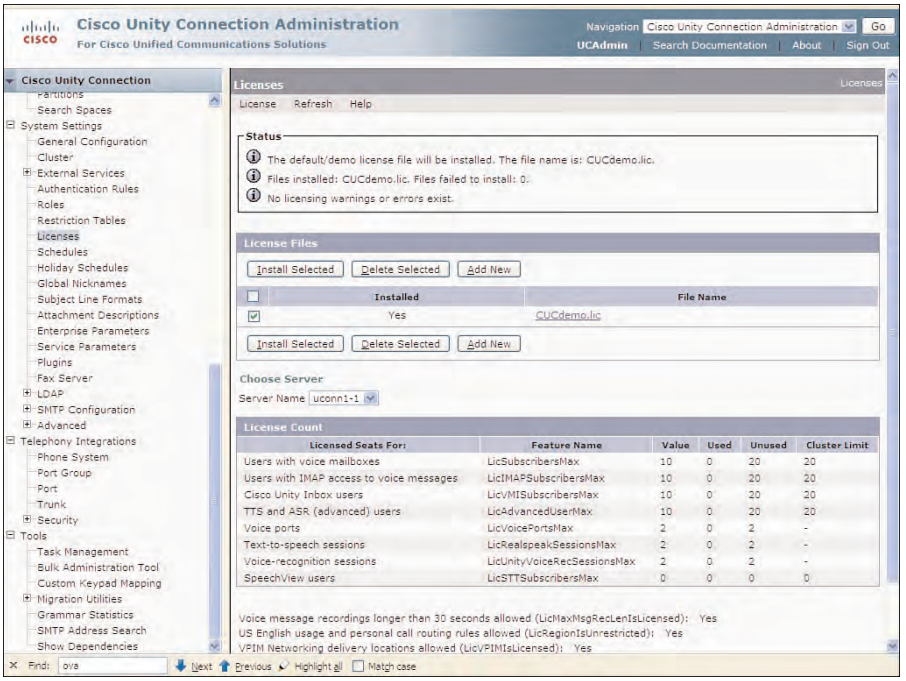

Figure 3-52 *Demo License in Cisco Unity Connection Administration*

The license count displays in the lower section of the screen. The demo license file provides support for 10 users with voice mailboxes, including Unity Inbox, IMAP, and TTS. Two voice ports are also provided for each server. Other features included with the demo license are active-active cluster pairs, VPIM networking, and voice recordings longer than 30 seconds. Demo licenses are automatically installed and not registered to a specific MAC address.

From this page, you can install a valid license file in Cisco Unity Connection by clicking the **Add New** button on the License page.

Depending on your specific implementation you need to acquire a number of different types of license files. These licenses consist of top-level software licenses, server licenses, user licenses, HA licenses, and speech connect licenses.

Top-Level Software License

First, you need to select the top-level product for the software when ordering your server. This product number is UNITYCN8-K9.

www.it-ebooks.info

Server License

After selecting the top-level software license, you can select the product code for the server. This is based on the platform. The platform determines the number of ports available. The currently available server licenses follows:

- UNITYCN8-7825
- UNITYCN8-7835
- UNITYCN8-7845

User License

Users are licensed on a per-user basis. The number of users is determined by the platform capabilities. The user license also provides all features (IMAP, Inbox, Voice Recognition, and so on). The currently available user license is UNITYCN8-USR.

HA License

This license is optional and required only for active-active cluster pair configurations. This license must be acquired for the subscriber server of the cluster pair. This license file must match the platform purchased and is available as follows:

- UNITYCN8-7825
- UNITYCN8-7835
- UNITYCN8-7845

Speech Connect

This license is optional and required only if using the Speech Connect feature. This license is purchased on a per-user basis. The product license available for this feature is UNITYCN8-SC-GUEST. If you are upgrading from a previous version of Cisco Unity Connection, the licenses will vary from those previously listed.

Users can be added as needed by purchasing the necessary licenses. Cisco Unity Connection Administration enables you to add files as required. The license files are cumulative. Therefore, when you add additional licenses, they are added to the current licenses and listed under **System Settings > Licenses** in Cisco Unity Connection Administration under the License Count.

License Ordering Procedures

The license file needs to be installed on the Cisco Unity Connection server. There is a separate license file for each server, publisher, and subscriber. Each license file is register

www.it-ebooks.info

to the MAC address of the network interface card on the respective server. You must obtain the license file from Cisco. However, you must first acquire two items:

- **MAC Address on the network interface card (NIC) of the Cisco Unity Connection server:** This can be located by entering the **show status** command from the CLI. From the Cisco Unified Operating System Administration page, also select **Show > System** from the toolbar to display the System Status. The system status displays the License MAC Address of the server. You can also obtain this information using the **show network eth0** command from the CLI.
- **The Product Authorization Key (PAK):** This is the code on the Cisco Unity Connection Application Software Media Kit.

If your server has dual network interface cards, you have two options:

- Disable one of the network interface card, and register the single MAC address of the NIC currently enabled.
- Configure fault tolerance and register a virtual MAC address to be used between the two NIC cards.

Virtual server license files are not based on a MAC address, but on a combination of the number of configuration elements, including the server time zone, NTP server, NIC speed and duplex, DHCP, DNS settings, SMTP hostname, and certificate information. If you change the server (for the physical platform), or any of the applicable configuration elements (for the virtual platform), you are required to acquire and install a new license file.

After you acquire these two items, you need to open a browser on the administrator workstation and select the Cisco website to register this PAK to the MAC Address of the server. This can be preformed from the following URL:

www.cisco.com/go/license

A valid Cisco.com login is required to use the Product License Registration. Figure 3-53 illustrates this web page where you need to enter the Product Authorization Key (PAK). Select the **Submit** button. The MAC address of the publisher server must be entered during this process because the licenses file is based on the PAK and MAC address of the publisher. You want to follow the prompt to complete the online registration for the license file. Cisco will email you the proper license file. The license file includes the MAC address of the server. You need to ensure that you install the license file on the correct server that corresponds to the specific license file.

To install the license file, select **System Settings > Licenses** from Cisco Unity Connection Administration. Then, from the Search License page, select **Add New**. The Add New License page displays. Select **Browse** and locate the license file on your workstation. Select the proper license file, and click **Add** to add the new license file to the server.

www.it-ebooks.info

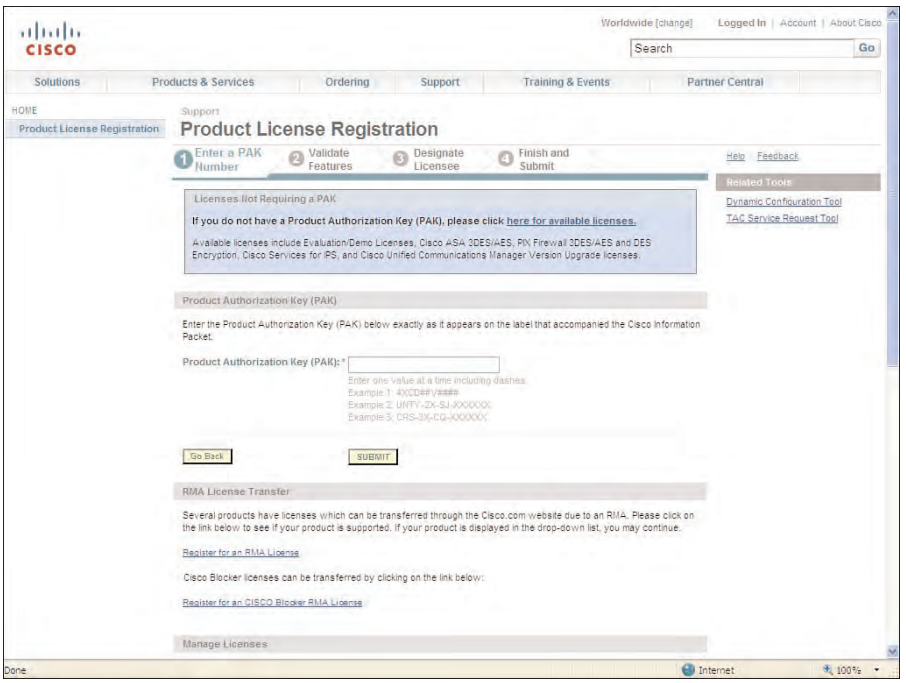

Figure 3-53 *Product License Registration*

Again, from Cisco Unity Connection Administration, select **System Settings > License**. Review the page to ensure that the new license file displays and the license count details are accurate according to your purchased licenses.

You are now ready to begin the integration of Cisco Unity Connection with your PBX or with CUCM. Chapter 4, "Integrating Cisco Unity Connection," explores the various types of integration available with Cisco Unity Connection.

Case Study

Elle-Mich, Incorporated, is a mid-size manufacturing firm in North America. It recently received its Cisco Unity Connection servers. The design calls for a Cisco Unity Connection cluster pair. The publisher and subscriber were installed in the data center on the second floor of its headquarters. The publisher is operating properly, but the subscriber does not appear to be operational.

The administrator logged in to Cisco Unity Connection Serviceability on the subscriber and noticed that the subscriber displays as Not Reachable. The network engineers verify that both servers are on the same VLAN and are reachable using ping. One of the network engineers had mentioned that he was reviewing the configuration on the publisher and might have inadvertently changed the security password.

www.it-ebooks.info

The first step in this solution is to log in to the CLI on publisher and subscriber and reset the security passwords on both servers to make sure they are the same. The subscriber should join the cluster and subscribe to the database. Verify the cluster operation under the Server Management in Cisco Unity Connection Serviceability web pages.

Summary

This chapter provided an understanding of Cisco Unity Connection installation and upgrade procedures and the various configuration requirements. You learned how to

- Install Cisco Unity Connection in a single-server and active-active cluster pair environment.
- Understand the configuration parameters required for a Cisco Unity Connection publisher and subscriber.
- Implement Cisco Unity Connection using the basic installation, upgrade during install, and unattended installation.
- Understand the supported virtual installations and the use the templates in creating virtual machines.
- Understand the various methods of upgrading Cisco Unity Connection from earlier version and from Cisco Unity.
- Understand Cisco licensing requirements for Cisco Unity Connection and the ordering and implementation procedures.

www.it-ebooks.info

This page intentionally left blank

www.it-ebooks.info

Chapter 4

Integrating Cisco Unity Connection

This chapter covers the following subjects:

- **Cisco Unity Connection Integrations:** Understand the various integrations supported with Cisco Unity Connection.
- **Protocols:** Understand the Skinny Client Protocol (SCCP) and Session Initiation Protocol (SIP) protocols as used in Cisco Unity Connection integrations.
- **Phone System Integration Configuration:** Explore the configuration and function of the various configuration options in Cisco Unity Connections.
- **Integration Configuration Element:** Explain the purpose and function of phone systems, port groups, and ports used to configure phone system integrations.
- **Call Flow:** Understand the various call flows in Cisco Unity Connection for direct and forwarded routing rules.

You have now completed the installation of the Cisco Unity Connection server or cluster pair. The software installation has been verified, licenses installed, and the various interfaces have been reviewed and confirmed as being operational. The next step is to integrate Cisco Unity Connection l with the phone system, PBX, or Cisco Unified Communications Manager (Cisco Unified CM).

Therefore, you need to understand the various integrations supported with Cisco Unity Connection. By definition, integration defines the act of combining processes, procedures, or various elements to provide a specific purpose, need, or feature to create a cohesive system. In the case of voicemail integration, you integrate Cisco Unity Connection with the call processing system (PBX, Phone System, or Cisco Unified CM) to provide voice-messaging services to new or existing IP Phones and users.

The specific integrations can vary depending on the type of phone system. All phone systems have different capabilities for what is supported and not supported. For example, some legacy PBX systems do not have IP network capabilities and therefore require another method of integration. In this case, PBX IP Media Gateway (PIMG) and T1 IP

www.it-ebooks.info

Media Gateway (TIMG) have the capability to convert digital and analog signaling conversion between these legacy systems and Cisco Unity Connection. Be advised that at press time, various PIMG and TIMG solutions have reached end-of-sale (EOS); however, most new deployments will be installed with Cisco Unified CM, where the IP integration is easily accomplished through the administration pages available on these products. In other cases, such as in legacy systems, these integrations might be more complex, requiring programming and updates to support the integration.

In the phased implementation approach, there might be instances in which the legacy system might need to coexist with a newly installed Cisco Unified CM. In these cases, multiple integrations are easily configured for temporary implementations or for continued service where the two call processing systems might continue to coexist and provide service for months or years to come.

After the integration in complete, the default routing rules determine the call flow within the Cisco Unity Connection system. The direct routing rules and forwarded routing rules can be adapted and modified to provide additional services according to the needs of the organization; however, routing rules should be configured only after thoroughly understanding their function and purpose because changes can directly affect all incoming call flows.

This chapter examines the various integrations and routing rules that you can configure in Cisco Unity Connection. Many issues can arise from an improper integrations configuration, such as loss of voicemail server connectivity. Therefore, you must understand these concepts thoroughly before beginning the integration of Cisco Unity Connection with your specific call-processing system.

Throughout this chapter, you should gain an understanding of the following:

- The various supported methods of integration using Cisco Unity Connection version 8.x software.
- The Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) to provide integrations with Cisco Unity Connection and supported call processing systems.
- The difference relating to SCCP and SIP as each is used to form and integration with Cisco Unity Connection.
- The difference between ports and port groups when using a standalone Cisco Unity Connection server or a cluster pair.
- How to integrate Cisco Unity Connection with CUCM, Cisco Unified Communications Manager Express (CME) and PIMG/TIMG units.
- The call flow in Cisco Unity Connection and the Direct and Forwarded Routing Rules.

www.it-ebooks.info

Attributes of an Integration

For Cisco Unity Connection to be useful in the voice-messaging network, the integration must be completed with the phone system, PBX, Cisco Unified CM, or another call-processing system. The type of integration depends entirely on the supported integration types between these two systems. All integrations require ports to be configured. These ports supply the necessary connection between the call-processing and voice-messaging systems. These ports can be physical ports (digital or analog) in the case of legacy PBXs that support only this type of architecture. For these systems, PIMG and TIMG provide the necessary integration device. For Cisco Unified CM and CME, these ports are actually virtual existing in software and controlled through Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP).

The attributes of the integrations between the different types can be similar for the information passed between the two systems. The PBX, Cisco Unified CM, or CME should all support the sending of the following information to Cisco Unity Connection:

- Calling Number (Caller ID)
- Called Number
- Reason for Forwarding (busy, no answer, Call Forward All, Direct)
- First/Last Redirecting Number

Cisco Unified Connection needs to send the following information to the call-processing system:

- Message Waiting Indicator (MWI)
- Message Notification

This information provides a number of features to be supported between the systems, such as the following:

- Easy Message Access (Users can retrieve messages from their phone, being recognized as a configured user.)
- Call forward to personal greeting (When calling a user and the call is transferred to voicemail, the personal recording is played for the caller.)
- Defined Routing Rules (depending on caller)
- Message Waiting Indicator (MWI):
  - Identified/configured users are sent to the sign-in conversation.
  - Unidentified calls are sent to the Opening Greeting conversation.

Note Part II of this book examines the various system call handlers including the opening greeting, directory handlers, and interview handlers.

www.it-ebooks.info

Figure 4-1 depicts an integration with Cisco Unity Connection; where ports create the integration with Cisco Unified CM or a PBX. These ports might be virtual (IP) or physical ports (PIMG/TIMG) to the call-processing system. The ports provide the required information between the systems and can be configured as incoming and outgoing from the perspective of Cisco Unity Connection to provide the required integration information.

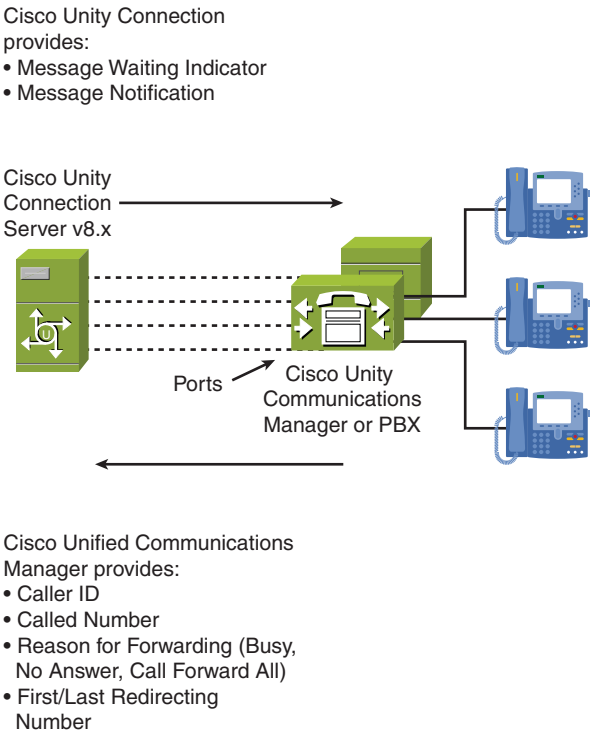

Figure 4-1 *Attributes of an Integration*

Integration with Cisco Unified CM Overview

Cisco Unified CM support SCCP and SIP integrations. In most cases, you use SCCP for integrations with Cisco Unity Connection; however, SIP integration can support all the required features. If you configure an integration with CallManager 4.x, you must use SCCP. SIP integrations are supported only with Cisco Unified CM 5.x and later. In either case, the specifics of the integration are similar.

From the perspective of Cisco Unified CM, you first need to create a hunt group designated for voicemail usage. This hunt group consists of a hunt pilot, hunt list, and line group. The line group actually contains a number of voicemail ports, rather than directory number, as would be the case for standard hunt group configuration in Cisco Unified CM. Configure the hunt pilot to be the directory number dialed for users to initiate calls

www.it-ebooks.info

to the voicemail server. It should be unique and configured to use the message button in the Cisco Unified CM by configuring the proper Voice Mail Profile and applying it to the directory numbers settings for each phone on the system. The hunt pilot is configured to point to a hunt list, which can include one or more line groups containing the various ports.

Then, configure Cisco Unity Connection with a phone system that includes one or more port groups. Each port group includes one or more ports. These ports are licensed in Cisco Unity Connection version 8.x according to your server platform licensing.

The configured port uses SCCP or SIP to register to their respective Cisco Unified CM. Figure 4-2 displays two examples of configuring multiple Cisco Unity Connection servers and cluster pairs. Also depicted is a Cisco Unity Connection cluster pair configured to support two Cisco Unified CM servers to provide redundancy for call processing.

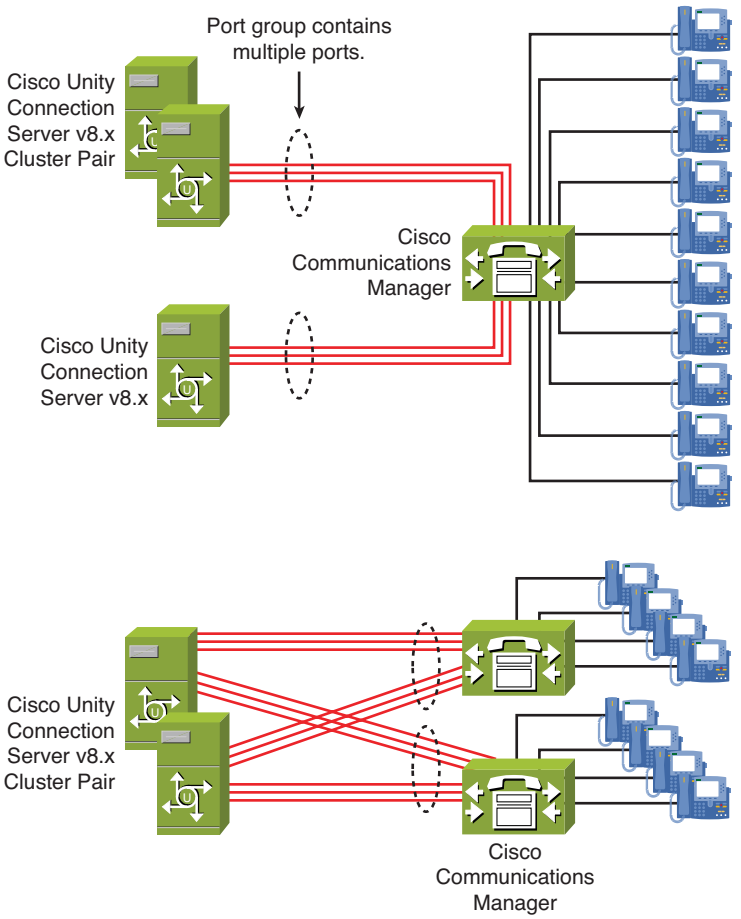

Figure 4-2 *Cisco Unity Connection Integration with Cisco Unified CM*

www.it-ebooks.info

Integration with CME Overview

Cisco Unity Connection supports integrations with Cisco Unified Communications Manager Express (CME). Multiple integrations are supported using SCCP or SIP. If using SIP, CME must be at least version 3.4, where SCCP supports all versions of CME. From the Cisco Unity Connection perspective, the integration for CME is similar to Cisco Unified CM.

Figure 4-3 depicts the integration of the Cisco Unity Connection with Cisco Unified Communications Manager Express.

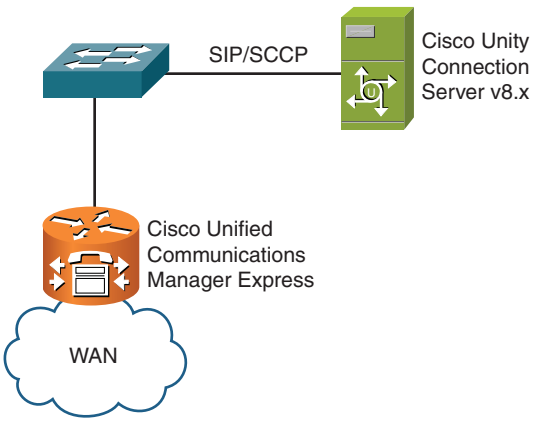

Figure 4-3 *Integrating Cisco Unity Connection with CME*

Integration with PIMG and TIMG Overview

There are instances that an organization might need to support a phone system that does not incorporate IP technology, and is composed of digital or analog ports, which are proprietary to the installed system. This would be the case for most legacy systems that predate the use of Ethernet in phone system technology. However, Cisco Unity Connection, being an IP server-based voice-messaging system, requires another method or device to integrate these older phone systems. PBX IP Media Gateway (PIMG) and T1 Media Gateway (TIMG) provide the means for Cisco Unity Connection to integrate with these phone systems.

PIMG units provide eight ports (either digital or analog) for connections to the respective phone system. Analog units deliver eight foreign exchange station (FXO) connections to the specific phone system analog line cards configured appropriately. Digital units provide eight digital connections that simulate digital phone set connections. An Ethernet

www.it-ebooks.info

connection on the PIMG unit provides IP connectivity using SIP to connect to the Cisco Unity Connection server or cluster pair. All notifications, message waiting indications (MWI), call control, and voice streams are translated from digital or analog to SIP within the PIMG units for integration to Cisco Unity Connection. The installed phone system can dictate the type and model of PIMG unit or units to be ordered. There are a number of PIMG units currently available. PIMG units can also be stacked to increase the port capacity.

TIMG devices provide T1 digital connections to phone systems that enable T1 connectivity. These units provide a single 24-port T1 connection to the phone system, while integrating to Cisco Unity Connection using a single SIP connection. TIMG units can also be stacked to provide additional T1 connections to the phone system. Be advised that at press time, various PIMG and TIMG solution have reached end-of-sale (EOS).

PIMG and TIMG units also provide a serial connection for systems that support Simple Message Desk Interface (SMDI), MCI, and MD-110 serial protocols. In this case, the first unit is the master unit providing MWI requests and call information through the SMDI serial (RS-232) interface for all attached ports. The other units are slave PIMG units.

These SMDI, MCI, and MD-110 serial protocols are used between systems to exchange call information. This information consists of the following:

- Calling number (caller ID)
- Called number (destination)
- The reason (call forward, call forward no answer, call forward busy, direct)
- MWI information

SMDI is an open standard protocol that uses a serial transport (RS-232) interface for connections between the PBX and voice-messaging system. MCI and MD-110 are proprietary protocols that provide signaling in a similar fashion for NEC (MCI) and Ericsson (MD-110) phone systems.

At press time, Table 4-1 describes a current listing of the available models of PIMG and TIMG devices. It is advisable to consult Cisco or a Cisco partner for the most current information. The model and type of phone system dictates the phone system integration and PIMG/TIMG unit. For example, two PIMG units are specific to Mitel and Rolm phone system integrations.

Figure 4-4 illustrates an installation using Cisco Unity Connection integrations using PIMG and TIMG units. In this case, master and slave units are used with SMDI to provide call information and MWI requests between the PIMG/TIMG unit and the attached PBX.

www.it-ebooks.info

Table 4-1 *PBX IP Media Gateways*

Product	Description
UNITY-PIMG-ANALOG	PBX IP Media Gateway for analog integrations (provides eight FXO ports).
UNITY-PIMG-DIG	PBX-IP Media Gateway for digital integrations (provides eight digital ports).
UNITY-PIMG-MTL	PBX-IP Media Gateway for integrations with Mitel SX200 and SX2000 PBXs (provides eight ports).
UNITY-PIMG-ROLM	PBX IP Media Gateway for integrations to Rolm 9751 phone systems (provides eight ports).
UNITY-TIMG-1	T1 IP Media Gateway for T1 integrations (provides a single 24-port T1 connection). This unit is now End-of-Sale (EOS).

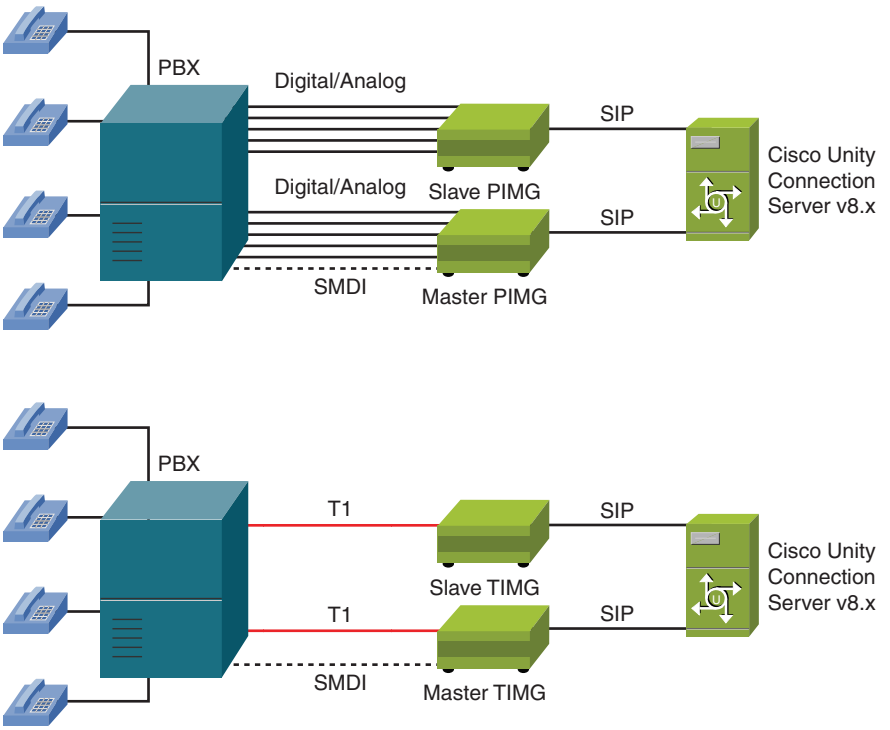

Figure 4-4 *Cisco Unity Connection Integrations Using PIMG and TIMG Units*

www.it-ebooks.info

Bandwidth Considerations Using PIMG and TIMG

When using serial ports (SMDI, MCI, and MD-110) there is a maximum distance limitation of 50 feet (RS-232). However, the PIMG master units should be located in close proximity to the phone system, even though RS-232 extensions or modems can be used to exceed this limitation, thereby using the IP networking to provide connectivity between Cisco Unity Connection and the PIMG/TIMG units. However, because the connection to the Cisco Unity Connection server or cluster pair is IP, the PIMG/TIMG units can be deployed across the WAN. For these type of deployments, you need to consider the bandwidth requirements based on the line side codec used by Cisco Unity Connection because voice streams will be sent via the SIP connection between the PIMG/TIMG units and Cisco Unity Connection. The bandwidth requirements when using PIMG and TIMG units are as follows:

- For G.729 allow 32.76 kbps per port.
- For G.711 allow 91.56 kbps per port.

Understanding Multiple Integrations

Cisco Unity Connection gives an organization the ability to support multiple phone systems using the same Cisco Unity Connection server or cluster pair. This ability provides for the administration of both phone systems on the continued service operations or for a phased approach when migrating users to the new system.

In Figure 4-5, a Cisco Unity Connection cluster pair supports users on the legacy phone system and Cisco Unified Communications Manager. A TIMG unit with SMDI provides 24 ports integrated to the PBX. SIP supports the TIMG integration, whereas SCCP supports the Cisco Unified CM integration.

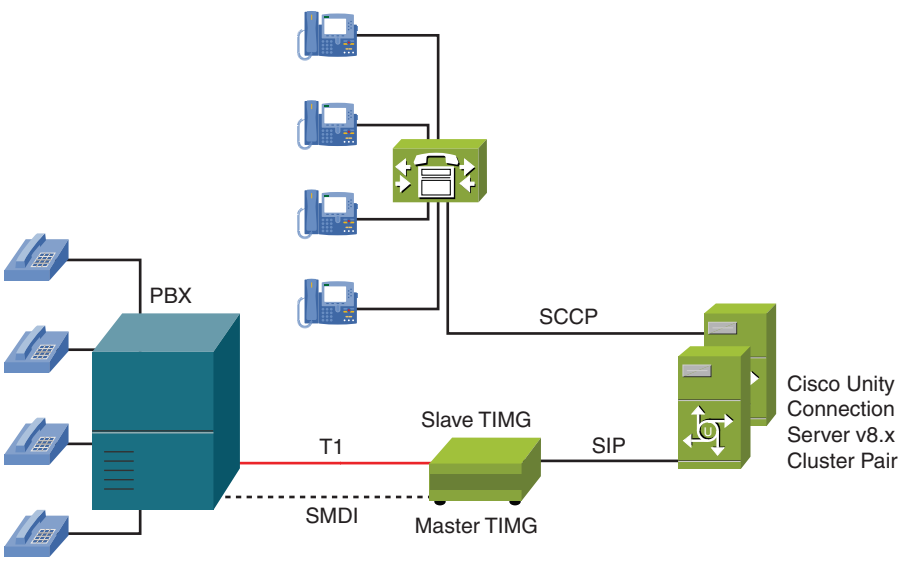

Figure 4-5 *Cisco Unity Connection Multiple Integrations*

www.it-ebooks.info

The limitation on multiple integrations is limited only by the number of ports supported by the platform licensing of the server and cluster pair configuration.

Messaging Deployment Models

The specific voice-messaging deployment can vary greatly between organizations. However, you need to understand three basic messaging deployment models:

- Single-site
- Centralized
- Distributed messaging

The location of the phone system or PBX dictates the use of the specific model.

Single-Site Messaging

The single-site messaging deployment model is the easiest model to understand—and the most common for most small-to-medium businesses. In this type of deployment, the call process and voice messaging infrastructure is located at a single site, or within a local campus network. There are no remote clients or users, meaning all users will be local to a single location. In this type of deployment, multiple integrations might exist. The main point here is that voice messaging is deployed at one location, as shown in Figure 4-6.

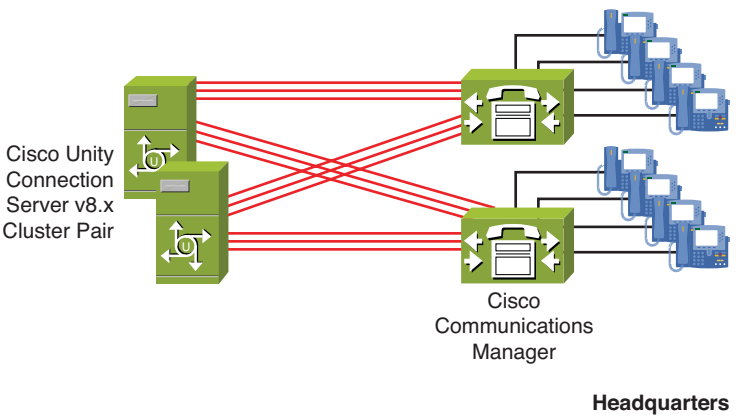

Figure 4-6 *Single-Site Voice Messaging Deployment Model*

www.it-ebooks.info

Centralized Messaging

The centralized messaging deployment is similar to the single-site deployment, where all messaging is centralized at a single location. The main difference here is that the users might be remote and be using a variety of remote messaging clients. Considerations need to be made to disallow telephone record and playback (TRaP) across the WAN, and all messages for remote clients should be downloaded before performing any playback. TRaP requires the use of ports for this operation, and therefore you need to consider bandwidth requirements. Also, transcoding and codec for remote users must be considered, as the G.729 codec will be used in most cases. In these instances, TRaP should always be disallowed across the WAN.

The centralized deployment model enables an organization to centralize their messaging and thereby centralize the administration; however, you need to consider the voice-messaging and call traffic in your specific design, and understand the necessary configuration for quality of service (QoS) and access to voice messages when the remote site is unreachable. Also, to provide service to remote users when the central site is unavailable, Survivable Remote Site Voicemail (SRSV) provides a backup solution for these remote users.

Figure 4-7 depicts a typical centralized messaging deployment model where remote user and clients might be retrieving messaging from the Cisco Unity Connection cluster pair located at the headquarters location. In this case, the call processing can either be centralized as in the perspective of Branch 1 or distributed call processing as in Branch 2.

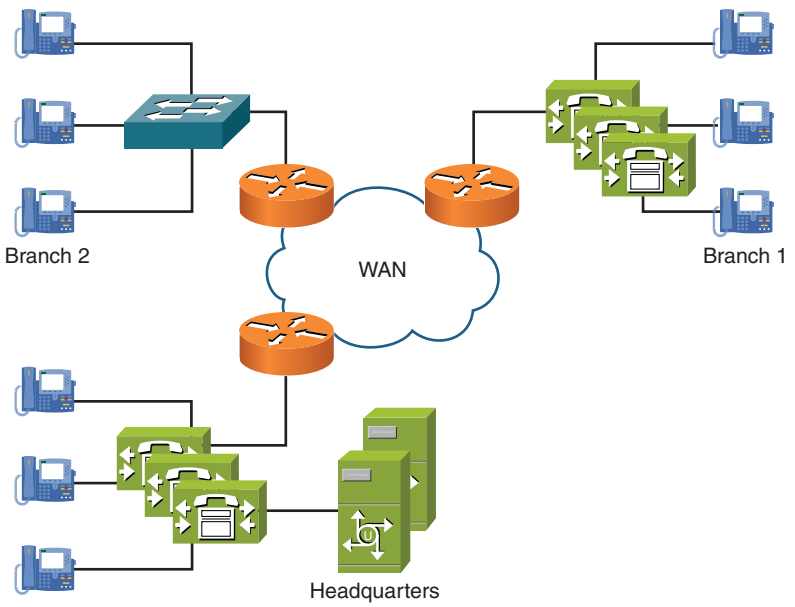

Figure 4-7 *Centralized Messaging Deployment Model*

www.it-ebooks.info

Distributed Deployment Model

The distributed messaging model consists of multiple servers or cluster pairs deployed at different locations. Even though there are multiple locations, all voice-messaging shares a common backbone or network. The voice messaging traffic is reduced by using the intrasite links, as opposed to using the centralized deployment because the actual message is delivered to the server closest to the user's location. The disadvantage to this deployment model is the administration because an administrator needs to perform configurations, backups, and tasks at multiple locations and servers.

Figure 4-8 illustrates a deployment that includes distributed call processing with distributed messaging. The Cisco Unity Connection servers are networked between the two locations to form the common messaging backbone required for distributed messaging. In this case, users can forward messages to users at the remote location and perform cross-server login and transfers. Chapter 5, "Cisco Unity Connection Users and Contacts," examines digital networks and the configurations necessary to create a common voice messaging backbone.

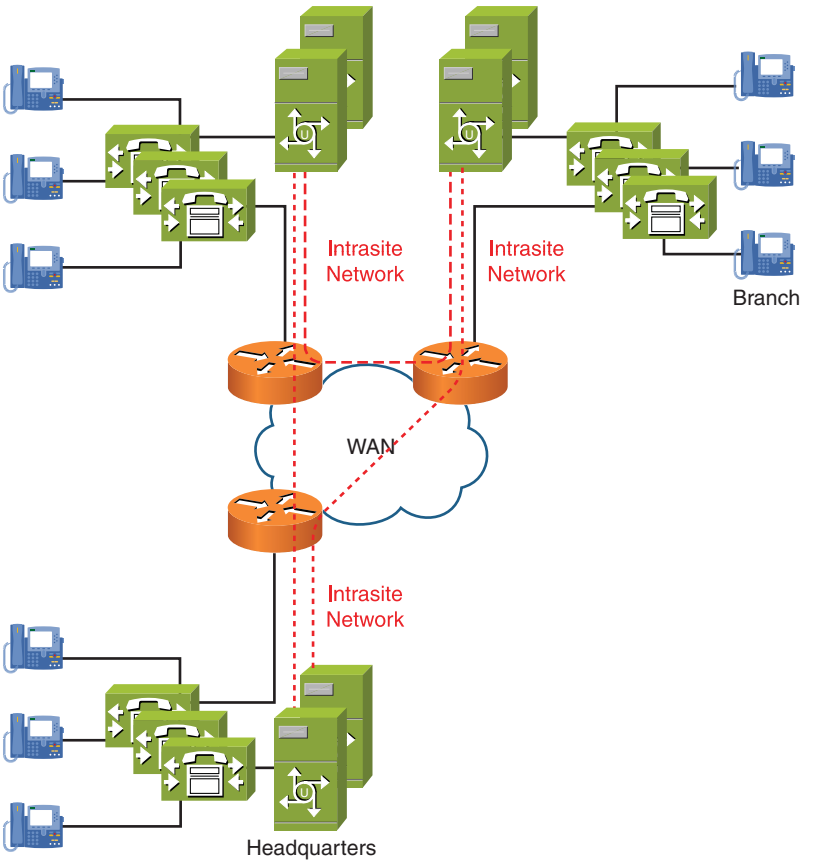

Figure 4-8 *Distributed Messaging Deployment Model*

www.it-ebooks.info

Case Study: Messaging Deployment Design

Mag's Cycle Corporation wants to implement a new voice messaging system. It currently has three locations in Columbus, Cleveland, and Indianapolis. Cleveland is its headquarters' location with a newly implemented Cisco Unified CM cluster with 500 users. The Columbus office currently has a legacy PBX with only digital ports. However, SMDI is supported. Only 25 users are on this system. The Indianapolis location has only 30 IP Phones that register to the Cisco Unified CM in Cleveland.

Traffic port considerations require that at least 6 concurrent ports are required in Columbus and 50 ports in Cleveland to support the required users. Based on the number of users and current design, Mag's Cycle decided to use a centralized messaging deployment because the majority of users are located at its headquarters' location in Cleveland. Because the Columbus PBX must remain, PIMG will be used at this site to provide SIP integration to headquarters.

Figure 4-9 illustrates the deployment where centralized messaging is used along with a PIMG unit to support the Columbus location. The Cisco Unified CM deployment exhibits centralized call processing, whereas the Columbus location depicts distributed call processing with the Cleveland location using PIMG.

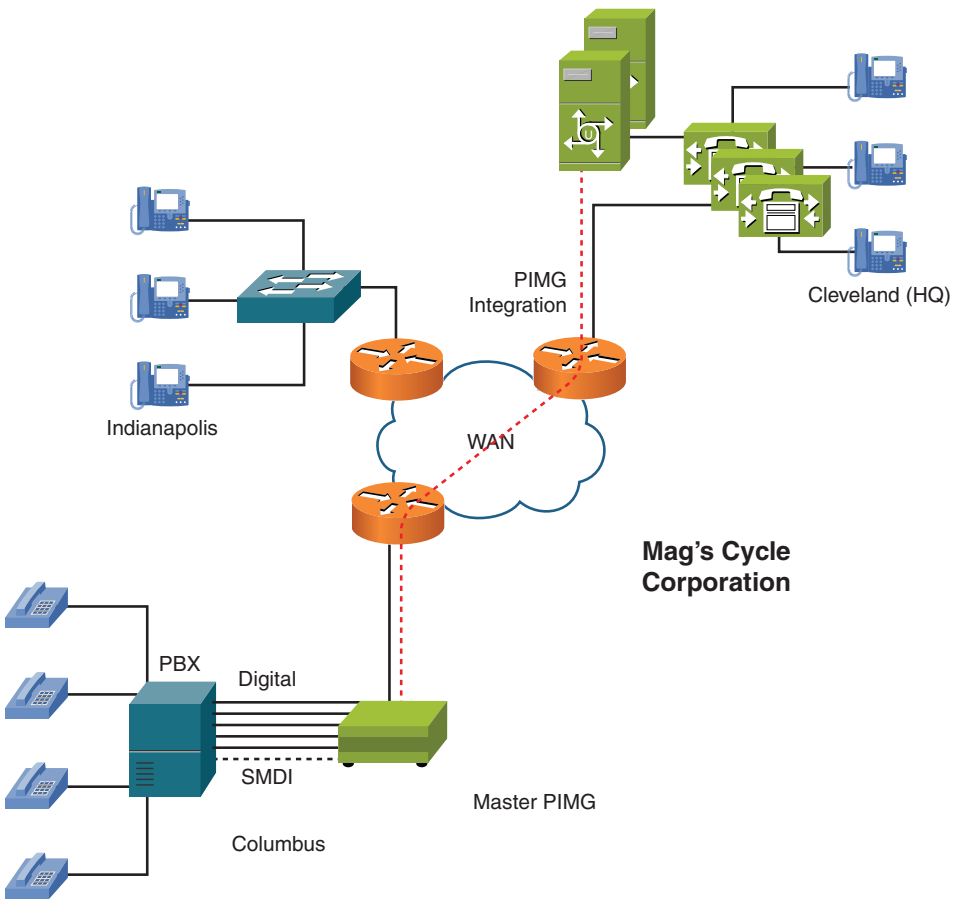

Figure 4-9 *Mag's Cycle Centralized Voice Messaging Deployment*

www.it-ebooks.info

Cisco Unity Connection Integration

Cisco Unity Connection integrations are built using a phone system configuration that includes one or more port groups. These port groups each contain one or more ports you can use to support connectivity between the phone system and Cisco Unity Connection. A single port can supply inbound, outbound, MWI, message notification, and TRaP capabilities.

When a phone system is created, it will be associated with a number of different objects (or configuration elements). These objects provide a number of different services, consisting of the following:

- Users
- User templates
- System call handlers
- Call handler templates
- MWI
- Notification devices

At the time of installation, Cisco Unity Connection creates a number of these default objects. Many of these objects are inter-related, meaning that certain objects are associated with other configurable objects. For example, a default phone system is created that includes each of these objects. You cannot delete this default phone system without first changing the phone system association within the configuration of these objects.

However, before this can happen, you must either create a new phone system and re-associate all existing objects to the new phone system, or use the existing default phone system, by adding a port group, ports, and completing the necessary configuration for the integration.

The next section covers integration with Cisco Unity Connection and Cisco Unified CM. The integration with CME and PIMG/TIMG is also explored.

Understanding Phone Systems, Port Groups, and Ports

Cisco Unity Connection integrations are configured by creating a new phone system in Cisco Unity Connection Administration, or using the existing default phone system. After the phone system is configured, you need to add one or more port groups to the system, which include one or more ports. The implementation determines the configuration of these port groups and ports. For example, the ports group configuration can vary if you configure Cisco Unity Connection as a single-server model, cluster pair, or a PBX with PIMG/TIMG devices.

www.it-ebooks.info

A phone system in Cisco Unity Connection describes a single integration with a PBX or Cisco Unified CM system, even though Cisco Unity Connection might either be a single-server or cluster pair configuration, or integrated to multiple Cisco Unified CM servers for call processing redundancy. Each phone system is identified in Cisco Unity Connection Administration and contains one or more port groups. The phone system configuration contains the global configurations that apply to the integration affecting all port groups.

Port groups contain most of the configuration settings for the integration, including the MWI, IP address, or hostname of the phone system, port numbers, advertised codecs, and other configuration settings that apply to the ports within the port group. For a single phone system, you need only one port group in an integration to provide all necessary features required for the integration. However, there might be other cases in which multiple port groups are required, such as the following:

- A separate integration is required for testing with a different phone system.
- When using multiple PIMG/TIMG units, a separate port group is required for each device, even though they are configured with integration to the same PBX.
- For Cisco Unified CM integrations using SCCP, it is recommended to configure two port groups:
  - Each port group includes half of the voice-messaging ports, along with MWI and message notification ports.
  - The Cisco Unified CM servers are listed in the reverse order for the second port group.

Note During call-processing failover, the ports can register quicker with this suggested configuration because the servers are defined as the primary server in the second port group. Also, a server failure for a cluster pair can result in only having half of the available ports. In this case, each port group provides half of the ports available.

Port groups include one or more ports. These ports are associated to a Cisco Unity Connection server (single-server, publisher, or subscriber) and configured to be part of a specific port group associated to a defined phone system. Ports in Cisco Unity Connection answer calls (inbound) to record, retrieve messages, and handle call transfers. They can also initiate calls (outbound), as in the case of MWI and message notification. If users use the clients to retrieve voicemails, ports are not used for this operation, as long as they download messages and listen to message from their workstation speakers. However, if users elect to send messages to their IP Phone, a port is used. This operation requires a port to be configured for telephony record and playback (TRaP). This is an

www.it-ebooks.info

important bandwidth consideration when remote users are doing centralized voice messaging, as discussed in the last section. In this case, messages are played across the WAN, a port is used, and bandwidth is required according to the advertised codec configured for the phone system.

Ports can be associated to only one port group. The total number of ports configurable is dependent on the platform and licensing as defined in the previous chapter.

The next sections examine the various configurations options and settings as they apply to an integration.

Integrating with Cisco Unified CM

Integration with Cisco Unified CM is probably the most common integration for new installations. When you purchased the version 8.x software, both Cisco Unified CM and Cisco Unity Connection were included on the media. Even though you might not decide to upgrade at this time to Cisco Unified CM, Cisco Unity Connection is backward compatible with earlier versions of Cisco Unified CM, as far back as version 4.1. Also, Cisco supports integrations with SCCP or SIP. However, SIP integrations are supported only with version 5.x and later.

The next pages illustrate the SCCP and SIP integrations with Cisco Unified CM. Because SCCP is a client-server protocol, where Cisco Unity Connection ports register with Cisco Unified CM, you need to first perform the Cisco Unified CM configuration.

Cisco Unified CM Voicemail Configuration

This text is not intended to cover all aspects of Cisco Unified CM, though required steps are necessary to configure the voicemail integration on Cisco Unified CM before beginning the Cisco Unity Connection integration.

To begin, login to Cisco Unified CM Administration on the Cisco Unified CM server using the proper credentials, by pointing your browser to the following:

https://*ip_address*/ccmadmin

From the toolbar, select **Advanced Features > Voice Mail > Cisco Voice Mail Port Wizard.** The wizard enables you to easily create the configuration required to complete the integration in a step-by-step method, ensuring that all configurations finish properly.

In the first step of the wizard, you need to add a new voicemail server. For new integrations, select **Create a new Cisco Voice Mail Server** and add ports to it. Click **Next,** as displayed in Figure 4-10. The name you choose here must be unique and match the associated configuration in Cisco Unity Connection. This configuration is vital to the integration and must match exactly with the configuration that will be completed in Cisco Unity Connection. If this configuration does not match between Cisco Unified CM and Cisco Unity Connection, the ports fail to register. The default name is CiscoUM1 (UM stands for Unified Messaging). You can change this name as needed. In Figure 4-10, the server name was changed to CorpIM. Typically, UM is configured for Unified Messaging,

www.it-ebooks.info

and IM is configured for Integrated Message; however, the usage and naming conventions can vary greatly between organizations.

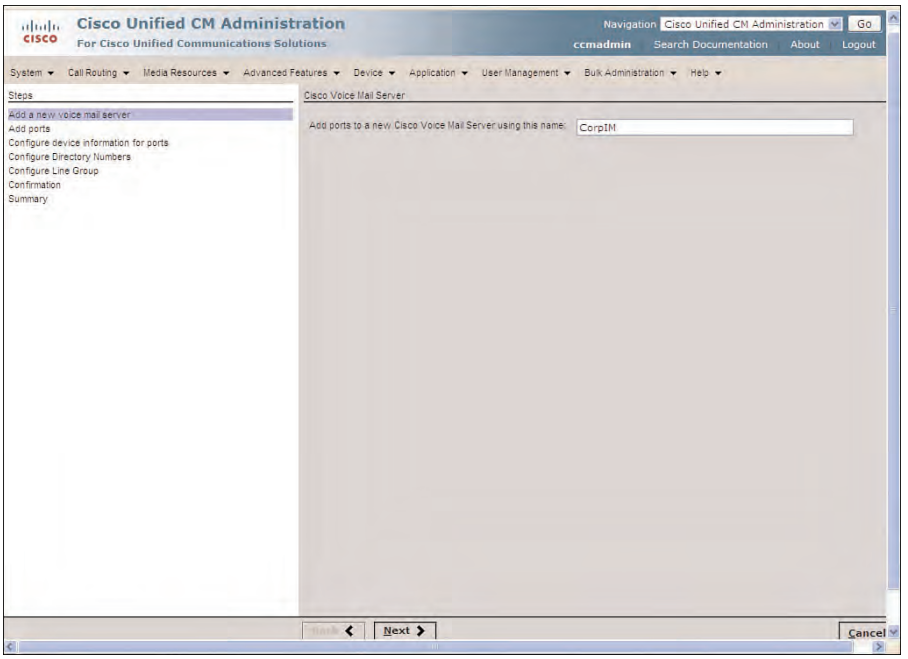

Figure 4-10 *Cisco Voice Mail Server Configuration in Cisco Unified CM*

Click **Next** to continue to the voicemail port configuration page.

The Voice Mail Ports configuration page is the next selection to be completed. This configuration can include up to 250 ports. However, you should never configure more ports than are licensed to the specific Cisco Unity Connection server that is to be integrated with this server. Figure 4-11 displays the voicemail port configuration in Cisco Unified CM, where four ports are selected.

Click **Next** to continue to the Cisco Voice Mail Device information page.

In the Cisco Voice Mail Device Information page, complete the following required configurations including the description, device pool, location, and device security mode, as displayed in Figure 4-12. The device pool includes most of the important Cisco Unified CM configurations required including the servers that will be used to register the ports and codecs supported (regions). Locations are used for call admission control to limit the number of concurrent calls that can be in use. Finally, Device Security Mode enables the installer to implement authentication, encryption, or both on the ports between Cisco Unified CM and Cisco Unity Connection. By default, all information is sent in clear text and security should be considered in instances in which voice-messaging security is a concern. Select Non Secure Voice Mail Port for unsecure. Securing voice conversations requires a separate configuration and use of CAPF profiles and USB security tokens on Cisco Unified CM. Select **Next** to continue the Voicemail Wizard.

www.it-ebooks.info

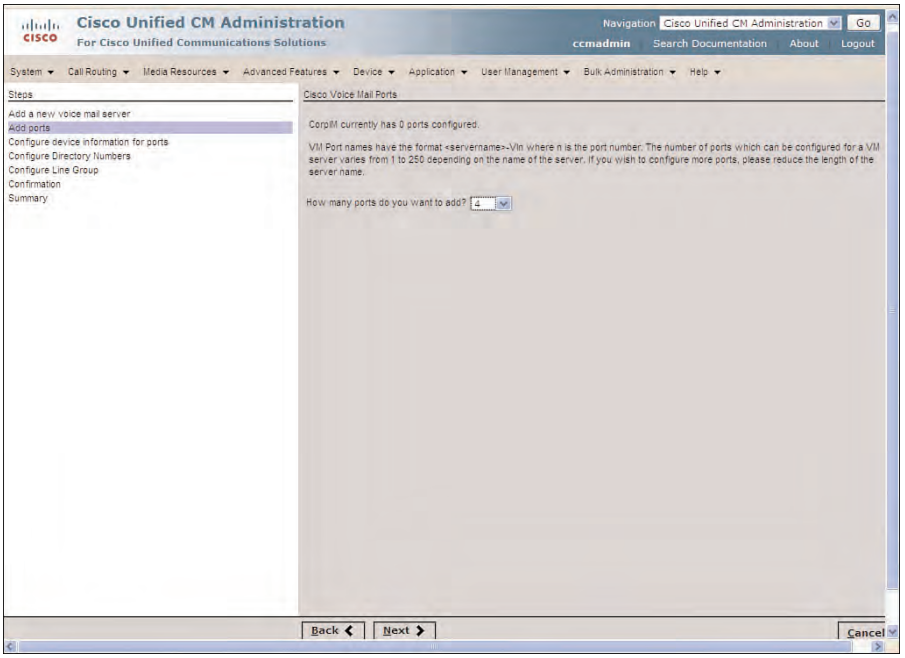

Figure 4-11 *Voice Mail Port Configuration in Cisco Unified CM*

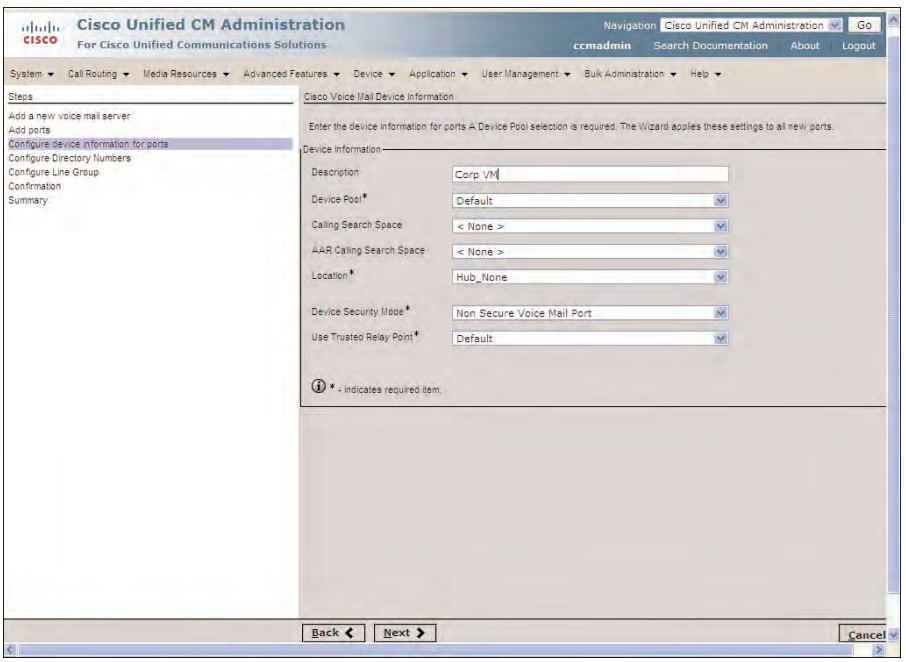

Figure 4-12 *Cisco Voice Mail Device Information in Cisco Unified CM*

www.it-ebooks.info

The Cisco Voice Mail Directory Numbers page now displays. From this screen, you enter the beginning directory number that will be assigned to the lowest numbered port. Keep in mind, each port will receive the next number, so the assigned ports (four), will be 2991, 2992, 2993, and 2994. These directory numbers must be unique to within the Cisco Unified CM dial plan and the configuration in Cisco Unity Connection. The Internal Caller ID Display corresponds to the descriptive name displayed on the phone when the user calls voice, directly, or uses the message button.

Figure 4-13 displays the Cisco Voice Mail Directory Numbers configuration page that includes the configuration for directory numbers, partitions, AAR Group, Internal Caller ID Display, and External Number Mask. The Internal Caller ID Display entered displays on the phone when users select the message button. Click **Next** to continue to the next screen for the Voicemail Wizard configuration.

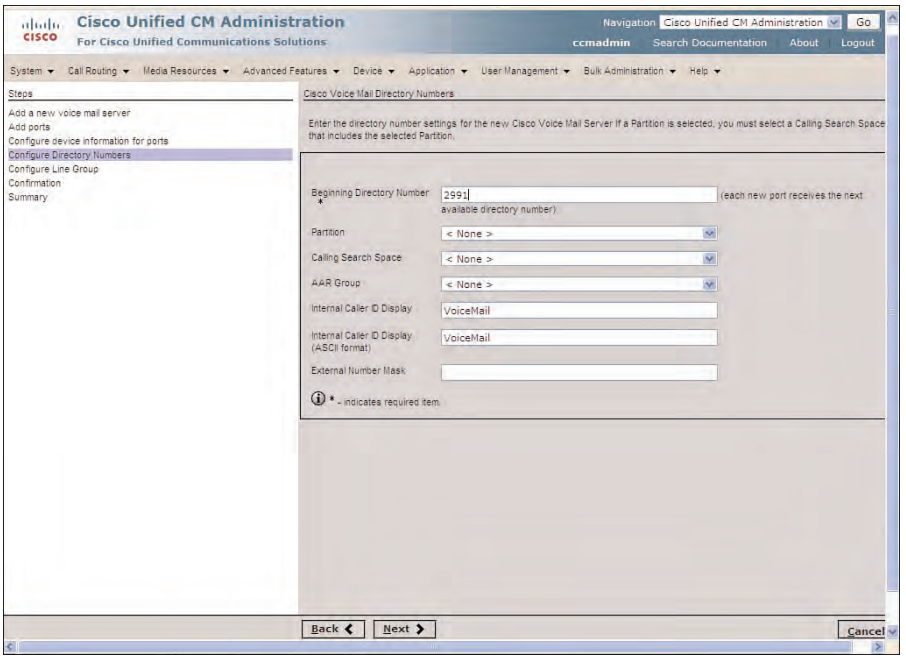

Figure 4-13 *Cisco Voice Mail Directory Numbers Configuration in Cisco Unified CM*

At this point, you are asked if you want to add the directory numbers to a new or existing line group. The line group is used specifically for hunt groups and voicemail integration because the integration actually hunts for an available or registered port. Each directory number is associated with a specific port. Therefore, you need to add these directory numbers into a line group. In this case, the directory numbers are added to a new line group, as shown in Figure 4-14, by selecting the radio button to add directory numbers to a new Line Group. Select **Next** to complete the configuration and continue.

www.it-ebooks.info

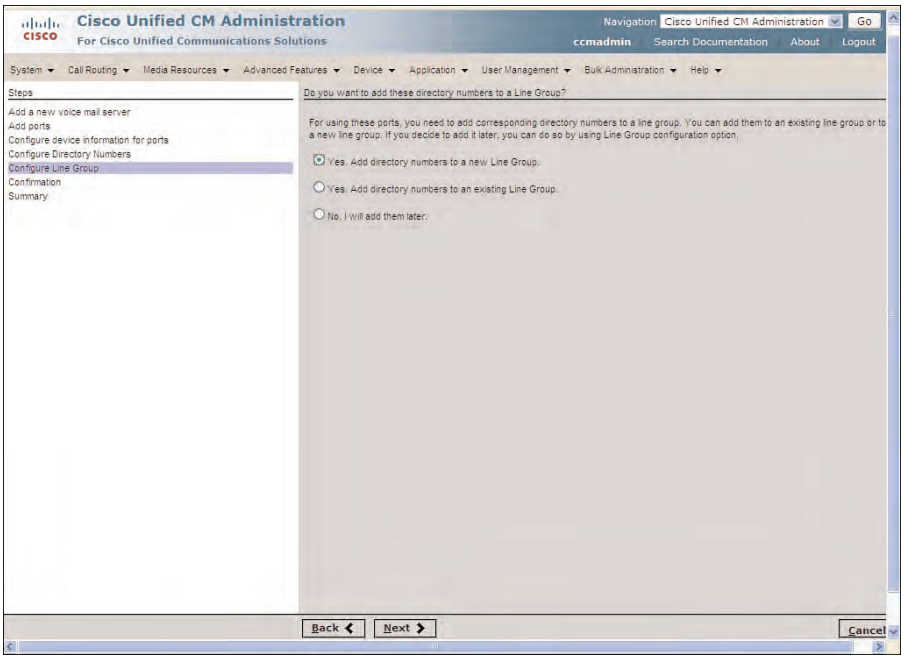

Figure 4-14 *Add Directory Numbers to a New Line Group*

Finally, create the line group by entering the line group name. The line group field is completed with a suggested default name of CiscoUM1. However, you can change this to make it more descriptive for your implementation. In this case, the line group is changed to **HQ_vm_lg**, as displayed in Figure 4-15. Click **Next** to complete the configuration of the line group.

The confirmation page now displays, as shown in Figure 4-16. This is the last opportunity to go back and make any necessary changes. Ensure that the ports, directory numbers, and all other configurations match the desired configuration. Selecting **Finish** creates the ports and line group and add the ports to the new line group as configured.

www.it-ebooks.info

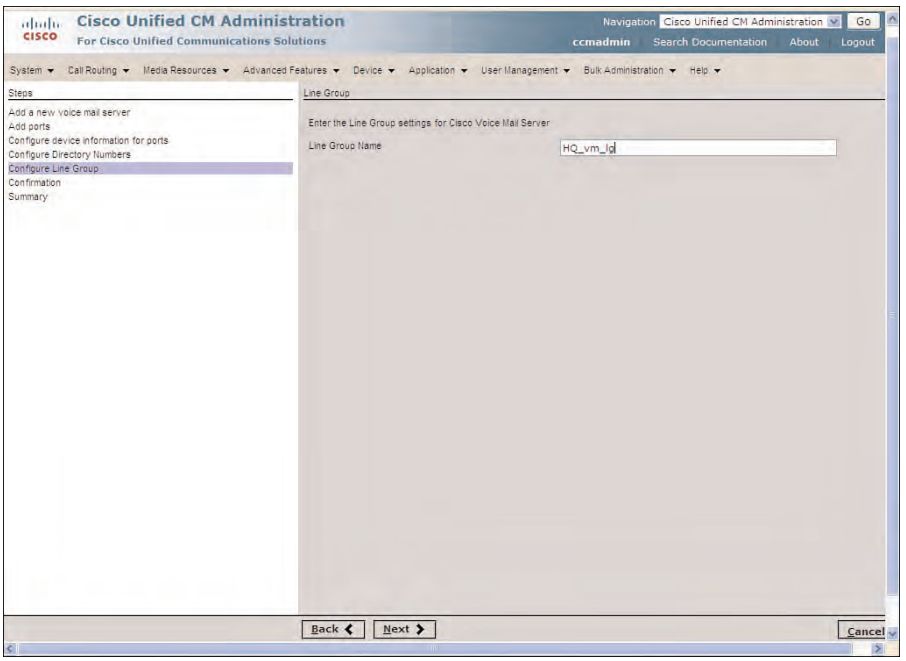

Figure 4-15 *Line Group Configuration in Cisco Unified CM*

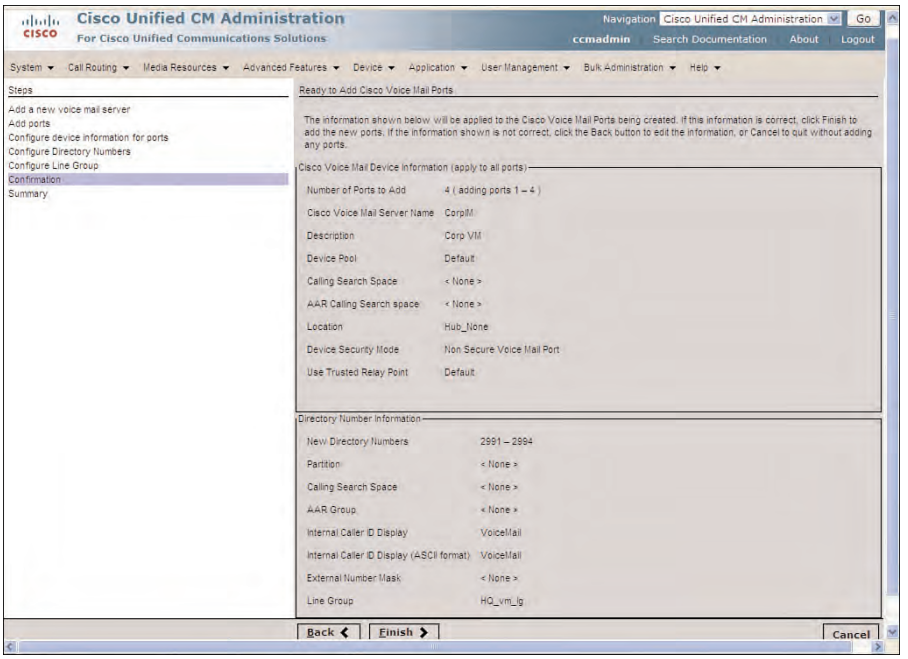

Figure 4-16 *Voice Mail Confirmation Screen in Cisco Unified CM*

www.it-ebooks.info

The Voice Mail Port Wizard Results page displays, as shown in Figure 4-17. However, you are not quite finished. You need to complete three configuration items. First, you must add the new line group to a new or existing hunt list. You can do this by clicking the link on the Wizard page associated with the Hunt List configuration.

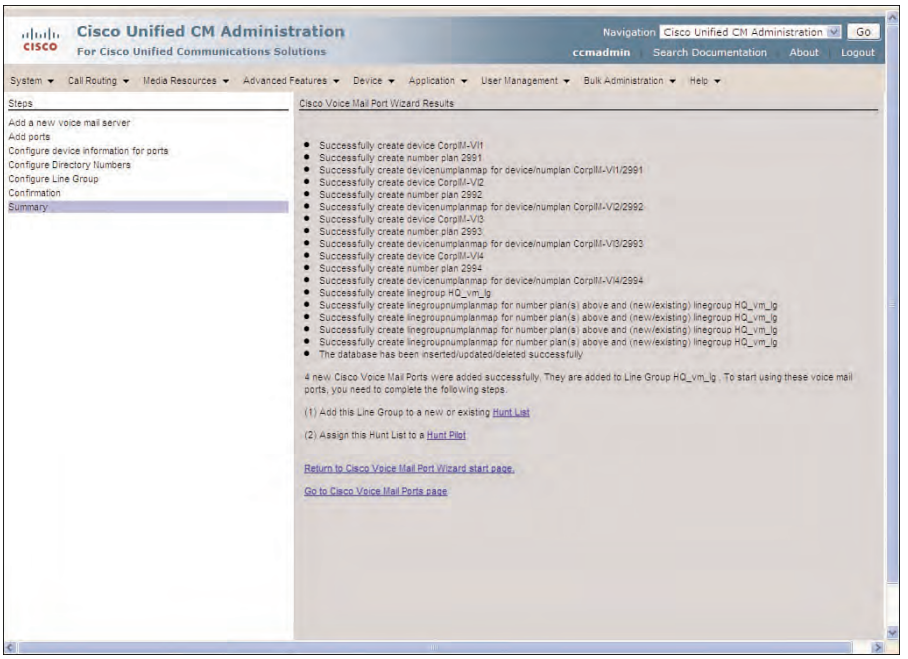

Figure 4-17 *Voice Mail Port Wizard Results*

Click **Add New** on the Hunt List Configuration page to create a new hunt list. On the Hunt List Configuration page, Enter a new Name for the hunt list, description, select a Cisco Unified Communications Manager Group, and check the **Enable this Hunt List** and **For Voice Mail Usage** check boxes, as shown in Figure 4-18. The name for this hunt list was entered as **CorpVM_hl**. A description can be added as needed. You can use the For Mail Usage check box to indicate that this hunt list is to be used for voicemail. Click **Save** when finished.

After the hunt list configuration is saved, the Hunt List Configuration page displays again but with the Hunt List Member Information section displayed. Click **Add Line Group**. At this point, the Hunt List Detail Configuration page displays. Select the line group configured in the previous step from the Line Group drop-down, and click **Save**. The Hunt List Configuration page now displays, as shown in Figure 4-19. This time, the line group now displays in the Selected Groups pane.

www.it-ebooks.info

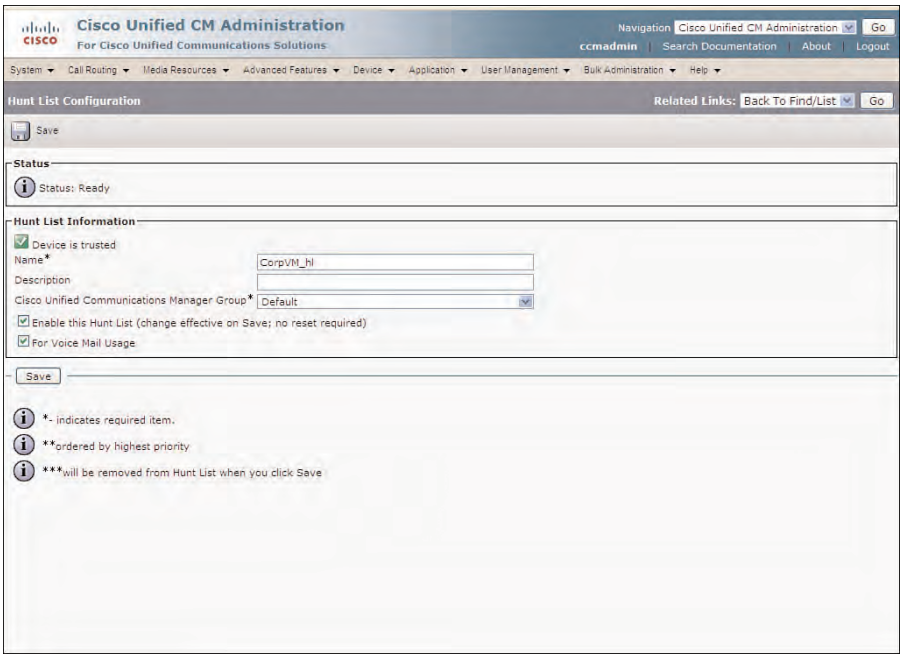

Figure 4-18 *Hunt List Configuration in Cisco Unified CM*

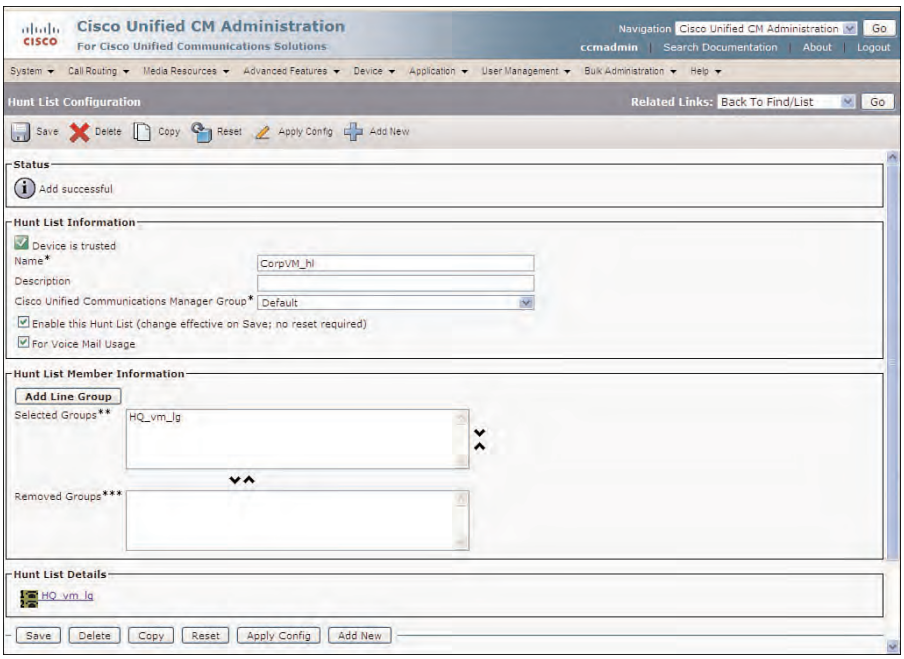

Figure 4-19 *Hunt List Configuration in Cisco Unified CM*

www.it-ebooks.info

Select **Advanced Features > Voice Mail > Cisco Voice Mail Port Wizard** to return to the wizard dialog. The next step is to create a Hunt Pilot configured to point to the hunt list used for voicemail. Click the **Hunt Pilot** link on the wizard page.

The Find and List Hunt Pilots page displays. Click **Add New** to create a new Hunt Pilot. The Hunt Pilot Configuration page displays. Enter the Hunt Pilot directory number. This must be a unique number that is configured specifically for access to voicemail by the users. This voicemail hunt pilot can be either dialed directly or selected by the user pressing the message button on the IP phone. Select the voicemail hunt list from the Hunt List drop-down, and click **Save**, as displayed in Figure 4-20. The hunt pilot was entered as **2990**, and the **CorpVM_hl** hunt list was selected.

The final steps include the configuration of the MWI extension and voicemail profile. Select **Advanced Features > Voice Mail > Message Waiting** and click **Add New** to add a new message waiting indicator (MWI).

The MWI ON number is created to turn on the MWI light on the users' phone when a new message arrives at their voice mailbox. Consequently, the MWI OFF number will be used to turn the light off when all messages are read or deleted.

Like the Hunt Pilot number, the MWI numbers must be unique in the dial plan. Also, they must match the numbers configured in the Cisco Unity Connection integration configuration, which is discussed in the next section.

On the Message Waiting Information page, enter the information for the MWI ON directory number and click **Save**. Select **Add New** and repeat this operation for the MWI OFF directory number, as shown in Figure 4-21. In this case, 2995 is selected for MWI ON, and 2996 is selected for MWI OFF.

Attention must be given to Calling Search Spaces and Partitions because the partition of the MWI ON and OFF indicated in Figure 4-21 should be included only in the Calling Search Space for the port (see Figure 4-13). If this step is not completed properly, Cisco Unity Connection cannot provide message waiting indication. You should never include the partition used for MWI in the user's Calling Search Space.

You must then associate the hunt pilot to a voicemail pilot. This is used so the users can use the messages button on their phones. Select **Advanced Features > Voice Mail > Voice Mail Pilot** from the toolbar on Cisco Unified CM Administration. The Find and List Voice Mail Pilots page displays.

www.it-ebooks.info

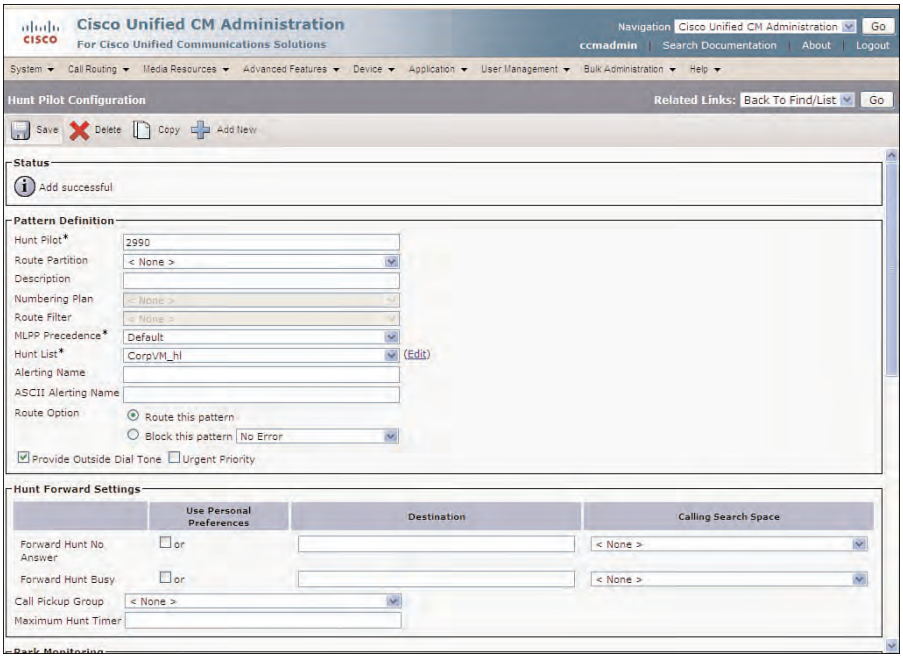

Figure 4-20 *Voicemail Hunt Pilot Configuration*

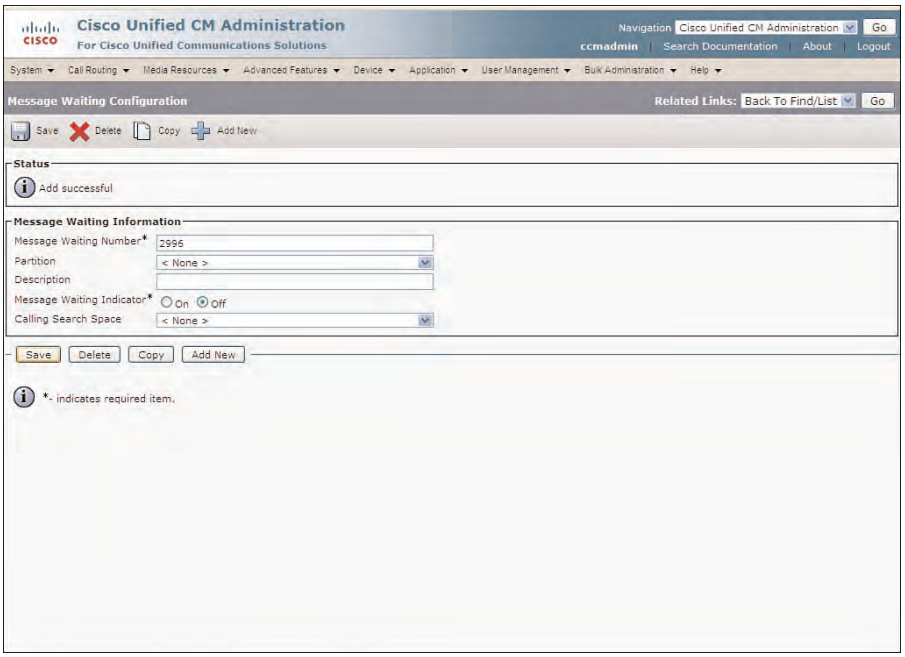

Figure 4-21 *Message Waiting Configuration in Cisco Unified CM*

www.it-ebooks.info

Click **Find** to display the current voicemail pilot numbers. If your configuration has a single voice-server or cluster pair, you can use the Default and assign the hunt pilot to the voicemail pilot. Select the Default voicemail pilot. The Voice Mail Pilot Configuration page displays. Enter the hunt pilot number in the Voice Mail Pilot Number field, and click the check box for **Make This the Default Voice Mail Pilot for the System**. Again, you should give careful attention to the configuration of Calling Search Spaces and Partitions as discussed previously. Click **Save**, as displayed in Figure 4-22.

After you configure the voicemail pilot, the default voicemail profile automatically is configured to use the hunt pilot. To view the voicemail profile configuration, select **Advanced Features > Voice Mail > Voice Mail Profile** and click **Find** to display the profiles, as in Figure 4-23.

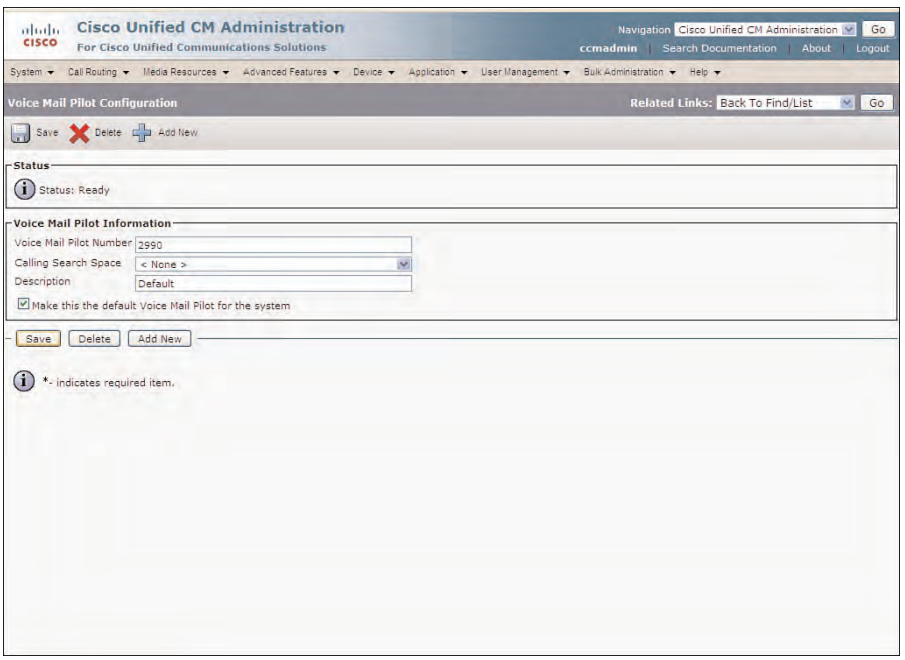

Figure 4-22 *Voice Mail Pilot Configuration in Cisco Unified CM*

You immediately notice that the default voicemail profile includes the hunt pilot number of 2990. This number will be used by users to access voicemail, by configuration performed under the Directory Numbers Configuration for the IP Phones.

The voice mail profile is selected under the directory number configuration for users to access voice mail by using the Messages button on their phones. Figure 4-24 illustrates this configuration option on the Director Number Configuration page.

www.it-ebooks.info

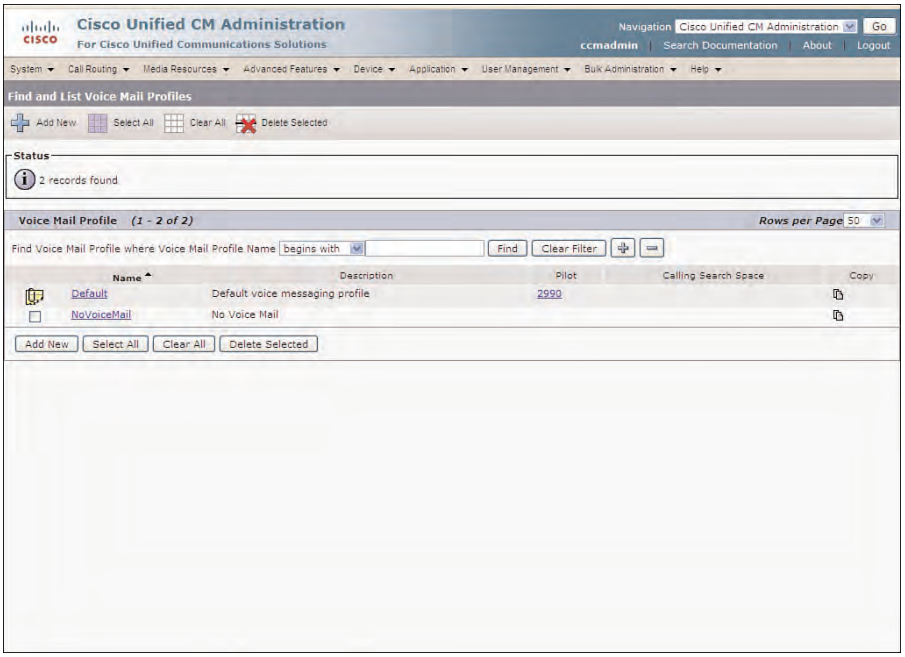

Figure 4-23 *Voice Mail Profile Configuration in Cisco Unified CM*

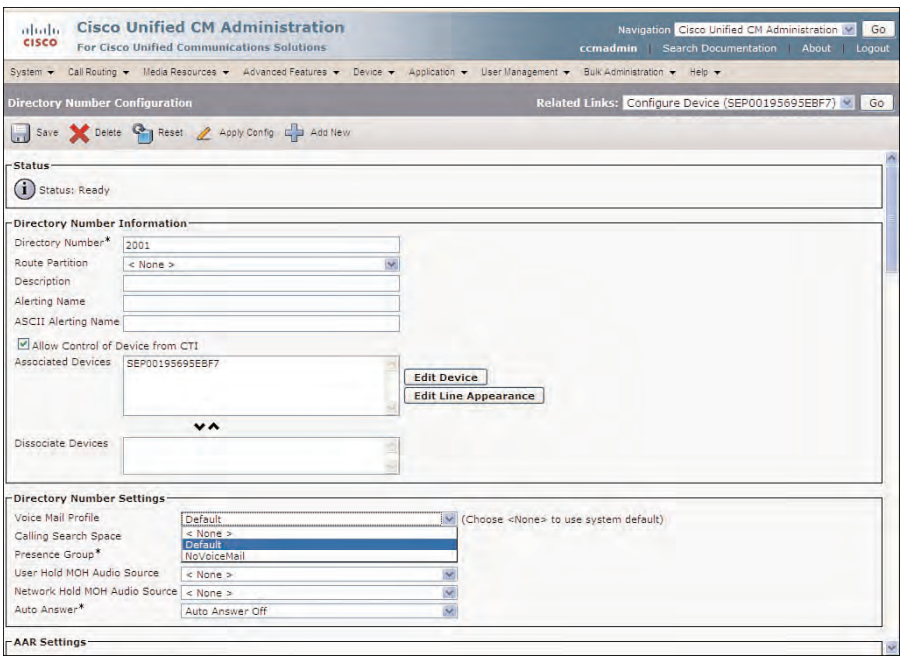

Figure 4-24 *Directory Number Configuration Page in Cisco Unified CM*

www.it-ebooks.info

If your specific deployment is deployed with multiple Cisco Unity Connection servers or cluster pairs, a separate voice mail profile is created for each server or cluster pair integrated with the Cisco Unified CM cluster.

This completes the configuration for voicemail integration in Cisco Unified CM. You must now complete the configuration in Cisco Unity Connection to finish the integration and create a working voice-messaging system integrated with Cisco Unified CM.

Cisco Unity Connection Integration Configurations

Cisco Unified CM is now configured and ready for the Cisco Unity Connection integration. In the next steps, you use the default phone system by renaming it, adding a port group, and associated ports for voice-messaging traffic, MWI, message notification, and TRaP.

In the following example, an active-active cluster pair is integrated with Cisco Unified CM to provide voice-messaging redundancy.

To begin, you must login to Cisco Unity Connection Administration by pointing your browser at the URL: https://ip_address_publisher/ucadmin and login with the application user credentials.

From the navigation pane on the left, select **Telephone Integrations > Phone System**. The Search Phone System page displays showing the default phone system listed as **PhoneSystem**, as illustrated in Figure 4-25.

Select **PhoneSystem** from the Display Name column. The Phone System Basics page is displays, as in Figure 4-26. From this page, you can select a number of options that apply globally to this specific phone system integration.

The Phone System Name can be changed by entering the new phone system name. It is advisable to change this to make it more identifiable in your organization. In the example, the display name changes to **Cisco Unified CM**.

The Default TRAP Phone System option provides the ability for users and administrators to record and playback messages, greetings, and names using their phone. Also, users with IMAP clients can listen to messages using their phone. Uncheck this box to disable TRaP, or use this feature from another configured phone system.

For remote clients in a centralized voice-messaging environment, you want to avoid the use of TRaP to conserve ports and bandwidth. In these cases, users should download messages and listen to them from their workstation. If users are located in public areas, or office cubicles, it might be necessary to use TRaP and use their phone for a certain level of privacy. This selection is enabled by default. If TRaP is disabled, the user's computer or laptop will be used to record and playback greetings and messages.

www.it-ebooks.info

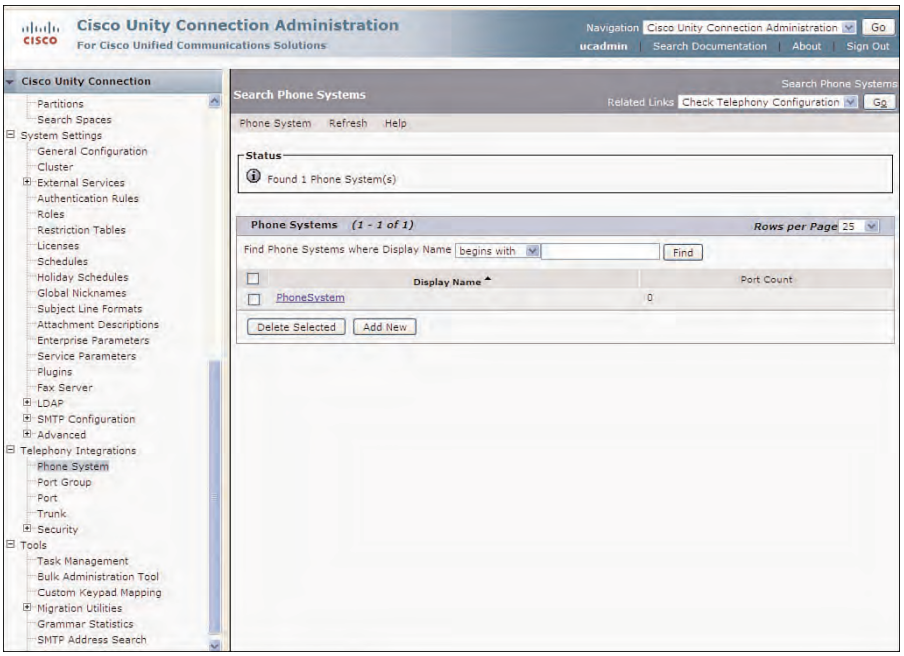

Figure 4-25 *Search Phone Systems Screen in Cisco Unity Connection Administration*

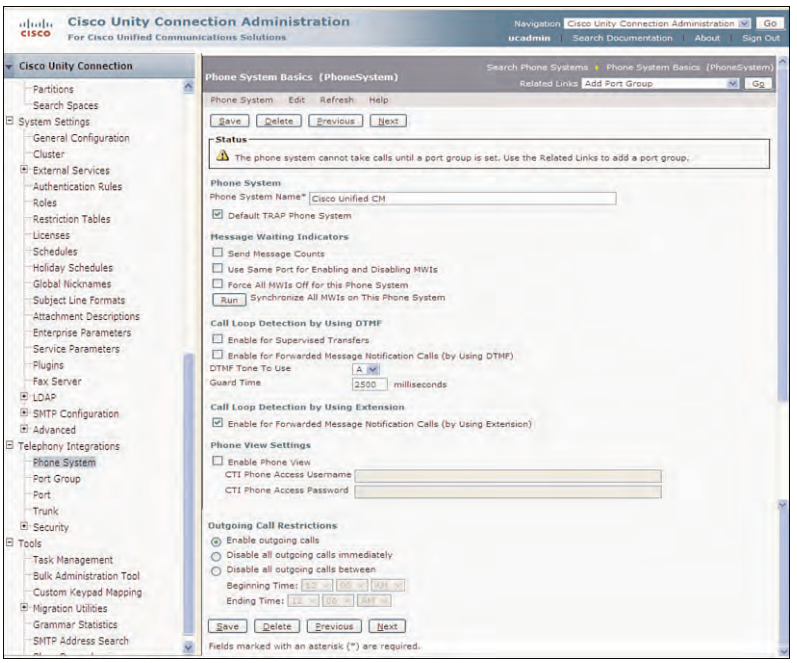

Figure 4-26 *Phone System Basics Page in Cisco Unity Connection*

www.it-ebooks.info

A number of configurable options apply to each phone system for MWI, which include the following:

- **Send Message Counts:** Enables Cisco Unity Connection to send message counts and requests each time a voice message is received. This option is disabled by default, meaning that Cisco Unity Connection does not send a message count and request to turn on the MWI light on the phone if the light is already on. Leaving this option disabled minimizes the port usage for MWI, by not sending redundant requests. Some of the newer integrations can display this information for the user.
- **Use Same Port for Enabling and Disabling MWIs:** Forces the MWI off request to use the same port used for the MWI on request. This might cause a delay in turning off the MWI light, where the specific port is busy. The default selection is disabled, meaning that any other available port might be used (that is, enabled for MWI) to turn off the MWI light. This option is useful when testing, where you might want to monitor the MWI requests sent by using remote port status monitor or Real-Time Monitoring Tool (RTMT). Also, some older PBXs enable only an MWI off command to come from the same port that activated it. These tools are explored later in this chapter.
- **Force All MWIs Off for this Phone System:** Forces all MWI lights off by sending the MWI off request for all user phones.
- **Synchronize All MWIs on This Phone System:** Synchronizes all the MWI lights for the current users' phones configured on this phone system.

If there is a problem with MWI being incorrectly set on the system, select the **Force All MWIs Off for this Phone System** option to force all MWIs off. Select **Save** to complete the operation. Then, click **Run** for the **Synchronize All MWIs on This Phone System** option to reset MWI to the correct status.

The next available options for the phone system have to do with loop detection. If a call is initiated from Cisco Unity Connection, as would be the case for supervised transfers and message notification, and the call is returned to Cisco Unity Connection because the user is busy, no answer, or not available, loop detection is required. Loop detection in Cisco Unity Connection rejects the message that has been forwarded back to itself. If loop detection is not detected, a new message notification is initiated. For supervised transfers, loop detection also rejects the call transferred back to Cisco Unity Connection. If a loop is not detected, Cisco Unity Connection records a voice message. Loop detection has two types, using Dual Tone Multi-Frequency (DTMF) or extension. DTMF enables the selection of the DTMF touchtone to use for loop detection and guard time that Cisco Unity Connection uses to play the tone. You want to select this for specific PBX systems where this can be tuned to match the phone system integration. For Cisco Unified CM, use the **Enable for Forwarded Message Notification Calls (by Using Extension)** option, which will be recognized by Cisco Unity Connection from Cisco Unified CM for loop detection.

www.it-ebooks.info

The Phone View Settings option provides the ability to enable and disable this feature and provides the necessary authentication. This option applies only to Cisco Unified CM 6.x and later when used with Cisco Unity Connection. The Phone View feature gives users the option to display a list of voice messages on their IP Phone (for supported models). This feature requires the configuration of an application user configured to be associated with the correct user groups. The Phone View feature is discussed in Part II along with a similar feature called Visual Voicemail.

The Outgoing Call Restriction enables the administrator to control the outgoing calls, which would entail MWI requests, message notifications, and transfers (TEST). By default, all outgoing calls are enabled. However, outgoing call restrictions can be disabled immediately or according to a specific scheduled time. These two options to disable outgoing calls might be required when the system is going through a maintenance or service condition for some reason.

After you complete the desired selection on the Phone System Basics page, click **Save** to save the information in the database. After any save operation, you should view the Status section at the top of the page. You need to make this a habit when configuring Cisco Unity Connection. By doing this, you avoid any missed configurations or locate errors that might have been made in the various selections. Also, the status indicates the next steps, as displayed in Figure 4-27, that inform you to use the Related Links to add a port group.

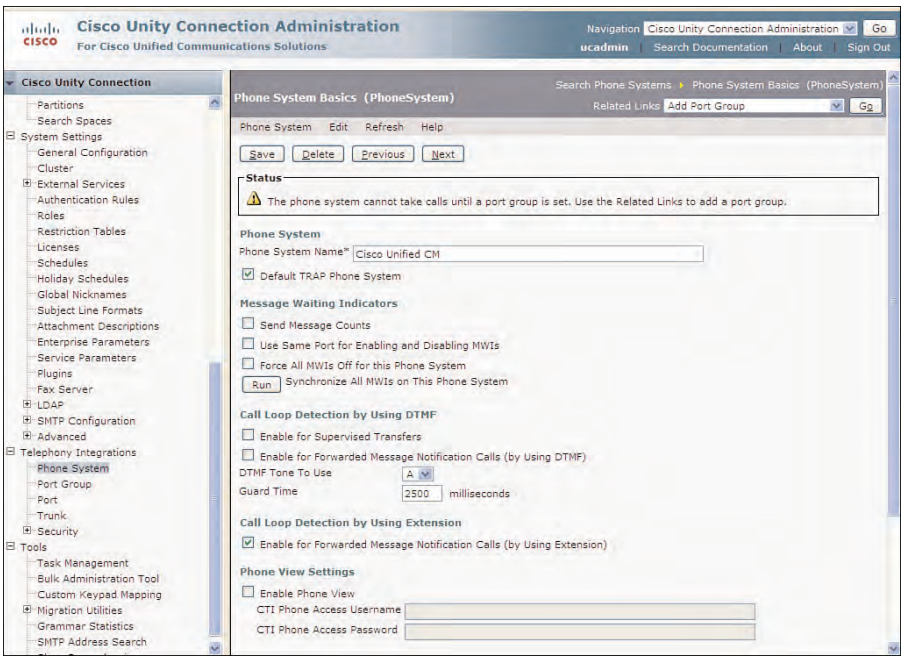

Figure 4-27 *Phone System Basics Status*

www.it-ebooks.info

At this time, you create a new port group by clicking the **Go** button for the Add Port Group selection in the Related Links drop-down. The New Port Group page displays, as shown in Figure 4-28. The port group contains most of the selections that apply to this integration. The various options selected in a port group apply only to the ports that are part of that port group.

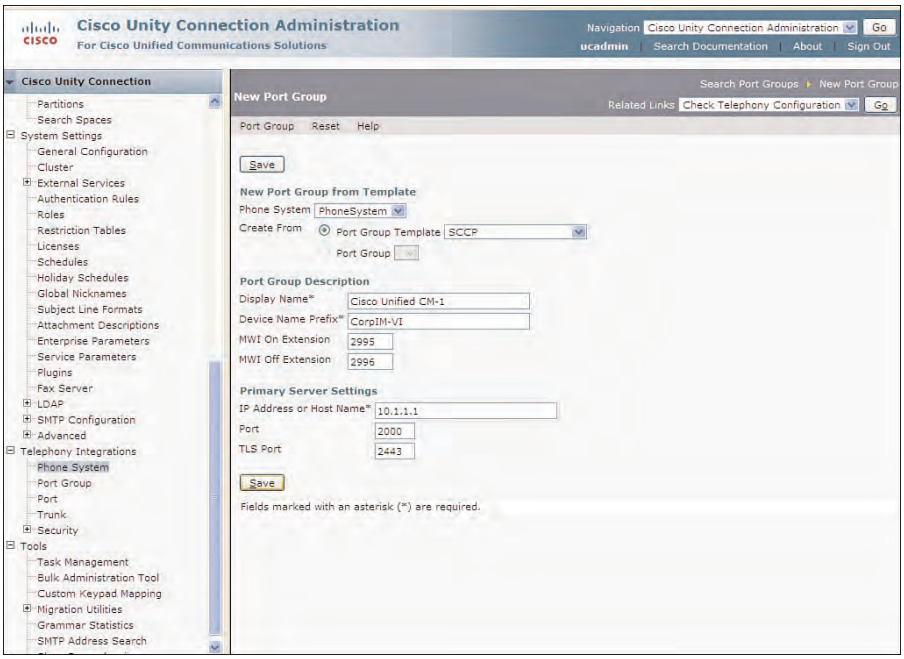

Figure 4-28 *Port Group Configuration in Cisco Unity Connection*

The Phone System drop-down enables the administrator to select the phone system association from the drop-down. In this case, there is a single phone system called Cisco Unified CM.

The Create From selection provides two possible choices. The Port Group Template enables the administrator to create the template using SCCP, SIP, or SIP to PIMG/TIMG. The Port Group option provides the ability to create the new template based on an existing port group. Currently no options are here because a port group has not yet been configured in Cisco Unity Connection.

The Port Group Descriptions include the display name, prefix, and MWI configurations.

The Display Name defaults to the phone system name with the -1 suffix. However, this can be changed and will be the identifier used in Cisco Unity Connection to reference this port group.

www.it-ebooks.info

The Device Name Prefix is the identifier that will be used for the registration of each port included in the port group. Therefore, the name selected here must match exactly with the configured device names for the port configured in Cisco Unified CM. In this case, **CorpIM-VI** has been entered as the name. The -VI suffix is required for all names because this was also added to the ports in Cisco Unified CM.

The MWI On and MWI Off directory numbers must be entered. These numbers must match those entered for the applicable settings in Cisco Unified CM. In this case, 2995 and 2996 has been selected for MWI On and MWI Off, respectively.

The Primary Server Settings include the IP Address or Host Name of the Cisco Unified CM integration that is to be used as the primary server. Other servers (secondary and tertiary) can be entered after the port group configuration is complete.

The Port and TLS Port enable changing the TCP port for SCCP (2000) and TLS (2443). Transport Layer Security (TLS) is defined in RFC 2246 and is a protocol that establishes a secure connection on ports between Cisco Unity Connection and the call processing system. To use TLS, Cisco Unified CM must also be configured for secure ports using TLS. The default uses SCCP (port 2000). It is advisable to never change these ports unless required because of firewalls or other issues. Click **Save** to complete the configuration of the port group.

After you save the new port group, review the Status section near the top of the page. As displayed in Figure 4-28, ports must be added to the new port group. At this point, you want to select **Add Ports** from the Related Links drop-down, and click **Go**. The New Port page displays.

Under the New Phone System Port section, make sure that the check box is selected for the Enabled option. Select the number of ports to be in the port group. The platform and licensing determine the total number of ports that can be configured. An attempt to configure more ports than allowed by the applicable licenses can end in a license violation. This displays on the Status section when you attempt the Save operation.

In the example, you need to eventually have four ports in this port group. However, if you select four for the number of ports, these four ports will be assigned to the phone system, port group, and server. This is advisable if you configure a Cisco Unity Connection server in a single-server deployment. However, an active-active cluster pair will be deployed in this example. Therefore, the first two ports should be configured to the subscriber, followed by the next two ports configured for the publisher. Therefore, select 2 for the number of ports and make sure that the subscriber server is selected from the Server drop-down, as displayed in Figure 4-29.

The Port Behavior settings determines the use of all ports to be added whether the ports are to be used for answering calls, message notification (outbound), MWI (outbound), and TRaP. The ports are also nonsecure by default. Select authenticated or encrypted to use TLS for port connections. Any of the aforementioned port behavior options can be changed individually after creation through the port configuration options. Select **Save** to apply the configuration options and create ports to be members of the specific port group.

www.it-ebooks.info

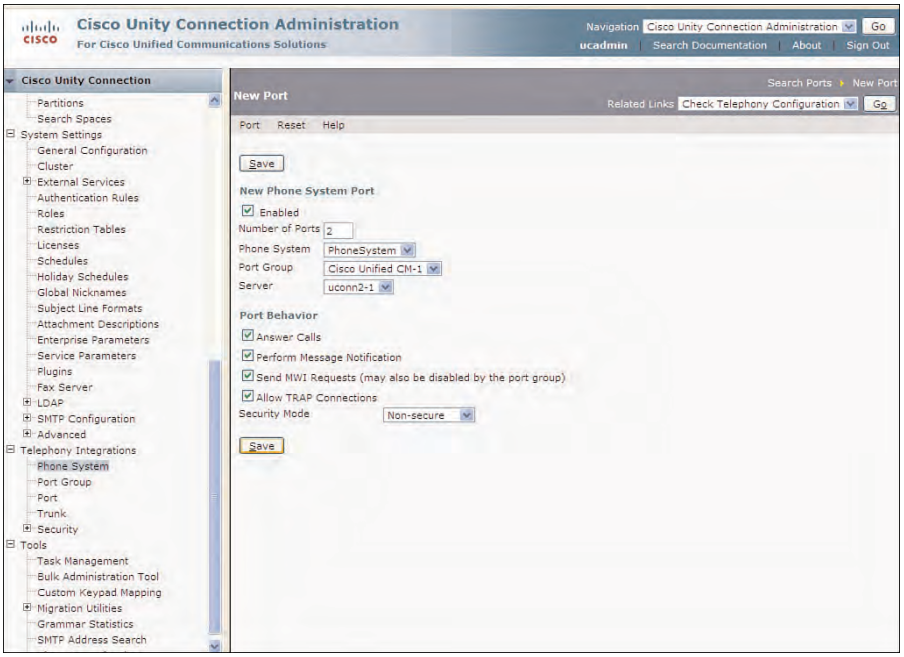

Figure 4-29 *Port Configuration in Cisco Unity Connection*

After you click **Save** for the new ports, the Search Ports page displays. The ports display followed by the -001 and -002 suffix. From this point, you can change each available port by selecting it from the Display Name column and making any necessary selections.

As mentioned earlier, two more ports will be added to this port group that is assigned to the publisher. Click **Add New** from the Search Ports page, and add two ports, making sure that the publisher server is selected from the Server drop-down. Click S **Save** S.

To verify the configuration in Cisco Unity Connection, select Check Telephony Configuration from the Related Links drop-down list, and click S **Go** S. You should immediately get a pop-up window stating that no problems were detected. If you receive an error, take note of the problem details, and make the necessary corrections as indicated. Repeat the test procedure again after any necessary adjustments have been made.

This configuration ensures that the majority of all call traffic will be sent to the subscriber. All client traffic, which does not require ports, should then be directed to the publisher. Of course, you need to make sure that a select group of ports for each server are used for MWI and message notification. For IP integrations, configure 1 port out of every 16 ports for MWI and message notification, according to design practices. However, some organizations adjust this according to their needs. For example, an organization might choose to use something similar to an 80/20 rule (20 percent of the ports for MWI and message notification). Of course, this might vary between organizations in

www.it-ebooks.info

accordance with the traffic flows. If you have fewer ports and an MWI port is not available, you might experience a delay with the MWI light turned on.

You have now completed the integration of the Cisco Unity Connection cluster pair with Cisco Unified CM. You now need to test the integration and troubleshoot issues with ports, MWI, message notification, and user features.

Voicemail Integration Verification

A number of verification steps need to be completed in a logical fashion. Verification steps begin with port registration on Cisco Unified CM. You need want to verify the voice mail pilot configuration from a phone on the system, by dialing the voicemail pilot number to access Cisco Unity Connection. Also, you need to verify the voicemail profile by selecting the Message button on the same phone. In both cases, you should access Cisco Unity Connection. To complete the verification process, explore the Remote Port Status Monitor and Port Status Monitor in Cisco Unified Real-Time Monitoring Tool.

Voicemail Port Verification

The first step in the verification of the integration is to verify the registration of the voicemail ports in Cisco Unified CM. For SCCP integrations, the individual ports register with the Device Name Prefix on the Cisco Unified CM server. Complete the verification of the voicemail ports by selecting **Advanced Features > Voice Mail > Cisco Voice Mail Port** from the Cisco Unified CM Administration toolbar and clicking **Find**. The Find and List Voice Mail Ports page displays showing the status of Registered for all ports, as illustrated in Figure 4-30. In this case, the Cisco Unity Connection cluster pair is registered to a single Cisco Unified CM as the ports are showing registered to 10.1.1.1.

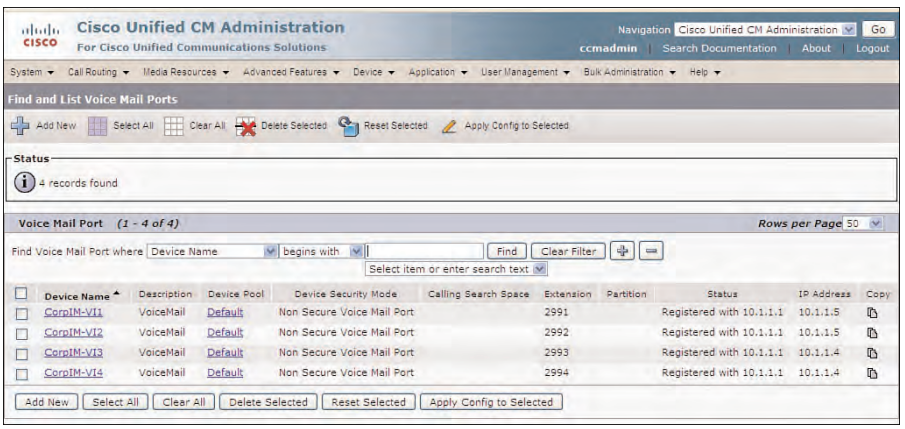

Figure 4-30 *Voicemail Ports Verification in Cisco Unified CM*

www.it-ebooks.info

If the ports are not registered, verify the Device Name Prefix within the port group configuration in Cisco Unity Connection. This must match exactly as listed under the Device Name column, as shown in Figure 4-30. These options are case-sensitive. Also, you need to verify the connectivity between Cisco Unity Connection and Cisco Unified CM. These are the main reasons for unregistered ports. You need to also verify the selections for protocol (SCCP, TLS) and make sure that the necessary services are enabled (Cisco CallManager Service) on Cisco Unified CM. SCCP and TLS are preconfigured for standard port numbers. If these are changed for any reason, this may affect the registration.

If you make changes, you need to save and reset the ports by selecting the specific ports on the Find and List Voice Mail Ports page and clicking the **Reset Selected** button. The Reset Selected button at the bottom of the screen and the Reset Selected icon at the top of the page perform the same operation. In Cisco Unified CM and above, the Apply Config option provides a more efficient selection to apply any changes or updates. A pop-up screen enables the administrator to perform a reset or restart. Read the option screen. In this case, you perform a reset to TFTP a new configuration after making changes. A restart restarts only the registration without requesting the new configuration file.

Voicemail Pilot and Profile Verification

The voicemail ports need to be reachable from the phone system, so the caller can leave messages in a user's voice mailboxes. The hunt pilot is configured as the voicemail pilot, which is configured to point to a hunt list that includes a line group. The line group includes the respective voicemail ports. Therefore, the user needs to access the voice-mail ports by dialing the hunt pilot. You need to test this in two ways:

- Call the hunt pilot number from any IP phone. You should hear the Opening Greeting recording as following:

  "Hello, Welcome to Cisco Unity Connection Messaging System, from a touchtone phone...."

- Press the Message button on the phone to ensure that you hear the same Opening Greeting. If this greeting is not played, you need to check the configuration under the directory number configuration for the phone and ensure that the voicemail profile is properly selected. The configuration of the voicemail profile dictates what occurs when the users presses the Messages button on the phone. The voicemail profile points to the voice mail pilot, which points to the hunt pilot.

Integration Troubleshooting

Cisco Unity Connection has many useful tools and reports and many others are available from the website www.ciscounitytools.com. Two tools that are powerful for troubleshooting integration issue are the Remote Port Status Monitor (rPSM), available from the www.ciscounitytools.com website, and the Port Monitor available with the Cisco Unified Real-Time Monitoring Tool (RTMT), which is downloaded directly from the Cisco Unity Connection server as a client-side application. The Remote Port Status Monitor is available from the aforementioned website, whereas the RTMT is available as a download directly from the Cisco Unity Connection Administration.

www.it-ebooks.info

Remote Port Status Monitor

The Remote Port Status Monitor (rPSM) is a powerful Windows-based application that provides monitoring capabilities to each individual voicemail port. Individual conversation data is presented in a readable format allowing administrators to view and troubleshoot call handler conversations and events as they happen in real-time.

To begin, open a browser to connect towww.ciscounitytools.com and locate the Port Status Remote Monitor for Connection (rPSM) and download it to your administrator workstation. On your workstation, select the .exe file to install the application by selecting **Run** and following the wizard prompts to complete installation procedure.

Before you can use the rPSM with any Cisco Unity Connection server or cluster pair, you must enable the application for each workstation. To enable the RPSM for your workstation, select **System Settings > Advanced > Conversations**. The Conversations Configuration page is shown in Figure 4-31. The last two options on this screen are used to configure rPSM. (The default is disabled.) Check the box for **Enable Remote Port Status Monitor Output** and enter the IP address for your workstation in the **IP Addresses Allowed to Connect for Port Status Monitor Output (Comma-Separated)** field. To locate the IP address of your workstation, select **Start > Run**, followed by **cmd** on the Run pop-up. Click **OK** and the command console now displays. Type **ipconfig** and press **Enter** to display the IP address of your specific workstation.

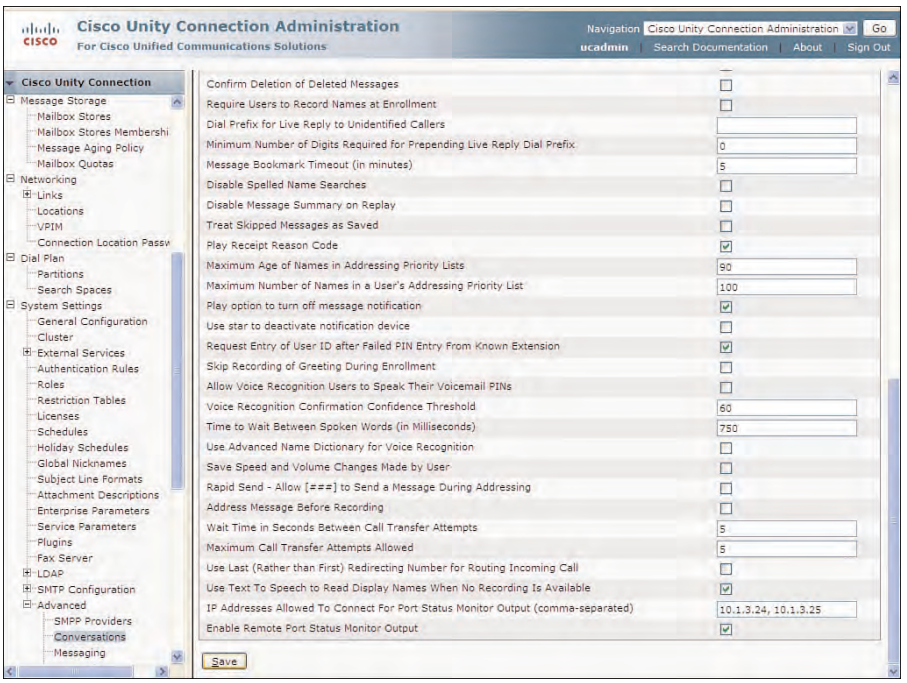

Figure 4-31 *Configure the rPSM Application in Cisco Unity Connection Administration*

www.it-ebooks.info

Complete the operation by clicking **Save**. You can enter as many as 70 addresses in this field separated by commas.

Open the rPSM application on your workstation. You see a pop-up, where you need to enter the IP address of the Cisco Unity Connection server you want to monitor. The application opens displaying the port activity in real-time, as illustrated in Figure 4-32. The port is listed on the left with the activity located on the right. The port and activity are coordinated with a specific color generated by the system to easily identify a different call. Selecting the port on the left displays the message activity for that port. In the latest version of the rPSM, the ports do not display until activity is detected. In most cases, this tool provides in-depth detail. In most cases, the Port Monitor in the RTMT will be the best tool to determine this information.

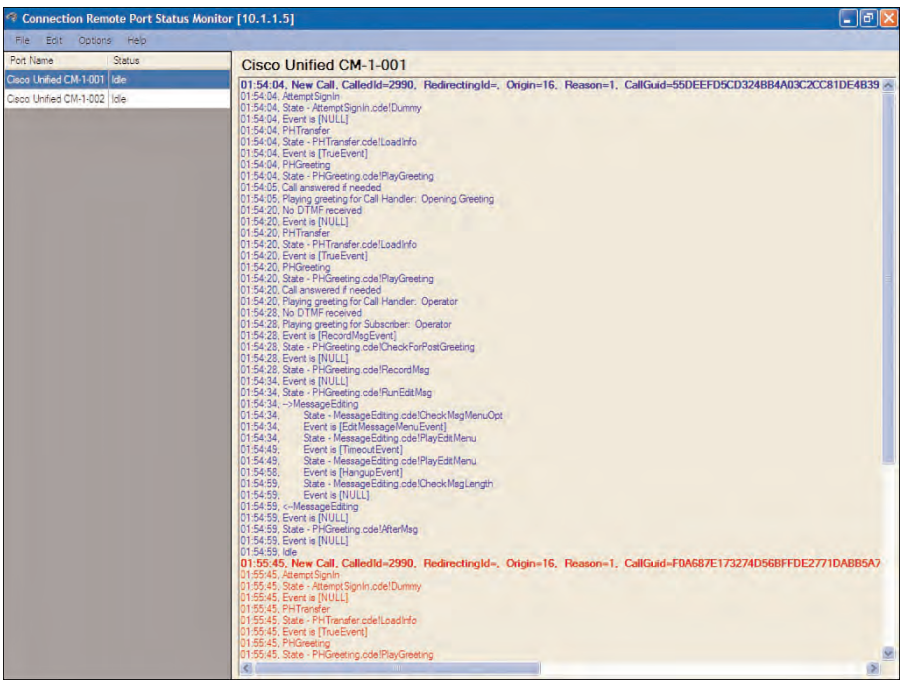

Figure 4-32 *Remote Port Status Monitor*

Port Monitor

The Port Monitor for Unity Connection is included as part of the Cisco Unified Real-Time Monitoring Tool, which is available as a plug-in from Cisco Unity Connection Administration. The Real-Time Monitoring Tool is explored in-depth in Part III; however, you need to understand the Port Monitor at this point because it is an important tool required to verify the integration.

To begin, you need to download the plug-in for the Cisco Unified Real-Time Monitoring to your workstation. The plug-in is available in a Windows and Linux version, depending

www.it-ebooks.info

on your workstation operating system. From Cisco Unity Connection Administration, select **System Settings > Plugins**. The Search Plugins page displays. Click **Find** to see the available plug-ins, as displayed as in Figure 4-33. Click **Download** for the applicable plug-in to download the application to your workstation.

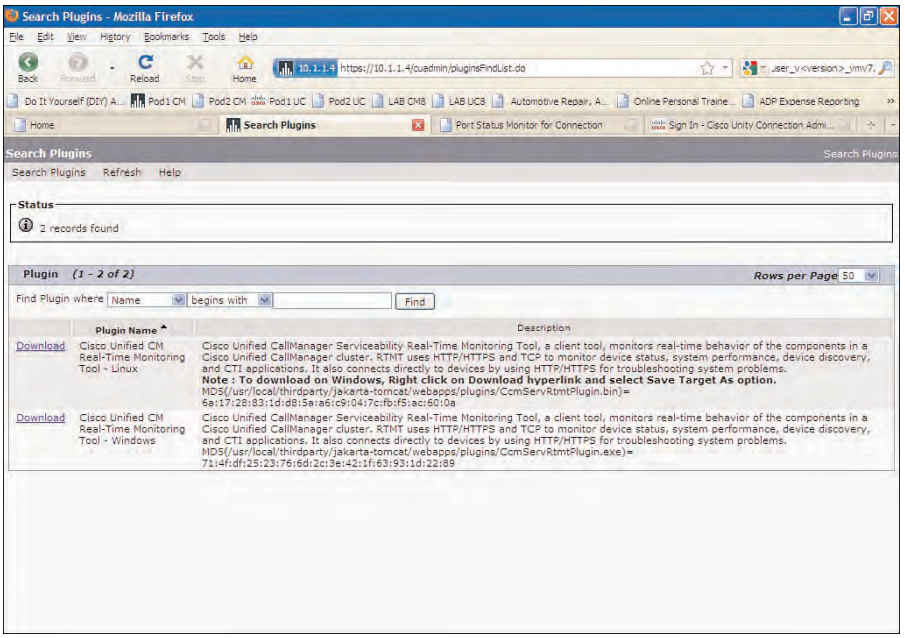

Figure 4-33 *Cisco Unified Real-Time Monitoring Tool*

When the Cisco Unified Real-Time Monitoring Tool application download completes, double-click the icon to open the application. A pop-up window displays requiring the administrator to enter the IP address and authentication information for the Cisco Unity Connection server. You need to enter the applicable information and click **OK**. The Real-Time Monitoring Tool now opens and displays the main page.

Select **Unity Connection > Port Monitor** from the toolbar. The Port Monitor page displays. Select the desired server from the Node drop-down near the top of the page. Then, click **Start Polling** near the bottom to begin the port monitoring for the respective server.

The Port Monitor now displays all ports for the selected server. From this page, all information for each call displays in real-time. The information displayed consists of the called and calling number, the reason, and the redirected information. Along with this information, you can see the status of Cisco Unity Connection for the specific call available in the Application, Display, and Conversation columns. In this section, the administrator can see the call handler and greeting played, as displayed in Figure 4-34.

www.it-ebooks.info

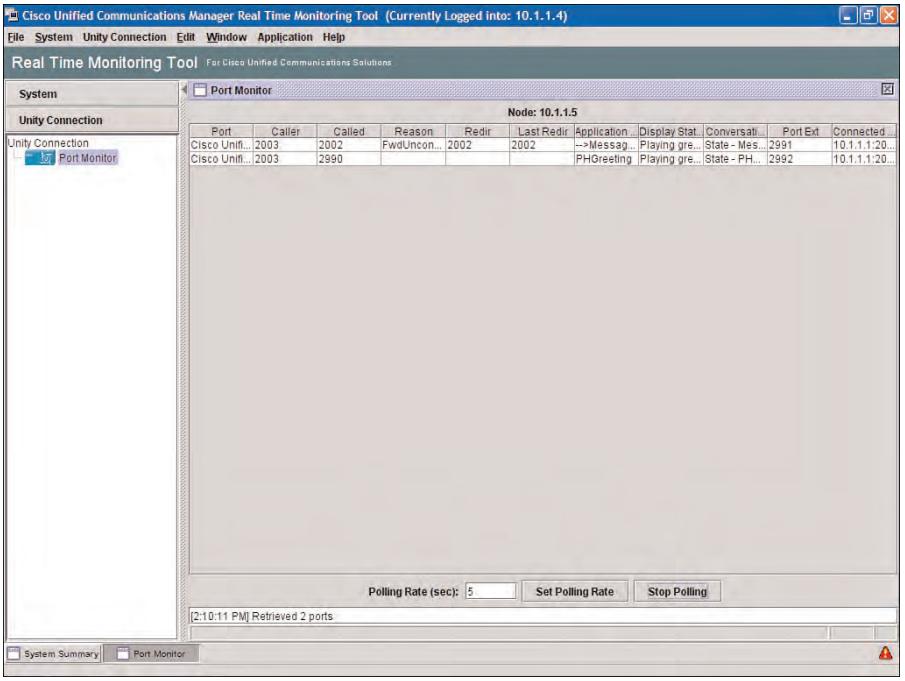

Figure 4-34 *Port Monitor in the RTMT Tool*

When used together, the Port Monitor and Remote Port Status Monitor (rPSM) become a powerful set of tools in testing and troubleshooting integration issues. This tool also enables viewing the callerID, outcalling for message notifications, and current greetings played.

SIP Integrations with Cisco Unified CM

Cisco Unity Connection can integrate with Cisco Unity Connection using SIP. You might encounter issues when you want to use SIP for your integrations with Cisco Unified CM; for example, to implement a distributed messaging deployment or specific security features. SIP integration uses a SIP trunk in Cisco Unified CM and a route pattern, rather than a hunt group scenario as described previously for the SCCP integrations. In the next section, you discover the integration steps required for SIP integrations. SIP might be required in some organizations depending on company policy requirements or the specific application design.

SIP Trunk Configuration in Cisco Unified CM

Understandably, this chapter is not intended to be a discussion of Cisco Unified CM; however, it would be remiss to not cover the integration concepts from the perspective of Cisco Unified CM. Therefore, the basics of how to complete the configuration of SIP

www.it-ebooks.info

trunks are covered, but a detailed explanation of all specific elements will not be described. Only those features that effect the integration are discussed in detail.

From Cisco Unified CM Administration, select **Device > Trunk**, and click **Add New**. The Trunk Configuration displays where you can select **SIP Trunk** and **SIP** for the Trunk Type and Device Protocol, respectively. Click **Next**. The Trunk Configuration page displays, as shown in Figure 4-35.

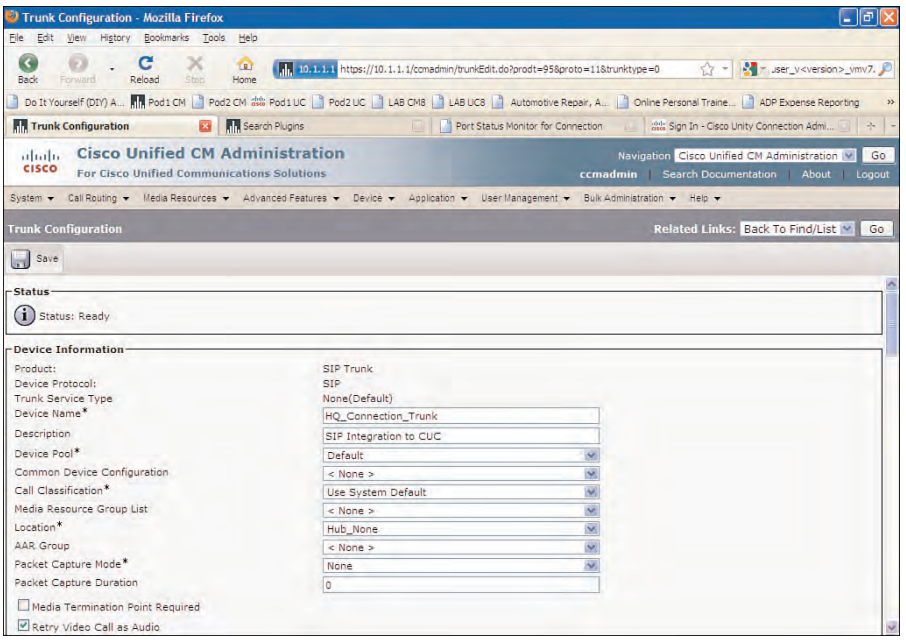

Figure 4-35 *SIP Trunk Configuration in Cisco Unified CM*

Enter a Device Name and Description in their respective fields. You need to always use a name and description descriptive to yourself and other users in the organization. In this example, **HQ_Connection_Trunk** has been chosen as the device name with the description of **SIP Integration to CUC**.

Select the required settings indicated by an asterisk, as follows:

- **Device Pool:** Default (or as desired).
- **SIP Trunk Security Profile:** Non Secure SIP Trunk Profile.

  Defines the security mode that will be applied to the trunk, such as encrypted, authenticated, or nonsecure.
- **SIP Profile:** Standard SIP Profile.

  Defines the various SIP timers and settings that will be applied to the trunk.

www.it-ebooks.info

- **Media Resource Group List (MRGL):** Should be designated for the trunk specifically where transcoding may be required for incoming calls. Cisco Unity Connection can perform transcoding for message recording and playback.

You need to select two remaining options for voice messaging on the trunk. Under the Inbound Calls, check the **Redirecting Diversion Header Delivery - Inbound** check box. Then, under the Outbound Calls, check the **Redirecting Diversion Header Delivery - Outbound** check box. These check boxes ensure that the Redirecting number Information Element, the first redirecting number, and reason are sent and accepted as part of the outgoing and incoming setup messages.

Finally, under the SIP Information, enter the IP address of Cisco Unity Connection in the Destination Address field.

Click **Save** and reset the trunk for the changes to take effect.

Next, you need to configure a route pattern to point to the SIP Trunk. If you use a single server, this can be configured by selecting **Call Routing > Route/Hunt > Route Pattern** from the Cisco Unified CM Administration toolbar. Click **Add New** to create a new route pattern. Only two configuration options are required here. Enter the directory number for the integration in the Route Pattern field. In this example, **2990** is selected for the route pattern, similar to what was used in the Cisco Unified CM integration using SCCP, as in the last example. Select the SIP trunk, **HQ_Connection_Trunk** from the Gateway/Route List drop-down, as displayed in Figure 4-36. Click **Save**.

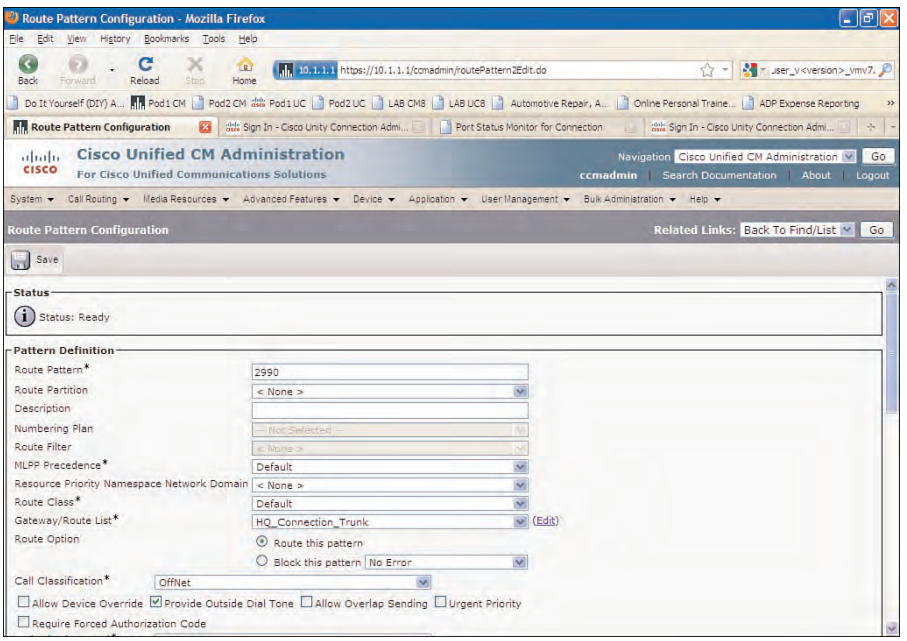

Figure 4-36 *Route Pattern Configuration for SIP Integration*

www.it-ebooks.info

This example is strictly for illustration purposes. It is always best practices to configure all route patterns to point to a route list, which includes the applicable route groups configured with the necessary trunks.

The configuration of the route pattern in Figure 4-36 illustrates the configuration for a single-server deployment. However, this needs to be done differently for an active-active cluster pair. In this case, you need to point this route pattern to a route list that includes a route group consisting of two SIP Trunks, as illustrated in Figure 4-37.

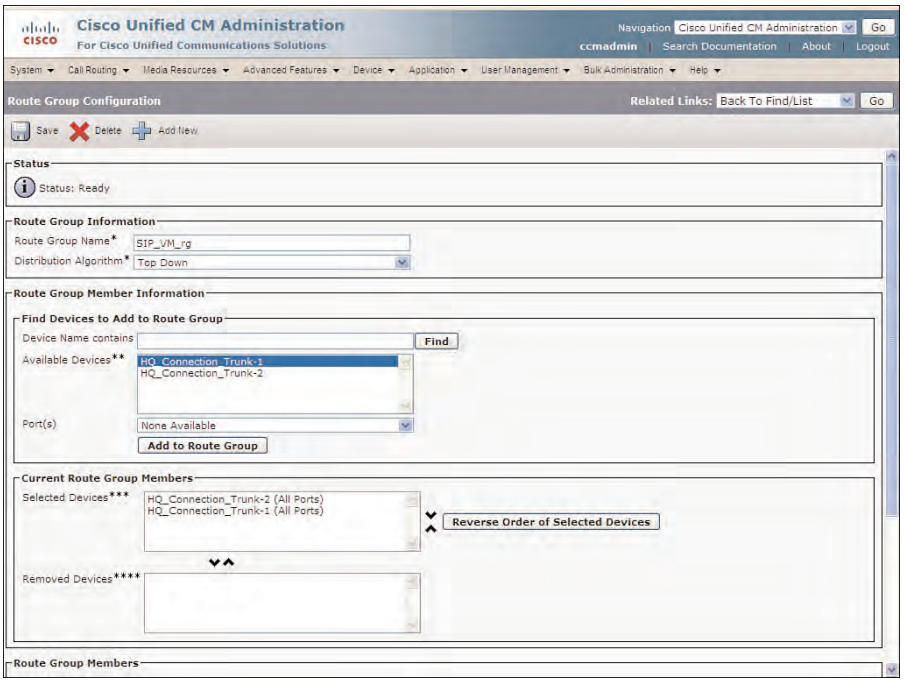

Figure 4-37 *Route Group Configuration for a Cluster-Pair SIP Integration*

The First SIP trunk is configured to the subscriber, followed by the second SIP Trunk configured to the publisher. This ensures that the majority of call traffic is sent to the subscriber as discussed previously.

The Voice Mail Profile still needs to be configured, similar to the SCCP integration; however, the respective voicemail pilot and profile for the phones must be configured. To complete this step, select **Advanced Features > Voice Mail > Voice Mail Pilot** from the toolbar. On the Find and List Voice Mail Pilots page, select the Default description, or other pilot configuration that is required and enter the route pattern. Click **Save** to save your changes. You might need change the Voice Mail Profile if using any other voice mail pilot other than the default.

www.it-ebooks.info

This completes the SIP Integration from the perspective of Cisco Unified CM. The next steps required will be the configuration of the ports and port group in Cisco Unity Connection Administration.

Cisco Unity Connection SIP Integration

The phone system configuration is identical to the configuration required for a SCCP integration in Cisco Unity Connection. Therefore, the configuration steps for SIP integration begin with the port group configuration in Cisco Unity Connection Administration.

You need to select **Telephony Integrations > Port Group** from the navigation on the left portion of the page in Cisco Unity Connection Administration. Click **Add New**. The New Port Group page displays, as shown in Figure 4-38.

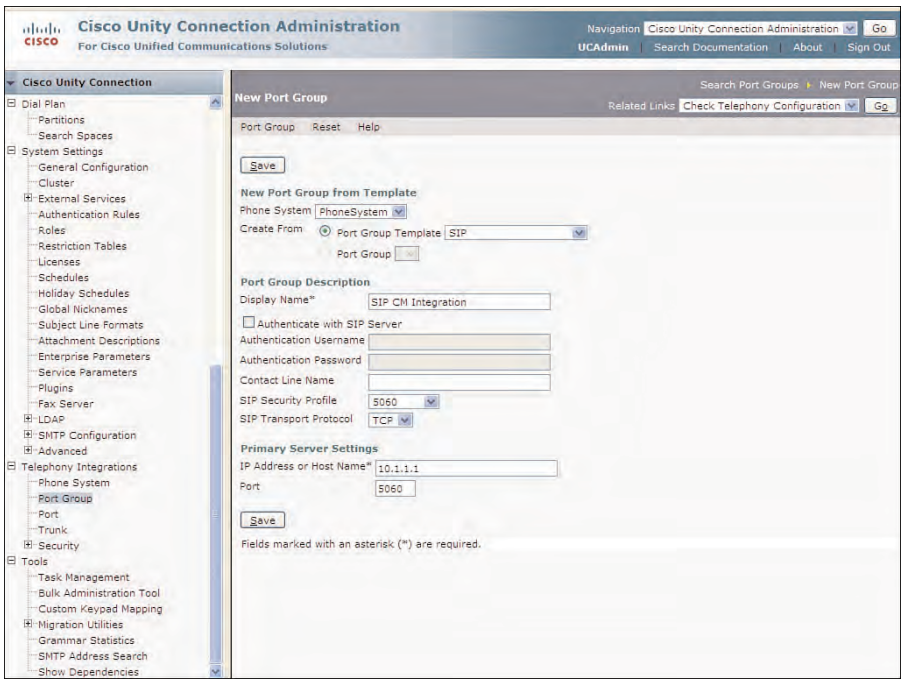

Figure 4-38 *Port Group Configuration for SIP Integrations*

Select the desired phone system from the Phone System drop-down. Then, select **SIP** from the Port Group Template drop-down in the Create From section. You can change the Display Name to provide a more descriptive name, or keep the default that adds a **–1** suffix to the Phone System for the default display name. In this case, SIP CM Integration is selected. Finally, under the Primary Server Settings, enter the IP Address or Host Name of the Cisco Unified CM server. For redundancy, you can enter a secondary and primary server in the port group configuration after saving the current options. At this point, enter the primary Cisco Unified CM server, and click **Save**.

www.it-ebooks.info

Add ports to the port group by selecting **Add Ports** from the Related Links drop-down and clicking **Go**. Enter the required number of ports and port behavior.

If you use the cluster pair, you need to complete this step in two parts. First, configure half the ports to the subscriber. Then, configure the remaining ports to the publisher. This ensures that the majority of call traffic is sent to the subscriber server as discussed previously.

After this operation completes, you need to return to the port configuration page and ensure that ports are configured on each server for MWI, message notification, and TRaP.

Finally, select **Check Telephony Configuration** from the Related Links drop-down and click **Go** to test the integration.

You have completed the SIP integration with Cisco Unified CM. To verify the integration, complete the same verification steps discussed at the end of the SCCP integration section.

The next section discusses the integration of Cisco Unity Connection with Cisco Unified CM Express.

Integrating with Cisco Unified CM Express

You can integrate Cisco Unified Communications Manager Express (CME) to Cisco Unity Connection using SCCP or SIP. In the following pages, the SCCP integration is explored from the perspective of Cisco Unity Connection; although, an overview of the CME integration is discussed.

For many small-to-medium sized businesses, the CME product provides the call-processing services to meet their requirements. However, CME might even be used in remote locations to provide support for phones during a WAN outage. In these cases, Survivable Remote Site Telephony (SRST) provides backup call-processing services to remote phones during an outage, or when the remote has lost connectivity to the host location. SRST provides backup services by enabling the remote phones to register to CME during this outage and provide the necessary services and functionality.

The following section discusses the integration steps with CME. First, you must complete the configuration with CME, followed by the configuration of the integration on Cisco Unity Connection.

Cisco Unified CME Integration Configuration

Cisco Unified CME is a Cisco IOS router-based product for small-to-medium sized businesses that provides call-processing and gateway capabilities for up to 450 phones. CME supports both SCCP and SIP and enables the use of either protocol to provide integration to voice messaging. The following discussion is limited to the integration features and configuration required for integrations of CME with Cisco Unity Connection.

The IOS Configuration in CME begins with ensuring that the IP phones are configured and registered. Cisco Unified CM uses the telephony-service to perform the global configurations for CME. Example 4-1 provides the basic telephony-service configuration,

www.it-ebooks.info

which defines the maximum number of ephone-dn and ephones, or directory numbers and devices, respectively. In this example, a maximum number of four ephones and 10 directory numbers can be configured on the CME system. This example defines IP Phones running SCCP. SIP phone configuration is markedly different in the configuration.

Example 4-1 *CME Telephony Service Configuration*

```
telephony-service
 max-ephones 4
 max-dn 10
 ip source-address 10.2.1.100 port 2000
 voicemail 6010
 max-conferences 4 gain -6
 transfer-system full-consult
 create cnf-files version-stamp 7960 Aug 10 2010 20:57:20
```

The **ip source-address** command defines the TCP and IP address that CME uses to source traffic. TCP Port 2000 is used specifically by SCCP. The **voicemail 6010** command defines the configuration of the Messages button on the registered phones. In this case, the pilot number of 6010 is configured; therefore, the phone attempts to dial 6010 when the Messages button is selected.

Even though a user presses the Message button and the attempt is made to dial 6010 automatically, there must still be a configured dial plan on CME. You accomplish this by using the **dial-peer** configuration command. In Example 4-2, the **dial-peer** command is configured to enable 6010 to be sent directly to the IP address 10.1.1.5, which is the Cisco Unity Connection subscriber. If no ports are available, call traffic is sent to the publisher at 10.1.1.4. The **preference** command in dial-peer selects this peer as a secondary path because **preference 0** is the default for the first dial-peer. This configuration provides the routing of the pilot number 6010 to Cisco Unity Connection, whether the Messages button is pressed or users dial the pilot number directly. Dual tone multifrequency (DTMF) relay is configured to provide out-of-band relay of tones using the H.245 signaling channel, as opposed to the audio channel. In this way, the correct tones are transmitted end-to-end. The use of low-bandwidth codecs can cause DTMF tones to become distorted because of compression. In this scenario, the G.711µ-law codec is configured for voicemail integration.

Example 4-2 *CME Dial Peer Configuration*

```
dial-peer voice 1 voip
 destination-pattern 6010
 session target ipv4:10.1.1.5
 dtmf-relay h245-alphanumeric
 codec g711ulaw
!
dial-peer voice 2 voip
```

www.it-ebooks.info

```
 preference 1
 destination-pattern 6010
 session target ipv4:10.1.1.4
 dtmf-relay h245-alphanumeric
 codec g711ulaw
```

The configuration for phones and voicemail ports is accomplished by using the **ephone** command. The **ephone-dn** command configures specific directory numbers. In Example 4-3, two directory numbers are defined with two phones.

Example 4-3 *CME* **ephone** *and* **ephone-dn** *Configuration*

```
ephone-dn  1
 number 2005
!
ephone-dn  2
 number 2006
!
ephone  1
 mac-address 0019.5695.EBF7
 type 7961
 button  1:1
!
ephone  2
 mac-address 001A.6DD3.055F
 type 7960
 button  1:2
```

A 7961 is configured as **ephone 1**. The first button on this phone is configured with **ephone-dn 1**, which is designated by the command **button 1:1**. The first number before the colon relates to the line button on the phone, whereas the next number after the colon correlates to the **ephone-dn** number. Therefore, this 7961 phone has one configured line with the directory number, 2005, whereas the second phone is a 7960 phone with line one configured with directory number, 2006.

Example 4-4 illustrates the most important configuration for the discussion because it configures the actual voicemail integration required for Cisco Unity Connection.

Example 4-4 *CME Voicemail Integration Configuration*

```
ephone-dn  3  dual-line
 number 6010
 description CME-VI1
 name Voice-Msg-Sys
!
```

www.it-ebooks.info

```
ephone-dn  4  dual-line
 number 6010
 description CME-VI2
 name Voice-Msg-Sys
!
ephone-dn  5
 number 4444
 mwi on VI1
!
ephone-dn  6
 number 4445
 mwi off
!
ephone  3
 vm-device-id CME-
button  1:3
!
ephone  4
 vm-device-id CME-VI2
 button  1:4
```

The **ephone-dn 3 dual-line** and **ephone-dn 4 dual-line** commands configure the actual ports to be used for integration to Cisco Unity Connection. There is a one-to-one correlation of the **ephone-dn** commands and the ports in Cisco Unity Connection. The **name** displays on the phone display when the user places a call to voice mail. In this case, the name **Voice-Msg-Sys** is configured. The **ephone-dn 5** and **ephone-dn 6** configurations designate the MWI On and MWI Off respectively using the **number** command. This configuration must match the MWI configured under the port group in Cisco Unity Connection Administration.

The **ephone 3** and **ephone 4** configurations associate two voicemail ports to the directory number used for the voice-messaging integration. In this case, the vm-device-id, **CME-VI1** is associated with **ephone 3**, whereas **CMEVI2** is associated with **ephone 4** through the configuration of the **button 1:3** command. Both **ephone-dn 3** and **ephone-dn4** are configured with the voicemail pilot of **6010**.

When the integration completes, and the phones connect, you can verify the integration and phones with the **show ephones** command. Example 4-5 displays this command verification. The main verification task that you want to complete is to verify that each ephone shows as REGISTERED, as in Example 4-5.

Example 4-5 *CME* **show ephones** *Display Output*

```
ephone-1 Mac:0019.5695.EBF7 TCP socket:[1] activeLine:0 REGISTERED in SCCP ver 19
and Server in ver 8
```

www.it-ebooks.info

```
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:11
IP:10.2.1.111 52331 7961   keepalive 63 max_line 6
button 1: dn 1  number 2005 CH1   IDLE


ephone-2 Mac:001A.6DD3.055F TCP socket:[2] activeLine:0 REGISTERED in SCCP ver 11
and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:10.2.1.112 49678 Telecaster 7960  keepalive 49 max_line 6continues
button 1: dn 2  number 2006 CH1   IDLE


ephone-3 Device:CME-VI1 TCP socket:[-1] activeLine:0 UNREGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:0
IP:10.1.1.5 36089 Unity Voice Port  keepalive 11 max_line 1
button 1: dn 3  number 6010 CH1   DOWN


ephone-4 Device:CME-VI2 TCP socket:[-1] activeLine:0 UNREGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:0
IP:10.1.1.4 37440 Unity Voice Port  keepalive 10 max_line 1
button 1: dn 3  number 6010 CH1   DOWN
```

You can see that ephone-3 and ephone-4 are showing as UNREGISTERED. These are the voicemail ports that register after the Cisco Unity Connection integration is configured.

To complete this step using SCCP integration, configure a new phone system in Cisco Unity Connection Administration for Cisco Unified CME. The Cisco Unity Connection integration will be the same as completed in the previous section as an integration with Cisco Unified CM. Figure 4-39 illustrates the port group configuration for the CME integration.

www.it-ebooks.info

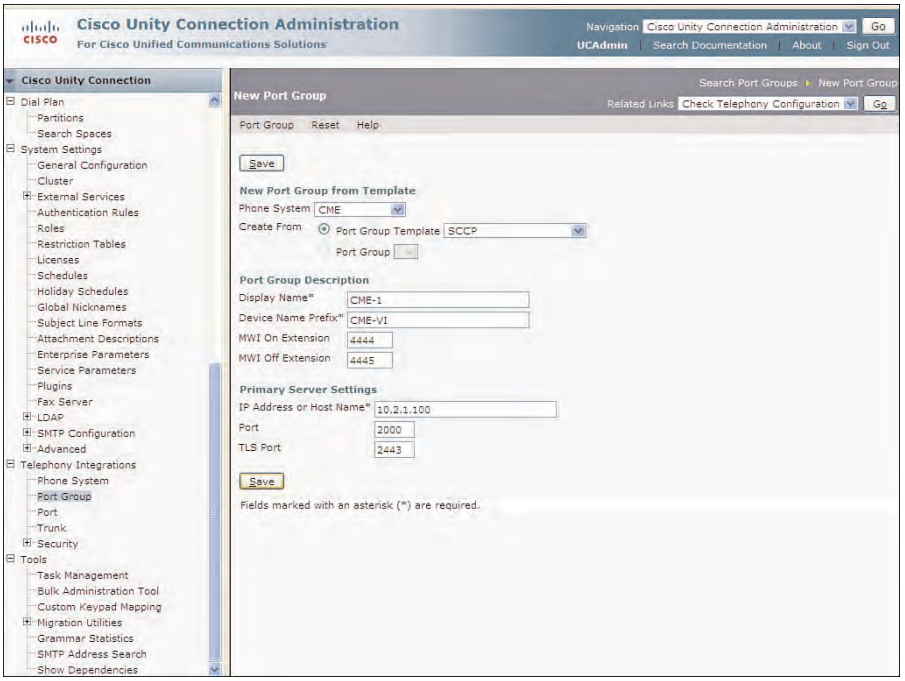

Figure 4-39 *Port Group Configuration for Cisco Unified CME Integration*

Again, enter the **show ephones** command on CME and review the port registration. Both ports should now display as registered, as illustrated in Example 4-6.

Example 4-6 *CME* **show ephone** *Display Output for Voicemail Integration*

```
ephone-3 Device:CME-VI1 TCP socket:[3] activeLine:0 REGISTERED in SCCP ver 18 and
Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:0
continues
IP:10.1.1.5 36477 Unity Voice Port  keepalive 181 max_line 1
button 1: dn 3  number 6010 CH1    IDLE          CH2    IDLE

ephone-4 Device:CME-VI2 TCP socket:[4] activeLine:0 REGISTERED in SCCP ver 18 and
Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:0
IP:10.1.1.4 38005 Unity Voice Port  keepalive 181 max_line 1
button 1: dn 4  number 6010 CH1    IDLE          CH2    IDLE
```

SIP integration can also be accomplished with CME. In this case, SIP dial-peers are configured on CME to provide the necessary integration, as described in Example 4-7.

www.it-ebooks.info

Example 4-7 *CME Voicemail SIP Integration Configuration*

```
dial-peer voice 60104 voip
description To Publisher
destination-pattern 6010
session protocol sipv2
session target ipv4:10.1.1.4
dtmf-relay rtp-nte
codec g711ulaw
dtmf-interworking rtp-nte
max-conn 15  (Number of ports on Publisher)
preference 1
no huntstop
!
dial-peer voice 60105 voip
description To Subscriber
destination-pattern 6010
 session protocol sipv2
session target ipv4:10.1.1.5
dtmf-relay rtp-nte
codec g711ulaw
dtmf-interworking rtp-nte
max-conn 15  (Number of ports on Subscriber)
preference 2
huntstop
!
```

Integrating with Cisco PIMG/TIMG

The configurations for the integration of Cisco PBX IP Media Gateway (PIMG) and T1 Media Gateway (TIMG) are beyond the scope of this book; although, the integration configuration is completed in a manner similar to the SIP integration for Cisco Unified CM. The main difference is to select SIP to DMG/PIMG/TIMG from the Port Group Template under the Create From section, as shown in Figure 4-40.

When configuring multiple PIMG/TIMG integrations, it is a requirement to configure a single port group for each unit. Therefore, if you have four PIMG/TIMG units, you have four port groups. A port group consists of 1 to 8 ports for PIMG units, regardless if the units are equipped with digital or analog ports. The TIMG units can have up to 24 ports per unit. PIMG/TIMG units can be configured individually, in a master-slave relationship, and with or without serial SMDI, MCI, or MD-110, or MCI configuration for call information and MWI requests. The type of integration used depends on the capabilities of the phone system.

www.it-ebooks.info

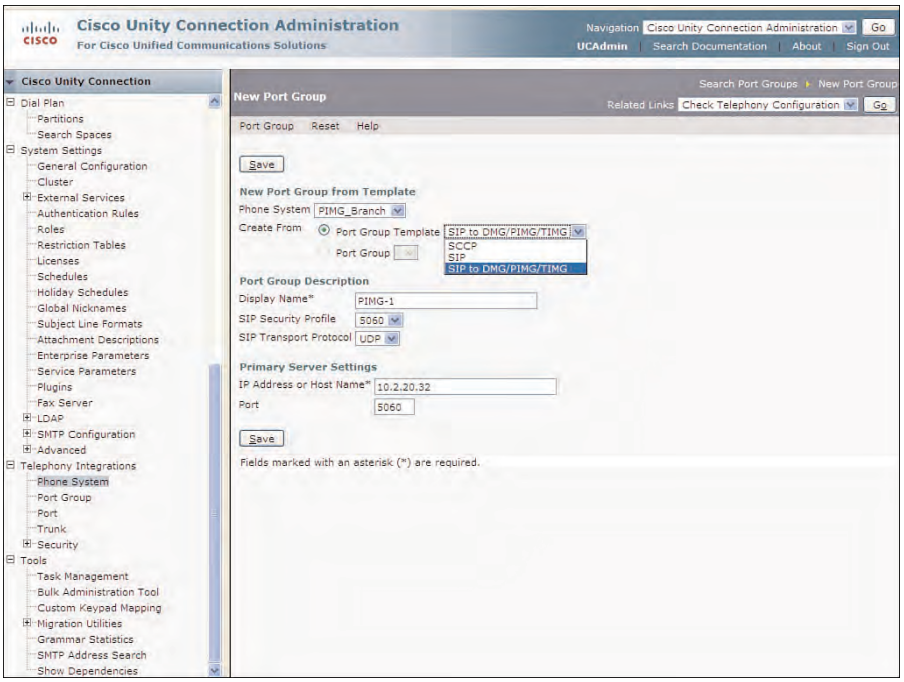

Figure 4-40 *Port Group Configuration for Cisco PIMG/TIMG Integration*

Call Flow and Routing Rules

You have now discovered how to integrate Cisco Unity Connection with a number of call-processing systems and verified the correction operation. In one of the verification steps, you called the hunt pilot of the voicemail system by either dialing the number from a phone, or pressing the Messages button. In either case, you received the Opening Greeting recording, stating, "Cisco Unity Connection Messaging System, from a Touchtone Phone...."

From the perspective of Cisco Unity Connection, this user experience was dictated by the default routing rules configured in Cisco Unity Connection Administration. Two different types of routing rules can be configured. These are direct and forwarded routing rules. The direct and forwarded routing rules are introduced here and developed more fully in Part II.

Understanding Direct and Forwarded Routing Rules

Routing rules influence the call routing as an incoming call is presented to Cisco Unity Connection on a voice port. There are default routing rules, which are created at the time of installation. These consist of two rules for direct calls and two rules for forwarded calls. Direct calls are defined as calls placed directly to the voicemail pilot. Forwarded calls are defined as those calls received at voicemail port on Cisco Unity Connection indirectly,

www.it-ebooks.info

meaning they were forwarded from an extension when a user either does not answer, is busy, or diverted the call to the voicemail pilot.

Following are the two direct routing rules that define two different user experiences depending on the caller:

- **Defined caller:** The user is defined in Cisco Unity Connection; therefore he experiences the Attempt Sign-In conversation.
- **Undefined caller:** Any unknown caller (the user with the calling number is not known) is directed to the Opening Greeting.

Figure 4-41 illustrates the Direct Routing Rules in Cisco Unity Connection Administration. Select **Call Management > Call Routing > Direct Routing Rules** from the navigation pane on the left. The first rule attempts to identify or match defined users or callers, sometimes known as subscribers in other voicemail systems, whereas the second rule matches all undefined callers. These two rules cannot be modified or deleted. However, you can add additional rules that override the default rules because rules are processed in a top-down fashion, as an access list. All new rules are added above the default rules. The ordering of the rules can be modified, except for the last rule for undefined callers, which is always the last rule. Rules can be configured based on the calling, called, or voicemail port.

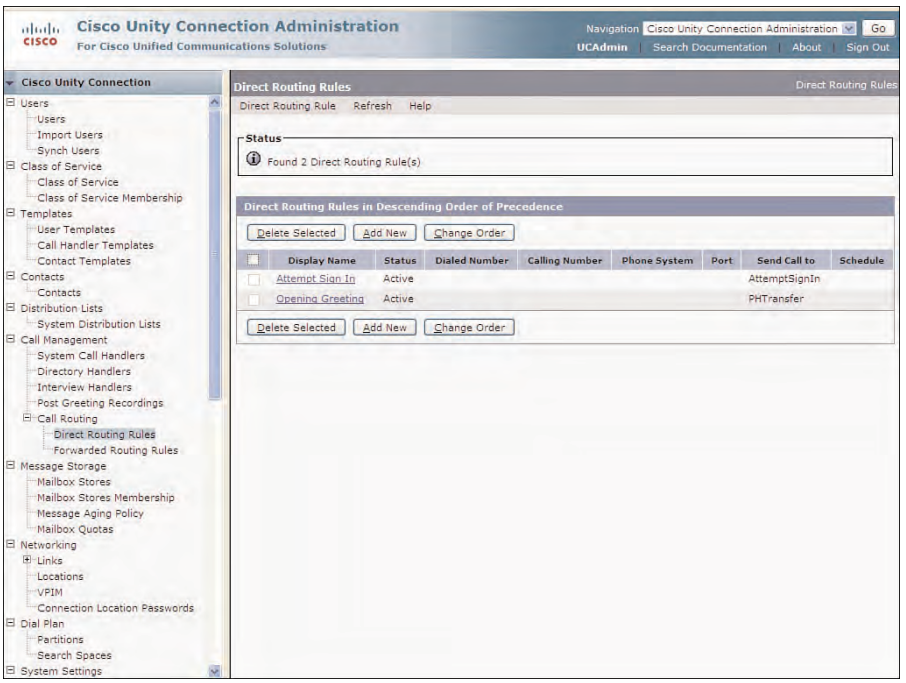

Figure 4-41 *Default Direct Routing Rules in Cisco Unity Connection*

www.it-ebooks.info

Figure 4-42 displays the default forwarded routing rules, where the first directs the caller to the users' personal greeting, whereas the second rule defines all other forwarded calls from unknown extension sent to the Opening Greeting.

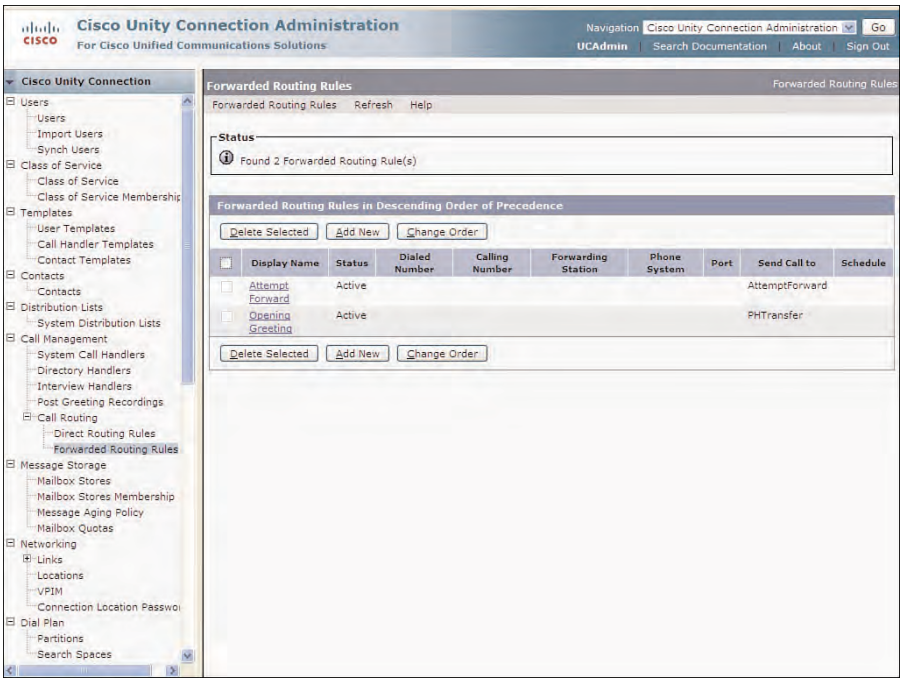

Figure 4-42 *Default Forwarded Routing Rules in Cisco Unity Connection*

You now understand Cisco Unity Connection, its installation, and integration. In the next part of the book, you explore the various administrative features and functions.

Case Study: Cisco Unity Connection Integration with Legacy Systems

Engineers for ANS Corporation plan to integrate a new Cisco Unity Connection server with two legacy PBX systems, and a Cisco Unity CM server. They have determined that they will use a centralized messaging system, even though the legacy systems are located at two different branch locations and must also be integrated with Cisco Unity Connection. Both of the legacy PBX system haves T1 ports equipped.

The Cisco Unity Connection server will be located at the headquarters location, along with the Cisco Unified Communications Manager. Cisco TIMG devices will be used for integration of the legacy system with Cisco Unity Connection, as shown in Figure 4-43. Centralized messaging is a valid solution because the branch sites for IP connectivity and

www.it-ebooks.info

the TIMG units provide SIP integration across the WAN and a single T1 digital connection to each legacy PBX.

This configuration consists of three configured phone systems in Cisco Unity Connection Administration, each with a single port group. There will be 23 ports defined for each TIMG unit. Because ANS Corporation has purchased licenses for the largest server, which supports 250 ports, these provide the capabilities for ANS engineers to configure up to 202 ports for the Cisco Unified Communications Manager integration. Twelve ports were designated as outbound for MWI and message notification, which was an average of 1 out of every 16 ports. This leaves 190 ports for inbound calls on the new Cisco Unified Communications Manager system. SIP integration can also be used for Cisco Unified CM integration and the two legacy systems using TIMG.

Summary

This chapter provided an understanding of Cisco Unity Connection integration concepts and configuration with various call-processing systems. You learned how to understand the following:

- The attributes of an integration using Cisco Unity Connection.
- The function, features, and relationships of port groups and ports in Cisco Unity Connection for creating integrations with Cisco Unified CM, Cisco Unified CME, and legacy PBX systems using PIMG/TIMG units.
- The configuration required for SCCP and SIP integrations with Cisco Unified CM and Cisco Unified CME.
- The differences between default direct and forwarded routing rules and how they influence call routing based on whether a caller is defined or undefined in Cisco Unity Connection Administration.

www.it-ebooks.info

This page intentionally left blank

www.it-ebooks.info

Chapter 5

Cisco Unity Connection Users and Contacts

This chapter covers the following subjects:

- **Cisco Unity Connection Administration:** Gain an understanding of users and contacts and the default users available in Cisco Unity Connection Administration.
- **User and Contact Configuration:** Understand the configuration of administrative and voicemail users in Cisco Unity Connection by applying a user template that includes Authentication rules, Class of Service, schedules, and holidays.
- **Cisco Unity Connection Bulk Administration Tool:** Understand how to create multiple users using the Bulk Administration Tool in Cisco Unity Connection Administration.
- **Cisco Unity Connection Users Import:** Understand how to import users from Cisco Unified CM (CUCM) using Administrative XML (AXL) Application Programming Interface (API).
- **Cisco Unity Connection LDAP Integration:** Understand the features, functionality, and configuration of Lightweight Directory Access Protocol (LDAP) integration and authentication in Cisco Unity Connection version 8.x.

After Cisco Unity Connection software is properly installed, configured, and integrated for the desired phone system, the next step is create users and contacts to provide user access to the voice-messaging system. This chapter explores the functionality and the various methods to configure the many different types of users and contacts in Cisco Unity Connection. In this chapter, you understand the purpose, function, and configuration of each type.

In some cases, users will be configured individually using the functionality provided for in Cisco Unity Connection Administration. This method works perfectly when only a few users or contacts need to be created and affords the administrator with the ability to

www.it-ebooks.info

quickly create users and contacts. However, when multiple users or contacts must be created, this procedure can be laborious, and therefore other means must be employed. This is where the Bulk Administration Tool, Cisco Administrative XML (AXL), and LDAP integration can assist the administrator in simplifying this process.

In this chapter, you discover the purpose and functionality of the various types of users and contacts. The default users created at the time of installation are also explored. Each of these default users has a defined purpose, which are described in detail. In this chapter, you understand the following:

- The purpose of users and contacts in Cisco Unity Connection.
- The default users created at the time of installation in Cisco Unity Connection.
- The configuration of users and contacts in Cisco Unity Connection Administration.
- The configuration of multiple users using the Bulk Administration Tool, Administrative XML (AXL), and LDAP integration methods.
- The function and configuration of LDAP authentication.

Introduction to Users and Contacts

In the previous chapter, you learned that two users were created during the installation process. These users were defined as the application administrator and platform administrator. Each of these user accounts enables the administration of the various web pages available in Cisco Unity Connection.

The platform administrator is specifically used to access the command-line interface (CLI), Cisco Unified OS Administration, and Disaster Recovery System (DRS). You can create additional platform administrator users through the CLI or change the existing password for the platform administrator accounts; however, platform administrator credentials are "hidden" from the view in Cisco Unity Connection Administration, and must be configured solely from the CLI.

The application administrator user is defined as a user without a voice mailbox and is used for ongoing administration of Cisco Unity Connection. This user account provides access to the Cisco Unity Connection Administration, Cisco Unified Serviceability, and Cisco Unity Connection Serviceability web pages. This user is "visible" in Cisco Unity Connection Administrator and can be managed directly from this interface. This user has System Administrator rights and can manage all objects in the aforementioned web pages.

The information for the application and platform administrator should be used only to provide the initial configuration. These users should be kept private and documented in a secure location. For security purposes, all other user credentials should be created that are specific to those users who need access to the various administration configurations in the Cisco Unity Connection system. Therefore, when a user leaves the organization, the credentials are removed thereby maintaining the security of the system.

www.it-ebooks.info

In most cases, administrators will need only the application administrator account to be configured because the applications controlled by this account are required most of the time for day-to-day administration of the system. Keep in mind, that all usernames and passwords should be configured in accordance with the organizations security policy. For example, if there are five administrators employed by the company to administer Cisco Unity Connection, each person should have his own username and password. If a person leaves the company, his authentication can easily be removed without affecting the security of the system. However, if everyone were to have the same username password, authentication credentials must be changed when a person leaves to maintain the highest level of security. The previous example is not a best practice and should be avoided. Also, the application administration user can be deleted, leaving no access to Cisco Unity Connection Administration. Therefore, it is advisable that at least one more backup user is created, even if you are the only person administrating the system. You can also use the platform administrator account and the CLI to reset or create additional application administrator accounts.

Understanding Users and Contacts

The default application administration user is an example of a user configured without a mailbox. This user has the highest level of rights to all pages in Cisco Unity Connection Administration, Cisco Unified Serviceability, and Cisco Unity Connection Serviceability. These rights are defined by the configured roles as a System Administrator. Roles provide access to the various administrator responsibilities. You will understand each of these roles and how to assign them to users within this chapter.

Users Without Mailboxes

Users without a voice mailbox are created for accounts that need to administer the voice-messaging system based on their assigned role. These users do not have an assigned phone or extension in Cisco Unity Connection Administration and cannot send, receive, or forward voice messages. The administrator can configure as many users without mailboxes as needed because each of these types of users is not counted as a voicemail licensed user.

User With Mailboxes

In most cases, you configure users with mailboxes. These users can send, receive, and forward voice messages. Each configured user is counted as a voicemail licensed user. The users' features and capabilities are dependent on the configured options, templates, and Class of Service (CoS), which are configured by an administrator. These options, templates, and CoS features are discussed throughout this section. A user with a mailbox can also be configured as an administrator by applying the System Administrator role to this applicable user.

www.it-ebooks.info

Contacts

Contacts have a number of purposes depending on the needs of the organization. These are similar to users without mailboxes; however, they have a phone extension, but no voicemail or administrative rights on Cisco Unity Connection. Quite possibly, they might have just a phone extension or voicemail on another system. These users can be configured for agents, staff, vendors, or contractors that have a phone extension or an external phone number and need to be reachable from the voice-messaging system.

Users in Cisco Unity Connection can be afforded the ability to access these contacts through the directory, name dialing, or personal call transfer rules. Each of these features is discussed later in this section. These contacts can be defined by the administrator, and made available to all users. Or they can be user-defined, which means that they are available only to a specific user.

Voice Profile for Internet Mail (VPIM) users can also be configured as contacts. In this case, these VPIM contacts have a directory listing, but their voicemail exists on another voice-messaging system. The voicemail can be recorded on the local Cisco Unity Connection server and forwarded to the configured contacts' voicemail via Simple Mail Transfer Protocol (SMTP).

Default Users

Along with the application administrator user created at the time of installation, the number of default users exist to provide various functions. These default user accounts cannot be deleted and will always be displayed in Cisco Unity Connection Administration. These users are defined as

- **Operator:** Configured as a User With a Mailbox. This is the default message recipient for the Operator call handler. Call handlers are explored later in this section. The default behavior can be modified as required to meet the needs of the organization; however, if the default behavior is used, someone should be assigned the job responsibilities to handle these calls and monitor this voice mailbox.
- **Replication:** Configured as a User Without a Mailbox. This user is the replication agent responsible for replicating all objects within the Cisco Unity Connection cluster and when replicating objects and directory information for VPIM and digital networking.
- **undeliverablemessagesmailbox:** Configured as a User With a Mailbox. This is the only user assigned as a member of the Undeliverable Message distribution list. If for any reason a message cannot be delivered, this distribution list receives all messages including mailbox quotas exceeded, or notifications of undeliverable messages (sending and forwarding messages). Distribution lists are discussed later in this section. Similar to the operator mailbox, someone should be assigned to monitor this mailbox. Additional users can be assigned to this distribution list as required.
- **UnityConnection:** Configured as a User Without a Mailbox, this user is the sender of voice messages to all outside or external callers. When a call is received at the

www.it-ebooks.info

gateway from a customer and directed to voicemail, the call is recorded and forwarded to the users' voicemail. If the user retrieves this message using Internet Message Access Protocol (IMAP), this message displays as originating from Cisco Unity Connection Messaging System, which is the display name for this user.

To view the users in Cisco Unity Connection, you need to log in to Cisco Unity Connection Administration using the application administration account credentials. Select **Users > Users** from the navigation section on the left portion of the page. The Search Users page displays. Figure 5-1 illustrates the Search Users page displaying the five default user accounts.

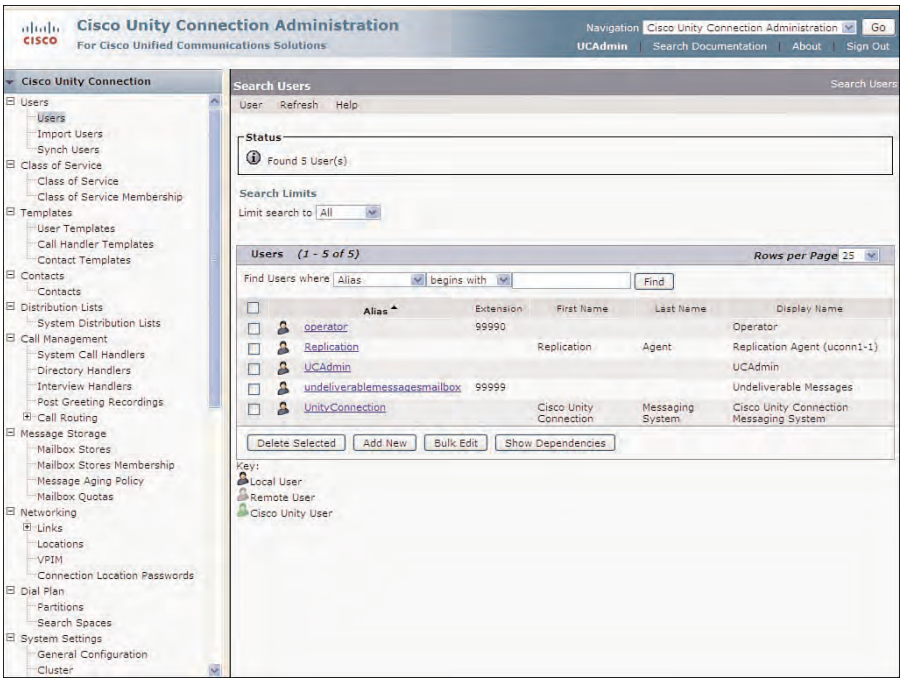

Figure 5-1 *Cisco Unity Connection Administration Default User Accounts*

Configuring Users

Before you can configure users, you need to be familiar with the various elements that affect the configuration of these users. Depending on the type of users configured, these elements consist of the following:

- Authentication rules
- Schedules and holidays
- Class of Service
- Templates

www.it-ebooks.info

Authentication Rules

Authentication rules control the authentication policy when a user attempts to log in. By default, two rule sets are defined: one for the voicemail and one for web applications. The voicemail password is commonly referred to as the PIN, whereas the web application is referred to as the password.

Additional rules can be defined as needed, or the default rules can be changed to meet the security policy requirements of the organization. The authentication rules enable the administrator to define the minimum credential length, stored credentials, and when the credentials expire and if the user is required to enter a new password or PIN.

Lockout policies are also a part of authentication rules. Lockout policies control the user experience when failed attempts are made at login. There are three levels of authentication rules that can an administrator can define to control the level of security:

- An administrator is required to unlock the account (the highest level).
- A lockout duration that automatically unlocks the account after a specified time period.
- No specified lockout policy (the lowest level).

By default, the minimum credential length is six characters with five stored credentials.

The Check for Trivial Password option is also configured by default. This feature, along with the default stored credentials option, means that the past five stored credentials are included in the trivial password check. In addition to the stored credentials, the trivial password check includes the following checks:

- Digits and characters are not the same or consecutive. For example, 111111 or 987654 would be disallowed.
- You cannot use the same digit more than twice consecutively. For example, 844476 would be disallowed.
- The password/PIN does not match the configured extension for the user, either forward or backward; nor can the password match the spelling of any configured names in Cisco Unity Connection Administration for that user (first name, last name, organization, company name, and so on).
- The password/PIN must contain at least three different digits and cannot be configured by changing a single-character from a previously stored credential.

The trivial password check can be restrictive (and sometimes annoying) to the user. However, it does afford the highest level of security and ensure the user selects strong passwords. When using these features, users might forget their password, which would require administrator intervention. In these cases, the administrator can reset passwords through Cisco Unity Connection Administration.

To view the default authentication rules, select **System Settings > Authentication Rules** in Cisco Unity Connection Administration. The Search Authentication Rules page

www.it-ebooks.info

displays showing the two default rules, as shown in Figure 5-2. Selecting each of the rules enables the administrator to view and modify the various configurations that apply to each rule.

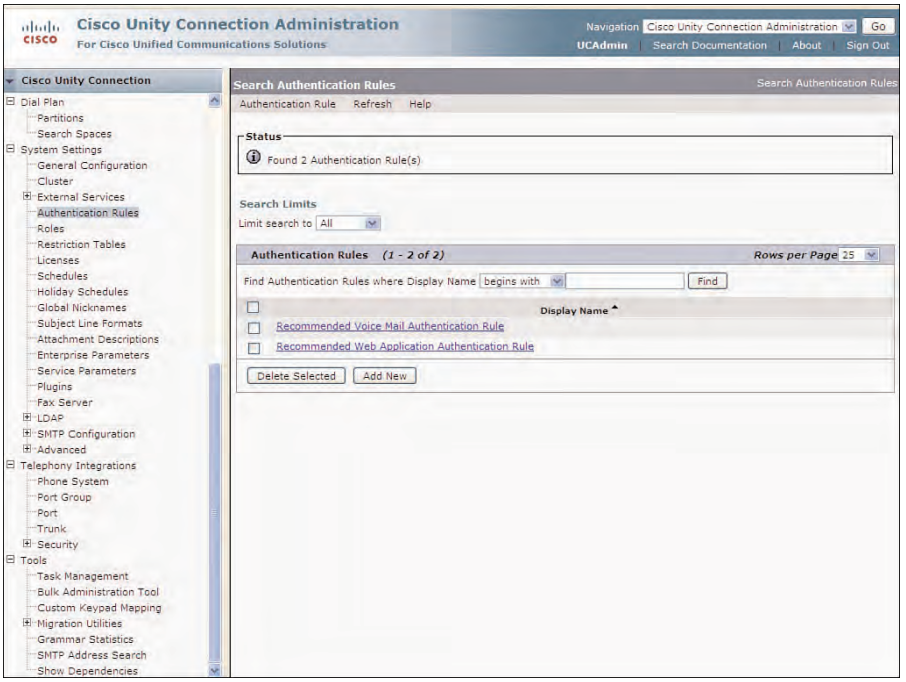

Figure 5-2 *Default Authentication Rules in Cisco Unity Connection Administration*

Figure 5-3 and Figure 5-4 display the default authentication rules for voicemail and web applications, respectively. The voicemail authentication rules are numeric only because they are used for logging to Cisco Unity Connection using the telephony user interface (TUI), where the web application authentication rules are alphanumeric because they are used to log in to the various web and interface applications.

Authentication rules should be changed or created before users are configured. The authentication rules are applied to newly created users through the user template configuration. The user template configuration is discussed later in this chapter. Changing the authentication rules after users have been created will apply the settings to existing accounts. When the user changes his password, these new changes will be subject to the currently configured authentication rules.

For the configuration of users without mailboxes, or administrative users, only the web application authentication rules apply. For the users with mailboxes, both the web application and voicemail authentication rules apply, depending on whether the configured users use the web application clients or are also configured with administration rights.

www.it-ebooks.info

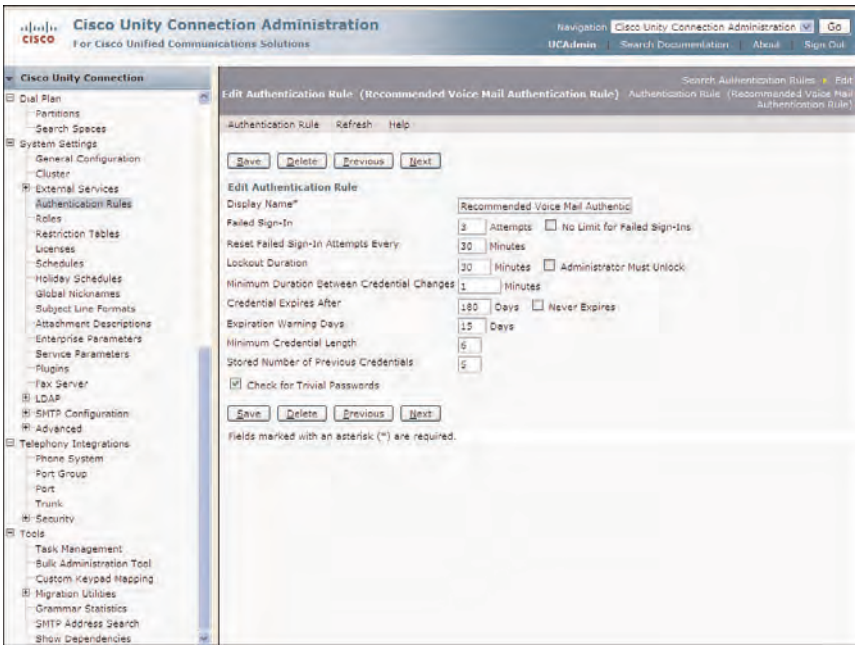

Figure 5-3 *Voicemail Authentication Rules*

Figure 5-4 *Web Application Authentication Rules*

www.it-ebooks.info

Schedules and Holidays

Schedules and holidays work together in Cisco Unity Connection to control greetings, transfers, and access rights based on a configured schedule. For example, a user might need to have calls transferred to an outside extension after work hours (based on a schedule) but sent to voicemail during normal business hours. Also, this same user might need to play a different greeting. These options can be controlled with schedules and holidays.

Before configuring a specific schedule, you must first define the holidays that apply to each user. Holidays are considered as exceptions to the actual schedule. For example, a user work day schedule is configured as Monday through Friday, 8 a.m. to 5 p.m., except when a configured holiday falls on one of these days. In this case, that day is understood to be a nonworking day, and closed hours greetings and transfers need to be applied.

In most cases, there is one holiday schedule; however, for companies with offices located in different countries, different holiday schedules are required as local holidays apply. There is currently a default holiday schedule configured called Holiday. You need to either add your actual observed holidays to this default holiday schedule or create a new holiday schedule. Currently, no holidays are configured by default.

From Cisco Unity Connection Administration, select **System Settings > Holiday Schedules** to display the Search Holiday Schedules page, as shown in Figure 5-5.

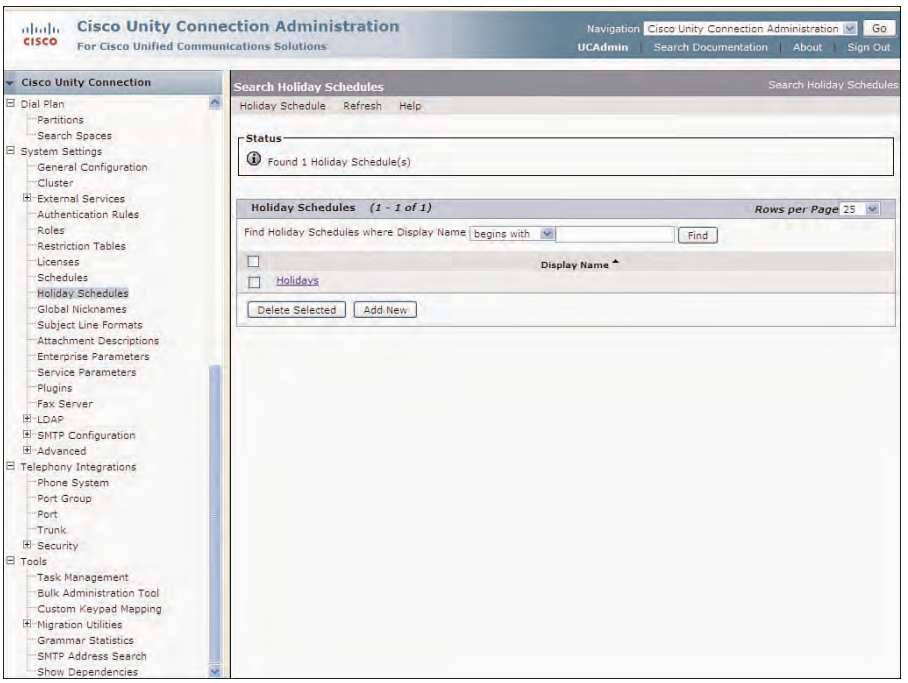

Figure 5-5 *Default Holiday Schedule*

www.it-ebooks.info

Select the **Holidays** link to display the default holidays schedule. The Holidays name can be changed as needed.

Click **Add New** to create a new holiday as needed, making sure to save each holiday. As the administrator, you can add as many holidays as required. The holidays that change yearly need to be adjusted each year. For example, this would apply to holidays such as Thanksgiving Day, Labor Day, or Memorial Day in the United States. Figure 5-6 illustrates the configuration of a new holiday for Christmas Eve and Christmas Day. In this case, the start date is December 24th and the end date is December 25th, where the check box for End of Day is selected. Click **Save** to save the new holiday. Through these various configuration options, holidays can be configured as partial days or a range of days.

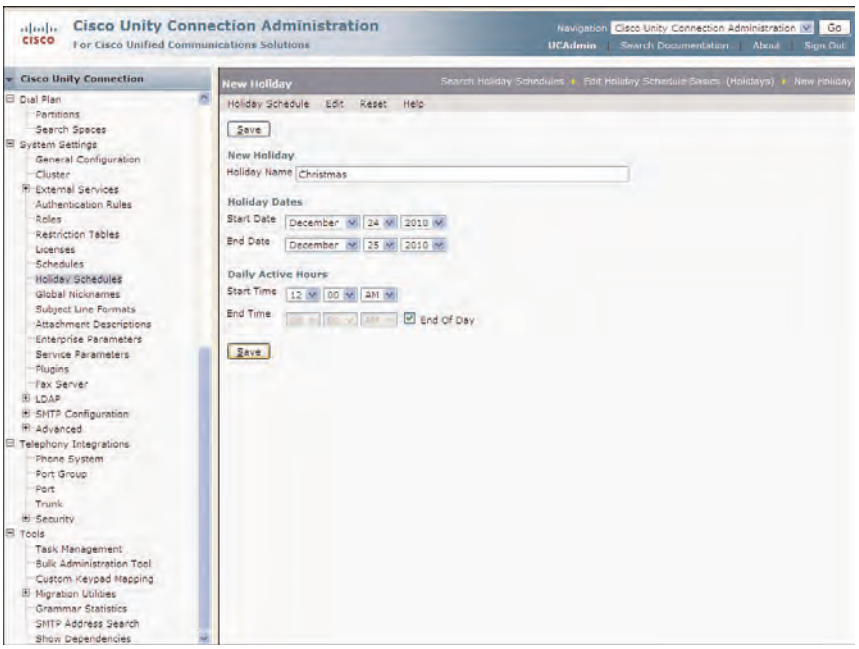

Figure 5-6 *New Holiday Configured For Christmas*

Select **Holiday Schedule > New Holiday** to add additional holidays to the schedule as wanted. After all the holidays are configured, select **Edit > Holiday Schedule Basics** to display the Edit Holiday Schedule Basics page for the U.S. Holidays schedule, as shown in Figure 5-7.

Holidays need to be applied to a specific schedule. Three schedules are currently available by default:

- All Hours
- Voice Recognition Update Schedule
- Weekdays Schedule

www.it-ebooks.info

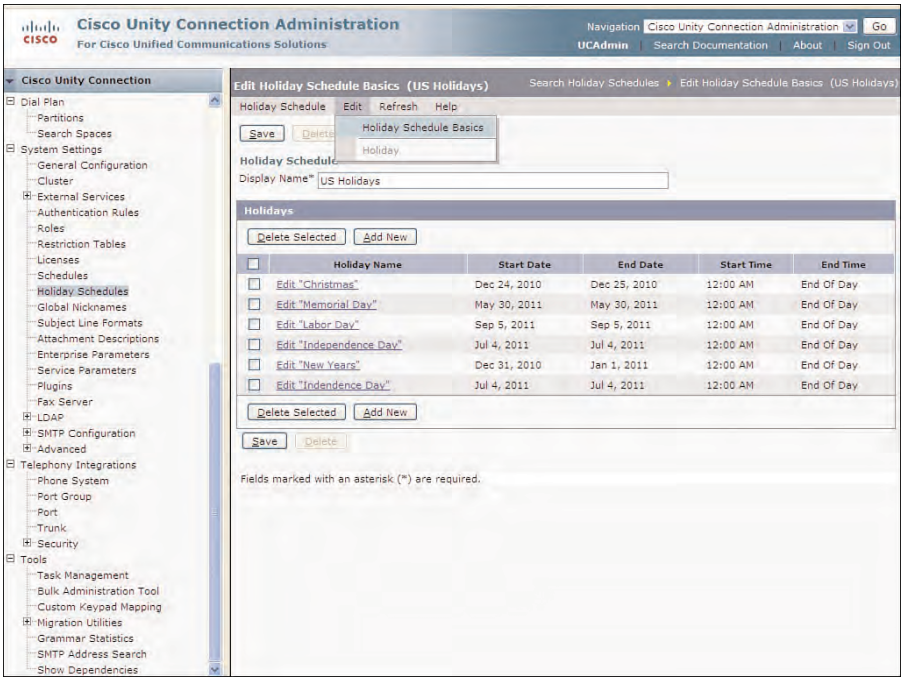

Figure 5-7 *Holiday Schedule Configuration*

The All Hours and Voice Recognition Update Schedules are configured by default for 24x7 operations with no holiday schedule. The Weekdays Schedule is configured by default for Monday through Friday (8 a.m. to 5 p.m.) operation with the default Holiday Schedule applied. These schedules cannot be deleted but can be modified as required.

To configure schedules, select **System Settings > Schedules** in Cisco Unity Connection Administration for the screen shown in Figure 5-8.

To modify an existing schedule, select the schedule to display the Edit Schedule Basics page. From this page, you can click the **Edit** link to change the existing schedule, or click **Add New** to add a new day to the existing schedule.

For example, to add Saturday hours (8 a.m. to 12 p.m.) to the Weekdays schedule, select the **Weekday** schedule to display the Edit Schedule Basics (Weekdays). Click **Add New** to display the New Schedule Detail page. Configure the Saturday Work Hours, as shown in Figure 5-9. You need to uncheck the End of Day check box to select the ending hours; otherwise, a schedule of 8 a.m. to midnight will be applied.

After configuring the New Schedule Details, click **Save.** Ensure that the Status section of the page displays Created Schedule Detail(s), thereby ensuring that the new configurations were saved in the database. To display the reconfigured schedule, select **Edit > Schedule Basics** from the toolbar. Figure 5-10 illustrates the Edit Schedule Basics.

www.it-ebooks.info

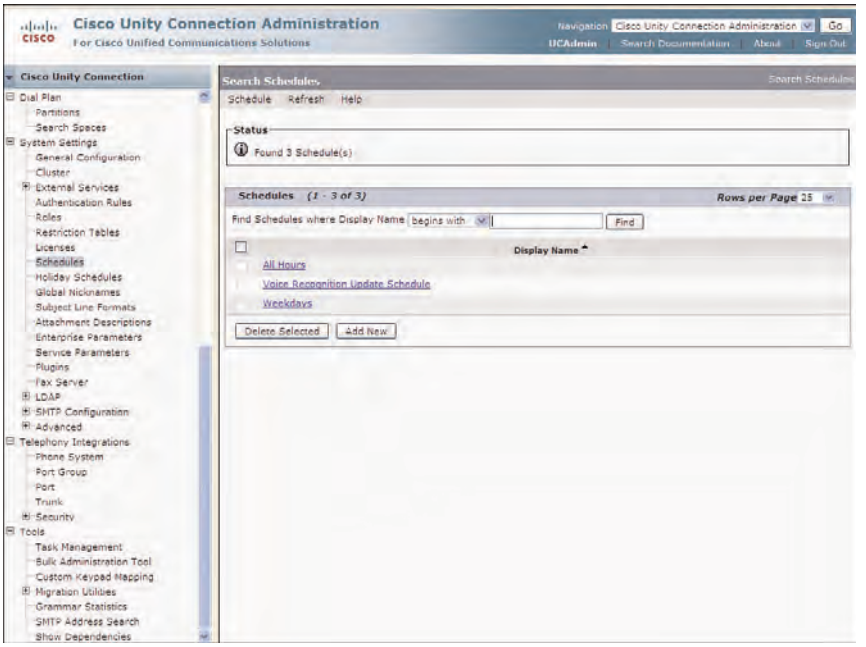

Figure 5-8 *Schedule Configuration in Cisco Unity Connection Administration*

Figure 5-9 *New Schedule Details Configuration*

www.it-ebooks.info

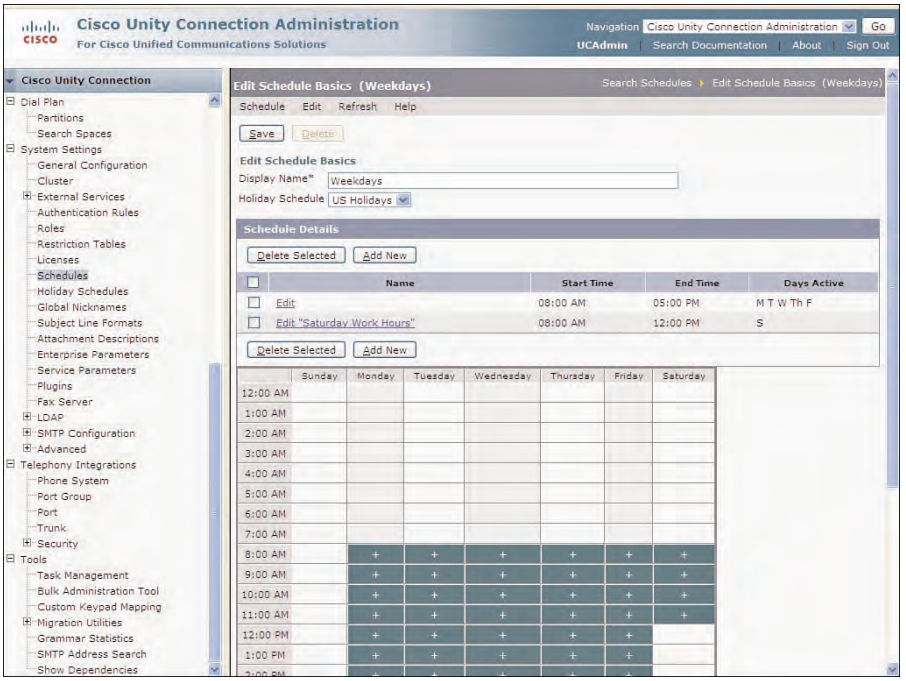

Figure 5-10 *Weekday Schedule Page with Saturday Hours and U.S. Holidays Schedule*

The schedules are applied to users and contacts using templates; however, another element that you must understand before configuring users is the Class of Service.

Class of Service

Class of Service (CoS) applies to users configured with voicemail boxes. The CoS controls user access to specific features and applications. It also controls options such as the message length, call screening capabilities, and whether the user can use an IMAP client and Personal Communications Assistant (PCA) features. By default, there are two classes of service defined during the installation of the software. These are the System and Voice Mail User CoS, where both classes of service cannot be deleted. The System Class of Service cannot be modified and provides a limited set of features. The Voice Mail User CoS is configured purely for a voicemail user with no access to the advanced licensed features. However, this CoS can be modified as needed.

From Cisco Unity Connection Administration, select **Class of Service > Class of Service** from the navigation menu on the left to display the Search Class of Service page. Figure 5-11 illustrates the two default CoSs. From this page, you can select a CoS or the **Add New** button to create a new CoS.

www.it-ebooks.info

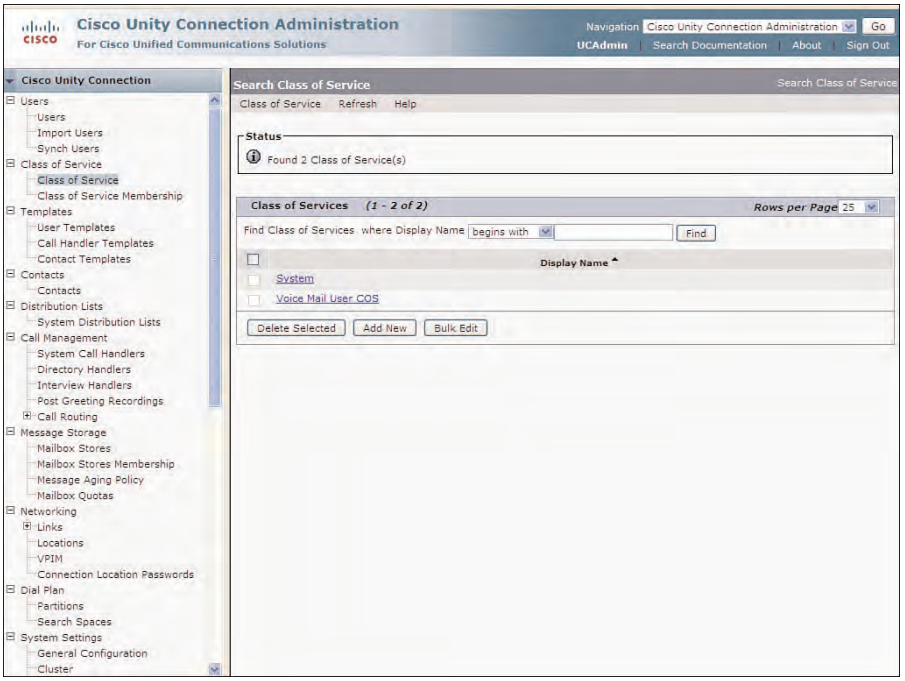

Figure 5-11 *Default CoS Options*

After the **Add New** button is selected, the New Class of Service page displays, as shown in Figure 5-12. Enter a Display Name for the new COS and select the features as required. The options listed in the CoS include the following:

- **Recorded Name:** Enables users to record their name and provide a maximum length. This length applies only to the recorded name, not the greetings.
- **Directory Listing:** Enables the user to be listed in the directory. In most cases, you list users in the directory. However, executive personnel might be configured to make this optional. The user can make changes to this selection in the personal options in his voicemail.
- **Licensed Features:** Controls access to advanced features and the use of IMAP clients, SpeechView, voice recognition, messaging inbox, and RSS feeds.
- **Non-licensed features:** Controls access to Personal Call Transfer Rules and Messaging Assistant.
- **Alternate Extensions:** Enables users to view and manage their alternative extensions.
- **Message Length:** Administratively set the maximum length for messages that callers can leave for the user.
- **Message Options:** Controls the sending, replying, and deleting of messages. Also controls access to the Live Reply feature.

www.it-ebooks.info

- **Private Distribution Lists:** Controls the number of lists and members that can be configured by the user.
- **Call Transfer:** Controls the call screening and holding capabilities for users.
- **Restriction Tables:** Controls the various configured restriction tables that apply to the user.

The various features are explored later in this section. In Figure 5-12, a new CoS called **IM_Exec_COS** was created to provide the least restrictive access to the various features in Cisco Unity Connection for executive users. After all desired options are configured, click **Save** to save the new CoS.

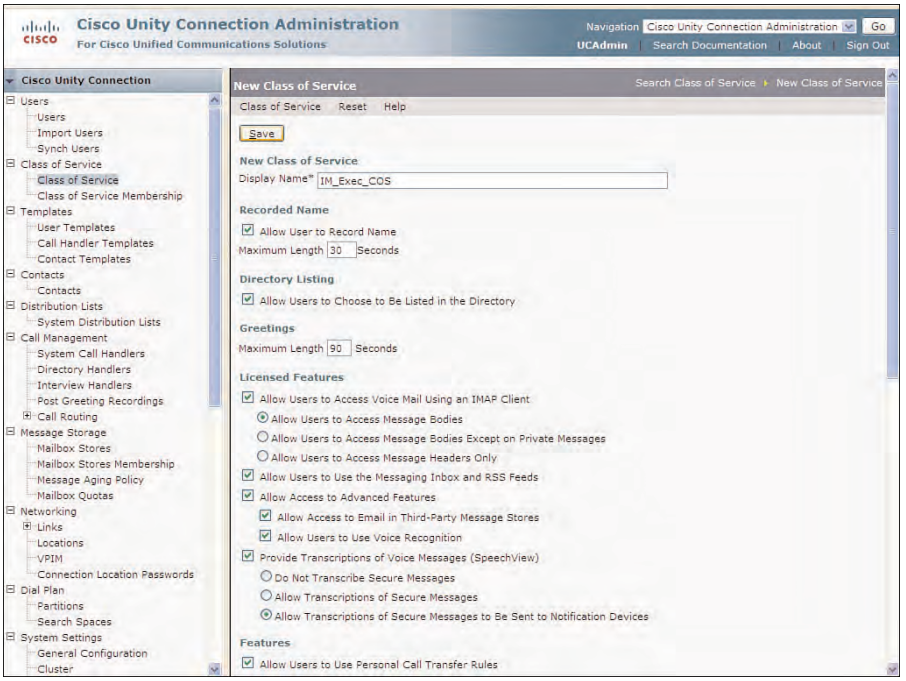

Figure 5-12 *New CoS Created for Executive Users*

All Users with Mailboxes are members of a CoS. This membership is applied at the time the user is created. Administrative users, or User Without Mailboxes, are not members of a CoS.

To view the CoS membership, select **Class of Service > Class of Service Membership** in Cisco Unity Connection Administration. The Search Class of Service Members page appears. The administrator can select each CoS to find user that are either **In**, or **Not In** a specific CoS. This page enables the administrator to move users between the various classes of service by selecting the Move Selected User button near the bottom of the

www.it-ebooks.info

page. The operator and undeliverablemessagesmailbox users are not members of the new IM_Exec_COS Class of Service, as shown in Figure 5-13.

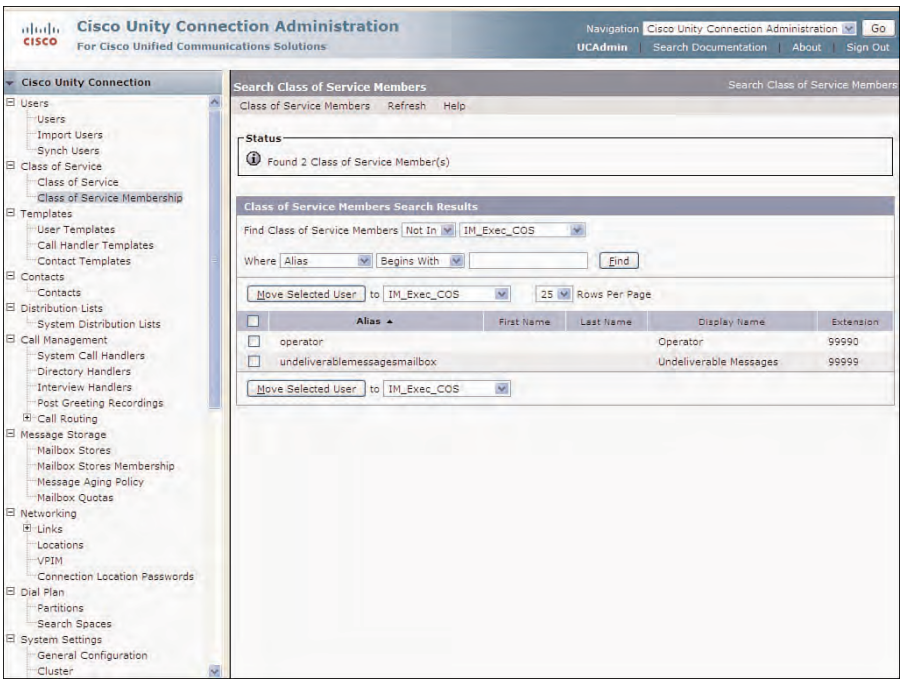

Figure 5-13 *CoS Membership*

Templates

Finally, the last element that must be configured is the template. A template can be viewed as a "cookie cutter" to create an object. There are user templates, contact templates, and call handler templates that exist in Cisco Unity Connection Administration. As a cookie cutter is used to make cookies, so a user template is used to create users. In the case of a user template, you apply a set of configurations to a new user. The user template actually consists of the authentication rules, CoS, schedules, and a number of other configuration options and settings. If you change the template in any way, the past users that were created with this template are not affected. However, new users can adopt all new changes that were made to the template. This is different than the CoS that includes membership, and changes to each CoS are applied to all members.

Two user templates are available by default:

- administratortemplate
- voicemailusertemplate

www.it-ebooks.info

These two templates apply a set of default configuration options. The *administratortemplate* uses only the Recommended Web Application authentication rule. A number of different options are configured for this template, which are used to configure administrators (Users Without Mailboxes) that have the System Administration rights. The *voicemailusertemplate* is used to create Users With Mailboxes and applies authentication rules, a CoS, and various template configurations to a created user.

Most of the configurations not included in the CoS are applied as part of the user template. To view and configure the user template, select **Templates > User Templates** from Cisco Unity Connection Administration. Figure 5-14 shows the Search User Templates page.

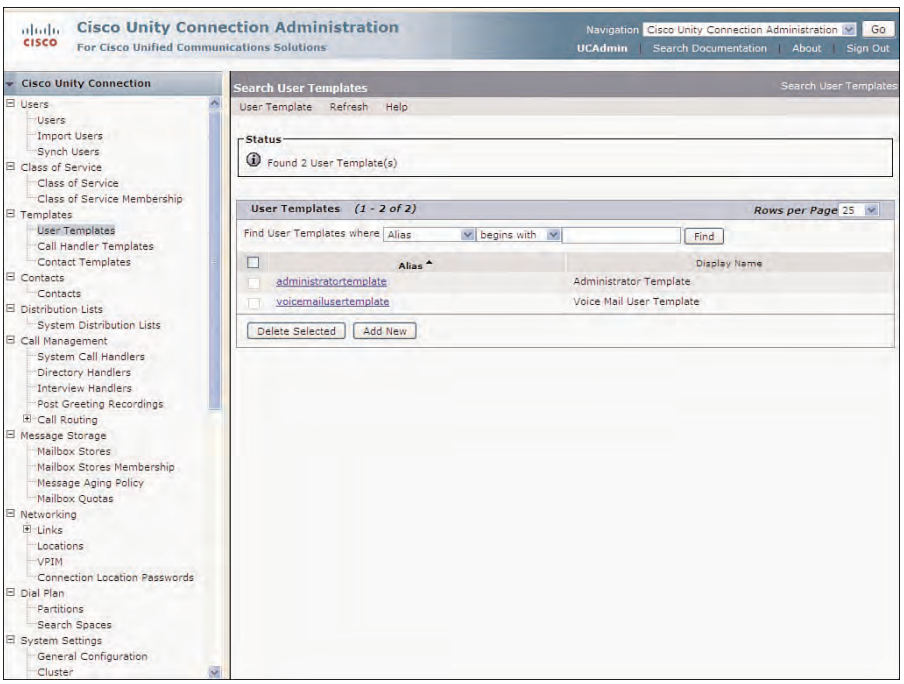

Figure 5-14 *User Templates in Cisco Unity Connection Administration*

Click **Add New** to create new user template. The New User Template page displays, enabling the administrator to create a new template based on an existing template and type, as shown in Figure 5-15. An Alias and Display Name is required. Click **Save** to create the new template. In this case, a new template was created for the executive users based on the voicemailusertemplate.

The Edit User Template Basics displays, enabling the administrator to select the applicable configuration options that apply to the type of template being created (users with or without Mailboxes). Figure 5-16 illustrates the Edit User Template Basics page for the **Exec_Users_Template** to be used to create Users with Mailboxes for the executive team.

www.it-ebooks.info

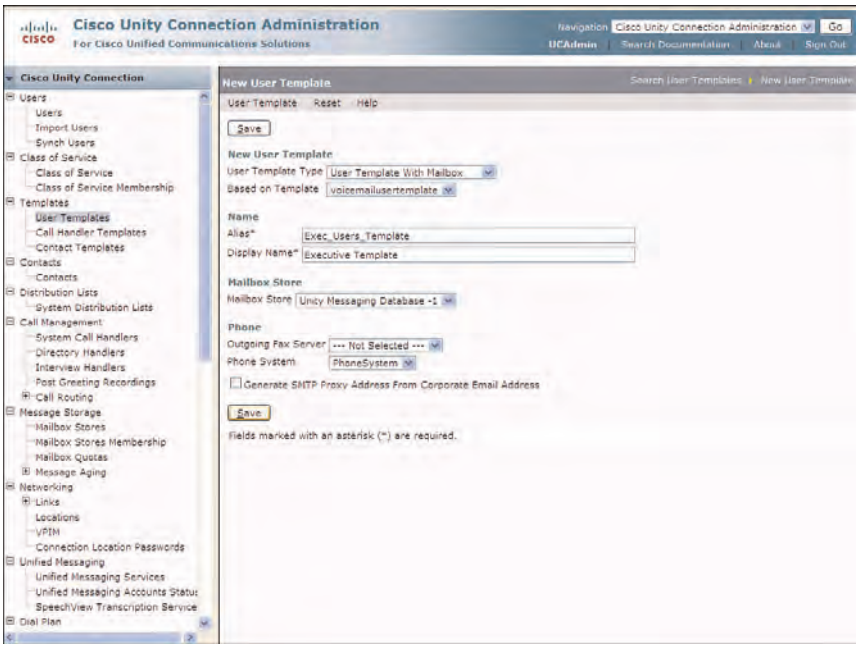

Figure 5-15 *New User Template Configuration*

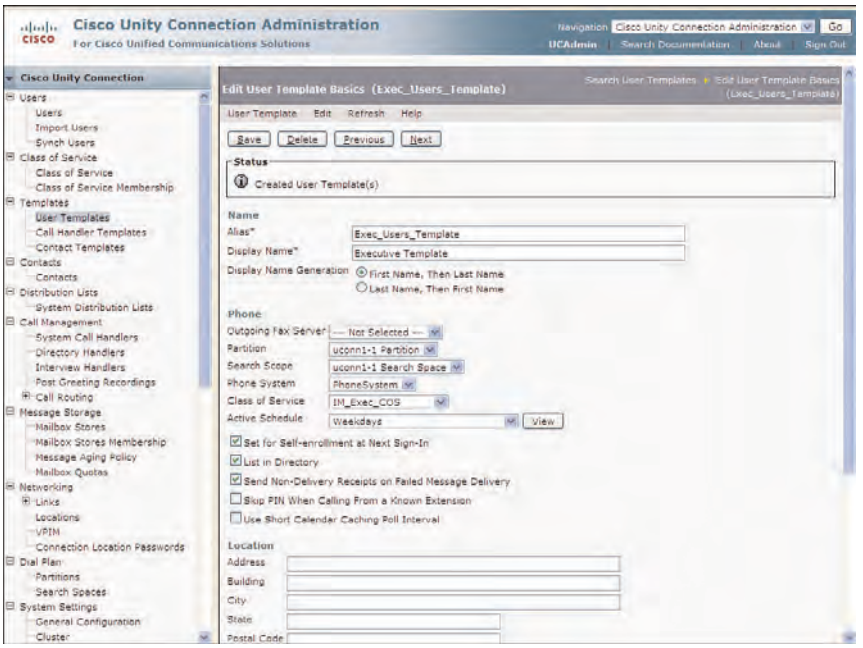

Figure 5-16 *User Template Configuration for Exec_Users_Template*

www.it-ebooks.info

This template configures a schedule and CoS. Also, the users are presented with the self-enrollment at the next sign-in. The self-enrollment procedure enables the users to change their greeting, recorded name, and voicemail password (PIN).

The authentication rules are applied in the password settings. To view or change these changes, select **Edit > Password Settings**, as shown in Figure 5-17. Ensure that the User Must Change at Next Sign-In check box is checked. From this page, the administrator could configure different authentication rules to be used for the user template. Click **Save** if any options were changed.

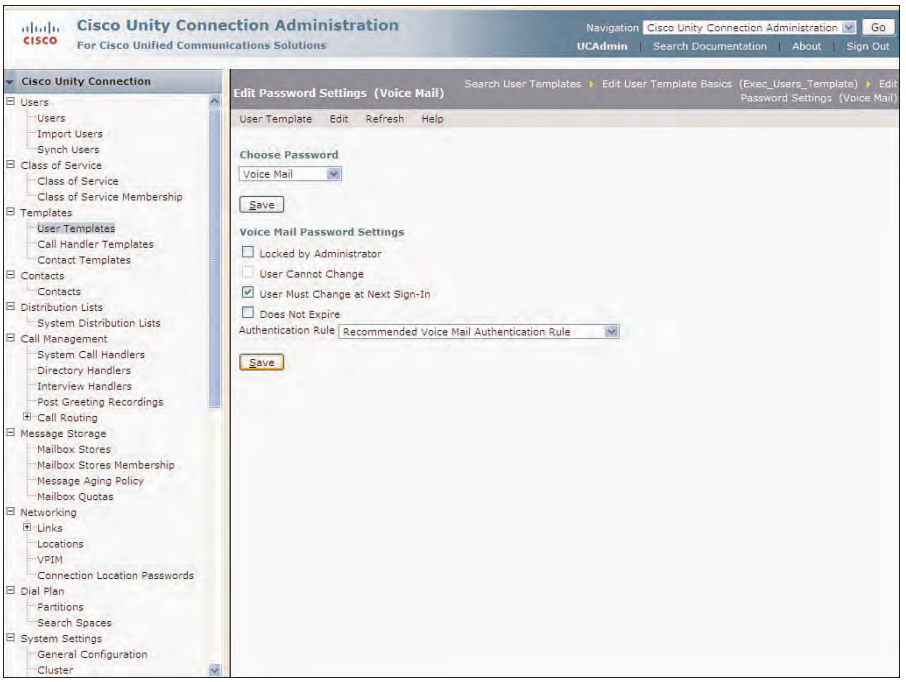

Figure 5-17 *Edit Password Settings Configuration for User Template*

Because this template creates individual and multiple users, you want to configure the password to a setting that is easy to remember and force the users to change it when they sign in the first time and complete the self-enrollment procedure.

To change the password that will be used for this template, select **Edit > Change Password** from the toolbar. The Change Password page appears, as shown in Figure 5-18. This screen enables the administrator to change the voicemail (PIN) or Web Application password by selecting the correct option from the Choose Password drop-down. The PIN is numeric because it will be entered from the telephone user interface (TUI). However, the web application password will be alphanumeric, because this password will be used to log in to all web interfaces and client applications. Enter the applicable password and confirm it.

www.it-ebooks.info

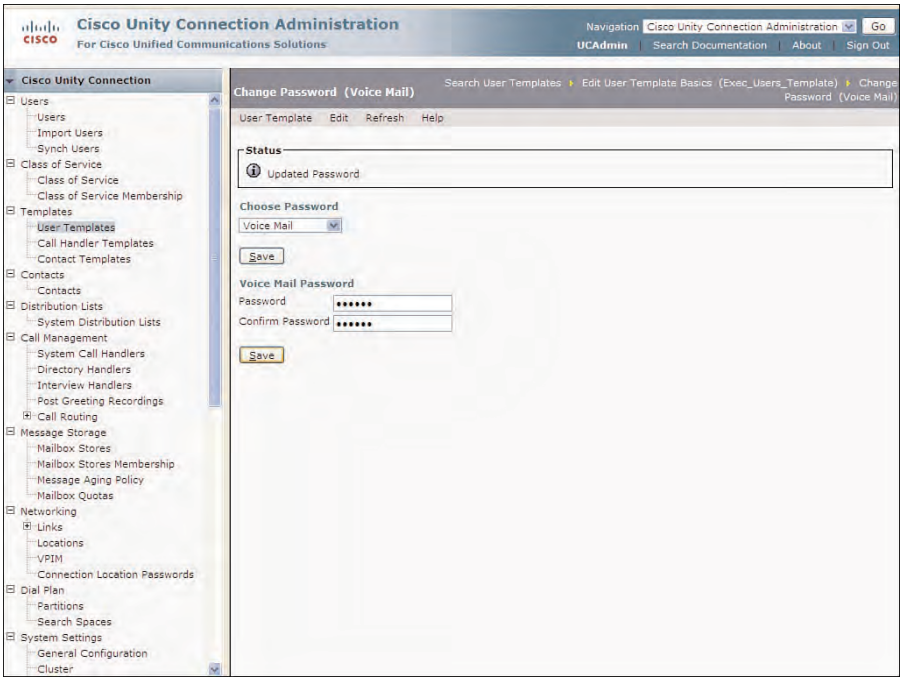

Figure 5-18 *Change Password Configuration for Users With Mailboxes*

All passwords are subject to the authentication rules. Click **Save** to commit the changes to the database. Now, when new users are created using this template, they have the same password but will be forced to change it at the time of enrollment.

Configuring Users

You have configured the authentication rules, schedules, CoS, and user templates, which are all the required elements needed to configure users. Therefore, you are prepared to configure both users and administrators. As mentioned previously, the default application administrator account is used to perform the initial configurations in Cisco Unity Connection Administration. After the initial configuration, this account should be kept secretive. It is strongly suggested that you create additional backup administrators with the assigned role of System Administrator, in the event that the original application administrator account is accidentally deleted.

These additional administrator accounts can be created as users without mailboxes use the administrator template. Most administrators are also voicemail users; therefore, you can create voicemail user accounts for each administrator of the voice-messaging system. Then, apply the System Administrator role to each user account that will have administrator privileges. Whichever procedure is used to configure additional administrators, each administrator should have his own account. This ensures that security and integrity is maintained when an employee with administrator privileges leaves the organization.

www.it-ebooks.info

Configuring Users Without Mailboxes

To configure a backup administrator account that does not have a mailbox, select **Users > Users** from Cisco Unity Connection Administration. Select the **Add New** button from the Search Users page. The New User page now appears.

Select **User Without Mailbox** from the User Type drop-down. The Based on Template automatically changes to **administratortemplate** because this is currently the only configured user template configured for a user without mailbox. Only the applicable templates are displayed according to the user type selected. For the Name section, enter the applicable Alias, First Name, Last Name. The Display Name automatically completes with the first and last, as shown in Figure 5-19. In the example, a new Backup Administrator account is configured using the alias, **buadmin**.

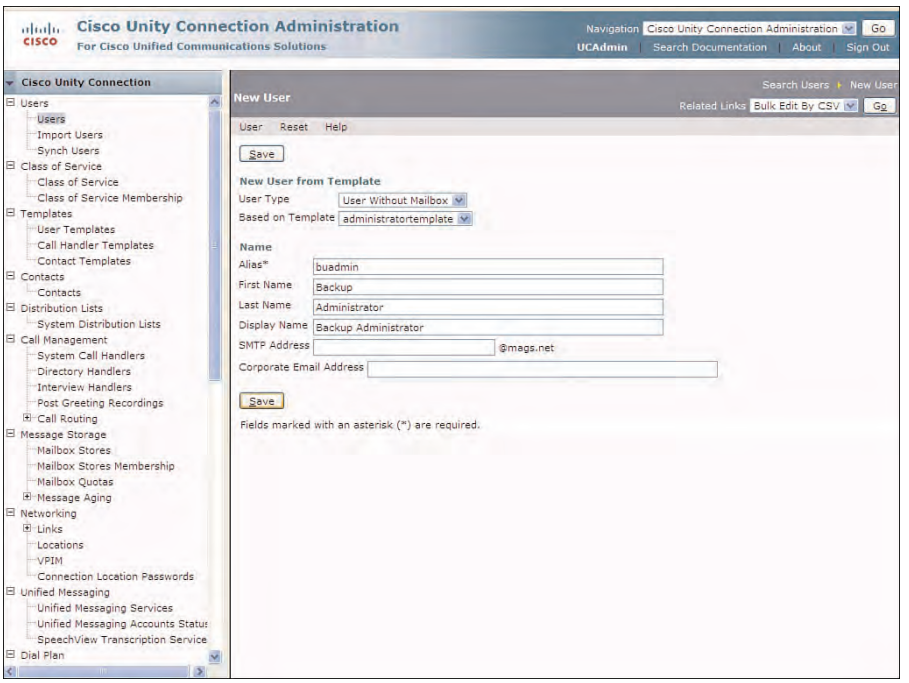

Figure 5-19 *Configuration for a User Without Mailbox*

After you click **Save**, the Edit User Basics page displays, enabling you to enter additional information that pertains to the location, time zone, and various departmental information. This information is purely information and can be used for accounting and keep track of the current users' location. If you enter or change any of the listed information on this page, click **Save** to write all changes to the database. The alias must be unique with a Cisco Unity Connection server or cluster pair.

The Backup Administrator account can now sign in as the System Administrator; however, the current password is applied through the configurations of the administrator

www.it-ebooks.info

template. Therefore, it is advisable to change the password for security purposes and keep this account secretive. In this case, the Backup Administrator account is used only if there is an issue with the original application administrator account.

To change this password, select **Edit > Change Password** from the toolbar. The Change Password (Web Application) page appears. This is the only option for this user. Because you configured a user without a mailbox, this user will have no configurable voicemail password.

In the Web Application Password section, enter the new password and confirm it, as shown in Figure 5-20. Select the **Save** button to commit the changes to the database.

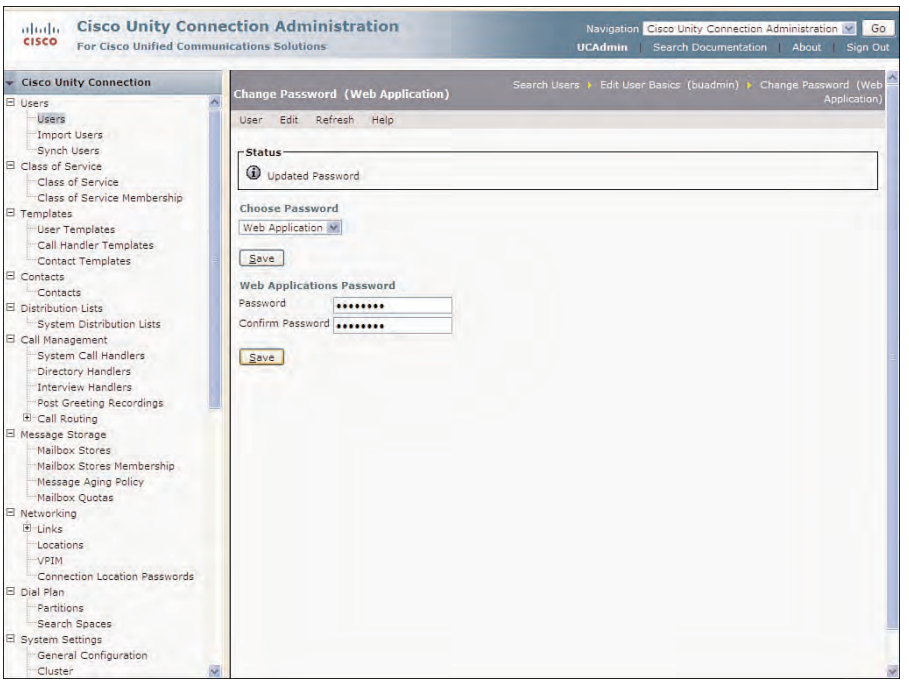

Figure 5-20 *Change Password Configuration*

The password entered must match the Web Application Rules selected for this user. Again, the authentication rules configured for a user can be viewed or changed by selecting **Edit > Password Settings**, as shown in Figure 5-21. To apply a different authentication rule for this user, select it from the Authentication Rule drop-down. If any modifications are made to this page, click **Save**.

www.it-ebooks.info

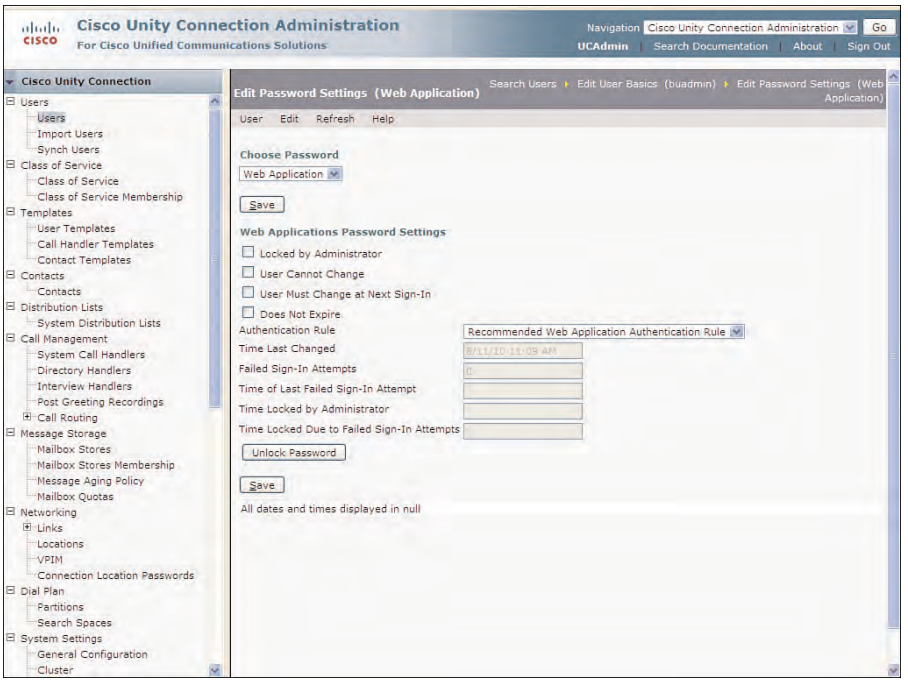

Figure 5-21 *Edit Password Settings Configuration Options for the Backup Administrator*

Configuring Users With Mailboxes

In most cases, you configure users with mailboxes. These users have the ability to send, receive, and forward messages to other users by phone. These users can also be given access to other options by their CoS. Some of these users might also be administrators of the Cisco Unity Connection messaging system. For these administrative users, they also need additional access to the various web pages available in Cisco Unity Connection Administration. This can be accomplished by assigning these users to the specific roles. In this section, you configure users with mailboxes that have administrative responsibilities in the voice-messaging system and therefore require access to these features.

You begin creating users with mailbox in the same way that you created the administrator accounts, by selecting **Users > Users** from Cisco Unity Connection Administration. Click **Add New** to display the New User page, as shown in Figure 5-22.

From the New User page, select **User With Mailbox** from the User Type drop-down. The Based on Template drop-down automatically changes to display the available user templates that are created based on users that can be configured with voicemail. The **administratortemplate** and any other templates that were created for users without a mailbox are not visible in the drop-down. In this example, you create a new executive user and base their creation on the features selected in the **Exec_User_Template**.

www.it-ebooks.info

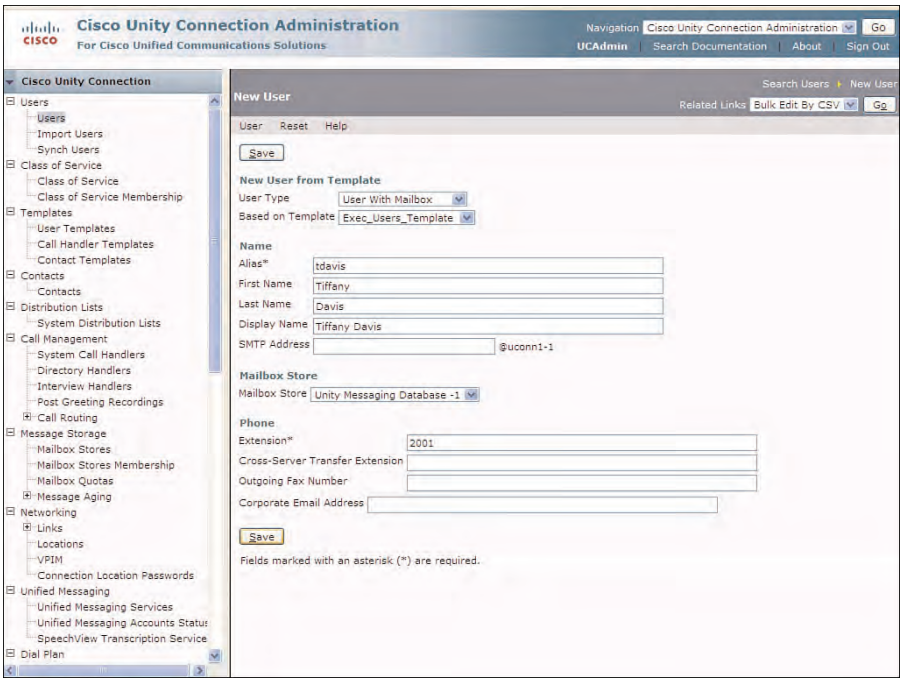

Figure 5-22 *New User With Mailbox Configuration*

Select the alias for this user. The alias is usually based on the first and last name of the user but can be any naming convention, as long as it is unique to other users. For example, a user with Tiffany Davis can be provided with any of these aliases:

- tdavis
- tiffany.davis
- tdavis123
- ti_davis
- Tiffany Davis

The alias chosen here will be used by the user to log in to the various web applications, such as Personal Communications Assistant, or Cisco Unity Connection Administration, if the user is a designated administrator of the system.

Enter the first name, last name, and display name of the user. These fields are not required; however, if they are not entered, voice recognition users cannot address messages or call this user by name. Additionally, you could select an alternative name for this purpose. The first and last name fields are used specifically for addressing messages to this user by name from the directories (spelling by name). The display name is used by voice recognition to play display name if the user has no recorded name. This option field

www.it-ebooks.info

enables the administrator to enter names phonetically to allow voice recognition responses to be correctly spoken.

The Simple Mail Transfer Protocol (SMTP) address is an optional field that is used by an SMTP client that is configured to receive the voicemail. SMTP is also used to send voice messages between Cisco Unity Connection locations and other messaging systems using Voice Profile for Internet Mail (VPIM).

The Extension field is required and should be configured with the users' main phone extension they use to access Cisco Unity Connection. This enables the user to be recognized as a user when they connect to Cisco Unity Connection using their phone. Click **Save** to complete the configuration.

In this case, the user, Tiffany Davis is presented with the Sign-In conversation when accessing voicemail from her phone with extension **2001**. It is not required that users have a physical phone on the system. There might be instances where you need remote users to have a voicemail on the system, even though they might not have a phone. This might be the case for remote or off-site personnel.

After clicking **Save**, the user is created with the chosen user template. The Edit User Basics page for this new user displays, as shown in Figure 5-23. The Active Schedule and Class of Service can be viewed and modified for this user from this page. The other various fields can be entered as required. Many of the options and features are discussed later in this section.

In most cases, the newly created user will be set for self-enrollment as discussed previously. The main difference on the authentication for users with mailboxes is that they have a voicemail password, unlike the administrative users without mailboxes. The currently set passwords cannot be viewed (for security purposes). However, the administrator can change or reset the current settings from the **Edit > Change Password** page. Select the **Voice Mail** option from the Choose Password drop-down. Enter the new password, confirm it, and click **Save**. Again, all passwords entered here are subject to the authentication rules, which were previously discussed.

This configured user can now use their voicemail. When they access the system the first time, they will be presented with the various options to set up their mailbox, as discussed previously. However, this user has no administrative rights. To provide administrative privileges, you need to assign this user to a specific role for this function. Therefore, the assignment of roles is the next task.

Roles

Users with voicemail have access to voice messaging, providing them with the ability to send, receive, and forward messages to other users. They cannot however access Cisco Unity Connection Administration to create mailboxes, users, and so forth until they are assigned to the proper role.

www.it-ebooks.info

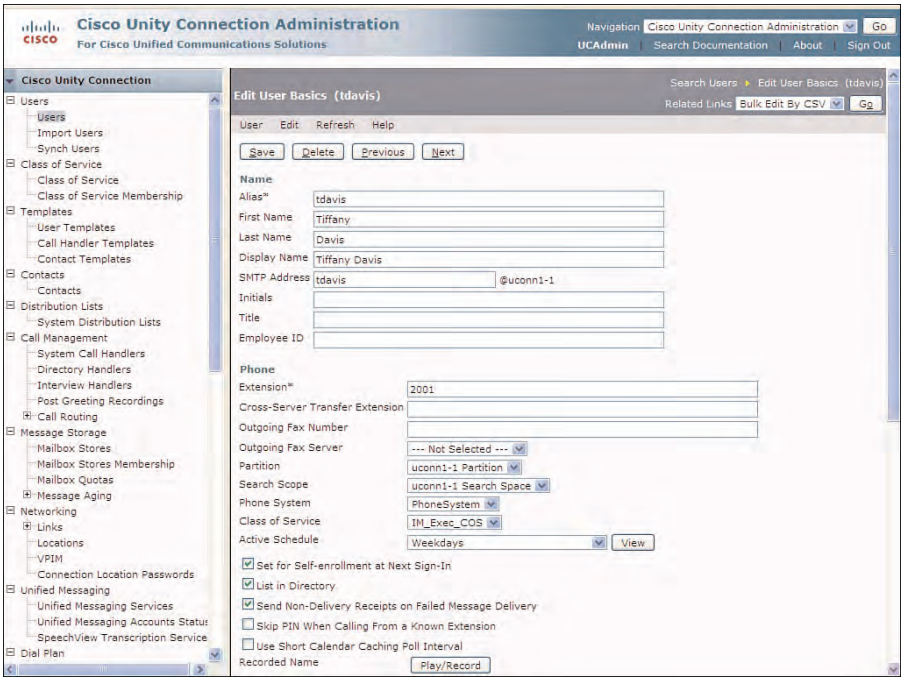

Figure 5-23 *Edit User Basics Page in Cisco Unity Connection Administration*

A number of predefined roles in Cisco Unity Connection provides users with various privileges. The following roles are created at the time of installation and cannot be changed, deleted, or modified:

- **Greetings Administrator:** Enables users to manage the greeting of call handlers. Call handlers that have assigned extensions can be managed by all greeting administrators. However, call handlers without extensions can be managed only by greeting administrators assigned as call handler owners for that specific call handler. The Greeting Administrator can manage only these greetings by phone; therefore, this role can be assigned only to users with a mailbox.
- **Help Desk Administrator:** Enables these users to manage user accounts. These administrators can reset passwords and PINs and unlock the account after an authentication rule has caused the account to be locked.
- **Mailbox Access Delegate Account:** An application user that has access to all voice messages. For example, Cisco Unified Mobility Advantage would use this user account to provide access to all voice messaging.
- **Remote Administrator:** This role is assigned to an administrator account for using any remote database tools, such as Cisco Object Backup and Restore Application Suite (COBRAS). The remote access must be enabled through Cisco Unity

www.it-ebooks.info

Connection Administration. For security purposes, Cisco Unity Connection Administration, includes a shutdown timer that automatically stops remote administration after a set number of days. Therefore, this shutdown timer must be enabled by selecting **System Settings > Advanced > Connection Administration** and entering the required number of days in the Database Proxy: Service Shutdown Timer field (0 = disabled).

- **System Administrator:** This role provides access to Cisco Unity Connection Administration and Serviceability. This is the highest level of administrative access, which is the same role assigned to the application administrator authentication.
- **Technician:** This role enables access to all platform-related functions, reports, and tools. This role does not provide access to user management features.
- **User Management:** This role provides access to all user management features, reports, and tools. This role does not provide access to platform-related functions.

Users with or without mailbox can be assigned to multiple roles as required (depending on the user type). Some roles can be assigned to users with or without mailboxes, whereas some roles can be assigned only to users with mailboxes. This would be the case as in the Greeting Administrator because this role can be assigned only to a user with a mailbox.

To assign a user with a mailbox to a role, begin by selecting **Users > Users** from Cisco Unity Connection Administration. The Search Users page displays. Then, select the desired user from the Search Users page. From the Edit User Basics page, select **Edit > Roles** from the toolbar. Figure 5-24 shows the Edit Roles page.

Select the desired role from the Available Roles pane, and select the Up Arrow to move the role to the Assigned Roles pane. One or more roles can be assigned to a user. Click **Save** to apply the role to the user. In this example, the user, tdavis, has been assigned to the System Administrator role, providing this user with the same access as the application administration password that was created at the time of installation. Depending on the security level required in organization, it might be advisable to use a separate account for administration and users voicemail, although this is not a requirement.

You have now learned how to create individual user accounts and assign roles to these accounts as needed. In the next section, you discover how multiple users can be created through the Bulk Administration Tool (BAT), AXL, and Lightweight Directory Access Protocol (LDAP) integration.

Bulk Administration Tool

Using a comma-separated variable (CSV) file, the BAT in Cisco Unity Connection Administration affords the administrator with the ability to export, create, update, and delete multiple users and contacts in a single operation. This ability greatly minimizes the time required to complete these administrative tasks and maximizes the efficiency of the installation and administrative teams.

www.it-ebooks.info

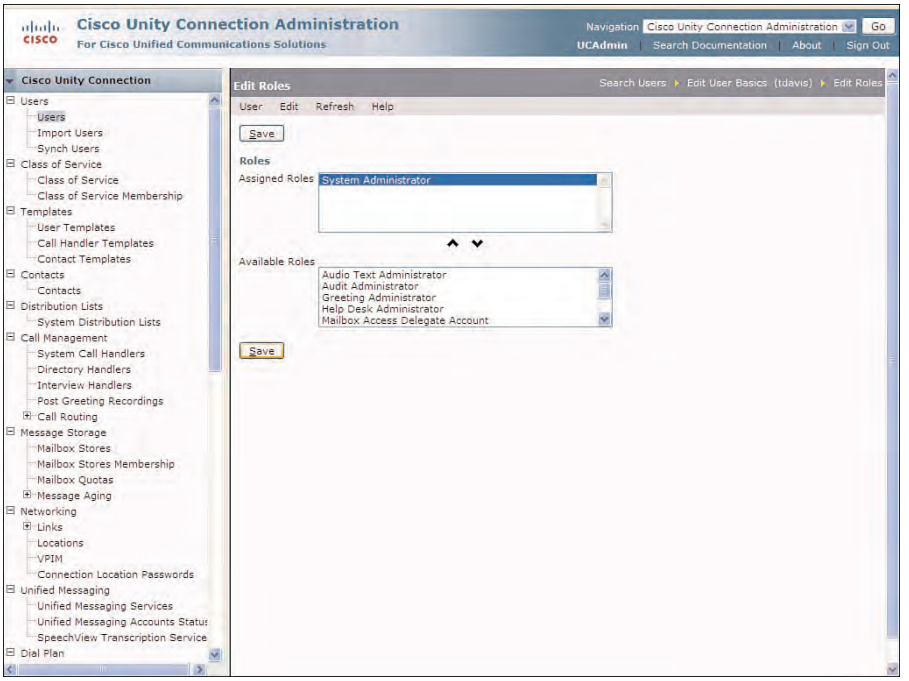

Figure 5-24 *Edit Roles Page in Cisco Unity Connection Administration*

BAT enables the administrator to export the current users and administrator using a CSV file. This is helpful to organizations in documenting their current user configurations. The exported CSV file can then be used for post-processing with an external reports program to catalog or document these same user configurations. The exported CSV can be used by the administrator to create new users, and update and delete multiple users in Cisco Unity Connection.

The Bulk Edit feature can also be used to updates users and contacts that have already been configured. You explore the Bulk Edit options later in this section.

To access the Bulk Administration Tool, select **Tools > Bulk Administration Tool** in Cisco Unity Connection Administration. The Bulk Administration page displays enabling the administrator to select the specific operation, which is to create, update, delete, or export.

Export Operation

You first need to download the CSV with the current user information. Therefore, select the **Export** radio button for Select Operation, as displayed in Figure 5-25.

Under the Select Object Type section, select the radio button that applies to the specific users or contacts to export. The valid types are Users (Users without Mailboxes), Users

www.it-ebooks.info

with Mailboxes, and System Contacts. The current release of Cisco Unity Connection version 8.5 also provides options for Distribution Lists, Distribution List Members, and Unified Messaging Accounts. Because you will be creating multiple users with mailboxes, select the **Users with Mailbox** radio button.

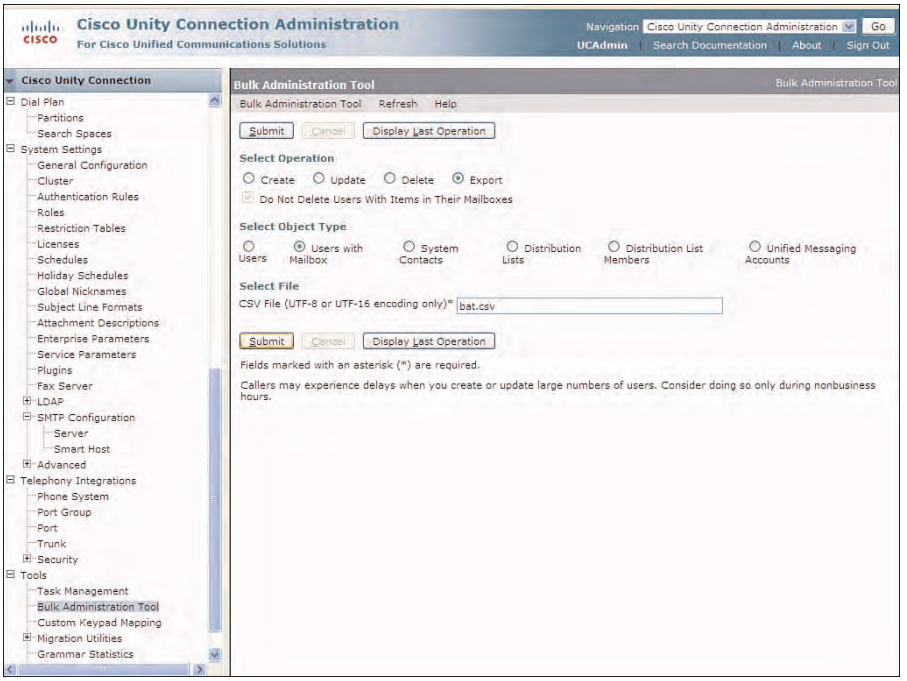

Figure 5-25 *Export Options Using the Bulk Administration Tool*

Finally, enter a descriptive name for the file, ensuring the extension is **.csv** and click **Submit**. In this example, **bat.csv** was selected.

As the BAT job is processed, the Status section at the top of the page displays the successes and failures in real-time, as shown in Figure 5-26. When this process finishes, a link displays enabling the administrator to download the file. Select the link and choose to save the file to your workstation.

After the CSV file has been downloaded, it can be used to create, update, or delete users. Select the downloaded CSV to open the file on your workstation. Using Microsoft Excel simplifies the editing process, by formatting all data in specific rows and column. Figure 5-27 illustrates the downloaded export file. When the file is complete, it must be saved and uploaded as a CSV file.

www.it-ebooks.info

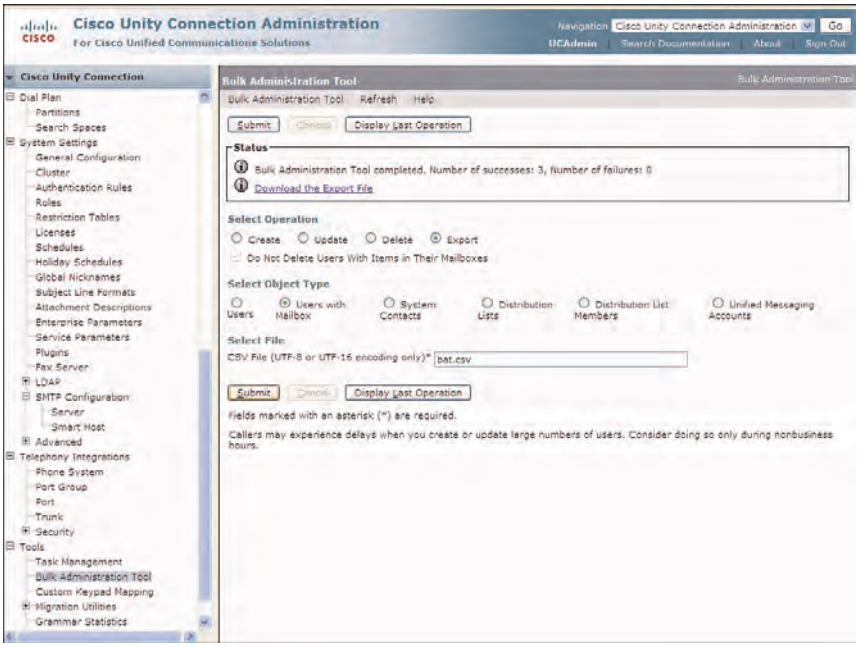

Figure 5-26 *Export Procedure in Bulk Administration Tool*

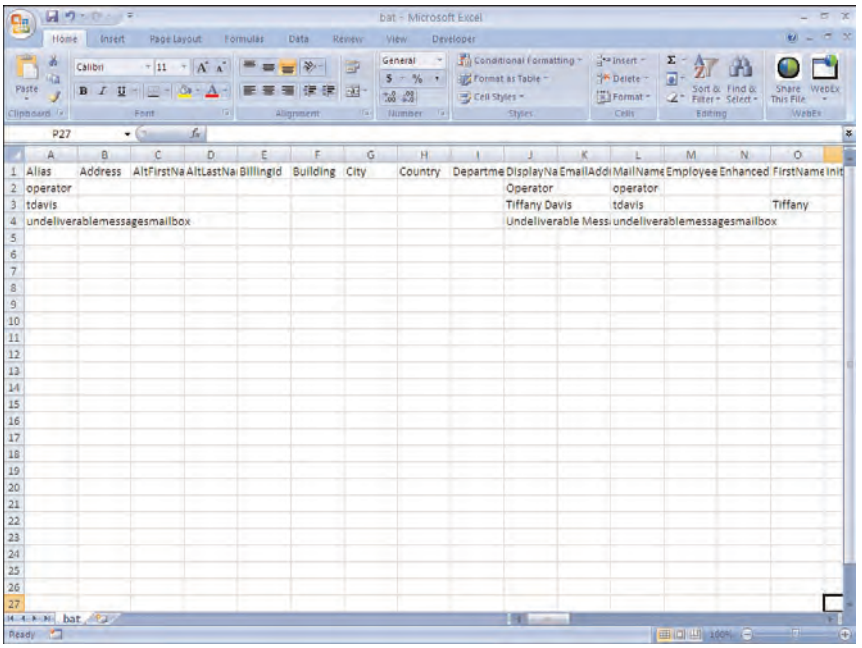

Figure 5-27 *Downloaded Export File Using the Bulk Administration Tool*

www.it-ebooks.info

Create Operation

After you open the CSV file, highlight all rows that include users, and click **Delete**, leaving the first row with the headings intact. You now need to add the list of users that you want to configure with mailboxes to the CSV file. The Alias and Extension fields are required to create a user with the mailbox. You have the option to enter all information using the CSV file or use existing user template information to perform this function. After all information is entered into the CSV file, you need to save the file on your workstation as a CSV file.

Then, return to the Bulk Administration Tool page in Cisco Unity Connection. Select the **Create** radio button from the Select Operation section, as displayed in Figure 5-28. Select the User with Mailbox radio button for the Object Type. If you want to use a user template to configure the various user options, select the **Yes** radio button to use a user template for the Override CSV Fields When Creating User Accounts section, and select the specific template from the drop-down. In this example, four new users are created from the CSV file based on the **voicemailusertemplate**.

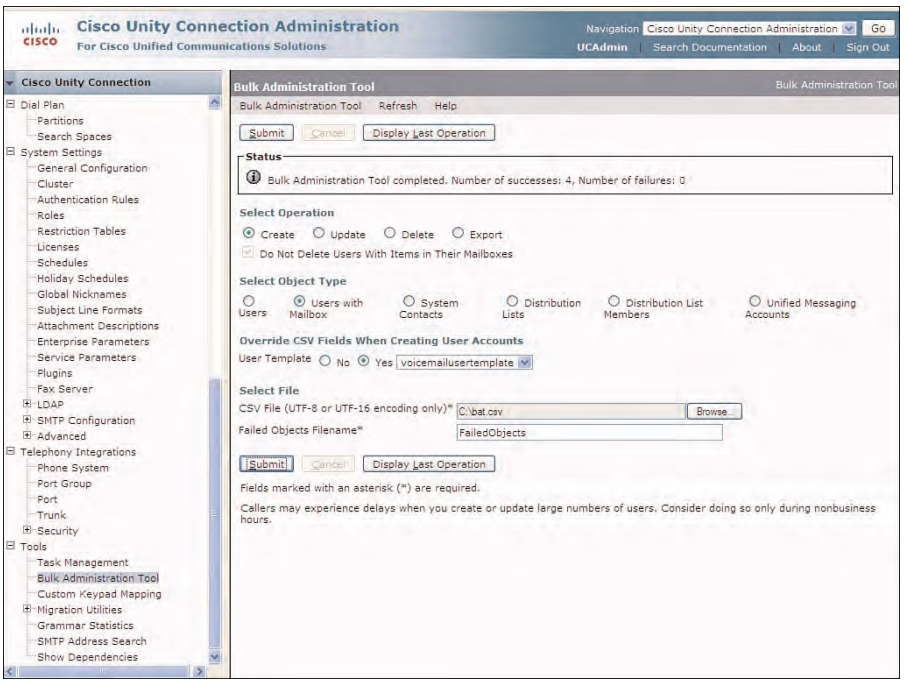

Figure 5-28 *Create Users Using Bulk Administration Tool*

Finally, click **Browse** and select the specific CSV file that you saved with the users to be created in Cisco Unity Connection. Enter a name for the Failed Objects Filename. If there is an error with the user creation, Cisco Unity Connection indicates the specific errors within this text file. This filename is required to complete the BAT operation, which will

www.it-ebooks.info

be used to log errors that occurred during the create operation. After all the options are selected, click **Submit** to create the new users. Review the Status section at the top of the page to ensure that all the success numbers equal the number of users created and that there are no failures. If an error occurred, the status displays a link enabling the user to download the failed objects file. In this example, four users were successfully created as indicated in the Status section of the Bulk Administration Tool.

Update Operation

After the users are created using the Bulk Administration Tool, the same CSV can then be used to modify these users by editing the file and saving again using the same CSV format. Then, select the **Update** radio button from the Select Operation section in the Bulk Administration Tool, as displayed in Figure 5-29.

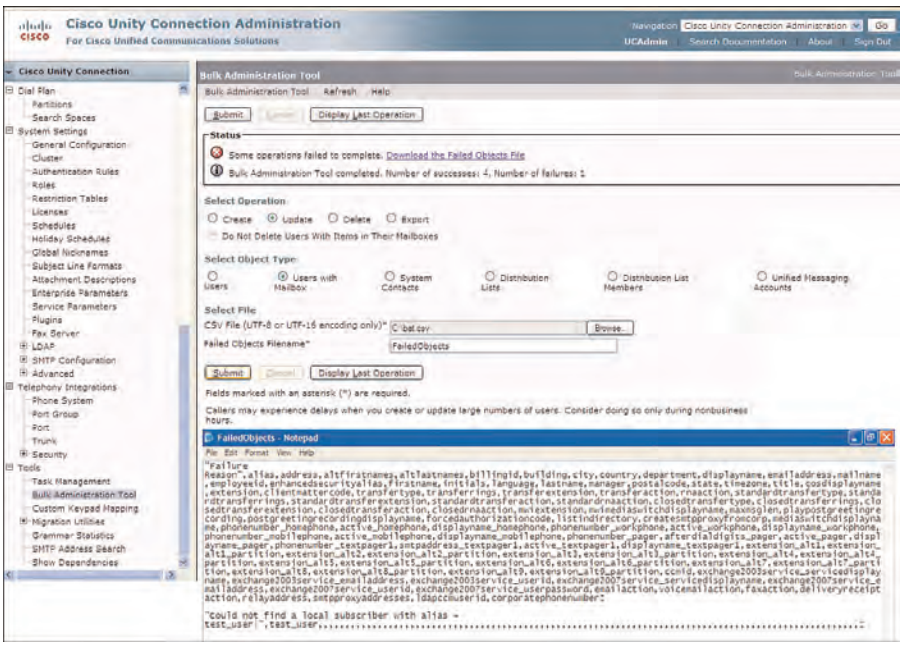

Figure 5-29 *Update User in Bulk Administration Tool*

Select the User with Mailbox radio button for the Object Type. Click **Browse** and select the specific CSV file that you saved with the users to be updated. Enter a name for the Failed Objects Filename as before. After you click **Submit**, all users entered in the CSV file will be updated in Cisco Unity Connection. This is an update operation, meaning the users must already exist in Cisco Unity Connection. In this case, you have attempted to update a user, **test_user**, that was never created. If you attempt to update a user that does not exist in the database, an error occurs and the failed object file contains the following error:

```
Could not find a local subscriber with alias = test_user
```

www.it-ebooks.info

Verification

Verify the users that were created using the Bulk Administration Tool by selecting **Users > Users** in Cisco Unity Connection Administration. The new users display on the Search Users page, as shown in Figure 5-30.

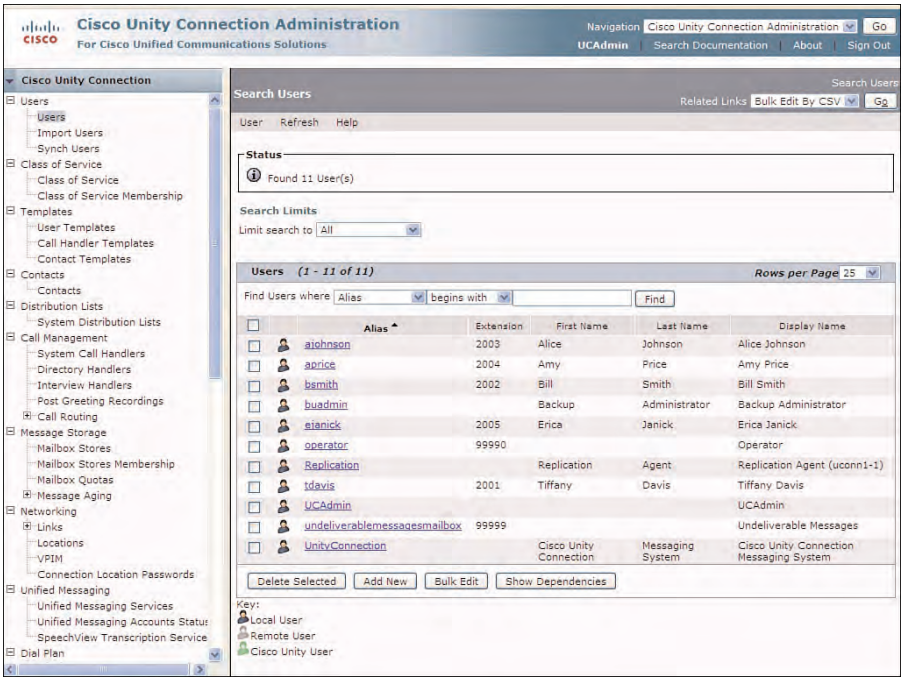

Figure 5-30 *New Users Created with the Bulk Administration Tool*

Bulk Edit

The Bulk Edit facility also affords the ability to modify the configuration of existing users. This feature has been moved and expanded in Cisco Unity Connection v8.x software, sp you can now edit users, contacts, system call handlers, classes of service, and the various templates.

The Bulk Edit is now accessed through the different pages for where the objects are configured. For example, to edit multiple users using the Bulk Edit feature in the Search Users page, select the user(s) to be edited by clicking the check box to the left of the user(s). Then, click **Bulk Edit** near the bottom of the Search Users page, as shown in Figure 5-31.

www.it-ebooks.info

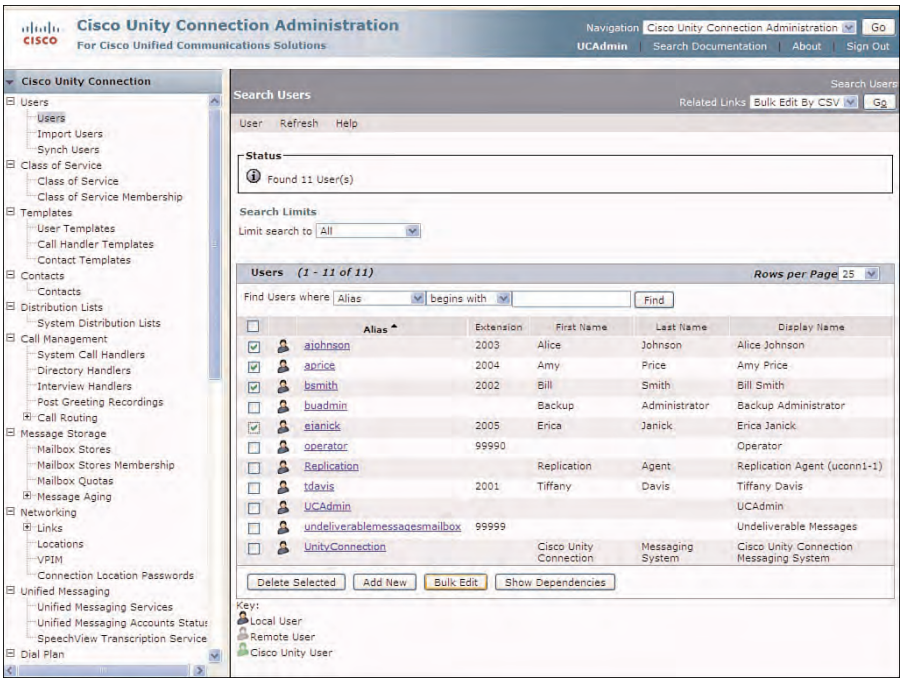

Figure 5-31 *Using the Bulk Edit Feature in Cisco Unity Connection Administration*

After you select the Bulk Edit option, you the Edit User Basics page appears, as shown in Figure 5-32. Check the box to the left of all options that you want to change, followed by the specific configuration options. For the other available user options, select **Edit** from the toolbar followed by the specific feature to be edited. After you make selections, click **Submit** to apply the changes. In this example, the CoS and active schedule are changed for the four users that were created with the Bulk Administration Tool. This operation could also be completed with the Update feature in the Bulk Administration Tool.

LDAP Synchronization and Authentication

Another method for adding multiple users in Cisco Unity Connection is by Lightweight Directory Access Protocol (LDAP) integration. This is the most popular method to add multiple users because most organizations already have a single directory of users, such as Microsoft Active Directory. This user information can be imported and synchronized with the user database in Cisco Unity Connection. Therefore, all user information can be managed directly on Active Directory and synchronized with Cisco Unity Connection. In this way, administrators have a centralized location to configure users' information. LDAP authentication can also be configured along with LDAP synchronization, enabling all web application traffic to use Active Directory for authentication, rather than the local Cisco Unity Connection database.

www.it-ebooks.info

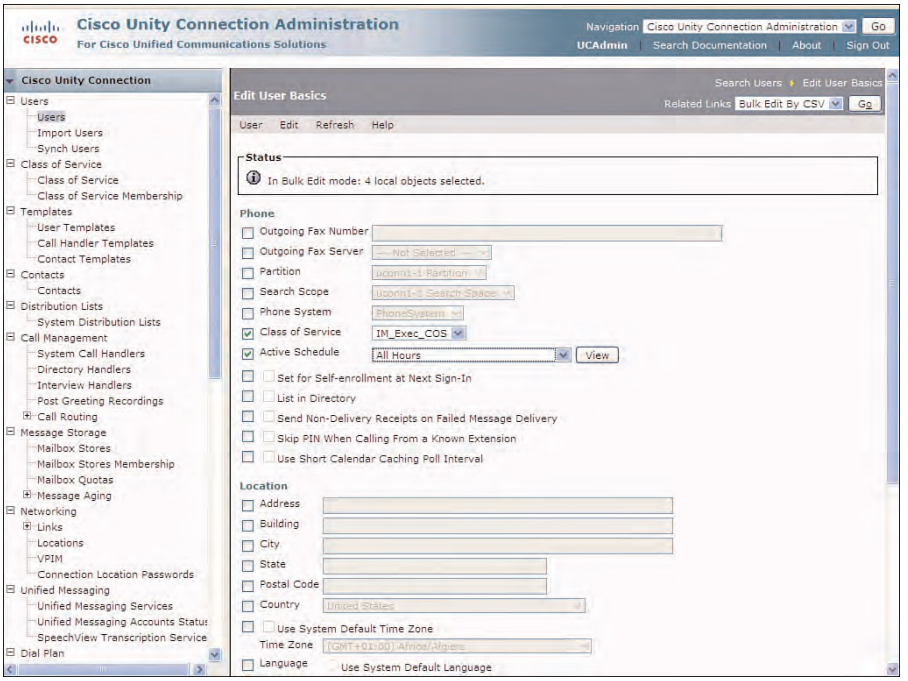

Figure 5-32 *Modifying Users Using Bulk Edit*

LDAP synchronization can be used without LDAP authentication; however, if you decide to use LDAP authentication, LDAP synchronization is required. Using both LDAP synchronization and authentication affords an organization with the capability to administer all usernames and passwords using its corporate LDAP directory.

LDAP synchronization is a six-step process:

Step 1. Configure the Administrator Account in LDAP.

Step 2. Enable the Cisco DirSync service in Cisco Unity Connection.

Step 3. Enable LDAP Synchronization on Cisco Unity Connection.

Step 4. Configure the proper synchronization agreements.

Step 5. Perform synchronization.

Step 6. Import users.

Depending on the type of LDAP server, you need to configure a user that has Domain Admin rights on the LDAP server. This will be the user used by Cisco Unity Connection to authenticate and perform the synchronization. Therefore, this user must be a member of the Domain Users Group, as shown in Figure 5-33 for the domain controller.

www.it-ebooks.info

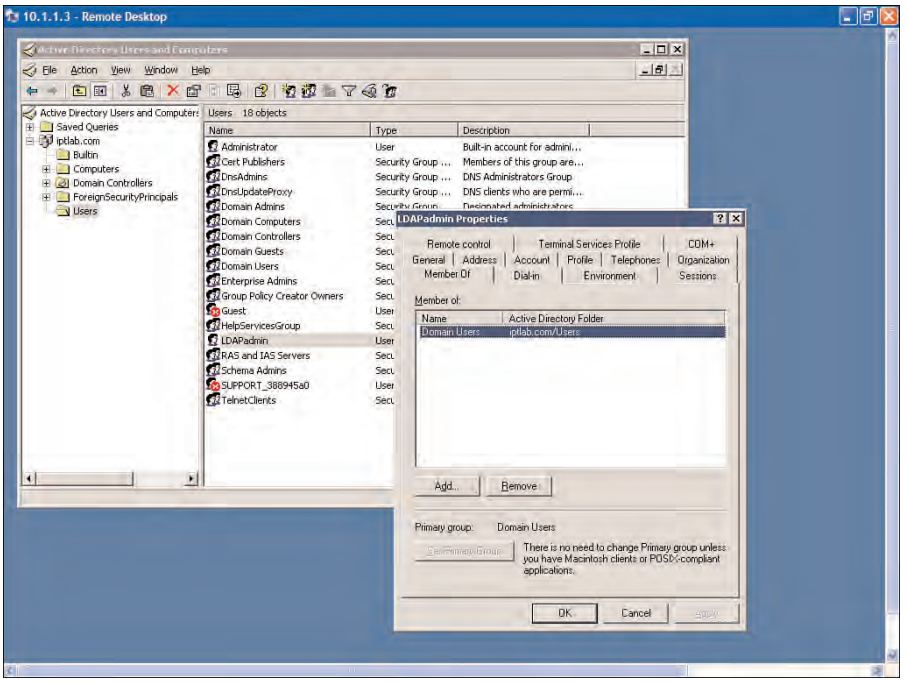

Figure 5-33 *Domain User Configured in Microsoft Directory*

Activate Cisco DirSync Service

The next steps are to configure the LDAP synchronization on Cisco Unity Connection. LDAP synchronization requires the Cisco DirSync service to be activated in Cisco Unity Connection. To complete this step, from the navigation drop-down on Cisco Unity Connection Administration, select **Cisco Unified Serviceability**, and click **Go**. Additionally, you could enter the link **https://***ip_address_CUC***/ccmservice**.

From the Cisco Unified Serviceability page, from the toolbar, select **Tools > Service Activation**. Figure 5-34 shows the Service Activation page.

On the Service Activation page, check the **Cisco DirSync** check box and click **Save**. The service might take a few seconds to activate. When the activation completes, ensure that the page displays Activated in the Activation Status column for the Cisco DirSync service.

LDAP Setup

Return to Cisco Unity Connection Administration by selecting **Cisco Unity Connection Administration** from the Navigation drop-down and clicking **Go**. Select **System Settings > LDAP > LDAP Setup** to display the LDAP Setup page. Check the **Enable Synchronizing from an LDAP Server** check box, as shown in Figure 5-35. Select **Microsoft Active Directory** for the LDAP Server Type. Other options available here are Netscape or Sun ONE Directory Server, Sun iPlanet or other OpenLDAP directory servers, or Microsoft Active Directory Application Mode. Finally, an LDAP object must

www.it-ebooks.info

be associated with the Cisco Unity Connection UserID. The UserID in Cisco Unity Connection must be unique, even though it will be synchonized to a specific object in Active Directory. These objects consist of the sAMAccountName, mail, employeeNumber, telephoneNumber, or userPrincipalNumber. In most cases, you choose the sAMAccountName because this object is already required to be unique in Active Directory. Click **Save** to complete the operation.

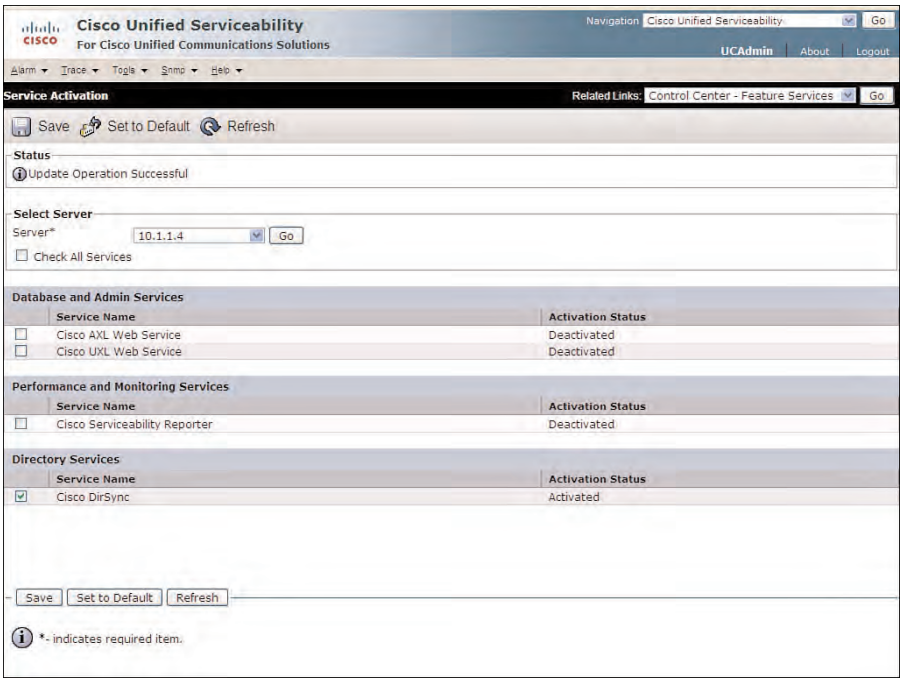

Figure 5-34 *Service Activation for Cisco DirSync Service*

LDAP Directory Configuration

Even though LDAP synchronization has been configured, you must create one or more synchronization agreement from where to import users. A synchronization agreement defines the location of the users to be used for the import operation. Select **System Settings > LDAP > LDAP Directory Configuration**. The LDAP Directory Configuration displays, where you are required to enter a descriptive name for the synchronization agreement in the LDAP Configuration Name field to identify the agreement. Up to five agreements can be configured per server, where each agreement defines a single search base. A search base defines the location from which users will be imported from the LDAP server. The objective of the agreement is to identify the search base, synchronization, and authentication for the synchronization agreement, as shown in Figure 5-36.

www.it-ebooks.info

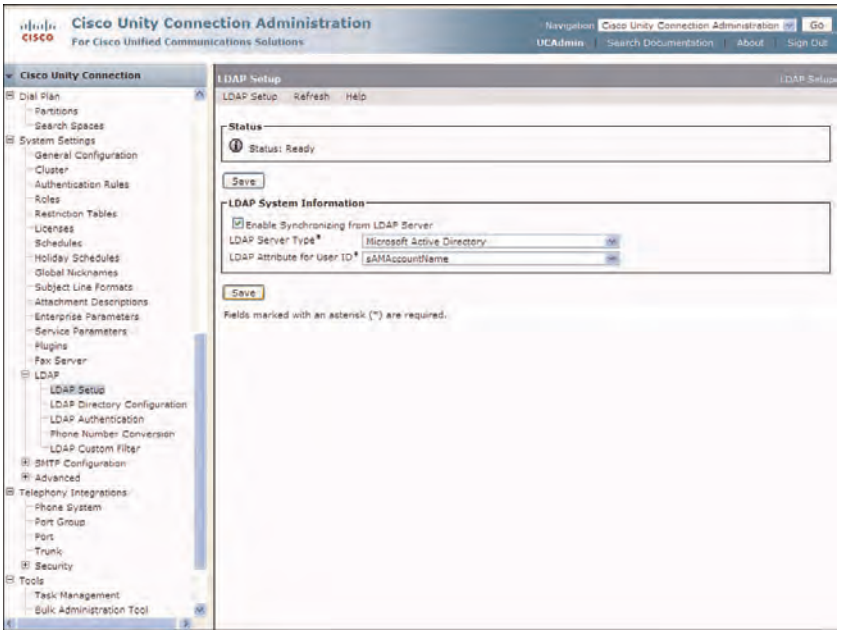

Figure 5-35 *LDAP Setup Configuration for LDAP Synchronization*

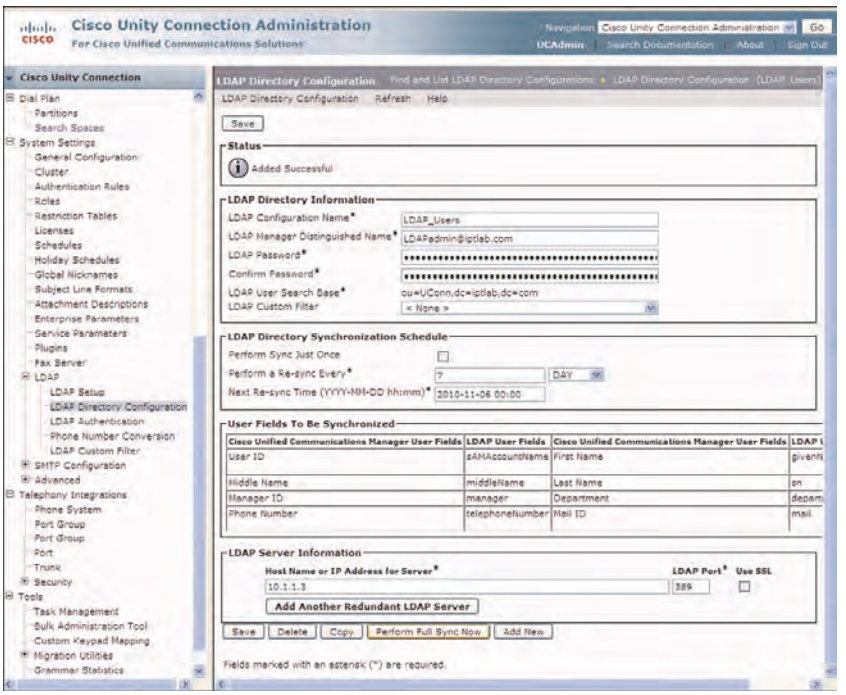

Figure 5-36 *LDAP Directory Configuration*

www.it-ebooks.info

A number of Active Directory objects need to be associated with Cisco Unity Connection. Finally, the IP address for hostname of the LDAP server must be specified. If you use Secure LDAP, the hostname must be entered. Selecting **Save** can save the synchronization agreement to the database and check the authentication specified in the synchronization agreement.

When the agreement has been saved, click **Perform Full Sync Now** to synchronize all users specified in the search base. The time to complete the synchronization process depends on the number of users in the search base. The first full sync always takes longer than subsequent syncs because of the amount of users and information to be synchronized.

Import Users from LDAP

The LDAP synchronization process does not automatically import users from LDAP into the Cisco Unity Connection database. You must specify the user or users one of three ways. That is, you can import selected users, all users, or use an LDAP filter to specific the users. The LDAP filter option is a new feature in Cisco Unity Connection v8 software.

To complete the import operation, select **Users > Import Users** to display the Import Users page, as shown in Figure 5-37.

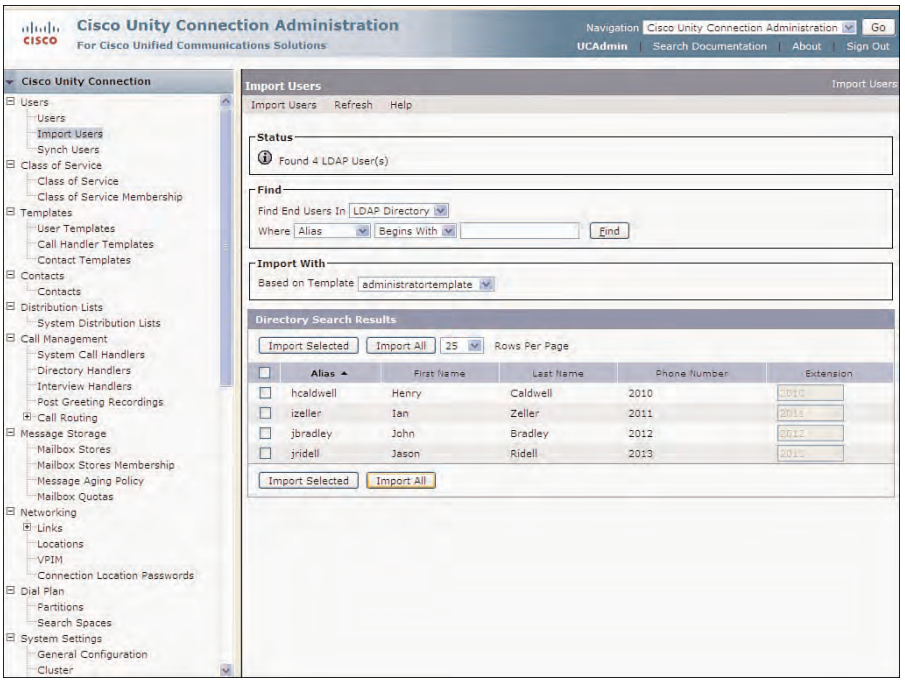

Figure 5-37 *Import Users from LDAP*

www.it-ebooks.info

The Import Users page provides the administrator with the ability to import users from the search bases selected within the configured synchronization agreements. On the Import Users page, from the Find Unified Communications Manager End Users In drop-down, select **LDAP Directory**, and click **Find**. All users in the various search bases are visible in the Directory Search Results section. From this page, select individual users, and click **Import Selected**. If you want to import all users, click **Import All**. You must select the template to use for applying the various features specific to Cisco Unity Connection; however, before you perform the import operation, you can use a filter to allow only specific users to be imported according to specific criteria.

LDAP Custom Filter Configuration

As of version 8.x, you can configure an LDAP filter. This provides the administrator with the ability to import users based on a specific defined filter. To use an LDAP Filter, you must first define the filter using regular expressions. This format is defined in RFC 4515, where you can filter on any number of attributes.

To configure the LDAP filter, in Cisco Unity Connection Administration, select **System Settings > LDAP > LDAP Custom Filter**. Click **Add New** to create a new filter. Enter the name for the custom filter in the Filter Name Field, followed by the regular expression for the filter, which must be entered into the Filter field. The filter text must be enclosed in parentheses, as shown in Figure 5-38. In this example, a filter is created to enable synchronization for all names with the common name (**cn**) beginning with the letter **J**. Click **Save**.

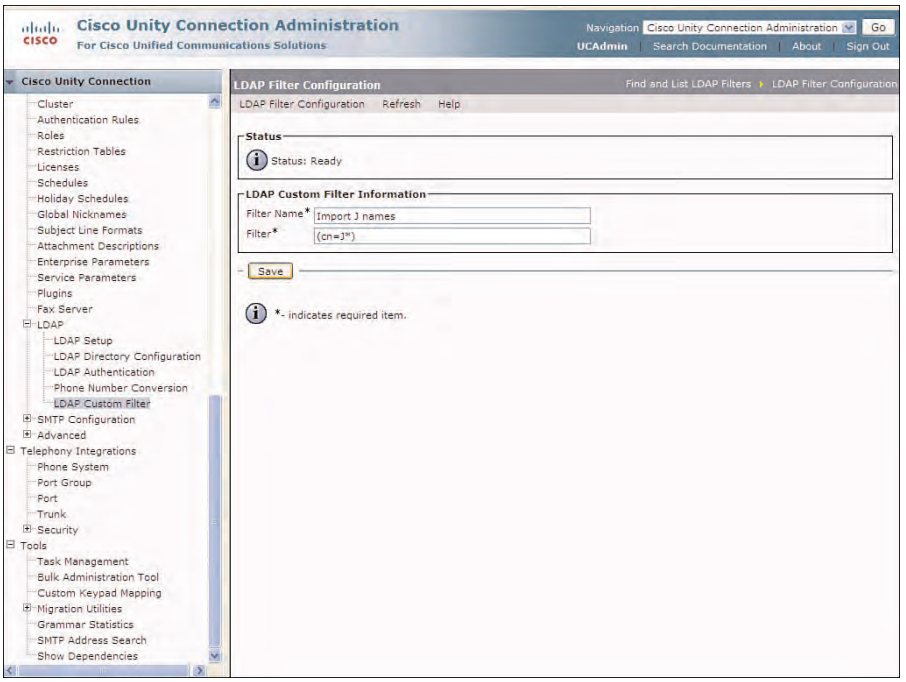

Figure 5-38 *LDAP Custom Filter Configuration*

www.it-ebooks.info

You can use custom filters with multiple attributes as required according to RFC 4515. For example, to allow just users with the last name beginning with the letter **T**, select the following:

```
(sn=T*)
```

To allow all users with their last names beginning with the **T** and **J**, use the **&** (AND) command:

```
(sn=T*)&(sn=J*)
```

To import all users except those users with the last name beginning with **T**, use the **!** (NOT) command:

```
(!(sn=T*))
```

Before importing users, the customer filter must be applied to the synchronization agreement. Return to the LDAP Directory Configuration page by selecting **LDAP > LDAP Directory Configuration** and selecting the LDAP configuration that was previously created.

Under the LDAP Directory Information selection, select the **Import J names** custom filter from the LDAP Custom Filter drop-down, and click **Save**. Only one filter can be applied to a specific synchronization agreement.

When the configuration of the custom filter is completed or modified, you need to perform a full synchronization for changes to be applied. To complete this step, click **Perform Full Sync Now** near the bottom of the page.

Again, select **Users > Import Users** to display the Import User page, as shown in Figure 5-39. On the Import Users page, from the Find Unified Communications Manager End Users In drop-down, select **LDAP Directory**, and click **Find**. You can now notice that only the users that have names beginning with the letter J display. Select the desired template to use for the import operation, and click **Import All** to import these users from LDAP to the Cisco Unity Connection database.

After the import operation is complete, review the Status section at the top of the Import Users page ensuring that there are no errors in the import operation. If changes are made to the custom filter, or, a new filter is applied to a synchronization agreement after the import operation, you need to restart the Cisco DirSync service, followed by performing a full sync within the modified agreement. Any users that you previously imported, but not included in the modified synchronization, are converted to standalone users. This action occurs after two synchronization periods or 24 hours, whichever is less.

www.it-ebooks.info

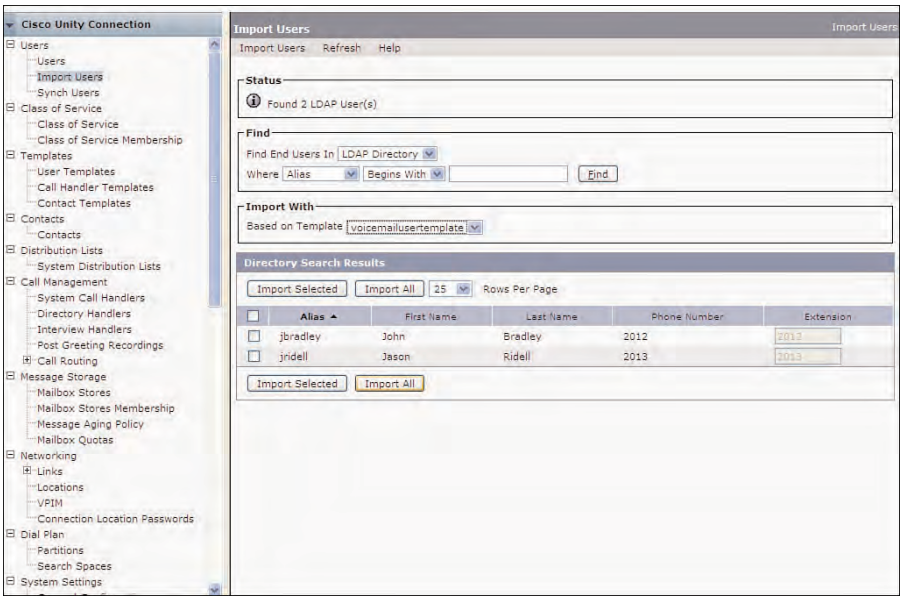

Figure 5-39 *Import Users Using an LDAP Custom Filter*

User Verification

After the import operation is complete, select **Users > Users** in Cisco Unity Connection Administration, and review the Search Users page. Ensure that the wanted users are visible, as shown in Figure 5-40.

Selecting a specific user displays the Edit User Basics page for that user. The status portion at the top of the page indicates that this user was imported from LDAP.

Phone Number Conversion

All users imported from LDAP to Cisco Unity Connection must have an extension and alias. These are both required fields for all users that have a mailbox. It might be necessary to modify the phone number currently configured in LDAP during the import operation. You can do this through the Advanced LDAP Setting in Cisco Unity Connection Administration.

To access these settings in Cisco Unity Connection version 8.5, select **System Settings > LDAP > Phone Number Conversion**. The Phone Number Conversion page has two options: the Matcher Regular Expression and the Replacement Expression. The default setting keeps the same number by matching any number **(.*)** and replaces it with the same, designated by the **$1** expression, as shown in Figure 5-41.

www.it-ebooks.info

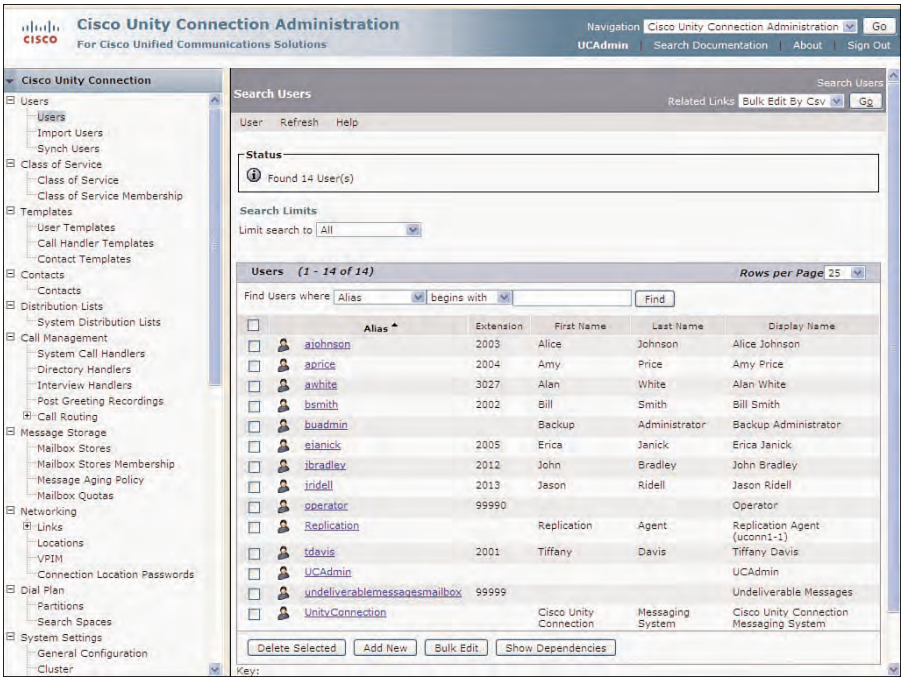

Figure 5-40 *Search Users Page After Importing Users from LDAP*

Case Study: Four-Digit to Six-Digit Phone Number Conversion

AET Inc. requires that all four-digit phone numbers in LDAP be converted to a six-digit extension in Cisco Unity Connection when they are imported. The prefix of 78 was determined to be used for all extensions.

In this solution, the administrators at AET Inc. have created a regular expression in the Phone Number Conversion page to accomplish this task. In this case, the Matcher Regular Expression was changed to (....), and the Replacement Regular Expression was changed to 78$1, as shown in Figure 5-42.

In this example, all four-digit phone numbers imported from LDAP will convert to a six-digit extension with the prefix of 78.

To access these settings in Cisco Unity Connection versions previous to v8.5, select **System Settings > LDAP > Advanced LDAP Settings**. The Filter to Convert LDAP Phone Numbers into Connection Extensions field enables for editing the default option. Currently the default setting is **[0-9]+**. This enables all numbers to import from LDAP to Cisco Unity Connection without modifications. You must use valid regular expressions within this field the advanced settings to function properly. The advanced settings are applied to all synchronization agreements. This is different than custom filters, which are applied to a specific agreement.

www.it-ebooks.info

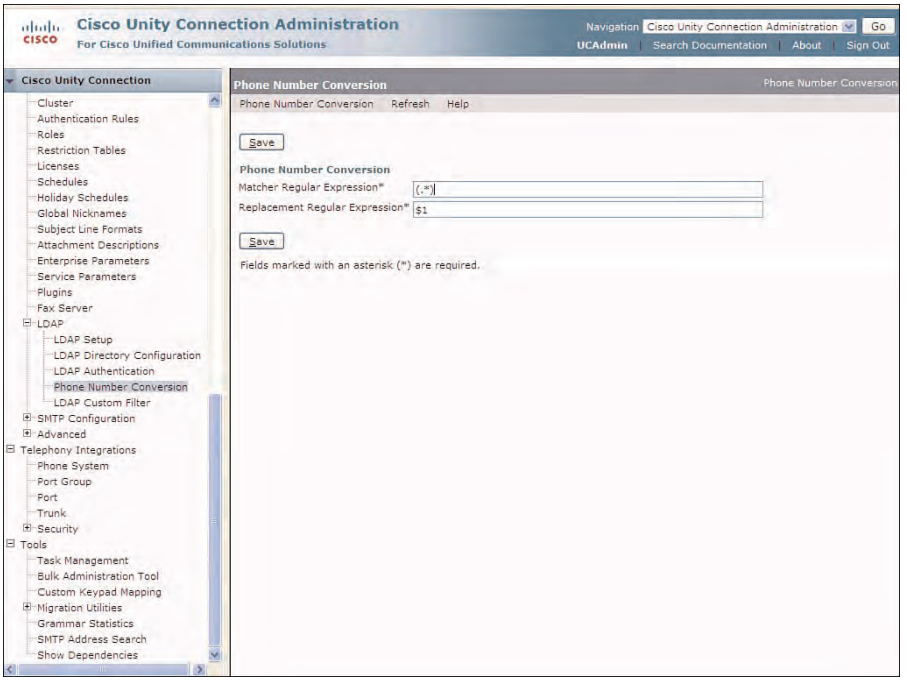

Figure 5-41 *Phone Number Conversion for LDAP Import in Cisco Unity Connection v8.5*

If you want to import all numbers of any length into Cisco Unity Connection and convert them to five digit extensions, you can use the following regular extension:

[0-9][0-9][0-9][0-9][0-9]$

Click **Save** to apply the settings. These options must be applied before the import operation, or a full synchronization must be performed to apply the necessary changes.

LDAP Authentication

Currently, all users that were synchronized and imported using LDAP can log in to voicemail, IMAP applications, and administration based on their CoS and assigned roles. The passwords required for all web applications must be configured in Cisco Unity Connection. The default password was applied from the selected template used at the time of import. Any changes to these passwords must be configured in Cisco Unity Connection Administration as well. This can be an issue because the user already has a password in LDAP. Therefore, if you use synchronization without authentication, passwords for email and voicemail must be managed separately. Using LDAP authentication enables the administrator to manage all users and password directly in LDAP, with a centralized point of administration. When LDAP authentication is enabled, the passwords

www.it-ebooks.info

configured in Cisco Unity Connection for web applications are no longer used; only the voicemail passwords are used for users to retrieve their voicemails via the phone.

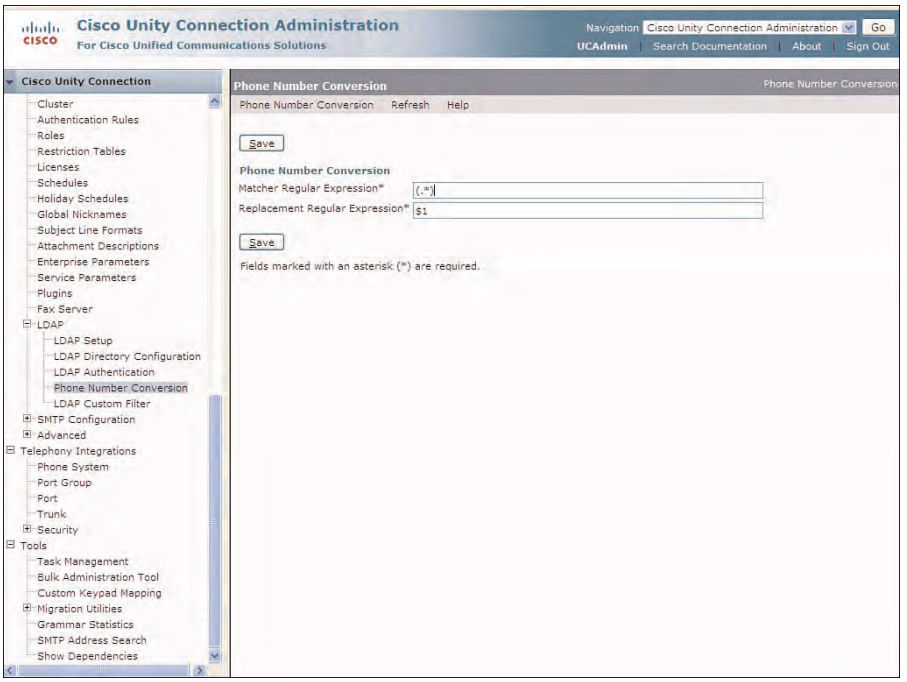

Figure 5-42 *Phone Number Conversion Solution for AET Inc to Prefix All Extensions*

You can configure LDAP Authentication by selecting **System Settings > LDAP > LDAP Authentication** in Cisco Unity Connection Administration. On the LDAP Authentication page, select the check box for Use LDAP Authentication for End Users. Then, enter the LDAP Manager Distinguisher Name, Password, and Search Base in the same methods done for LDAP Directory Configuration, as displayed in Figure 5-43. The LDAP Manager Distinguished Name and password must have Domain Admin rights and have access to all directories in the configured search bases. Finally, enter the hostname or IP address of the LDAP server. You can also specify up to three redundant servers for LDAP synchronization and authentication. Click **Save** to commit all configurations to the database and enable LDAP Authentication.

At this point, all users that have been imported are synchronized with LDAP. Cisco Unity Connection also authenticates to LDAP for all web applications.

The final method to configure multiple users in Cisco Unity Connection will be through the integration of Cisco Unified Communications Manager using Administrative XML (AXL).

www.it-ebooks.info

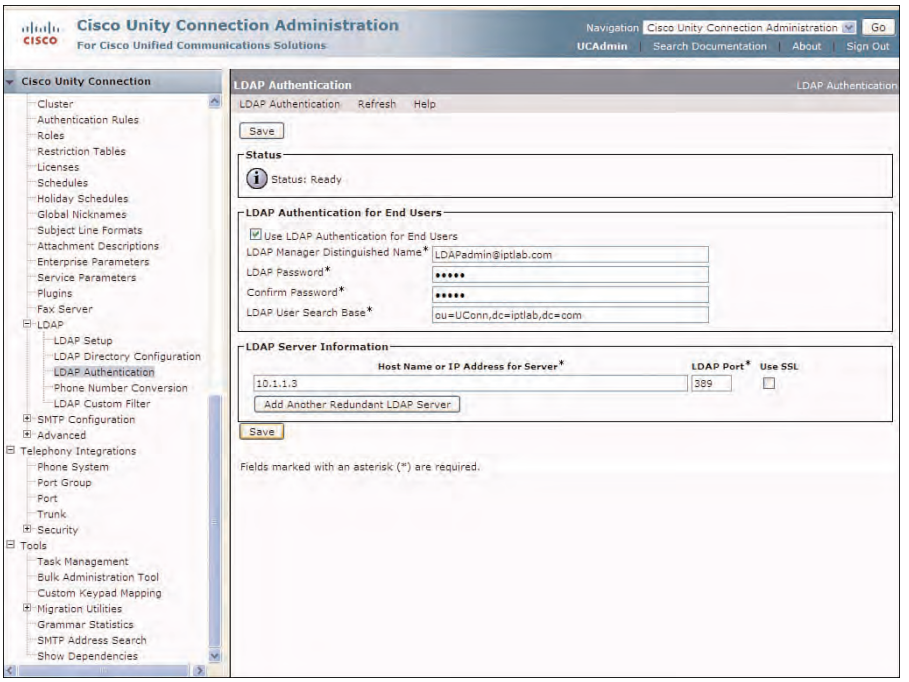

Figure 5-43 *LDAP Authentication in Cisco Unity Connection Administration*

Administrative XML Integration with Cisco Unified CM

Administrative XML (AXL) enables Cisco Unity Connection to integrate with Cisco Unified CM for the purpose of importing users from Cisco Unified CM to the Cisco Unity Connection database. Users can be imported and synchronized, provided that Cisco Unity Connection has the AXL service activated and is properly configured with administrative rights for the respective Cisco Unified CM server.

Before beginning the configuration of Cisco Unity Connection, you need to ensure that the Cisco AXL Web Service has been activated on the Cisco Unified CM publisher server.

To synchronize and import users from Cisco Unified CM database to Cisco Unity Connection, select **Cisco Unified Serviceability** from the Navigation drop-down in Cisco Unity Connection Administration, and click **Go**. The Cisco Unified Serviceability page displays. Select the server and click **Go**. If you configure a cluster pair, select the publisher server. Select the check box for the Cisco AXL Web Service, and click **Save**, as shown in Figure 5-44.

Return to Cisco Unity Connection Administration by selecting it from the Navigation drop-down and selecting **Go**. In the next step, you need to define the Cisco Unified CM server as an AXL server under the phone system integration because this is where the Cisco Unified CM server was configured for the phone system integration. Select

www.it-ebooks.info

Telephony Integrations > Phone System to display the Search Phone Systems page. Select the Cisco Unified CM phone system to display the Phone System Basics page for the integration. Select **Edit > Cisco Unified Communications Manager AXL Server** from the toolbar. The Edit AXL Servers page displays, where you need to click **Add New** to add a new server and supply the proper authentication credentials. The username selected must be an application user that has CCM Super User rights on the Cisco Unified CM server. Enter the IP Address, port, order, and proper authentication credentials that apply to the Cisco Unified CM server, and click **Save**. The selected port for AXL should be selected as port 8443.

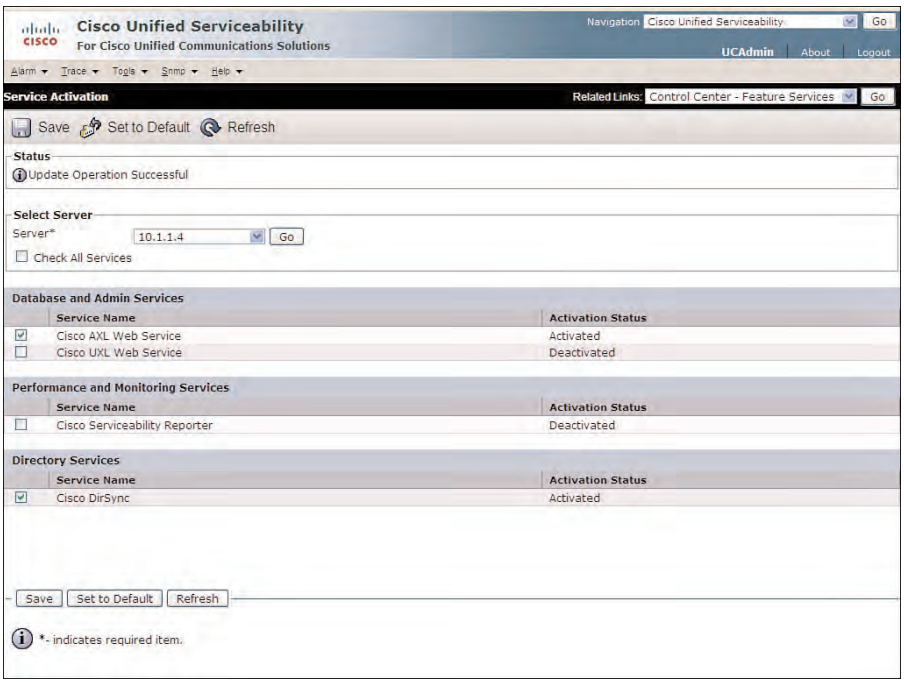

Figure 5-44 *Activate the Cisco AXL Service*

The order of the servers determines the priority. A lower number defines a higher priority. The AXL Server page also enables the administrator to test the integration by selecting the **Test** button. A pop-up page with the test results displays, as shown in Figure 5-45. You need to ensure that the test is successful before beginning the import operation.

Importing Users Using AXL

The AXL synchronization process does not automatically import users from Cisco Unified CM to the Cisco Unity Connection database. You must import users using the Import Users page. Select **Users > Import Users** to display the Import User page, as shown in Figure 5-46.

www.it-ebooks.info

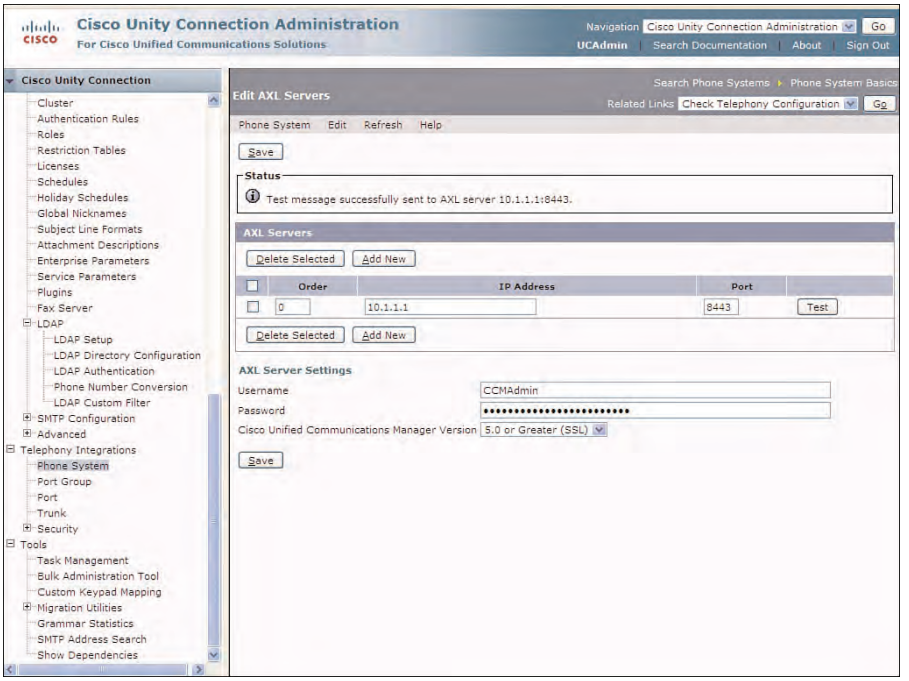

Figure 5-45 *Cisco Unified Communication Manager AXL Server Configuration*

The Import Users page provides the administrator with the ability to import all users or specific users from the Cisco Unified CM database. On the Import Users page, select the phone system name for the Cisco Unified CM integration from the Find End Users In drop-down, and click **Find.** All users in the Cisco Unified CM database that have a defined phone number for their Primary Extension in Cisco Unified CM will be visible in the Directory Search Results section. Users that do not have a defined extension do not display and cannot be imported because an extension is required to create a user.

From the Import Users page, select the desired user(s) to import, and click **Import Selected.** Or import all users by clicking **Import All.** Similar to the LDAP import procedure, you must also select the template to use for import to apply the various features specific to Cisco Unity Connection. In this example, you import only one user, Alan White at extension 3027, by selecting the check box next to his name and clicking **Import Selected.**

Again, select **Users > Users** in Cisco Unity Connection Administration, and review the Search Users page to ensure the imported users now display. Selecting a specific user displays the Users Basic page for that user. The status section at the top of the page displays the method in which the user was imported, as shown in Figure 5-47. In this case, the user was imported using AXL from Cisco Unified Communications Manager.

www.it-ebooks.info

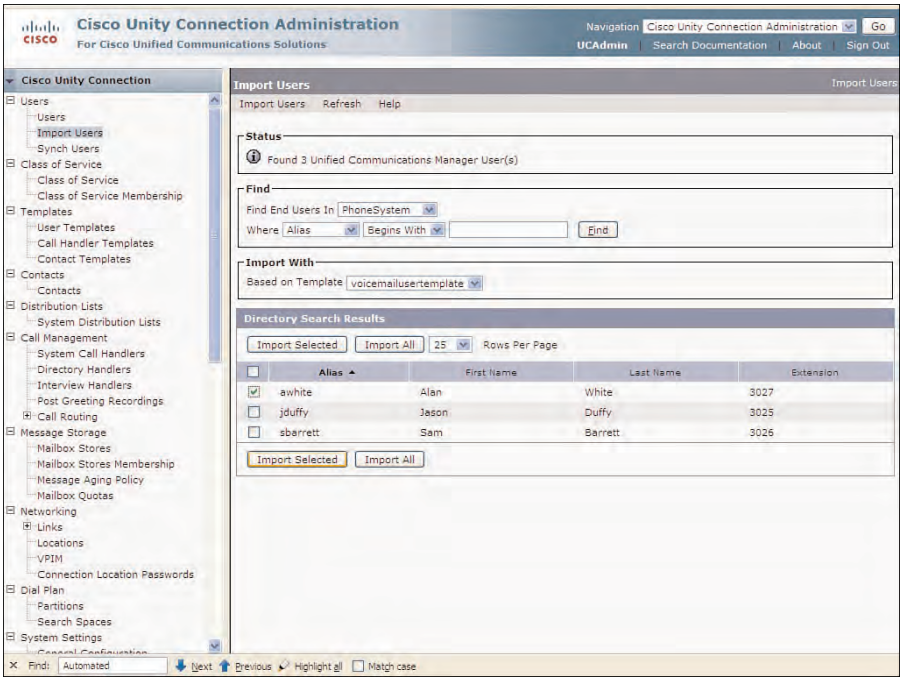

Figure 5-46 *Import Users from Cisco Unified Communications Manager AXL Server*

In Cisco Unity Connection, users can be imported using all methods and coexist. Users that were imported or created using one method can be converted to another type of user. For example, users that were created manually can be converted to LDAP users. This is accomplished using the BAT by exporting the current user, modifying the CSV file, and uploading the file to modify the user attributes in Cisco Unity Connection. A common task where this might be required is where users that were configured as stand-alone must now be synchronized and managed from LDAP, as shown in the following case study.

Case Study: Importing Users

Pegeramy Corporation, a manufacturing firm in the Midwest, has an existing Cisco Unity Connection implementation. They have 500 users managed directly on the Cisco Unity Connection platform. However, in recent months, management has made the decision to migrate to the Microsoft Exchange environment for its email. The IT director would like to manage these existing users from Exchange, thereby centralizing the user configuration and password administration for web applications in Cisco Unity Connection. However, management has decided to test this feature by converting one user, Amy Price, to an LDAP user.

www.it-ebooks.info

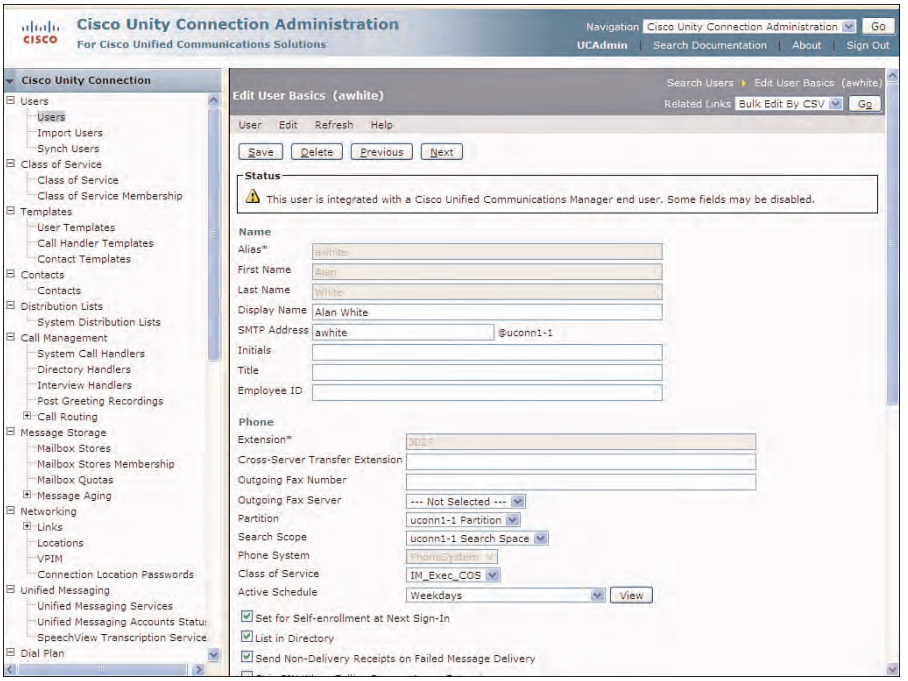

Figure 5-47 *Edit Users Basic Page for Imported Users*

This is easily accomplished using the Bulk Administration Tool in Cisco Unity Connection Administration. Select **Tools > Bulk Administration Tool** to display the Bulk Administration Tool page. From the Bulk Administration Tool page, select the **Export** radio button followed by the **Users with Mailbox** radio button in the Select Object Type section. Enter a filename in the CSV File textbox with the .csv extension, and click **Submit**, as shown in Figure 5-48.

Review the status section to ensure that no errors occurred, and select the **Download the Export File** link. Save the file to the administrator workstation and open it using the Excel application to begin the editing operation.

After the CSV file opens, locate the column with the heading **LdapCcmUserId**. In the applicable row, enter the name that will be used for the UserID in this field for any user that you want to convert to an LDAP synchronized user. Finally, remove all other rows, and save the editing file to your workstation.

Before you return to Cisco Unity Connection, you must go to the LDAP server and create the users with the exact same UserID as selected in the aforementioned CSV file.

www.it-ebooks.info

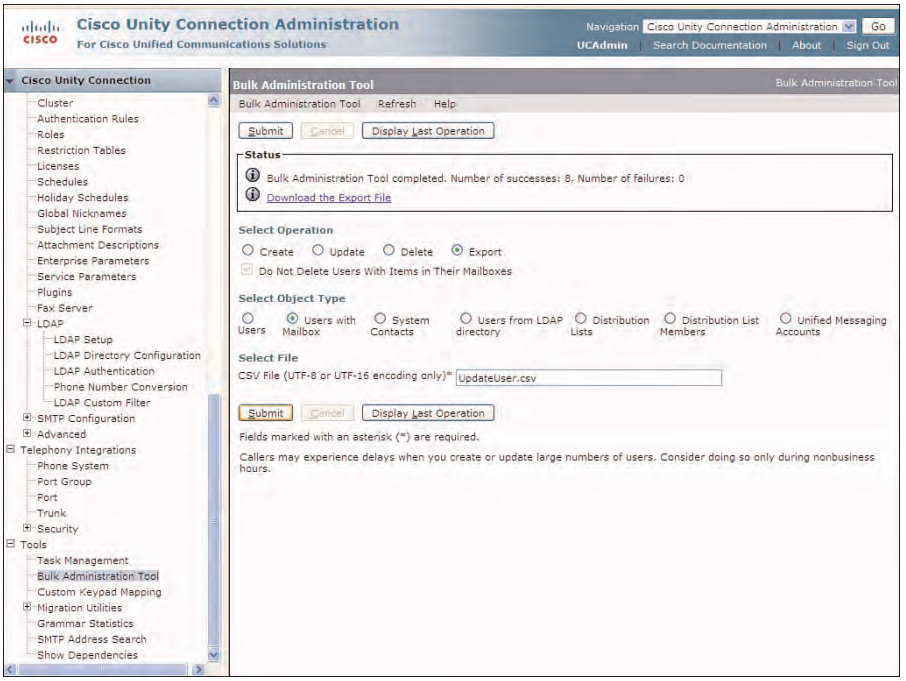

Figure 5-48 *Export Users Using the Bulk Administration Tool*

Finally, return to Cisco Unity Connection Administration and perform a full sync under the corresponding LDAP synchronization agreement. Then, using the Bulk Administration Tool, select the **Update** radio button and respective CSV file, as shown in Figure 5-49. In this example, one user was successfully updated and has been converted to an active user imported from the LDAP directory, as shown on the status of the Edit User Basics page. Before beginning this operation, the user must be created in LDAP with the exact UserID and information.

In this chapter, you learned how to create and modify users. In the few next chapters, you discover some of the important features, applications, and voicemail options required by users through Cisco Unity Connection.

www.it-ebooks.info

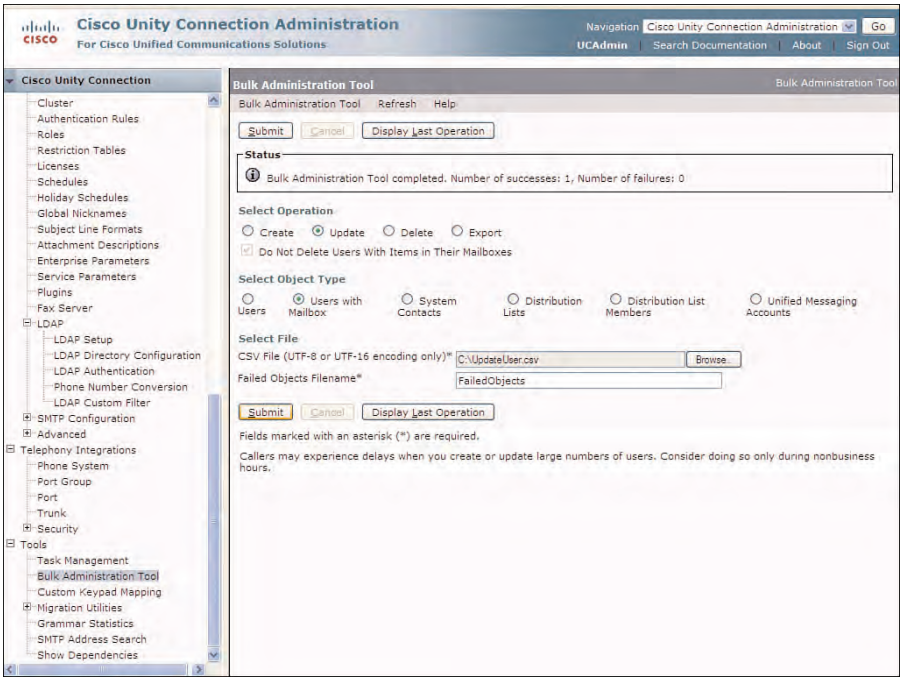

Figure 5-49 *Updating Users with the Bulk Administration Tool*

Summary

This chapter provided an understanding of Cisco Unity Connection integration concepts and configuration with various call-processing systems. You have learned how to

- Understand the purpose and configuration of users and contacts in Cisco Unity Connection Administration.
- Determine the relationship of the various configuration elements required to create users, including authentication rules, schedules and holidays, Class of Service (CoS), and templates.
- Determine the configuration and relationship of voicemail and administrative users and the various configuration settings in Cisco Unity Connection that can be applied through user templates.
- Explore the function, features, and capabilities of the Cisco Unity Connection Bulk Administration Tool and Bulk Edit tools, which can be used to create and modify new users or contacts.

www.it-ebooks.info

- Learn the various methods of user administration, including importing of users from Cisco Unified CM using Administrative XML (AXL) Application Programming Interface (API), and creating users individually in Cisco Unity Connection.
- Understand the functions and configuration of Lightweight Directory Access Protocol (LDAP) integration and authentication in Cisco Unity Connection version 8.x and the ability to update users from standalone to LDAP users.

www.it-ebooks.info

This page intentionally left blank

www.it-ebooks.info

Chapter 6

Providing Users Access to Voice Messaging

This chapter covers the following subjects:

- **Voicemail Access and Recording:** Explains user access to voice messaging using the telephone user interface (TUI).
- **Web Applications for Voicemail:** Covers Cisco Unity Connection web applications for access to voicemail, including Cisco Unity Inbox, IMAP clients, ViewMail for Outlook, and Really Simple Syndication (RSS).
- **Cisco Unified Communications Manager Applications:** Describes the integrations of Phone View and Visual Voicemail applications to be used with Cisco Unified CM to access Cisco Unity Connection voice messaging.
- **Mobile/Voicemail Applications:** Explores special applications that integrate with Cisco Unity Connection, including Personal Communicator, Mobility Advantage, and Outlook calendar integration.

Users and contacts have now been created and configured in Cisco Unity Connection. The functions and features available to these users to access their voice messages must now be understood by administrators and communicated to each group of users. Numerous different methods are available to the user within Cisco Unity Connection to access voice messaging. However, each organization must determine the specific needs of each group and provide the necessary access method required to allow users to perform their job functions efficiently and without frustration. An important factor to eliminating this frustration is to provide users with adequate user training, where all the necessary functions and features are explained thoroughly and users gain a working knowledge of the voice-messaging system from a user perspective. It is through the users' understanding that they will adopt and use the features, thereby providing the necessary benefits and efficiencies to the organization.

www.it-ebooks.info

However, the first step is for the administrator themselves to clearly understand all the various methods to access the voice-messaging system, decide which tools will be configured and provided, and clearly communicate and explain the functions and features to these users.

These different access methods include the following:

- Phone access to voicemail (on-site and remote)
- Phone access using the voice recognition feature
- IMAP client (Microsoft Outlook/ViewMail for Outlook)
- Messaging Inbox
- Phone View and Visual Voicemail
- Really Simple Syndication (RSS)
- Mobile applications (Cisco Unified Personal Communicator/Cisco Unified Mobile Communicator)

In many cases, users can access voice messages from their phone; however, it might be more convenient for users to use a web client, such as Messaging Inbox, Outlook, or RSS feeds using a web browser. The method used depends entirely on an individual user's job role, functionality requirements, and their individual skill level. A road warrior might be more apt to use various mobility features than someone that works within the local office. In other cases, these choices might be decided based on convenience, accessibility, or the type of business involvement.

In this chapter, you gain an understanding of the following:

- Various methods to access voice messages
- Various web applications to access voice messaging, and the configuration required to provide this access
- Configurations required for IMAP clients, such as Messaging Inbox and Outlook using ViewMail
- RSS client access and the required configuration to provide access to this feature
- Function, features, and differences between Phone View and Visual Voicemail
- Various mobility feature of Cisco Unity Connection

Voice-Message Features and Applications Overview

Users have a number of options to send, retrieve, and forward voice messages. By default, all users with mailboxes can perform most of the basic voicemail functions from their phone, or any remote phone outside the organization. Other options and features are enabled through the user Class of Service (CoS). As discussed in the previous chapter, the

www.it-ebooks.info

CoS is assigned to a user or group of users through the user template at the time the users were created. However, a new CoS can be assigned to any user as required, or an existing CoS can be modified. If you intend to modify an existing CoS, be aware that the changes are applied to all members of that CoS. Therefore, ensure that all members require these new features allowed in the modified CoS.

The simplest CoS is the default CoS called Voice Mail User CoS. This CoS is discussed in the previous chapter, providing users with the basic phone access to voice messaging. The next section begins with a discussion of this access method to use the phone and the various features available to these users.

Phone Access to Voice Messaging

All users with mailboxes have access to voice messaging using their phone. In most cases, internal users in the organization can have a phone to access their voicemails. In other cases, such as remote or traveling users, these types of users might not have an extension associated with a physical phone. In either case, the experience of callers leaving messages and the user experience retrieving these messages is similar.

The caller and user experience when they access Cisco Unity Connection is determined by the direct and forwarded routing rules. When a caller attempts to contact a user, the call can be forwarded to Cisco Unity Connection based on a number of conditions. This chapter explores the various options and configurations features that affect the callers' experience of leaving messages, and the users' experience of sending and retrieving messages. Later in this section, you discover other features that can be implemented to enhance the user experience.

In Chapter 4, "Integrating Cisco Unity Connection," you learned that default routing rules, specifically the Forwarded Routing Rules, determine the callers' experience when they are forwarded to voicemail. In these cases, users might be busy, not available, or have their phone forwarded to voicemail by personal call routing rules, such as iDivert, Do Not Disturb, or some other forwarding features supported by the phone system. In any case, the default Forwarded Routing Rules in Cisco Unity Connection determines the caller experience.

If the user is configured in Cisco Unity Connection as a User with Mailbox, the caller hears the user's personal greeting, followed by the option to leave a message. If the called phone is not a configured user with a mailbox and forwarded to Cisco Unity Connection, the caller hears the Opening Greeting, by default. Of course, these are the default Forwarded Routing Rules, which cannot be changed or deleted; however, new rules can be added to supersede these existing rules.

In many cases, organizations send all incoming calls to Cisco Unity Connection, where they hear a personalized Opening Greeting, followed by a series of choices that callers can select from. This is defined as an Audiotext Application, or what is sometimes referred to as an *Auto Attendant*. Cisco Unity Connection provides a robust set of tools to create a professional and easy to implement audiotext application. This application will be created using a number of objects, such as a system call handlers, directory handlers,

www.it-ebooks.info

and interview handlers. This application will be explored in its entirety in Chapter 9, "Understanding Cisco Unity Connection Networking."

Transfer Rules

While callers listen to the opening greeting, they have the option to select from the various options or dial the user's extension. If this user's extension is selected, the call is forwarded to the user's phone based on the default configuration of Standard transfer rule. You can view the transfer rules by selecting **Users > Users** in Cisco Unity Connection Administration. Then, select the specific user that you want to view, and from the Edit User Basics toolbar, click **Edit > Transfer Rules**. Figure 6-1 shows the Transfer Rules page. There are three transfer rules, with only the Standard rule enabled by default.

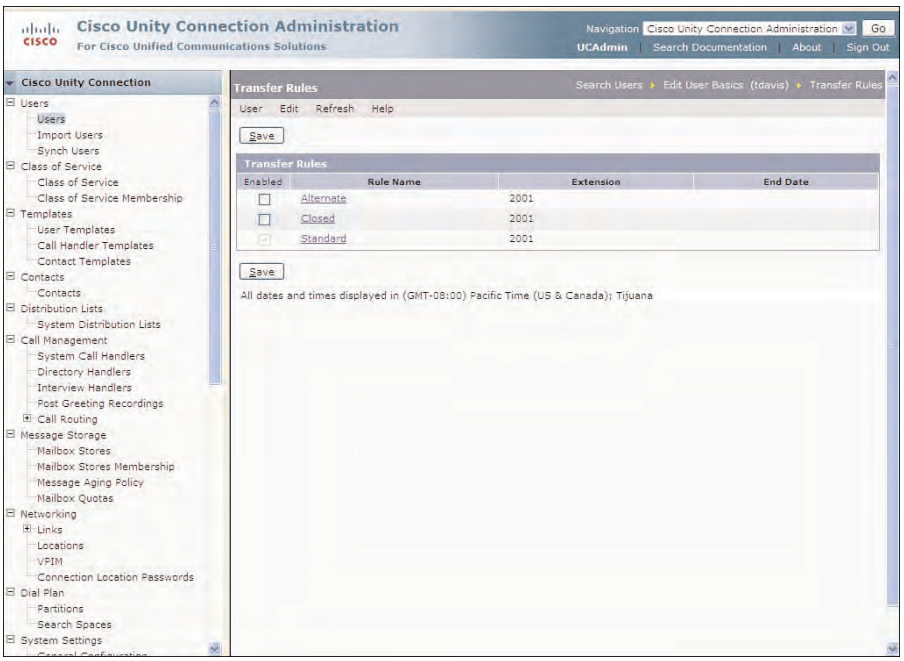

Figure 6-1 *Transfer Rules in Cisco Unity Connection Administration*

The three transfer rules in Cisco Unity Connection Administration follows:

- **Standard:** The Standard transfer rule settings are applied to all users based on the user template used to create the user. If the default options are used in the template, the Standard rules settings always transfer the callers to the user's extension, if they select this option during listening to the opening greeting or from any directory.
- **Closed:** The Closed transfer rule is not enabled but can be selected to follow the Active Schedule (configured under the Edit User Basics page). This feature provides

www.it-ebooks.info

the user with the option to send calls directly to voicemail or another extension, such as a cell phone or directly to voicemail after the close of the business day.

- **Alternate:** The Alternate transfer rules are applied by an action from the administrator or user. In some cases, seasonal workers or traveling on-call employees might require this option based on a specific set time but do not want to change their standard or closed transfer rules. For this reason, a Closed transfer rule supersedes the Standard transfer rule based on the Active Schedule, where the Alternate transfer rule overrides both the Standard and Closed transfer rules. In other words, the Alternate transfer rule takes precedence above all other rules.

To review and change the Standard transfer rule, select **Standard** from the Rule Name column. The Edit Transfer Rule (Standard) now displays, as shown in Figure 6-2. The transfer rules page for the Closed and Alternate includes the same options and features.

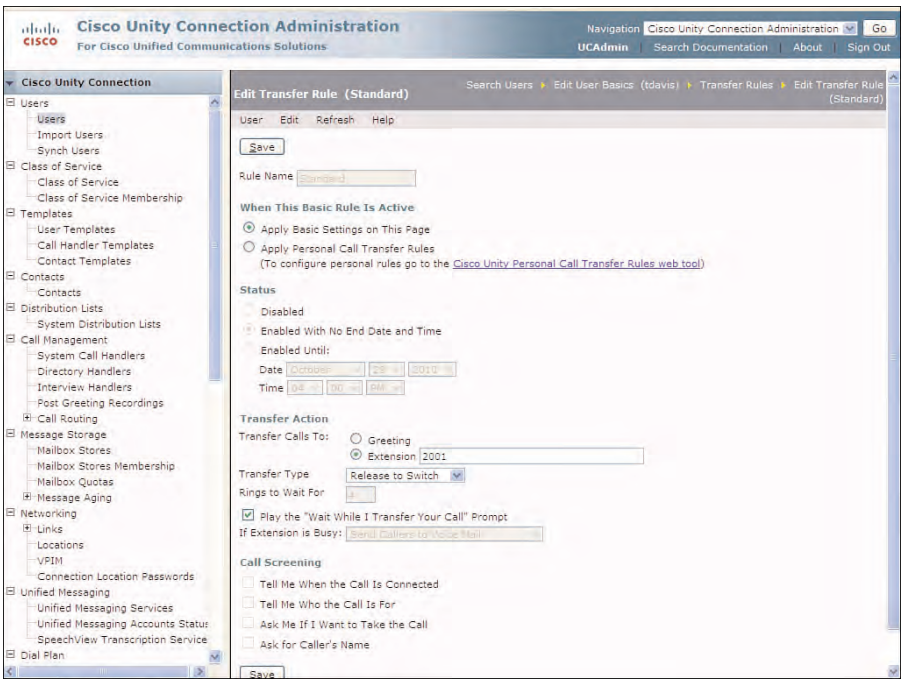

Figure 6-2 *Edit Transfer Rule (Standard)*

From the Edit Transfer Rule (Standard) page, the administrator can change a number of options. The first option enables the administrator to apply the options selected in the Standard transfer rule, or apply Connection Personal Call Transfer Rules.

The Connection Personal Call Transfer Rules enables the administrator or user to configure specific rules based on the caller or groups of callers, depending on the time of day and meeting schedules. The administrator can enable and configure these options directly by selecting the link on this page that directs them to the Connection Personal Call

www.it-ebooks.info

Transfer Rules page. However, any user must be a member of a CoS that enables access to this feature through the Personal Communications Assistant to make changes to their Connection Personal Call Transfer Rules. This application is discussed later in the section, "Web Application Access to Voice Messaging."

The Status section for the Standard transfer rule page is always selected as **Enabled with No End Date and Time** and cannot be changed. However, the status for the Closed and Alternate transfer rules can be changed as needed, depending on the work schedules of the organization. Configurable options enable administrators to enable, disable, or enable until a specific date and time.

The Transfer Action section enables the administrator to select transfer features when a user is called from another user or outside caller directly from Cisco Unity Connection. In the default options of Figure 6-2, the caller is directed to the user's phone associated with the user's configured extension on the Edit User Basics page. However, this could be directed to a different phone extension or outside phone, or sent directly to the user's personal greeting without ringing the user's extension. For users that do not have a physical phone on the system or work off-site, these other options might be an optimal choice.

A number of other features exist for transfer rules. These options are related directly to call screening and queuing features. The Transfer Type option displays the default of **Release to Switch**. By selecting this option, Cisco Unity Connection dials the users' extension and release the call to the integrated phone system associated with this user. The **Supervise Transfer** options enables the administrator to configure call screening and queuing features, such as having the caller's name announced and the options to accept or pick up the call.

Additionally, the administrator can provide options to the caller using the **If Extension Is Busy** feature. In most cases, you leave the default options to send callers to the user's voicemail if their extension is busy. However, the decision can be made to provide a queuing option where either the caller can be put on hold and queued, or given the choice to hold.

These call screening features are useful to users that require screening and queuing features, because of high phone usage or depending on their job function. The users could be enabled to change the call screening option through their CoS membership, as shown in Figure 6-3.

Message Waiting Indicators

When the caller leaves a message for a user in Cisco Unity Connection, the user needs to be notified of the message. Message Waiting Indicators provide this function. The message waiting indicator (MWI) command must be sent to the user's phone to turn on the light and provide visual indication on the phone display. When the users listen to their messages, Cisco Unity Connection must send the proper MWI command to turn this indicator light off. Each integration of Cisco Unity Connection with the phone system enables for a unique number configured for MWI ON and MWI OFF and must agree with the configuration of the phone system for proper operation of MWI. Best practice

www.it-ebooks.info

dictates that the MWI numbers should be assigned to partitions accessible only from the calling search space of the voicemail ports in Cisco Unified CM.

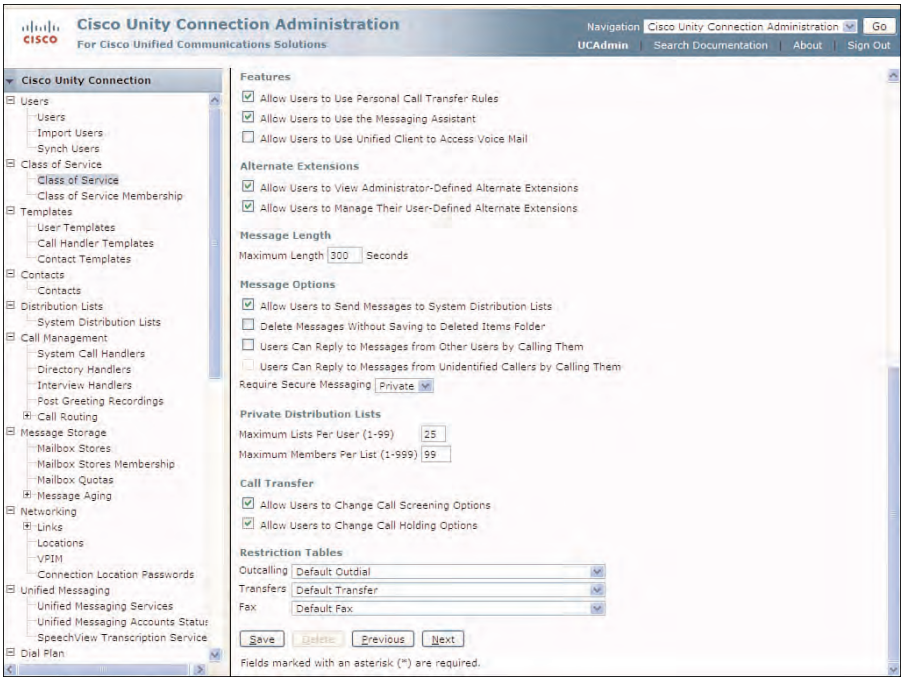

Figure 6-3 *CoS to Enable Call Transfer Changes*

Administrators can also configure additional phones for MWI indication that applies to the same mailbox. This is practical when users have an office phone but work in multiple locations. For example, engineers in the organization have an office outside of the data center where their desk phone is located; however, they might work in the data center most of the day. This feature enables them to provide an MWI indication on the remote data center phone, letting them know when they have new messages. As many as ten alternative MWI extensions can be configured for each user.

To configure additional MWI indicators, from the Edit User Basics page, select **Edit > Message Waiting Indicators** to display the Message Waiting Indicators page, as shown in Figure 6-4.

The Message Waiting Indicators page enables the administrator to view the current status and configured MWI configuration option, and to reset the indicators as needed. To add a new MWI, click **Add New**, and enter the Display Name and Extension for the new, additional MWI, as shown in Figure 6-5. Click **Save** when the configuration is complete.

www.it-ebooks.info

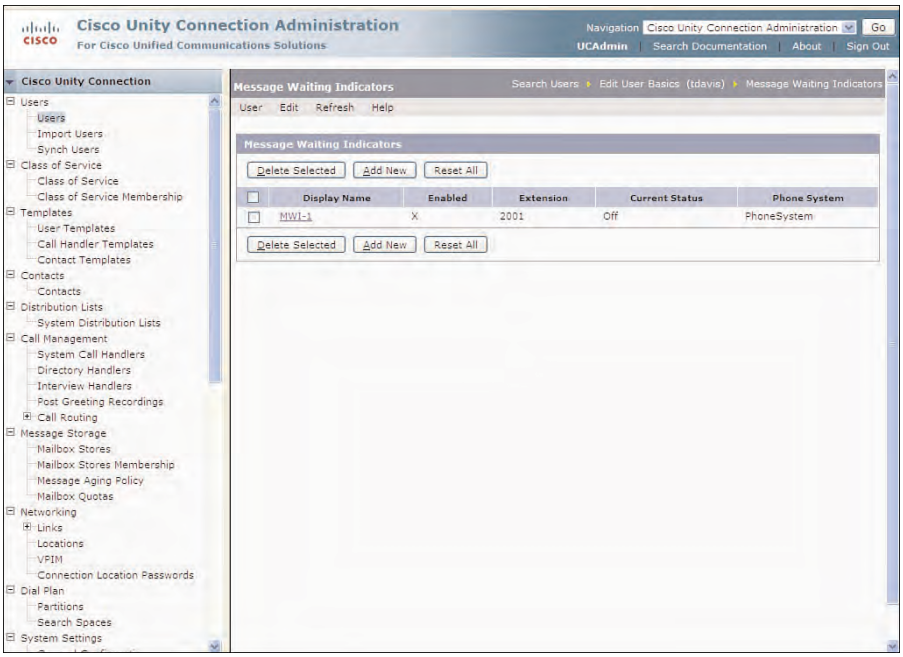

Figure 6-4 *Message Waiting Indicators Configuration Page*

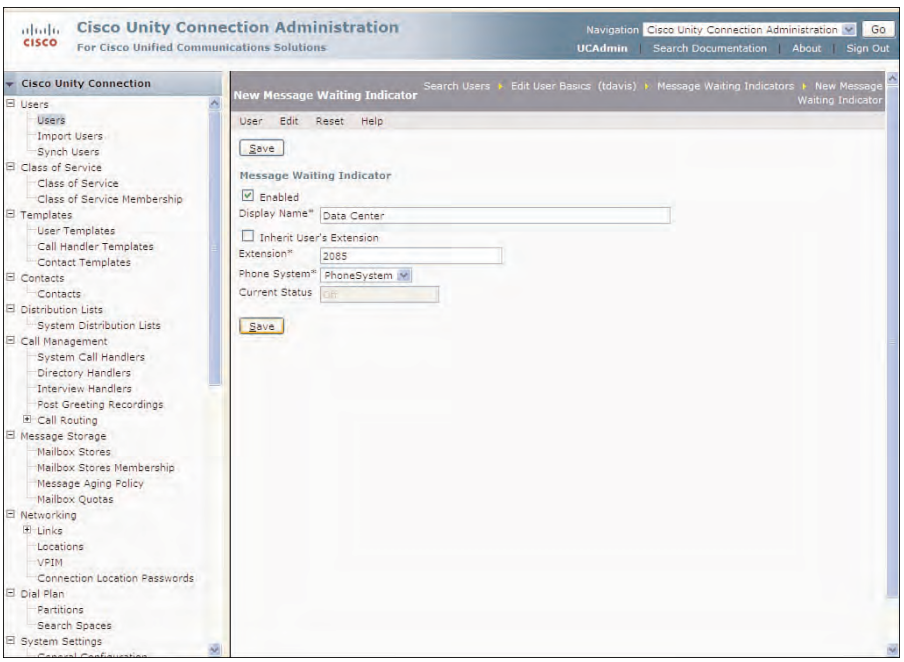

Figure 6-5 *Edit Message Waiting Indicator Page*

www.it-ebooks.info

When users decide to access Cisco Unity Connection to retrieve their voice messages, they can do this by either selecting the Messages button on the IP phone, or call the voicemail pilot number directly. In either case, if users access Cisco Unity Connection from their configured phone, they will be directed to the Attempt Sign-In conversation, based on the Direct Routing Rules. This is referred to as *Easy Message Access* because the users' phone extension is known and configured in Cisco Unity Connection. Otherwise, they are directed to the Opening Greeting, where they can access their voicemail by selecting the * key, and then entering their extension and voicemail password. This experience is determined by the default Direct Routing Rules.

Alternate Extensions

Additional phone numbers can be associated with the user's extension, which are called *Alternate Extensions*. Alternate Extensions extends Easy Message Access to the user's cell phone, home phone, work phone or other configured extension enabling the user to direct access to his voice mailbox, simply by entering his voicemail password. If workers do work-at-home functions as part of their work week, they could be configured to allow Easy Message Access to voicemail from their home or cell phone. This enables remote users the same access to voice messaging as workers located in the office using their IP phone. The Alternate Extension feature is configured by the administrator but can also be viewed or managed by the user, depending on the CoS, as shown in Figure 6-6. In this case, the user can use the Messaging Assistant and can view and manage all alternative extensions.

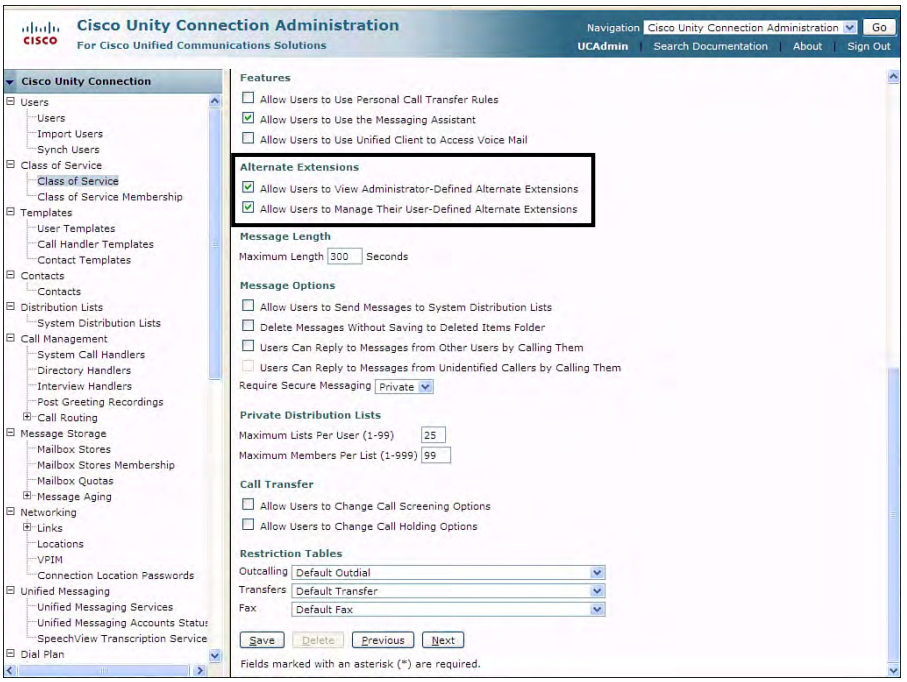

Figure 6-6 *CoS Configuration for Alternate Extension*

www.it-ebooks.info

To configure the Alternate Extension for users, select **Edit > Alternate Extension** from the Edit User Basics page. Select **Add New** to add a new alternative extension. From this page, the administrator can enter the Display Name and Phone Number, and select a number of phone features that apply to this extension, as shown in Figure 6-7. Click **Save** when all configurations are complete.

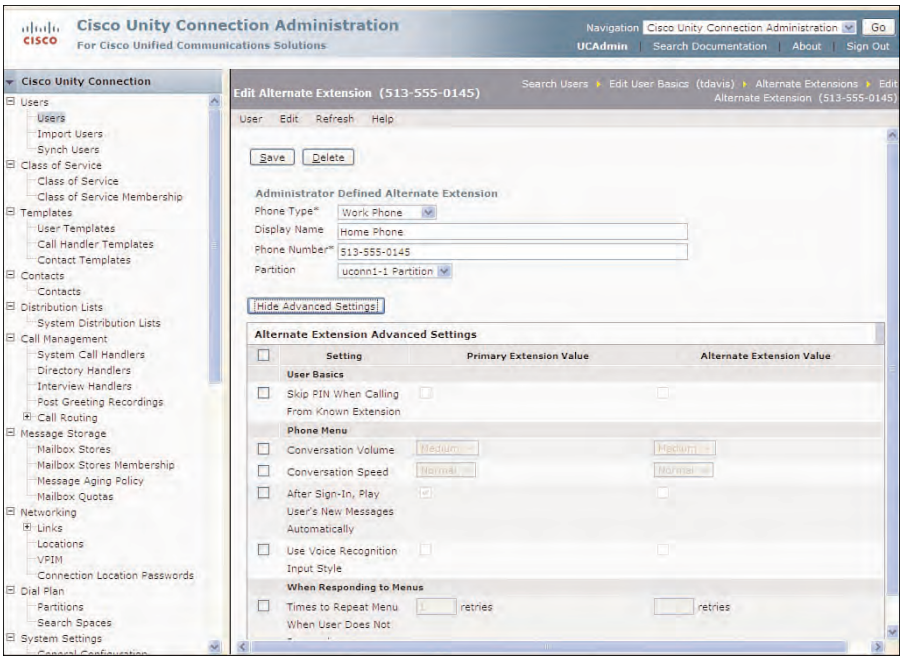

Figure 6-7 *Edit Alternate Extension Page*

After the alternative extensions are configured, the Alternate Extension page enables the administrator to view both the administrator and user defined alternative extensions, as shown in Figure 6-8.

After users access their voice messages, they have the ability to delete, save, or forward these messages to other users or distribution lists. This is accomplished with the use of the various options selected from the keypad. In some cases, an organization might want to customize these options or use a keypad mapping that matches their existing system. The Phone Menu provides these configuration features.

Phone Menu Options

Administrators have the ability to adapt the user experience when accessing voice messaging from their phone. Some users might need to use the voice recognition feature to address messages, rather than the phone keypad. Still other users might require a different key stoke combination that reflects what they performed previously with their older,

www.it-ebooks.info

legacy voicemail system, even though you might be implementing Unity Connection as a dual integration with a legacy VM System, which you plan to remove at a later date.

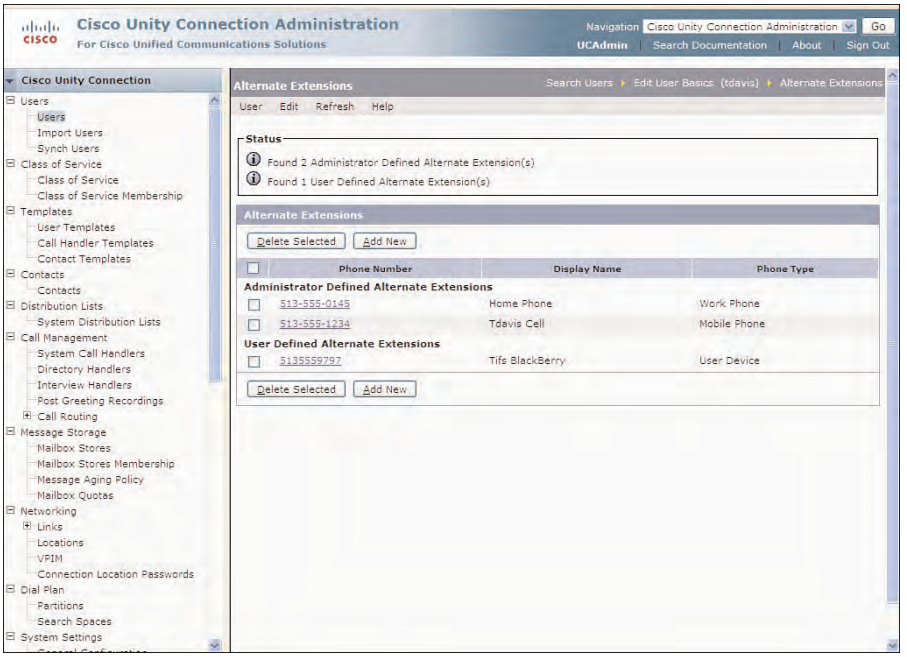

Figure 6-8 *Configured Administrator and User-Defined Alternate Extensions*

Whatever the reason, the entire user experience can be customized through the Phone Menu features from the time the user logs in to Cisco Unity Connection via their phone. The options include the following:

- **Phone Menus:** Controls menu style, volume, and speed the menus are played back to the user.
- **Time Format:** Selectable time format in 12-hour or 24-hour clock.
- **Conversation Style:** Enables the selection of alternative and custom keypad mappings, and the standard classic conversation (default) used by Cisco voice-messaging products. The Optional and Alternate include keypad mappings that mimic Avaya Octel Aria, Serenade, Audix, or Nortel Meridian Mail voice-messaging systems. This feature enables users to more easily adapt to new Cisco Unity Connection without having to learn a new series of the keypad command, thereby leveraging the users' existing knowledge.
- **Voice Recognition:** The user can also be enabled to use voice recognition from this option. By default, this feature is disabled.

www.it-ebooks.info

- **Message Locator:** This feature enables users to search for messages from specific callers by extension or phone number. If configured, users can also be enabled to use the Phone View feature, which enables them to view and select messages through the Cisco IP Phone integrated with Cisco Unified CM.
- **Menu Responses:** Enables the administrator to configure various key press and voice recognition timings.
- **After Sign-In:** Enables the administrator to customize the users' experience after they sign-in to their mailbox. The recorded name, alternative greeting, and new messages can be enabled from this section.
- **After Exiting:** Enables the administrator to customize the users' experience as they exit the email conversation. Exiting out of voicemail is accomplished by the user selecting the * key. By default, the user is directed to the Opening Greeting call handler. However, this option can be configured to direct the user to any system call, directory, or interview handler, and a specific user, conversation, or call action.

To review and edit the Phone Menu options for a specific user, from the Edit User Basics page, select **Edit > Phone Menu** to display the Phone Menu page, as shown in Figure 6-9.

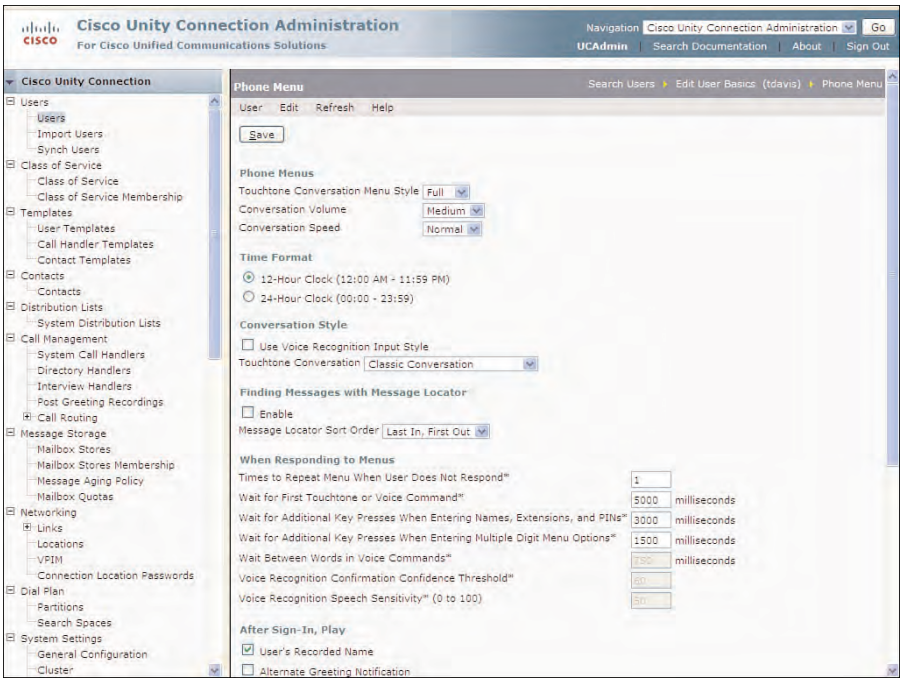

Figure 6-9 *Phone Menu Options Page*

www.it-ebooks.info

Message Settings Options

A number of different options affect the messages settings. These are configured within four different pages selected from the Edit User Basics page:

- Message Settings
- Message Actions
- Playback Message Settings
- Send Message Settings

The following sections explain these options in further detail.

Message Settings

The Message Setting options configure the various options and customize the experience of the caller in the process of leaving a voicemail for the user. These configurations determine the maximum message length, whether the callers can edit messages, mark the message urgency and security, and what the callers' experience will be after the recording is complete. By default, the caller hears the goodbye message followed by a call termination. However, this can be customized to send the caller to any specific call handler.

To review and customize the Message Settings, from the Edit User Basics page, select **Edit > Message Settings** to display the Edit Message Settings page, as shown in Figure 6-10.

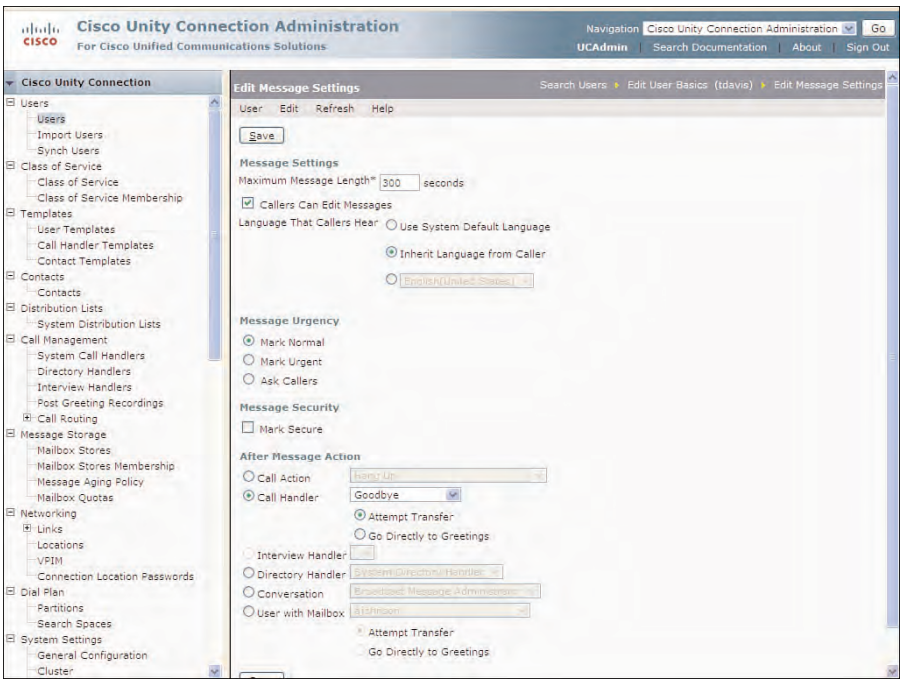

Figure 6-10 *Edit Message Settings Configuration*

www.it-ebooks.info

Message Actions

The Message Actions option enables the administrator to configure the specific mailbox to either Accept, Reject, or Relay messages to an SMTP address. The default is to accept all messages. However, this could be configured separately depending on the message type consisting of voicemail, email, fax, or delivery receipts.

To review or modify the Message Actions, from the Edit User Basics page, select **Edit > Message Actions**, as shown in Figure 6-11.

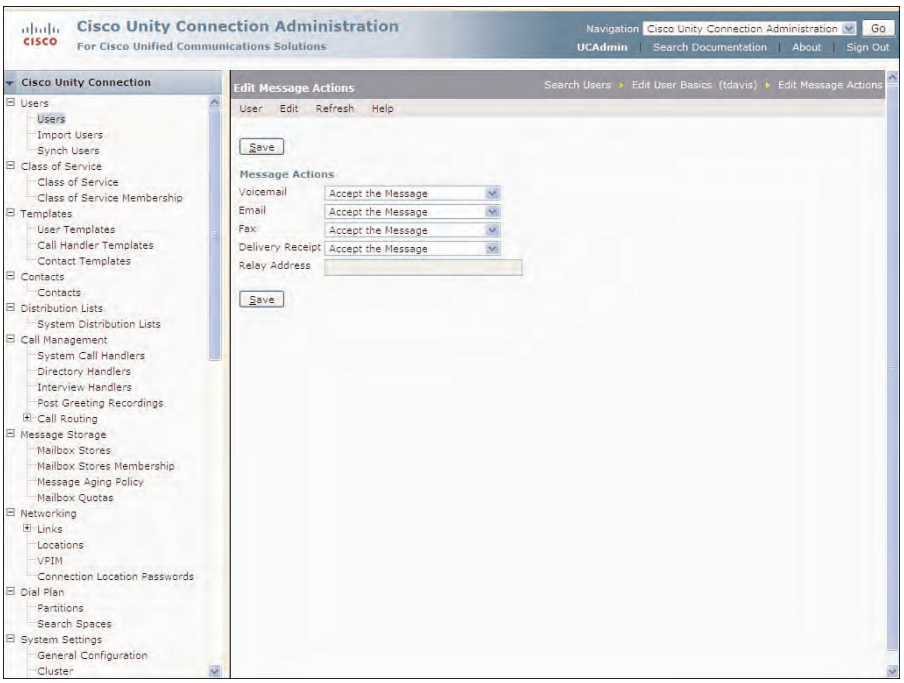

Figure 6-11 *Edit Message Actions Configuration*

Playback Message Settings

The Playback Message Settings affect the users' experience when they retrieve and listen to their messages. From this page, the playback of messages can be configured to adjust the volume and speed of the playback; to provide envelope information about the sender information, time the message was sent, and message counts—and fast forward and rewind options. Also, the message play order can be changed from the default of playing urgent messages and the newest first.

To select the playback message settings, from the Edit User Basics page, select **Edit > Playback Message Settings**, as shown in Figure 6-12.

www.it-ebooks.info

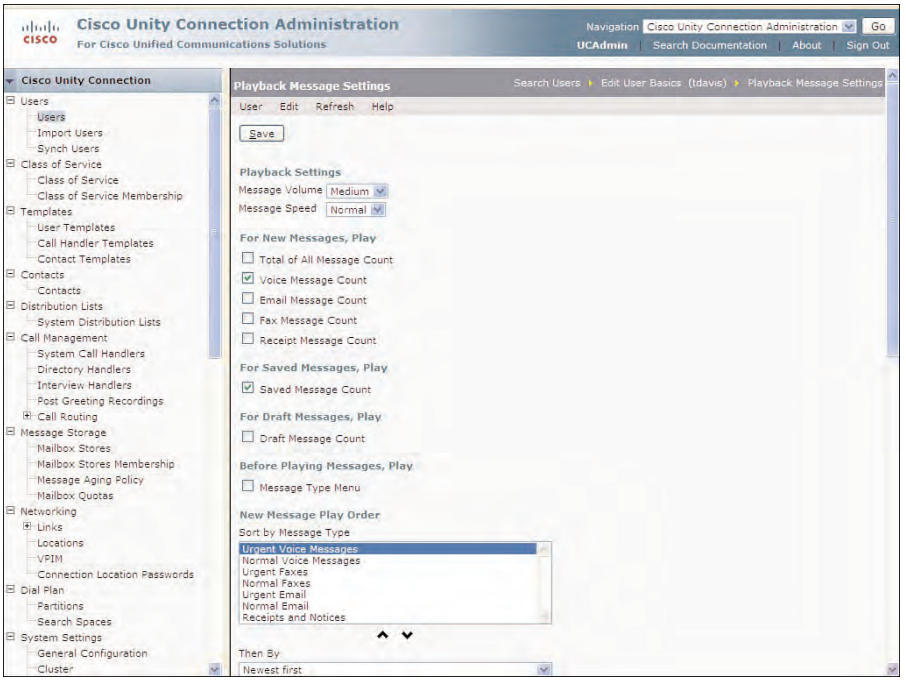

Figure 6-12 *Playback Message Settings Configuration Page*

Send Message Settings

The final page that affects messages is the Send Message Settings page. This page enables the administrator to configure options for the users when they send or forward messages directly from Cisco Unity Connection. The Send Message Settings options include the capability to enable users to send and update broadcast messages, and specify how messages are addressed and sent.

Broadcast message is a useful feature for management and support administration to notify all users of company information or system maintenance issues and schedules. Broadcast messages are sent to all users configured with a mailbox on the server. Broadcast messages can be scheduled for a later time or sent immediately through the use of the broadcast administrator feature. Users that receive a broadcast message must listen to the message in their entirety before all other messages. Also, the MWI light is not lit specifically for this type of message to avoid sending MWI message to all phones.

Distribution lists can also be used to send a message to a group of users. In this case, a dispatch message is sent to each member of the list, in contrast to the broadcast message stored once and all mailboxes point to the single message. A distribution list creates a copy of the message (a dispatch message) for every member, which will have a much larger impact on drive space and message storage.

To review and modify the Send Message Settings, from the Edit User Basics page, select **Edit > Send Message Settings**, as shown in Figure 6-13.

www.it-ebooks.info

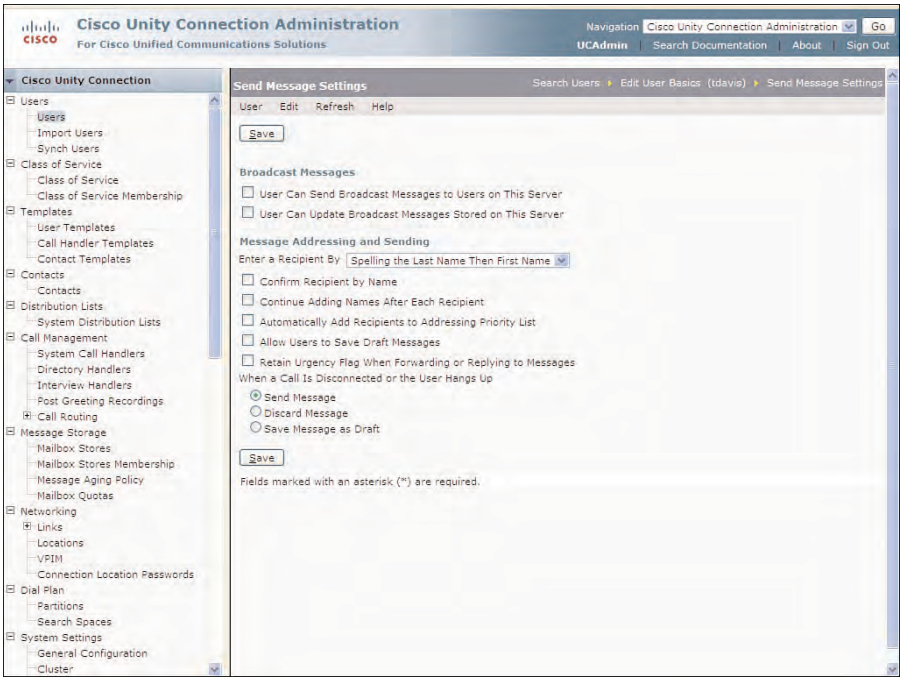

Figure 6-13 *Send Message Settings Configuration Page*

Web Application Access to Voice Messaging

In some organizations, the user's phone might be the most common method used to send and retrieve the voice messages; however, this can vary between organizations. The use of web and mobile applications might possibly be the most prevalent method from which users perform their basic voice-messaging functions. Web applications can include Messaging Inbox, Really Simple Syndication (RSS) web pages, and various Internet Message Access Protocol (IMAP) clients including ViewMail for Outlook. In either case, a user can authenticate to Cisco Unity Connection using the Web Application password. If the system has been integrated with Lightweight Directory Access Protocol (LDAP), the authentication will be performed to the LDAP server. However, if LDAP integration is not configured, the authentication will be performed directly on Cisco Unity Connection using the Web Application password that was configured for that specific user. In this section, you discover the various applications and their configuration that can be used to perform voice-messaging function in Cisco Unity Connection.

Personal Communications Assistant

Personal Communications Assistant (PCA) is a series of tools and web pages integrated in Cisco Unity Connection to provide the user with a number of customizable options and features. These features are divided into three specific web pages:

www.it-ebooks.info

- **Messaging Inbox:** Provides a web-based application for users to send, receive, and forward voice messages from their voice mailbox.
- **Messaging Assistant:** Enables the users to implement a number of customizable features and options in their voicemail.
- **Connection Personal Call Transfer Rules:** Enables users to customize their transfer settings based on the caller or callers.

Users' access to these features is controlled by their CoS membership. Using the CoS, the administrator has the ability to allow or disallow each feature as required. Figure 6-14 illustrates the CoS configured to allow the users access to these applications.

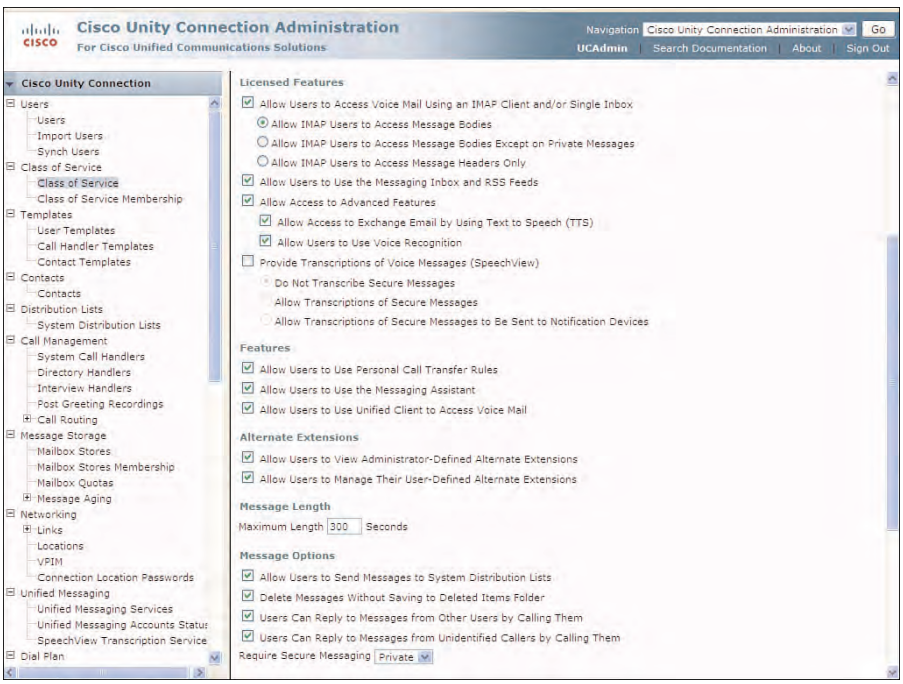

Figure 6-14 *CoS to Provide User Access to Cisco PCA*

The Cisco Unity Connection user is allowed access to the PCA features with the options selected, as follows:

- Allow Users to Use the Messaging Inbox and RSS Feeds
- Allow Users to Use Personal Call Transfer Rules
- Allow Users to Use the Messaging Assistant

www.it-ebooks.info

After the users are provided with access to PCA by their CoS, they need to use their browser to access the PCA website integrated in Cisco Unity Connection. This URL is as follows:

https://ip_address_publisher/ciscopca

The IP address is mentioned as the IP address of the publisher, although using the IP address of the subscriber server of a cluster pair can also work properly. However, it has been mentioned previously that best practices dictate that web and client traffic should be directed to the publisher server. The Personal Communication Assistant web page displays, enabling the users to sign-in using their alias and Web application password, as shown in Figure 6-15.

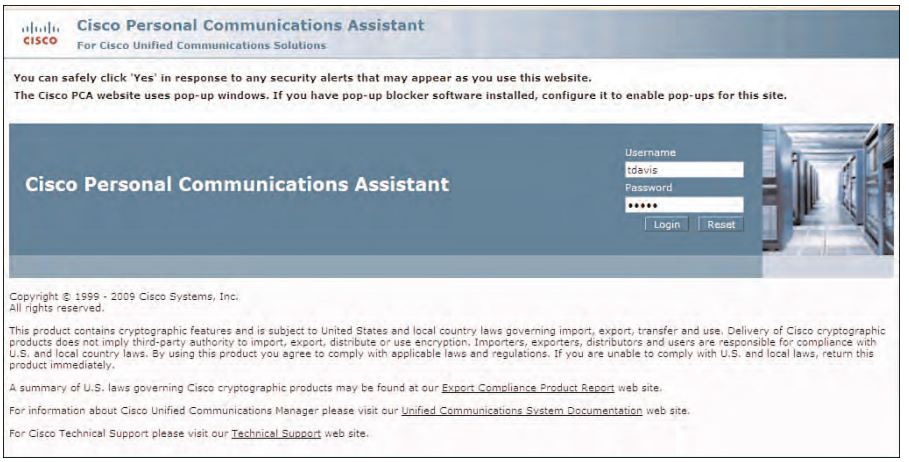

Figure 6-15 *Personal Communications Assistant*

After the users have logged in to PCA, they are presented with the various options, including the Messaging Assistant, Messaging Inbox, and Personal Call Transfer Rules, as shown in Figure 6-16.

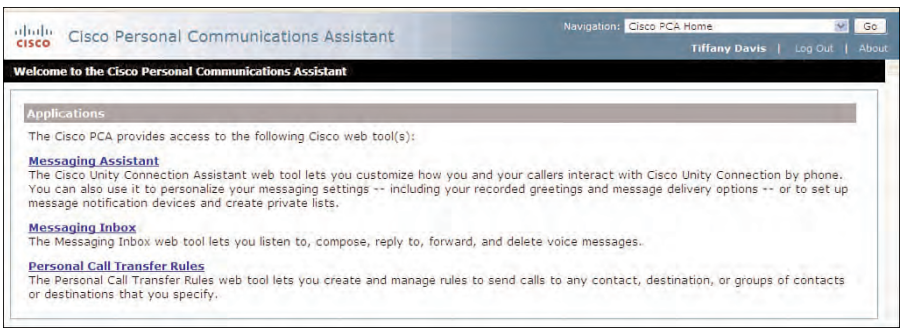

Figure 6-16 *Applications Page of Cisco Personal Communications Assistant*

www.it-ebooks.info

Introduction to Messaging Inbox

Selecting the Messaging Inbox provides a web-based application enabling the users to send, retrieve, delete, and forward messages directly from their mailbox, as displayed in Figure 6-17. Licensing requirements provide access to the maximum concurrent users allowed to use the Messaging Inbox. When using a cluster pair, it is advisable that all web-based applications be directed to the publisher server, whereas phone applications primarily access the subscriber server for optimum performance.

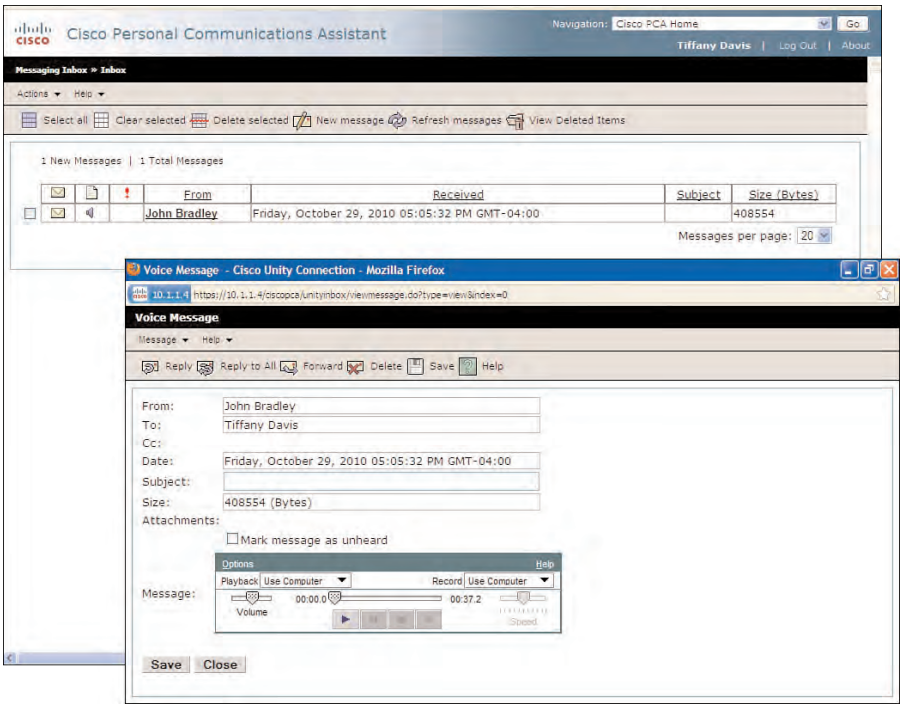

Figure 6-17 *Messaging Inbox*

As Figure 6-17 shows, the user has the options to select playback from the computer or the phone. Using the phone for playback can require a port on the server configured for Telephony Record and Playback (TRaP) to provide this function. When there are a significant number of users using this application, high port activity can occur. Therefore, best practice dictates enforcing the download of messages to the computer and uses the PC speakers for playback operation. This is especially important for remote users, or where bandwidth limitations exist. The default option is for PCA to play the message while downloading, which can result in choppy audio and undesirable results.

To optimize the Messaging Inbox for these cases, select the New Message icon in the Messaging Inbox application. Then, from the **Options** drop-down on the toolbar of the Media Master, select **Playback & Recording** to display the Playback & Recording Setting pane, as shown in Figure 6-18. To optimize the playback and recording features,

www.it-ebooks.info

select **Use Computer for both** Playback Device **and** Recording Device. Also, select the **Download Complete Message Before Playing** radio button, and click **OK**.

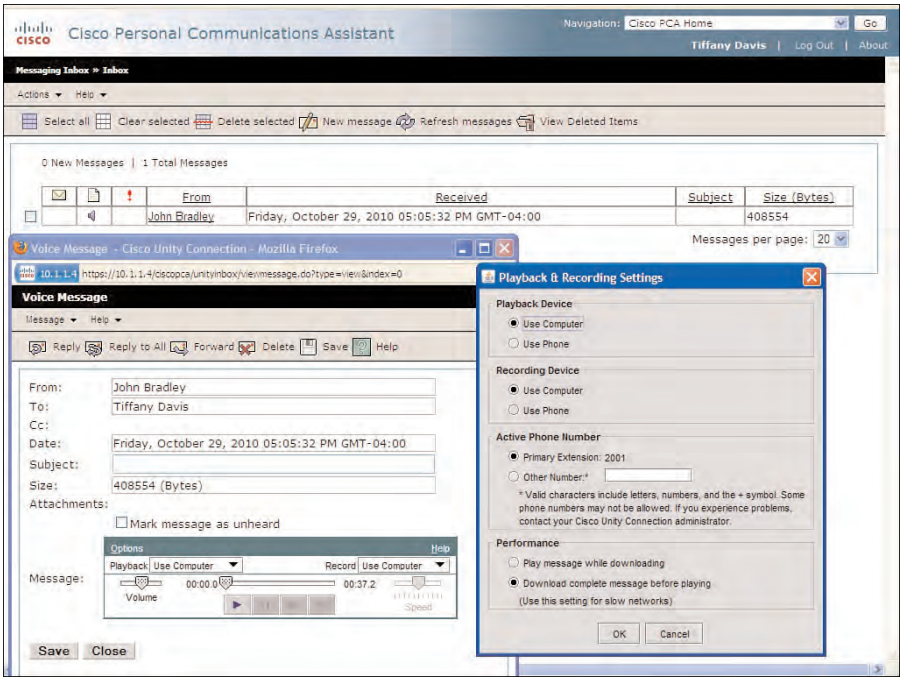

Figure 6-18 *Playback and Recording Settings Optimized for Bandwidth Performance*

Introduction to the Messaging Assistant

The Messaging Assistant can be accessed from the Navigation drop-down on the upper-right portion of the PCA home page; then, click **Go**. Figure 6-19 shows the Messaging Assistant personal options page. Users now have the options to configure alternative spellings for their name and rerecord their name. The alternative name option is convenient for users who are known by a different name, nickname, maiden name, or have a difficult spelling in their actual name. In this way, the user can be reached from directories or through name spelling using any of the configured alternative names. Also, as discussed earlier, for the alternative devices, if the CoS enables this feature, the user can view the administrator configured alternative devices and manage and configure additional alternative devices as needed. Finally, the users can be allowed to make the choice to be listed in the directory, if their CoS enables.

Additionally, the user also has the ability to configure passwords, greetings, notification devices (if using message notification), contacts, and private lists. The private lists are discussed later in this section. Private lists are similar to distribution lists but only available to the specific user.

www.it-ebooks.info

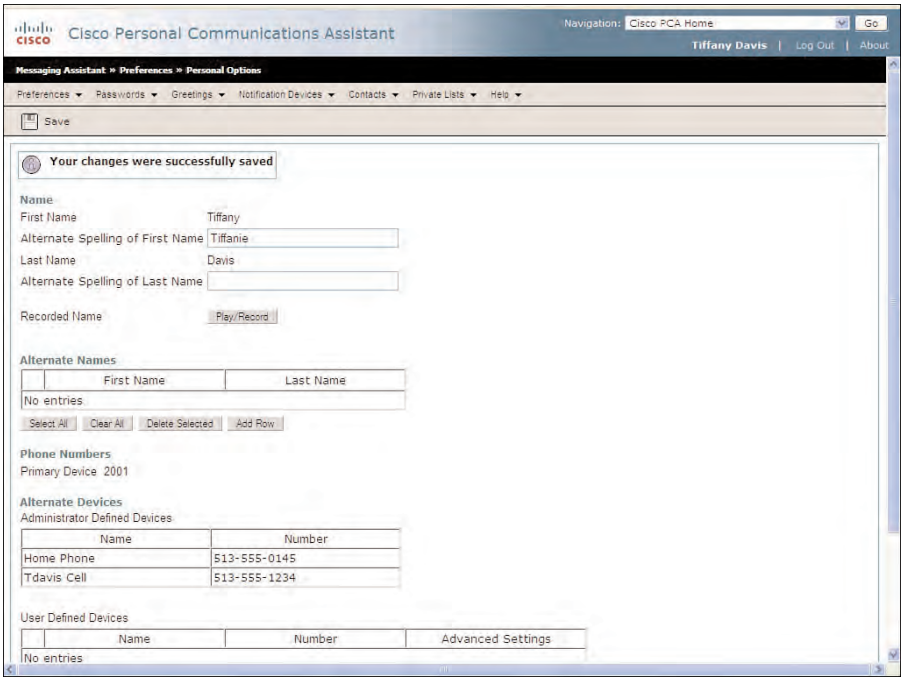

Figure 6-19 *Messaging Assistant*

Introduction to Connection Personal Call Transfer Rules

The final option that users can access within PCA is the Connection Personal Call Transfer Rules. By default, the basic transfer rules are applies as discussed in the transfer rule pages. To enable the Connection Personal Call Transfer Rules, the administrator needs to perform this function for the user under the **Edit > Transfer Rules** pages. Optionally, the users must perform this function under the Messaging Assistant by select **Preferences > Transfer & Screening** and then selecting the specific transfer rule. The options on the transfer rule needs to be enabled to **Apply Personal Call Transfer Rules**, as shown in Figure 6-20.

Finally, from the Navigation drop-down, select **Connection Personal Call Transfer Rules** and click **Go**. The Connection Personal Call Transfer Rules page displays, as shown in Figure 6-21. From this page, the user can create a number of rule sets having one or more rules based on the caller, caller group, phone number, or source and then direct these callers to voicemail, or transfer to a specific location based on the time of day or schedule. Rules can be prioritized or disabled within a specific rule set as wanted.

www.it-ebooks.info

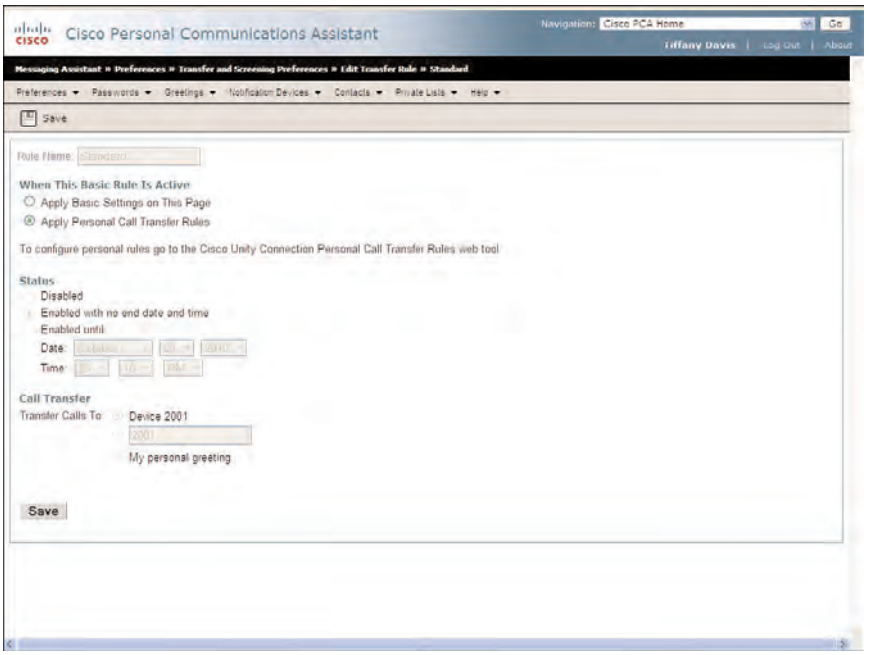

Figure 6-20 *Messaging Assistant: Personal Call Transfer Rule Configuration*

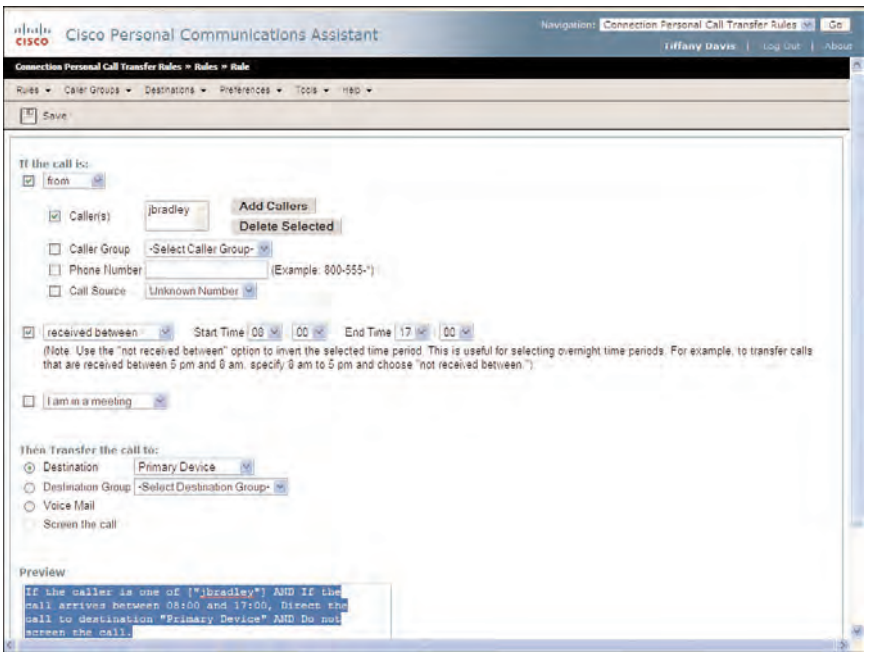

Figure 6-21 *Connection Personal Call Transfer Rules*

www.it-ebooks.info

In this example, a specific rule is configured that directs calls from jbradley to the user's primary device. The Preview displays the results of the rule as follows:

```
If the caller is one of ["jbradley"] AND If the call arrives
 between 08:00 and 17:00, Direct the call to destination "Primary
 Device" AND Do not screen the call.
```

Using Really Simple Syndication (RSS) Feeds for Voice Messaging

Along with using the Messaging Inbox to send and retrieve messages, users have an additional method to access voice messaging. This method is achieved by accessing voice messaging through RSS feeds.

RSS readers are web-based software programs that enable users to receive new and updated information from various RSS feeds to which they subscribe. The publisher of the RSS feeds updates the information, and it is immediately available to the subscribing device, or RSS feed reader. Because RSS is web-based, most browsers, such as Internet Explorer version 7 and above, Firefox, and others can be used as RSS readers to access RSS feeds information.

With Cisco Unity Connection, RSS feeds provide the convenience of receiving voice messages directly to a feed reader without checking for new messages. Also, RSS enables the receiving and updating of voice messages to mobility devices as needed.

The RSS service is enabled by default at the time of installation and can be stopped or restarted under the Optional Services section in the Service Management of Cisco Unity Connection Serviceability. However, before users can access the RSS feeds for their account, they must have a CoS that provides access to this feature. The RSS option is located under the Licensed Features section within their specific CoS. The option for **Allow Users to Use the Messaging Inbox and RSS Feeds** must be checked, as previously shown in Figure 6-14.

To begin using the RSS reader, the users must access the following link from their browser or reader and enter their username and web application password:

https://*ip_address_of_publisher***/cisco-unity-rss/rss.do**

As mentioned earlier, the IP address used could be the subscriber server of a cluster pair; however, best practices dictate that web and client traffic should be directed to the publisher server.

If using Internet Explorer to access the voice-messaging RSS feeds, the messages will be displayed, as shown in Figure 6-22. The users are also presented with a link to subscribe to this feed to receive updates of voice messages to their feed reader as wanted.

Cisco Unity Connection enables RSS feeds using secure connections by default. This feature can be changed in the System Settings to provide RSS feeds using nonsecure connections; although this is not advisable because authentication credentials are then sent in clear text. The author discourages this option for this reason. However, some RSS readers do not support secure connections, and if these readers are required in your organization,

www.it-ebooks.info

nonsecure connections must be allowed. Be advised that when you select this option, all RSS connections to Cisco Unity Connection must now be nonsecure, meaning that secure connections are not possible.

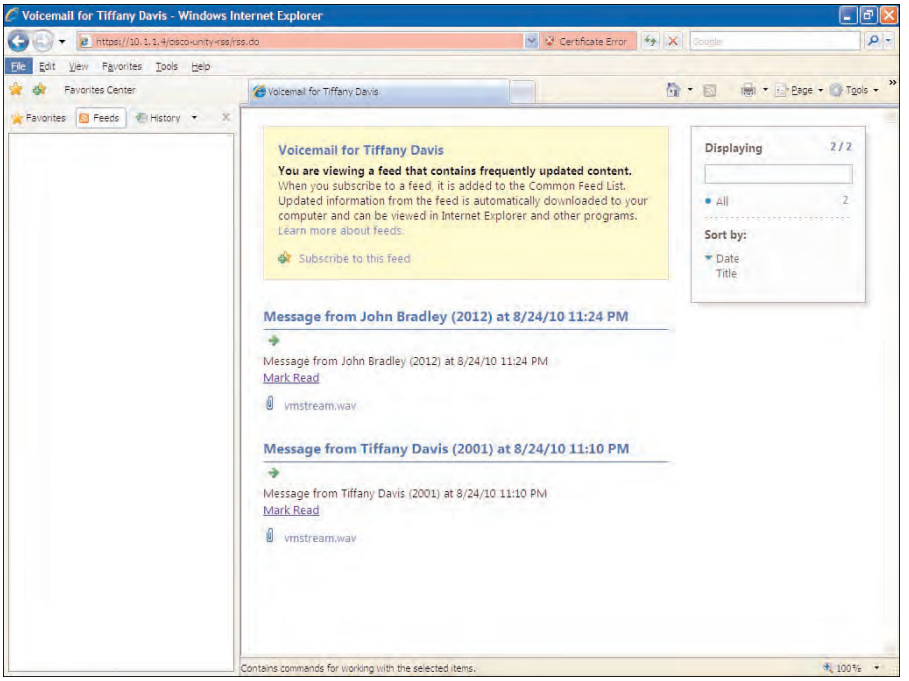

Figure 6-22 *RSS Feeds for Cisco Unity Connection Voice Messaging*

To configure nonsecure RSS feeds, select **System Settings > Advanced > RSS** to display the RSS Configuration page. Then, select the check box to **Allow Insecure RSS Connections** and click **Save**, as shown in Figure 6-23. Users can no longer access the RSS feeds using an SSL connection and must use the following URL:

https://*ip_address_of_publisher***/cisco-unity-rss/rss.do**

RSS feeds are an effective way for users to access their voice messages when traveling or via mobile devices equipped with RSS feed capabilities. However, user must be aware of a number of limitations when using this method to retrieve voice messages. For instance, RSS provides access to only the last 20 messages and cannot include broadcast messages. Users can listen to their voice messages via the PC speakers, but messages cannot be deleted, only marked as read. Finally, private, secure, and dispatch messages cannot be access by RSS feeds. Dispatch messages are voice messages sent to a distribution list for which the user is a member. The user has the ability to either accept, decline, or postpone the message for a later time or another member.

www.it-ebooks.info

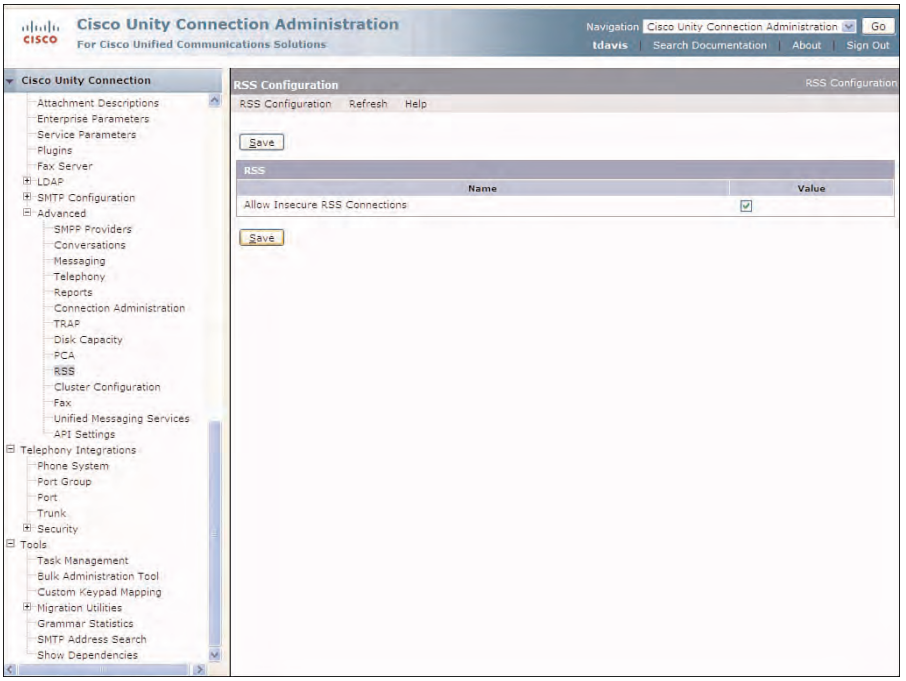

Figure 6-23 *RSS Configuration Page in Cisco Unity Connection Administration*

The use and access to voice messaging using RSS feeds depends on the security policy of the organization. Some security policies disallow web access to the voice-messaging server; therefore, this feature is not an option.

IMAP Client Using Outlook

Using an IMAP client is one of the most popular and efficient methods that users can access their voice methods. IMAP is supported in Microsoft Outlook, which many users are already familiar with, therefore minimizing the learning curve on this technology and leveraging their current knowledge. The convenience afforded by Outlook enables users to access email and voice in two separate Inboxes using the single application.

ViewMail for Outlook is a client plug-in for the Outlook application that enables users to listen and send their voice messages directly from Outlook. Users using Outlook as an IMAP client to listen to voice messages need to download and install this application on their workstation. This is easily accomplished by downloading the latest ViewMail for Outlook (VMO) application from the URL:

http://tools.cisco.com/support/downloads

A valid Cisco.com login is required to access this website and complete this procedure. Select the option to download the applications, as shown in Figure 6-24.

www.it-ebooks.info

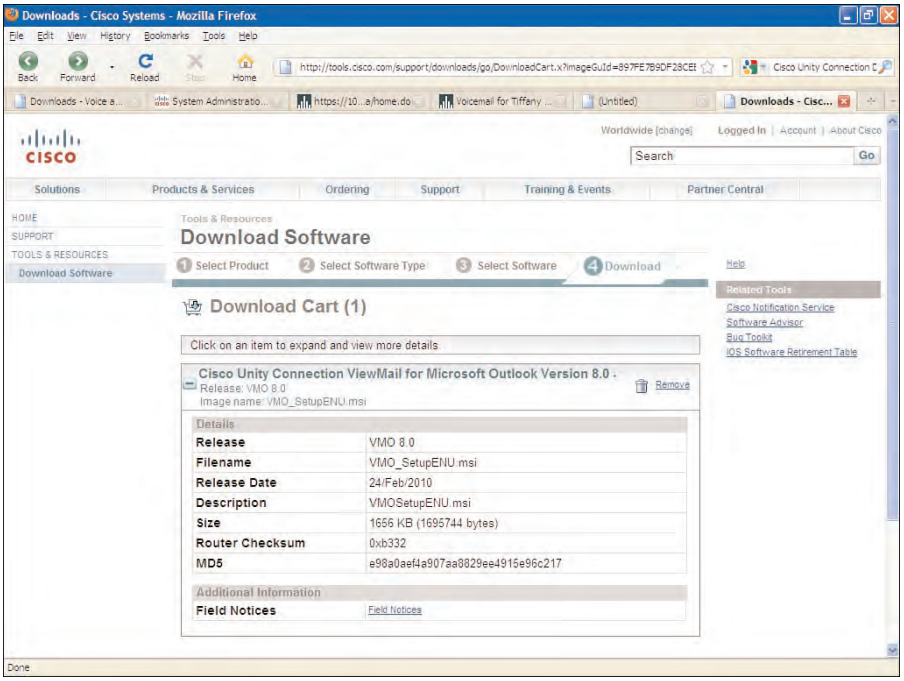

Figure 6-24 *Download ViewMail for Outlook Page*

You are prompted for the login credentials and asked to accept the software download agreement before the download can begin. If you complete this download procedure from the workstations from which you will be using Outlook, choose the **Run** option on the pop-up prompt to either Run or Save the download file. You need to ensure that the Outlook application is closed before installing the ViewMail application.

If you choose the **Save** option to download the file, select the executable file to install the application on the workstation, answering each of the various questions. ViewMail is a plug-in application for Outlook, so no application will be presented or displayed after the installation completes successfully. The ViewMail application can now be part of the Outlook application as is verified in the next task.

After the ViewMail application is installed, open Outlook and select the **Help** option from the toolbar. The **ViewMail Help** and **About** options should be visible and the various ViewMail options under the **Tools** drop-down. This is your indication that ViewMail for Outlook has been properly installed.

Before configuring the IMAP client in Outlook, the users must be allowed access via the IMAP client through their CoS membership. The CoS options must have the **Allow Users to Access Voice Mail Using an IMAP Client** option selected under the Licensed Features in their CoS (refer to Figure 6-14). Also, under this option the administrator has the ability to select what messages are displayed or disallowed, all messages, private, or only the message headers. In the later case, the user needs to retrieve the actual message using the

www.it-ebooks.info

phone access to voice messaging in Cisco Unity Connection. At this point, the users are now ready to configure their Outlook client for IMAP.

For Microsoft Outlook 2007, begin the configuration of the IMAP client by selecting **Tools > Account Settings > New** from the Outlook toolbar. Then, select the option for Microsoft Exchange, POP3, IMAP, or HTTP and click **Next**. On the Add New E-mail Account page, select the **Manually Configure Server Setting or Additional Server Types** check box and click **Next**, followed by **Next** to select the default of Internet E-mail. Finally, on the Internet E-mail Settings page, enter the required user information and credentials, as shown in Figure 6-25. Enter the credentials for the desired user along with the web application password, and click **Next** when all options have been properly configured. Finally, click **Finish** on the final wizard page to complete the IMAP account configuration.

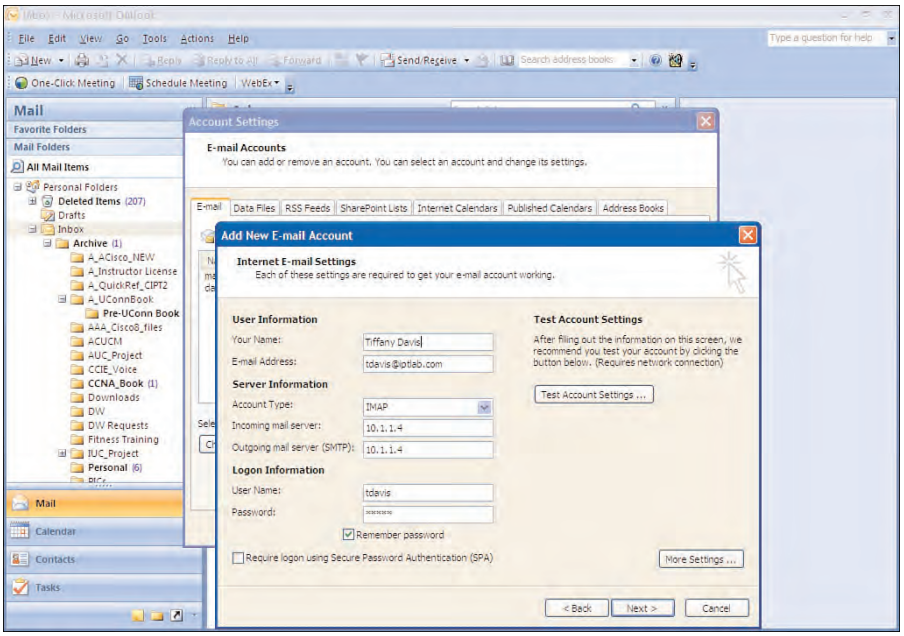

Figure 6-25 *IMAP Account Configuration in Microsoft Outlook 2007*

For the Server Information section, you want to ensure that the Account Type is IMAP and that the Incoming and Outgoing mail server are configured as the Cisco Unity Connection servers' IP address. When using a cluster pair, ensure that the publisher server is selected for this option because best practices dictate that all web applications should be directed to the publisher for voice messaging.

For Microsoft Outlook 2003, begin the configuration of the IMAP client by selecting **Tools > E-mail Accounts** from the Outlook toolbar. Then, select the option to **Add a**

www.it-ebooks.info

New E-Mail Account and click **Next**. On the E-mail Account page, select the **IMAP** radio button and click **Next**. On the Internet E-mail Settings (IMAP) page, enter the required user information and credentials, as shown in Figure 6-26, as previously described and select **Next**. Finally, select **Finish** on the final wizard page to complete the IMAP account configuration.

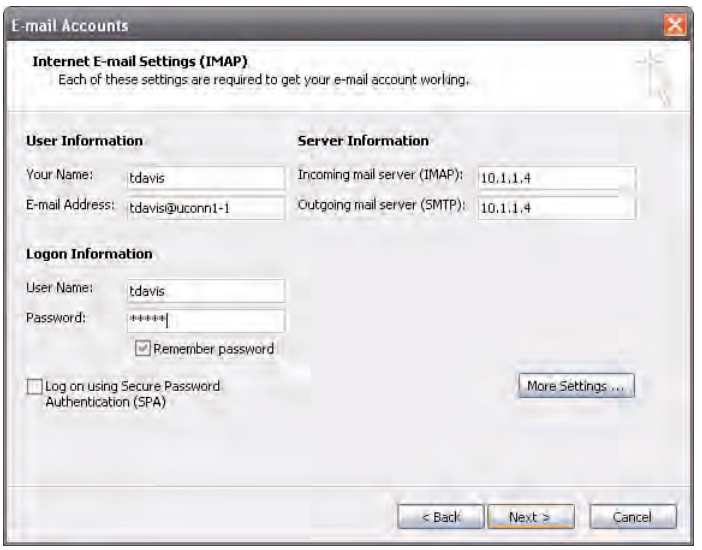

Figure 6-26 *IMAP Account Configuration in Microsoft Outlook 2003*

After the installation is complete, the users now have access to both their email and voicemails within the same Outlook application, but in different Inbox locations, as shown in Figure 6-27. You might want to change the name of the Inbox to a more descriptive option, such as Messages or Voicemail to assist the user.

If a voicemail is selected, the Media Master form is presented as part of the voice message enabling the user to listen, record, and forward messages directly from the Outlook client. This is the function and features included with the ViewMail application. Figure 6-28 shows a voice message with the Media Master form.

Phone View and Visual Voicemail

Two additional methods can be used by users to view, send, forward, and retrieve their voice messages using their IP phones: Phone View and Visual Voicemail, both of which require Cisco Unity Connection to be integrated with Cisco Unified CM and require Cisco IP Phones.

www.it-ebooks.info

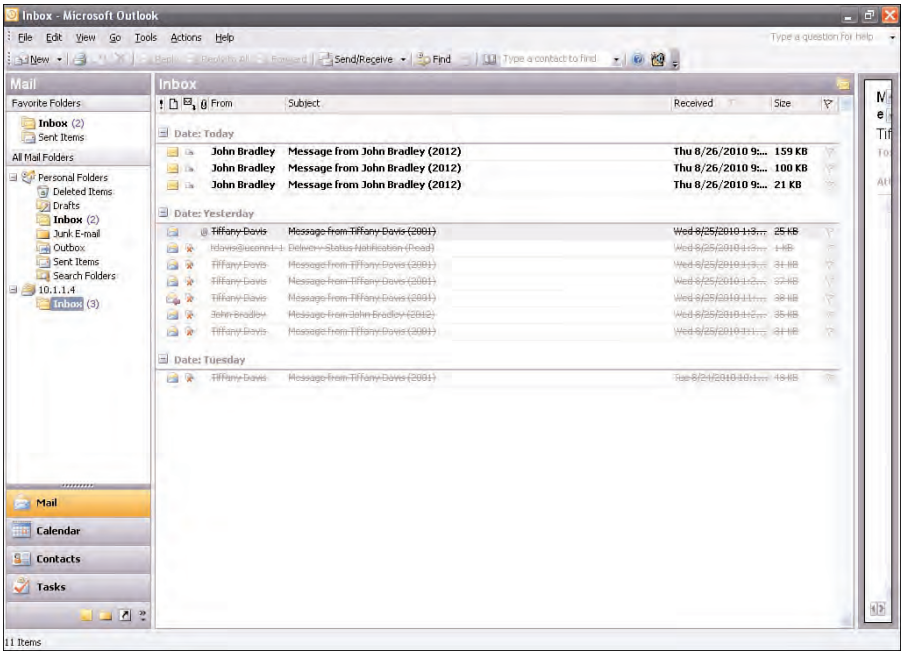

Figure 6-27 *Microsoft Outlook 2003 with Configured IMAP Account*

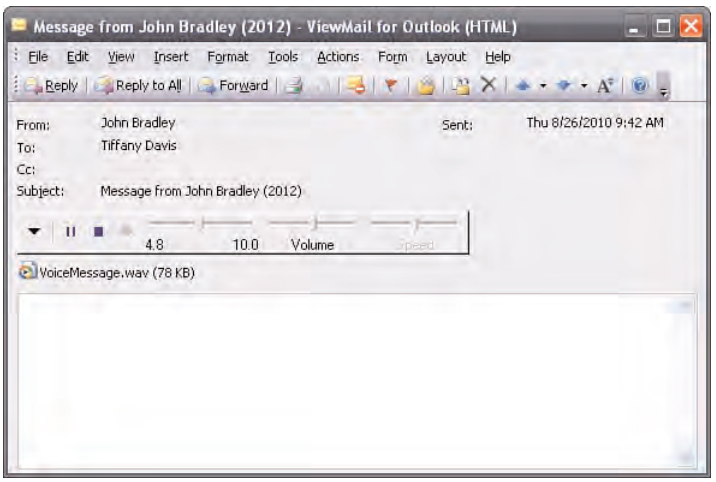

Figure 6-28 *Voice Message Using ViewMail for Outlook*

www.it-ebooks.info

Phone View requires an application user to be configured in Cisco Unified CM that is configured to control a specific supported IP Phone. Users can view and select their phone messages on the phone display after they have dialed in to Cisco Unity Connection. Users can view the messages from their phone or another supported phone on the system.

Visual Voicemail provides more management of voice messaging, enabling users to not only play and delete messages, but also to select softkey options to mark messages, forward, increase/decrease speed, or provide a number of various messaging editing features. Visual Voicemail runs as a Java Midlet service from the Messages button on the IP Phone. Therefore, the user is not required to dial into Cisco Unity Connection to retrieve the envelope information of voice messages. A port is used only when the user selects the option to play messages. These options, and the extensive features provided by Visual Voicemail, make it a more effective tool for viewing and playing message on the IP phone. Both applications are explored in the following sections.

Phone View

Phone View is the older of these supported applications for viewing voice messages on the IP Phone with integrations with Cisco Unified CM. This feature has a number of limitations, where the user must be configured for this feature, the integration, and an application user on Cisco Unified CM. The Cisco 7911 phone is not supported for the Phone View application.

Three steps are required for the configuration of Phone View:

Step 1. Configure the application user and credentials for the Standard CTI user group.

Step 2. Configure Cisco Unity Connection integration for Phone View.

Step 3. Configure the users to provide Phone View access to voice messages.

The configuration details of Cisco Unified CM must be explored first, which require the configuration of an application user. This step requires the administrator to access Cisco Unified CM Administration and select **User Management > Application User**. Select the **Add New** button and create a new user. Enter a unique User ID, password, and the credential policy must be created with the following option unchecked: User Must Change at Next Login.

Finally, all phones that use the Phone View applications must be associated with this application user, as shown in Figure 6-29. Associate the user with the Standard CCM Admin user groups, and click **Save** to complete the application user configuration in Cisco Unified Communications Manager Administration.

Next, you must configure the integration for Cisco Unity Connection to enable for Phone View by using the previously configured application user credentials.

From the Cisco Unity Connection Administration navigation pane, select **Telephony Integrations > Phone System**, and select the name of the phone system associated with the Cisco Unified CM integration. Under the Phone View Settings section, select the

www.it-ebooks.info

Enable Phone View check box, and enter the application user credentials that were created for the application user in the previous step. This is selected in Cisco Unified CM Administration for the CTI Phone Access Username and Password fields, as shown in Figure 6-30. Click **Save** when all options are complete.

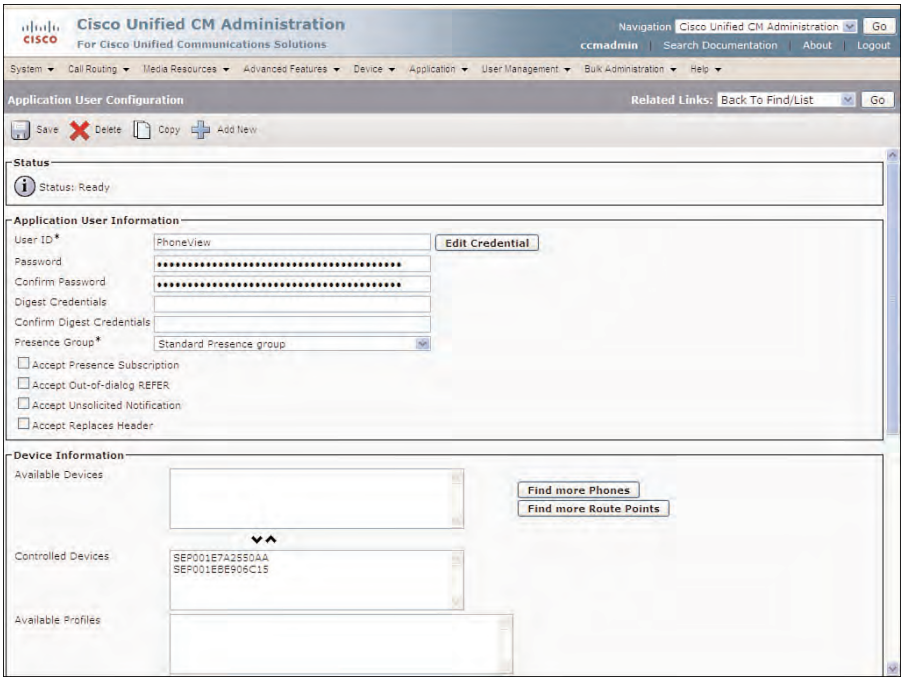

Figure 6-29 *Application User Configuration for Phone View in Cisco Unified CM*

Finally, each user account needs to be enabled for Phone View. To complete this final step, select **Users > Users** from Cisco Unity Connection Administration, and select the user that should be enabled for Phone View. Then, from the Edit Users Basics toolbar, select **Edit > Phone Menu**. The Phone Menu page displays. Under the Finding Messages with Message Locator section, check the **Enable** and **Enable Phone View** check boxes, as shown in Figure 6-31. The message locator feature is required for phone view and therefore must be enabled before Phone View can be configured. Click **Save** to complete the configuration of Phone View in Cisco Unity Connection Administration.

When the user logs in to voicemail, a message states the number of current messages followed by "Searching" indicating that the Phone View feature is retrieving messages to be displayed. After messages display, the user can view the envelope information and select specific users for message retrieval, where they can listen, delete, and forward each specific message as wanted.

www.it-ebooks.info

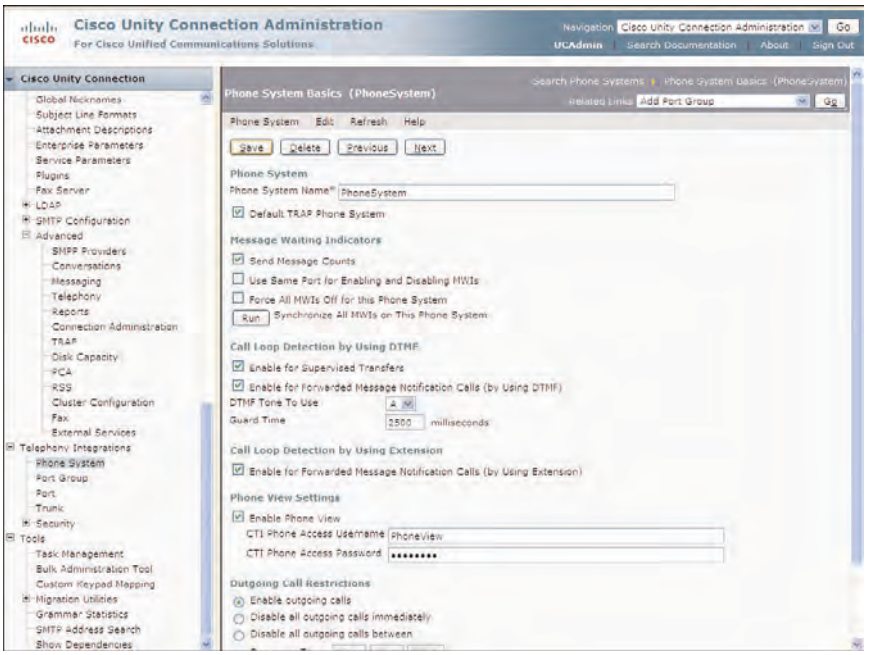

Figure 6-30 *Phone System Integration Configuration for Phone View*

Figure 6-31 *Phone Menu Options to Configure Phone View for Users*

www.it-ebooks.info

Visual Voicemail extends this capability by enabling the user to not only review envelope information on the phone, but also to mark, forward, delete, and compose new messages directly from this application on the phone. A port is used only when the user chooses to play new messages. Therefore, the port utilization is the same as using the phone to retrieve messages.

Visual Voicemail

Visual Voicemail runs as a messaging phone service on Cisco Unified Communications Manager integrated with Cisco Unity Connection as a Reverse Trap connection to Cisco Unity Connection. Before beginning to configure the Visual Voicemail service, you must ensure that your version of Cisco Unified Communications Manager supports the Visual Voicemail feature.

To configure Visual Voicemail, complete the following steps:

Step 1. Configure a Visual Voicemail pilot in Cisco Unified Communications Manager Administration.

Step 2. Configure Connection Administrator options in Cisco Unity Connection.

Step 3. Configure Direct Routing Rules for Reverse Trap.

Step 4. Configure the Visual Voicemail Services in Cisco Unity Connection Administration.

Step 5. Subscribe phones to use the Visual Voicemail application.

Step 1: Configure a Visual Voicemail Pilot in Cisco Unified Communications Manager Administration

To begin, you need to log in to Cisco Unified Communications Manager Administration and select **Call Routing > Route/Hunt > Hunt Pilot**. Click **Add New** to create a new hunt pilot number. This number will be referred to as the Visual Voicemail pilot. This pilot number will be used specifically for the Visual Voicemail integration with Cisco Unity Connection. Select the same hunt list from the Hunt List drop-down that was used for the integration with Cisco Unity Connection, as shown in Figure 6-32. In this example, **2880** was chosen as a unique number for the Visual Voicemail pilot, configured to use hunt list **VM_rl**. This is the same hunt list used in the integration to Cisco Unity Connection. However, the voicemail hunt pilot number is 2990. The other options in this display are beyond the scope of this book.

To test this new hunt pilot, call the Visual Voicemail pilot from any IP phone. You should hear the same Cisco Unity Connection prompts as if you pressed the Messages button on your phone, or called the voicemail pilot directly from the keypad.

Step 2: Connection Administration Configuration for Visual Voicemail

Cisco Unity Connection must be configured to provide the Visual Voicemail feature and use the voicemail and Visual Voicemail pilot numbers configured in Cisco Unified CM.

www.it-ebooks.info

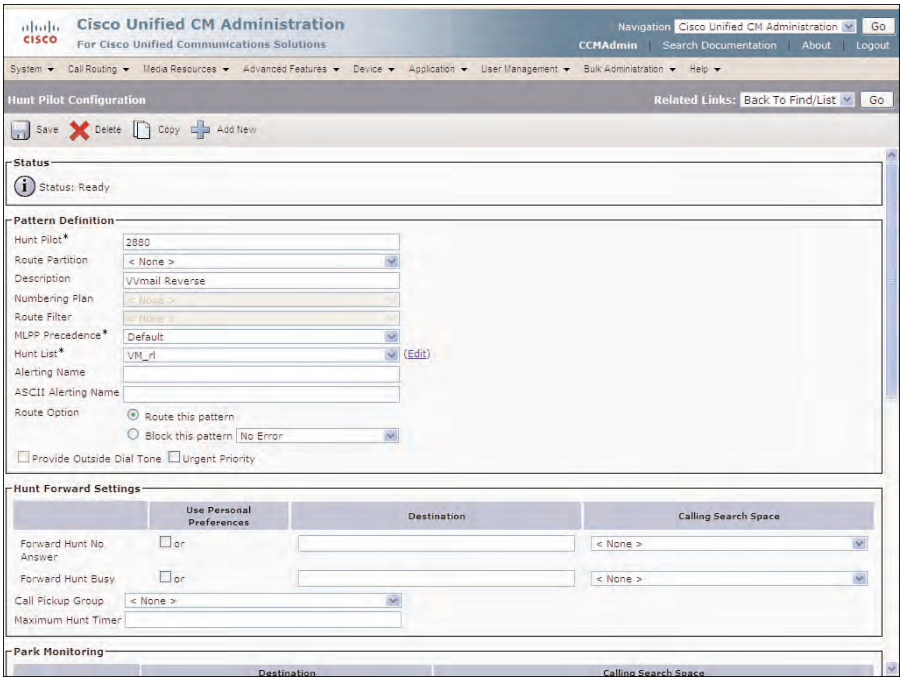

Figure 6-32 *Hunt Pilot Configuration for Visual Voicemail*

In Cisco Unity Connection Administration, select **System Settings > Advanced > Connection Administration**. The Connection Administration displays. Enter the following configuration options, and click **Save**, as shown in Figure 6-33:

- **Applications Can Cache the Cisco Unity Connection Password:** Select this option if want users to be allowed to be kept signed in (optional).
- **Voice Mail Web Services: Session Timeout (in Seconds):** 300
- **Voice Mail Web Services: Pilot Number for Voice Mail:** <Voicemail pilot number>
- **Voice Mail Web Services: Pilot Number for TRAP Connections:** <Visual Voicemail pilot number>

Step 3: Configure Direct Routing Rules for Visual Voicemail

The direct routing rules must now be configured to send direct calls from the Visual Voicemail pilot to the Reverse Trap conversation. In Cisco Unity Connection Administration, select **Call Management > Call Routing > Direct Routing Rules**. Click **Add New** and enter a name for the new rule. Click **Save**.

www.it-ebooks.info

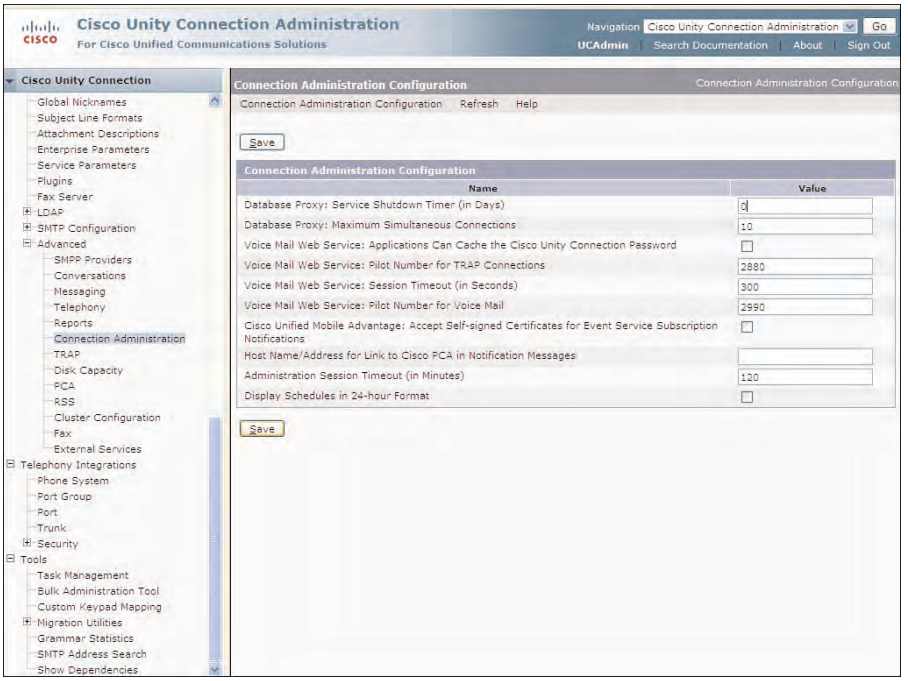

Figure 6-33 *Connection Administration Configuration for Visual Voicemail*

For the new direct routing rule, click **Add New** in the Routing Rule Conditions section. Create a new routing rule condition for direct calls based on the dialed number equal to the Visual Voicemail pilot. Finally, select **Edit Direct Routing Rule** from the toolbar, and click the **Conversation** radio button. Then, select **Reverse Trap** from the conversation drop-down, and click **Save**, as shown in Figure 6-34.

At this point, you should test the Visual Voicemail pilot for the routing rule you created. To complete this testing, dial the Visual Voicemail pilot. You no longer hear the Cisco Unity Connection conversation; however, you hear silence followed by a disconnect. If this is not case, check the configuration on the previous steps to ensure that all configuration options were completed and properly saved.

Step 4: Configure the Visual Voicemail Service in Cisco Unified CM

Before beginning the services configuration in Cisco Unified CM, review the information in a couple Java files that Visual Voicemail uses to provide the application services. It was stated earlier that Visual Voicemail is configured to operate as a Java midlet. A *midlet* is an application that runs in a device and is managed by an application. Midlets use HTTP

www.it-ebooks.info

and HTTPS to provide network access for graphical interface control to these devices. In the case of Visual Voicemail, these Java midlets create the display on the IP Phone to display, compose, forward, and delete voice messages. The two files copied to the server at the time of installation, which are used by the Visual Voicemail service follows:

- VisualVoicemail.jad (A jad file type is a Java Application Descriptor file.)
- VisualVoicemail.jar (A jar file type is a Java Archive file.)

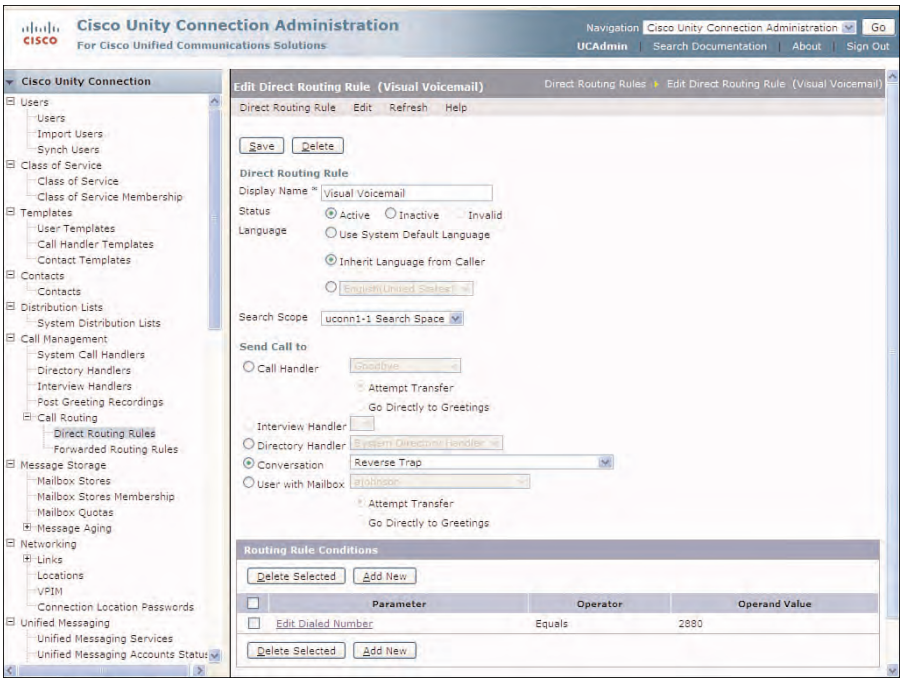

Figure 6-34 *Direct Routing Rules Configuration for Visual Voicemail*

You need to download the VisualVoicemail.jad file before you proceed with the configuration because the configured options need to agree with the details in this file. To complete this step, open a browser and enter in this URL:

http://*ip_address_of_CUCM_publisher_server***/midlets/VisualVoicemail/VisualVoicemail.jad**

When prompted to save this file, save this file to your workstation. This is a text-based file. Choose to open the file with Notepad or another text editor. The content of the VisualVoicemail.jad file displays, as in Figure 6-35.

To configure the Visual Voicemail service, you must first log in to Cisco Unified Communications Manager Administration. Select **Device > Device Settings > Phone**

www.it-ebooks.info

Services, and click **Add New** to add a new service. Enter the following parameters for the new phone service:

- **Service Name:** Enter the MIDlet-Name from the VisualVoicemail.jad file (This name must be exact for Visual Voicemail to function properly.)
- **ASCII Service Name:** Same entry as the Service Name.
- **Service URL:** Enter the URL as http://ip_address_of_publisher_server/midlets/VisualVoicemail/VisualVoicemail.jad.
- **Service Category:** Java MIDlet.
- **Service Type:** Messages.
- **Service Vendor:** Enter the MIDlet-Vendor from the VisualVoicemail.jad file.
- **Service Version:** <leave blank>.
- **Enable:** Selected.
- **Enterprise Subscription:** Unselected.

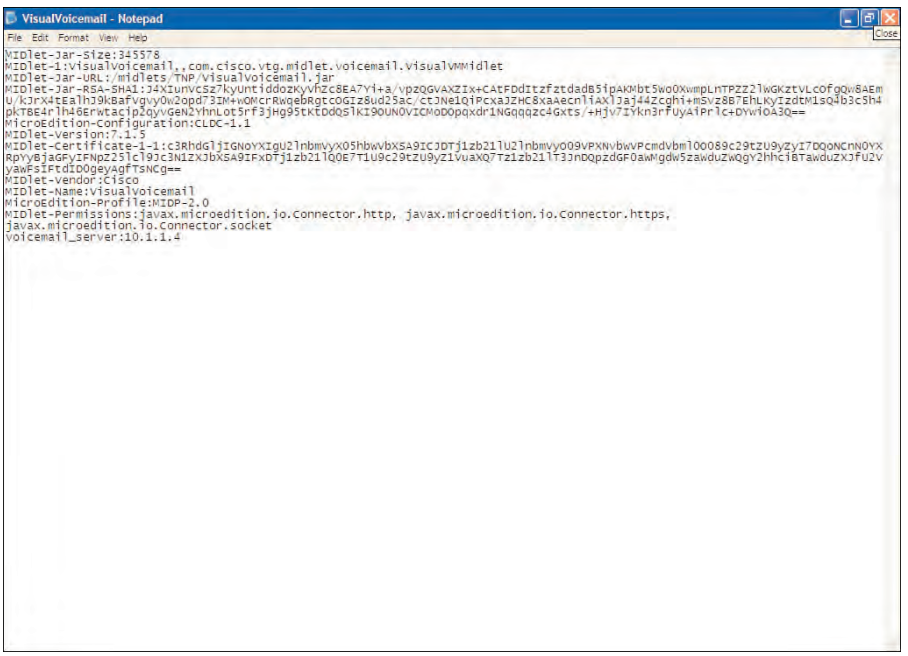

Figure 6-35 *VisualVoicemail.jad file*

Note If Enterprise Subscription is selected, you cannot enter the required options as described in the next steps.

www.it-ebooks.info

Click **Save** and **Add the New Parameters** to add three new parameters to this service as follows:

- **First Parameter Option - Cisco Unity Connection hostname configuration**
  - Parameter Name: voicemail_server
  - **Parameter Display Name:** <Enter a display name that relates to this parameter>
  - **Default Value:** <hostname_Cisco_Unity_Connection_publisher_server>
  - **Parameter Description:** <Enter a description of the parameter>
  - **Parameter Is Required:** Selected
  - **Parameter Is a Password:** Unselected

Note The Default Value parameter uses the hostname of Cisco Unity Connection to access the Visual Voicemail service. Therefore, you must have a Domain Name Service (DNS) accessible by the phones and configured for resolution of the Cisco Unity Connection hostname. Also, ensure that the domain name and DNS server options are configured for the DHCP scope of the phone using the Visual Voicemail feature. Otherwise, you get a server not available error when attempting the Sign-In operation. To review this option, select **Settings > Network Configuration** on the IP Phones.

- **Second Parameter Option**
  - **Parameter Name:** call_connect_delay
  - **Parameter Display Name:** <Enter a display name that relates to this parameter>
  - **Default Value:** 1000
  - **Parameter Description:** <Enter a description of the parameter>
  - **Parameter Is Required:** Selected
  - **Parameter Is a Password:** Unselected
- **Third Parameter Option**
  - **Parameter Name:** log_level
  - **Parameter Display Name:** <Enter a display name that relates to this parameter>
  - **Default Value:** info
  - **Parameter Description:** <Enter a description of the parameter>
  - **Parameter is Required:** Selected
  - **Parameter is a Password:** Unselected

www.it-ebooks.info

When all options are selected, click **Save** and review the options, as shown in Figure 6-36.

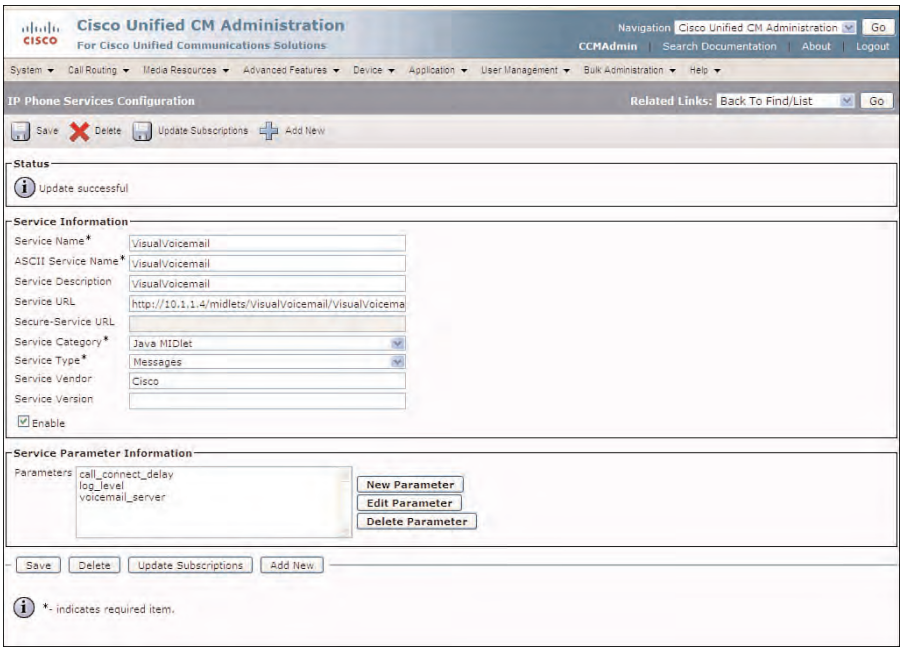

Figure 6-36 *Phone Service Configuration for Visual Voicemail*

Step 5: Subscribe to the Visual Voicemail Phone Service

The previous step used the Enterprise Subscription for the Visual Voicemail to provide this service to all phones; however, if you do not use this feature, this must be completed on each phone using the Visual Voicemail service. If using multiple phones, the Bulk Administration Tools can be used for ease of administration and convenience.

Select **Device > Phone** from Cisco Unified Communications Manager Administration. Click **Find**, and select the phone from the Device Name column that will use Visual Voicemail. Then, select the **Subscribe/Unsubscribe Services** from the Related Links drop-down, and click **Go**.

On the Subscribed Cisco IP Phone Services pop-up, select the **Visual Voicemail** service from the Select a Service drop-down, click **Next**, andt hen click **Subscribe**.

Finally, select the **Visual Voicemail** link from the Subscribed Services section. The options for this service display, as shown in Figure 6-37.

This completes the configuration of the IP Phone for Visual Voicemail. You will need to reset the phones and TFTP service for this service to be used by the phones.

www.it-ebooks.info

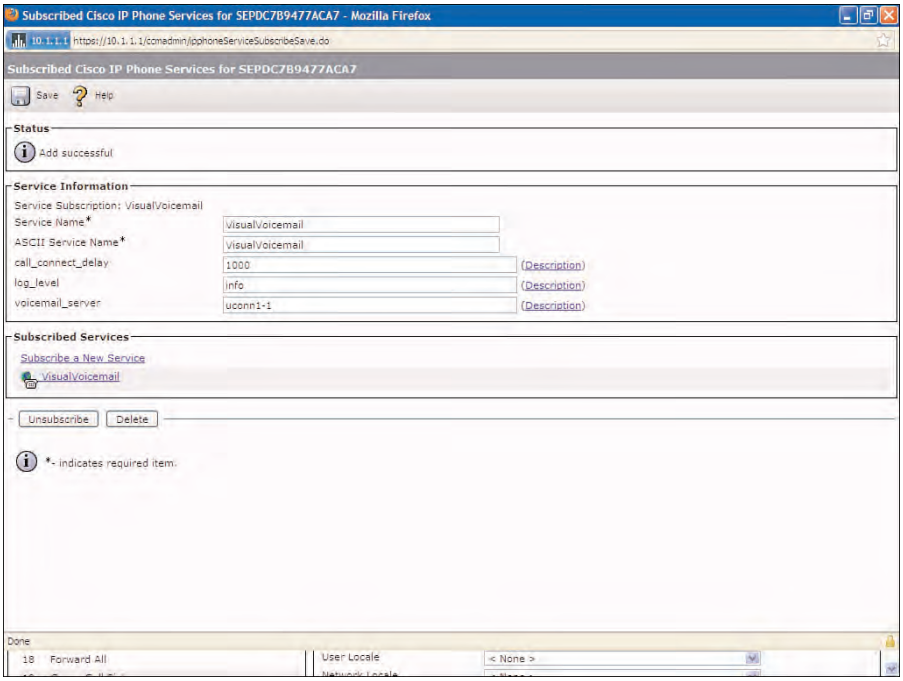

Figure 6-37 *Subscribing an IP Phone to Visual Voicemail*

After the phones reset, test the Visual Voicemail service by clicking the **Messages** button on the IP Phone. You have two options: Voicemail or Visual Voicemail. Select the Visual Voicemail service.

At this point, the Sign-In page on the phone will be presented, where the user's extension and password can be entered. This password is the Voicemail password configured for the user in Cisco Unity Connection Administration. After the credentials have been entered, press the **Sign-In** softkey. The mailbox of the user will immediately be presented for all voice messages in the users' mailbox. The user can now Play, Delete, Forward, Mark, Reply, or Compose, or change any specific options that apply to their mailbox using the Visual Voicemail service.

Mobility and Unified Communications

Mobility and Unified Communications have been growing areas of technologies, as the mobile workforces in many countries around the world continue to experience extensive growth. This growth has gives rise for application services to be reachable at multiple locations, even when they are not in their office. Along with this, more simplified tools are required to coordinate multiple applications from multiple devices to a single, effective mobile tool. This is where the power and growth of the mobile technology has focused and helped workers become more effective in their electronic workspace. A number of mobility devices and applications provide access and integration with Cisco Unity

www.it-ebooks.info

Connection. Two of these applications, Cisco Unified Personal Communicator and Cisco Unified Mobile Communicator extend mobility access to Cisco Unity Connection voice messaging.

Cisco Unified Personal Communicator is a desktop client that can be used to access a number of applications including voice messaging on Cisco Unity Connection and other various applications, including IM, voice, video, presence, and conferencing.

Cisco Unified Mobile Communicator (CUMC) can be deployed to enable users access to voice messaging using various mobile device. This implementation requires Cisco Unified Mobility Advantage (CUMA) Server to be configured on the network and integrated with Cisco Unity Connection to provide voice messages to Mobile Communicator devices. Figure 6-38 illustrates the integration of CUMA with Cisco Unity Connection.

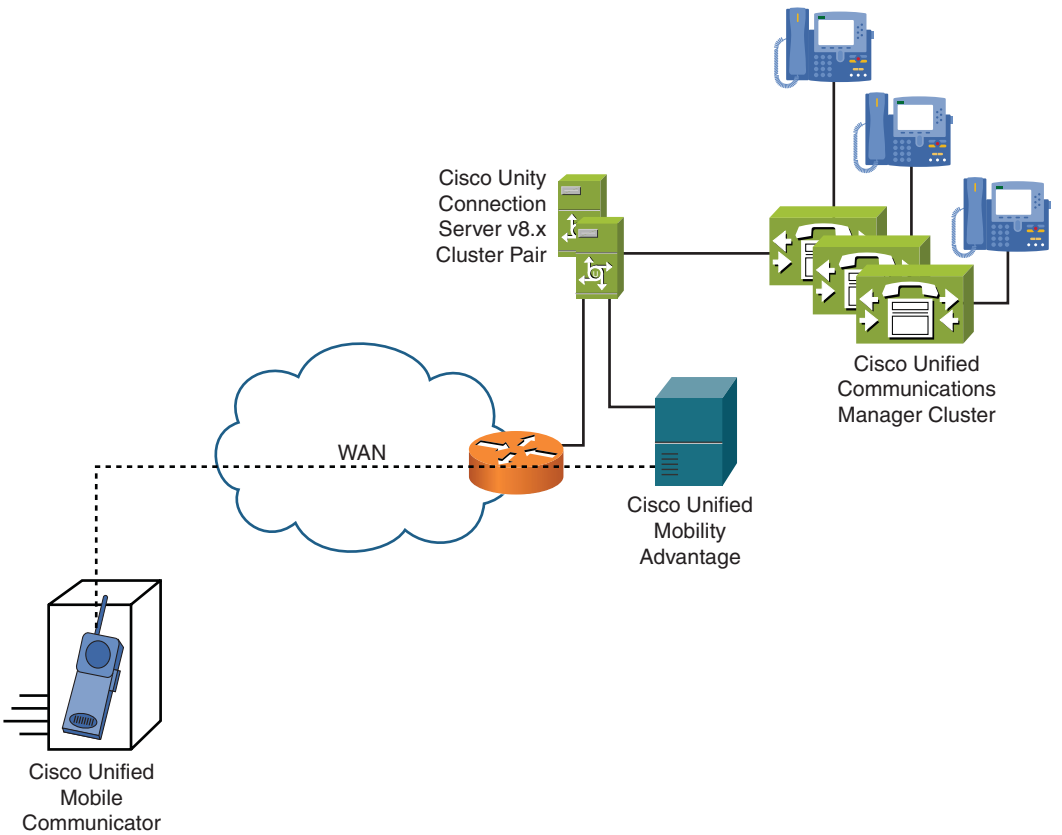

Figure 6-38 *Cisco Unified Mobility Advantage Integrated with Cisco Unity Connection*

This is accomplished in CUMA by creating a voicemail adapter on the CUMA server with the IMAP information for the Cisco Unity Connection server. CUMA does not support IMAP Idle for the connection to Cisco Unity Connection. Therefore, each Mobile device,

www.it-ebooks.info

using Mobile or Mobile Communicator counts as four connections. This must be taken into consideration for server sizing and design.

Finally, any users requiring access to their voice messaging with Mobile Communicator devices must be a member of a CoS that enables access to voice messaging using an IMAP client. Therefore, the **Allow Users to Access Voicemail Using an IMAP Client** option in the users' CoS must be selected.

A detailed discussion of the integration of these devices and applications is beyond the scope of this book.

Case Study: Mobility

Pegeram Corporation has 300 users at a remote location in the Southwest. One hundred and fifty of these users are agents located in the Service Center. These users are phone users only that use their IP Phones to retrieve messages. The remaining users use Outlook with ViewMail to retrieve messages. The IT management at the headquarters location is concerned about the bandwidth and server resources.

The solution that was chosen was to implement a cluster pair at the headquarters location and direct all Service Center phone traffic to the subscriber server and direct all IMAP clients to the publisher server.

Finally, all IMAP clients have been configured to use the workstations of the users for record and playback, and download the entire voice message to the workstation before playback. This solution reduces the resource utilization on the servers by sending all web traffic to the publisher server and phone traffic to the subscriber server. Also, the port utilization is reduced by enforcing the users' workstations to be used for playing voice message. Because bandwidth might be limited, the option was chosen to download the message before playing to ensure the quality of the playback.

The next chapter discusses the Cisco Unity Connection dial plan configuration, where partitions and search scopes allow or deny reachability to specific dialable objects, such as other users, distribution lists, and directories when dialing from Cisco Unity Connection.

Summary

This chapter provided an understanding of the various methods that users can access voice messaging in Cisco Unity Connection. These methods consist of their IP Phone, IMAP clients, Cisco Unity Inbox, Phone View, Visual Voicemail, and various mobility devices and applications. You learned how to

- Understand the purpose and configuration of setting up a users' voicemail for phone access.
- Describe the purpose, function, and features of Cisco Personal Communications Assistant and the various applications including the Messaging Inbox, Messaging Assistant, and Connection Personal Call Transfer Rules.

www.it-ebooks.info

- Configure Cisco Unity Connection for IMAP client configuration, including the installation procedures for ViewMail for Outlook and RSS configuration and support.
- Determine the different applications available for users to manage voice messaging directly on their IP Phone, including Phone View and Visual Voicemail.
- Understand the advantages, limitation, and configuration of Phone View and Visual Voicemail.
- Explore the function of various mobility applications that can be integrated with Cisco Unity Connection to provide access to voice messaging.

www.it-ebooks.info

This page intentionally left blank

www.it-ebooks.info

Chapter 7

Understanding User Features and Applications

This chapter covers the following subjects:

- **Mailbox Storage Settings and Administration:** Explore the administration and design of Cisco Unity Connection message storage, mailbox quotas, and message aging policies.
- **Greetings and Caller Input:** Understand the various greetings and caller input configuration that can be applied to a users' voicemail.
- **Message Notification:** Describe the features, function, and configuration of message notification in Cisco Unity Connection.
- **Alternative Extension Features and Restriction Tables:** Discover the function and purpose of alternative extensions and how they are automatically added. Understand restriction tables that disallow alternative extensions from being automatically added.
- **Distribution Lists - System and Private:** Explore the purposes, function, and configuration of both System and Private distribution lists.
- **External Service Accounts:** Discover the features and capabilities of Cisco Unity Connection to provide integrations with Microsoft 2003, 2007, Cisco Unified MeetingPlace, and MeetingPlace Express for contact and calendar integration.
- **Unified Messaging Service:** Understand the new Cisco Unity Connection version 8.5 feature for Exchange, MeetingPlace, and MeetingPlace Express.
- **SMTP Proxy Addresses:** Explore the purpose and configuration of SMTP Proxy Addresses for users' voicemail accounts.

Chapter 6, "Providing Users Access to Voice Messaging," discusses most of the user features that affect message sending and retrieval. However, a number of other features are available to users to increase their efficiency and productivity. Many of these features existed in earlier versions of Cisco Unity Connection, whereas others have been newly

www.it-ebooks.info

introduced in the latest release of version 8.x software. Not every option and feature are covered, rather, the focus of this chapter is on those features important to most users and organizations. In this chapter, you discover these features and applications, which consist of the following:

- Mailbox Storage Settings and Administration
- Greetings and Caller Input
- Message Notification
- Alternate Extension Features and Restriction Tables
- Distribution Lists - System and Private
- External Service Accounts
- SMTP Proxy Addresses

Understanding User Features

At the time of installation, the default mailbox store (mailstore) is created for the storage of voice messages and attachments. You can create and manage additional messages stores in Cisco Unity Connection Administration to ensure that disk space is used efficiently and system resources are maintained at optimum operational parameters. This chapter discusses message storage and system design in Cisco Unity Connection.

In most cases, users employ Cisco Unity Connection to send and retrieve voice messages between users. However, Cisco Unity Connection has many more capabilities that you can discover in the following pages that increase the options and features provided for these users.

Message Storage Settings and Administration

At the time of installation, the operating system and database installation creates a number of different storage areas on the server. By default, these storage areas function using their default configuration and do not require any changes and consist of the following:

- Database for system configurations
- Mailbox store for user voice-message storage
- Directory of voice messages

The system configuration, or directory database, contains all configuration and current operating parameters configured by the system administrator and users. This information also contains the configuration of the users in Cisco Unity Connection. However, the users' mailbox information is located in a separate location, the message store. This storage area contains information and location of all voice messages and envelope

www.it-ebooks.info

information (who the message is from, time and date, reason for message). This information also contains the specific location for the voice messages, located in a separate directory. These voice messages are stored as .WAV files in the voice-message directory according to the recording codec selected. The default recording codec is G.711uLaw discussed in Part One.

In Chapter 2, "Designing Voicemail Systems with Cisco Unity Connection," you learned that the Cisco Unity Connection server installation consisted of the Cisco Unity Connection application running the Linux operating system using the Informix database. This database consists of the database and message storage. As you investigate the structure of this database, you will further understand that the installation consists of a number of locations created for separate functionality. As shown in Figure 7-1, the Database and Message Store displayed contains the system configuration directory, the message store, and the voice-message directory.

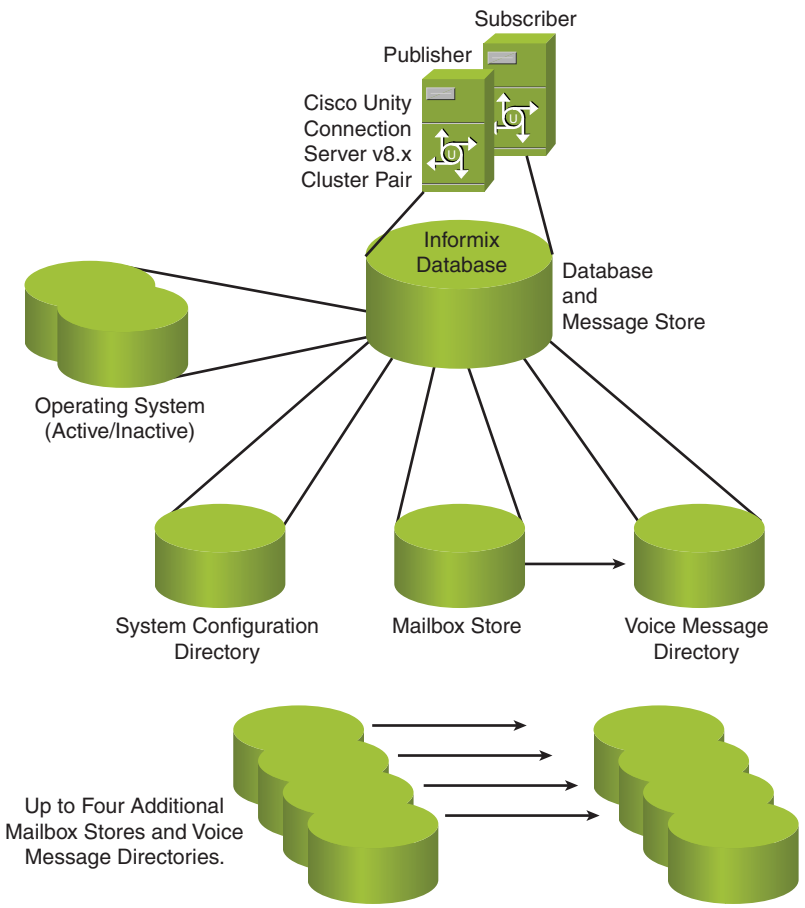

Figure 7-1 *Cisco Unity Connection Database and Message Store Design*

www.it-ebooks.info

System Configuration Directory

As you discovered in the discussion of upgrading the operating system in Chapter 3, "Installing and Upgrading Cisco Unity Connection," the database design consists of two partitions, an active and inactive partition. When you upgrade the operating system, the new software is installed on the inactive HEADFIRST partition. This assists the administrators in their procedures because the upload of the new operating system software can be complete on the current system without affecting current users and operating parameters. Later, the administrator can complete the switch version procedure, which completes the upgrade process by enabling the operating system installed in the inactive partition to now be operational. In this case, the inactive partition is now active, and the previously active partition is now inactive. There still exists a single database for system configuration information. The systems configuration database is configured by the operating system at the time of installation and cannot be changed. The key concept of the upgrade process is that anytime an upgrade is performed for the operating system, the software is always installed on the inactive partition.

Mailbox Store

A single mailbox store is created at the time of installation. The mailbox store is named **UnityMbxDb1**. These parameters are fixed at the time of installation; however, up to four additional message stores can be create by the administrator. Each of these message stores can contain up to 1.25 GB of message information and cannot be changed after the mailbox store is created. This size of message store can support approximately 10,000 users, however, depending on the amount of message storage. The actual voice messages contained in .WAV files are contained in a separate directory (the voice-message directory), which are also created at the time the new message store is created, as shown in Figure 7-1.

You might not need to create additional message stores, even though Cisco Unity Connection provides this feature. One reason to create an additional message store is because of the performance of backups. The backup utility, Disaster Recovery System, requires the backup to complete for the entire message store and its associated voice-message directory information. Therefore, it might be expedient to segregate users in separate message stores to ensure that backups are successfully completed during non-business hours. Separate backups could then be run on different message stores at different times.

Part III covers the Disaster Recovery System in detail. If separate backups are required for separate mailbox stores, the mailbox settings can be configured separately from the defaults. Users can be assigned to a mailbox store at the time they are created by the options on the Edit User Basics page, or through the options included in the User Template. Users created by the administrator can be moved from one mailbox store to another as required; however, the system default users created at the time of installation are located in the default mailbox and cannot be moved.

You can view and create mailbox stores in Cisco Unity Connection Administration. From the navigation pane on the left portion of the Cisco Unity Connection Administration

www.it-ebooks.info

page, select **Message Storage > Mailbox Stores.** The Search Mailbox Store page displays, as shown in Figure 7-2.

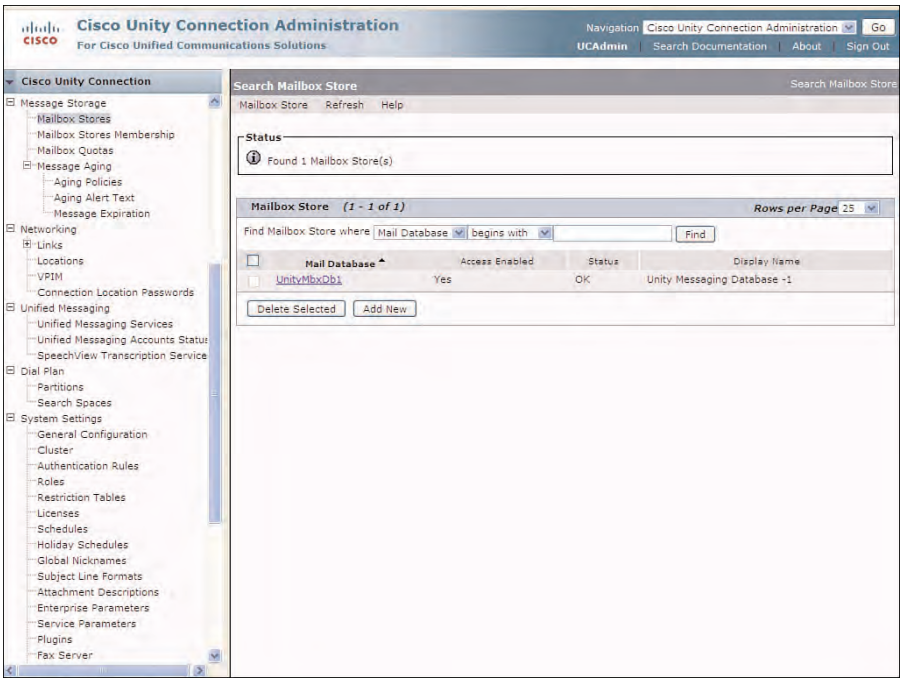

Figure 7-2 *Search Mailbox Store Page in Cisco Unity Connection Administration*

This mailbox is enabled and diagnostic status displays as **OK**. The actual name of the database is listed as **Unity Messaging Database -1**. This is the default database that includes all current and default users with mailboxes. To review the options of this message store, from the Mail Database column, select the **UnityMbxDb1** message store. The Edit Mailbox Store page displays, as shown in Figure 7-3.

This page shows that all options, with the exception of the display name, warning, and mounting of the mailbox store, are informational. This page includes the following:

- **Display Name:** Required name field describing the specific purpose or users included in this mailbox store. In the example, the default name is changed from Unity Messaging Database -1 to Corporate Users.
- **Mail Database:** The UnityMbxDb1 is the default message store and cannot be changed. This is the internal location of this database on the server that includes all system and default users.

www.it-ebooks.info

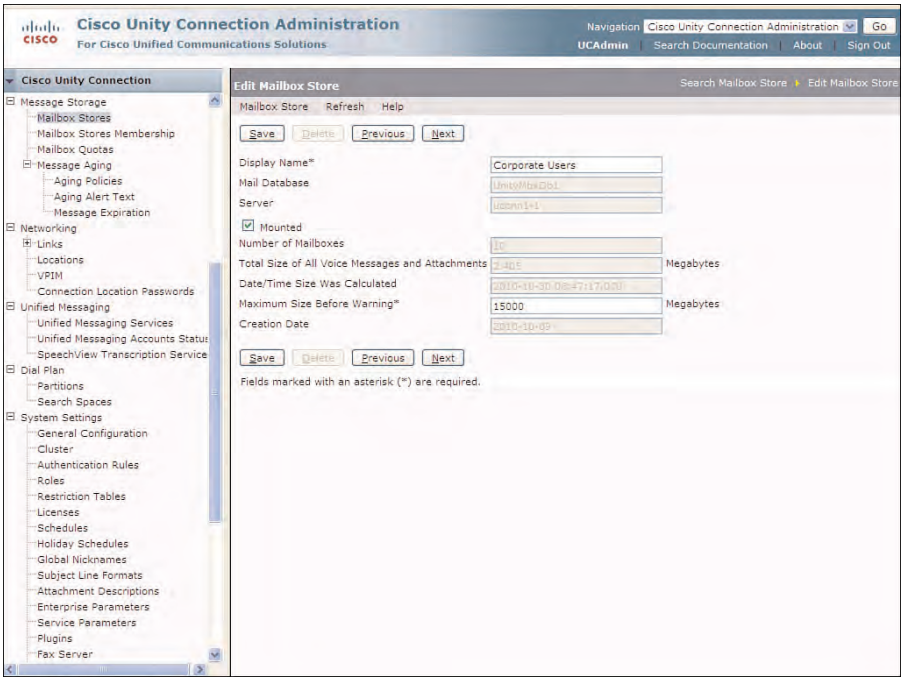

Figure 7-3 *Edit Mailbox Store for Default Message Store*

- **Server:** The server is the Cisco Unity Connection publisher server that hosts this mailbox store. This is important when using digital and VPIM networking, which are discussed in Part III.
- **Mounted:** When checked, this checkbox indicates that the message store is functioning properly, meaning that messages can be retrieved, sent, and forwarded. If unchecked, users cannot access their mailbox until the mailbox store is enabled. Messages left for users are queued until the message store is mounted.
- **Number of Mailboxes:** This field lists the current number of users with mailboxes assigned to this message store. In this case, seven users were created by the administrator and three default users, which are the undeliverablemessagesmailbox user, the operator, and the Unity Connection Messaging System.
- **Total Size of All Voice Messages and Attachments:** Total current size of the message store in megabytes. This can vary depending on the recording codec. G.711 is the default recording codec as discussed in Chapter 2. This codec yields the best recording quality but uses the most disk space.
- **Date/Time Size Was Calculated:** Date and time that the preceding calculations were made by the system.
- **Maximum Size Before Warning:** This is the maximum size of the message store. A warning is logged when 90 percent of mailbox storage capacity is reached.

www.it-ebooks.info

- **Creation Date:** The date that the message store was created in the database. The number listed here for the default message store is the installation date of Cisco Unity Connection. Cisco Unity Connection provides for the creation of four additional mailbox stores configured by the administrator. For these message stores, their creation date will be reflected in this field.

New users can be created directly in the default message store, or existing users can be moved to the new message store. To create a new message store, on the Search Mailbox Store page, select the **Add New** button. The New Mailbox Store page displays, enabling the administrator to enter the Display Name and Maximum Size for the new Message Store, as shown in Figure 7-4.

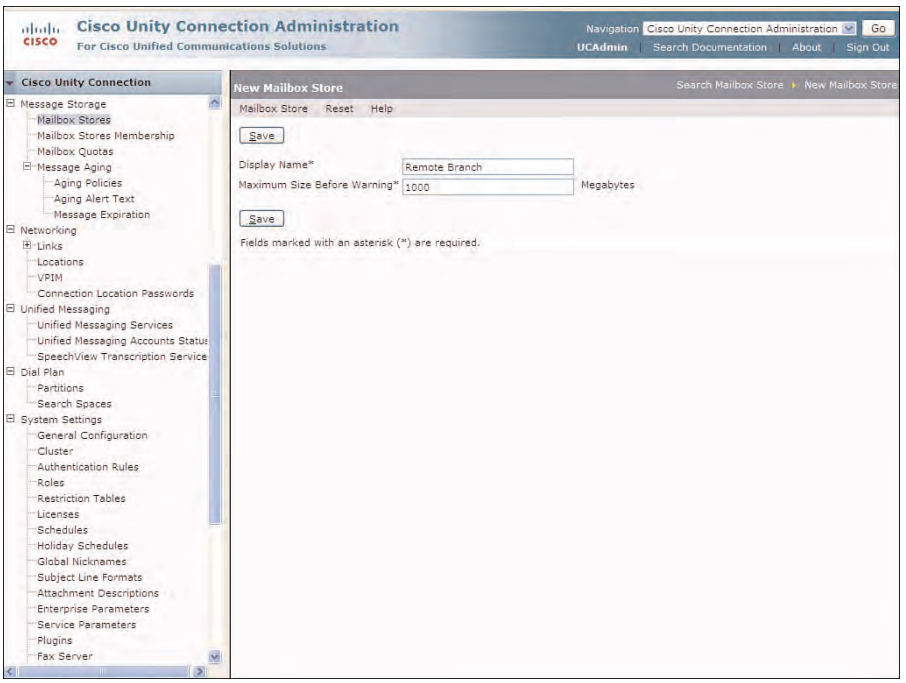

Figure 7-4 *New Mailbox Store Being Created in Cisco Unity Connection Administration*

In this case, the new mailbox store is sized at 1 Gigabyte for the remote branch users to conserve disk space. As you create a new message store, the disk space is reserved for this use and cannot be changed after the time the message store is created. Ensure that you have disk space available on the server to create the message store; otherwise, the new message store will fail to be created. You can delete a message store only if there are no user mailboxes currently assigned to the message store.

www.it-ebooks.info

Click the **Save** button to create the new message store. A message appears in the Status section of the Search Mailbox Store page stating:

```
Creating Mailbox Store. This may take several minutes or longer. Please wait...
```

After the mailbox is created, the Search Mailbox Store lists the new mailbox store for the remote branch users, as shown in Figure 7-5. This new mailbox store is created with the display name of Remote Branch, but the internal identifier in the Cisco Unity Connection database is listed as UnityMbxDb2 (the second mailbox database). As new mailbox stores are created, this number is automatically incremented from UnityMbxDb2, UnityMbxDb3, UnityMbxDb4, and UnityMbxDb5.

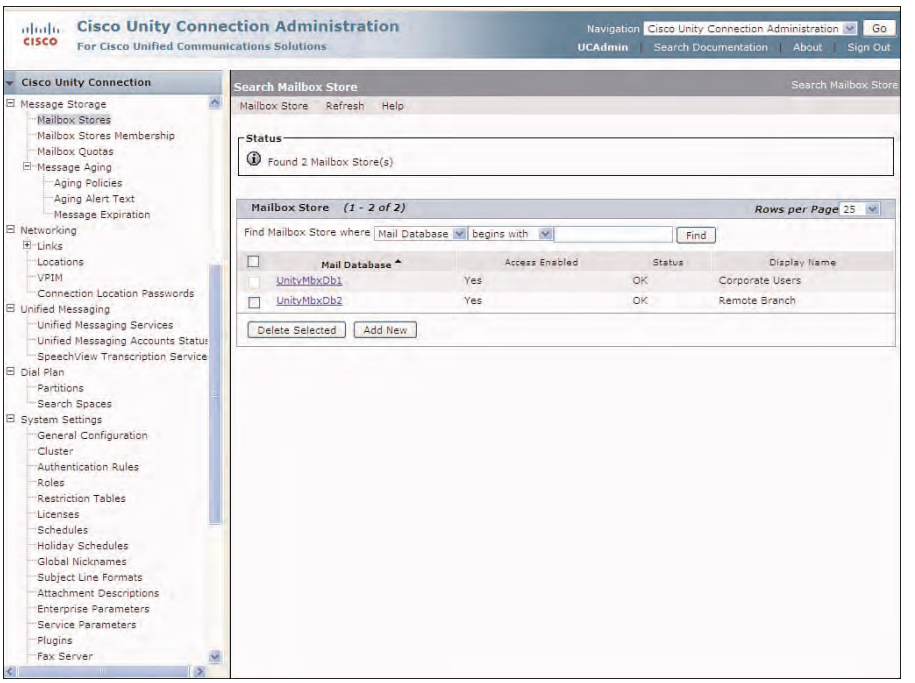

Figure 7-5 *Search Mailbox Store Page Displaying the New UnityMbxDb2 Mailbox Store*

To view or change options for the newly created database, from the Mail Database column on the Search Mailbox Store page, select **UnityMbxDb2**. The Edit Mailbox Store page displays, as shown in Figure 7-6. The details of this page are similar to those listed for the default message store.

Currently, no mailboxes or messages are in this message store. In versions previous to Cisco Unity Connection 8.5, there are approximately 5 kilobytes of base information for each message store. The number of mailboxes and total size of all voice messages increment according to the users created in the message store. Of course, the size of the message store is dependent on the installation and server platform.

www.it-ebooks.info

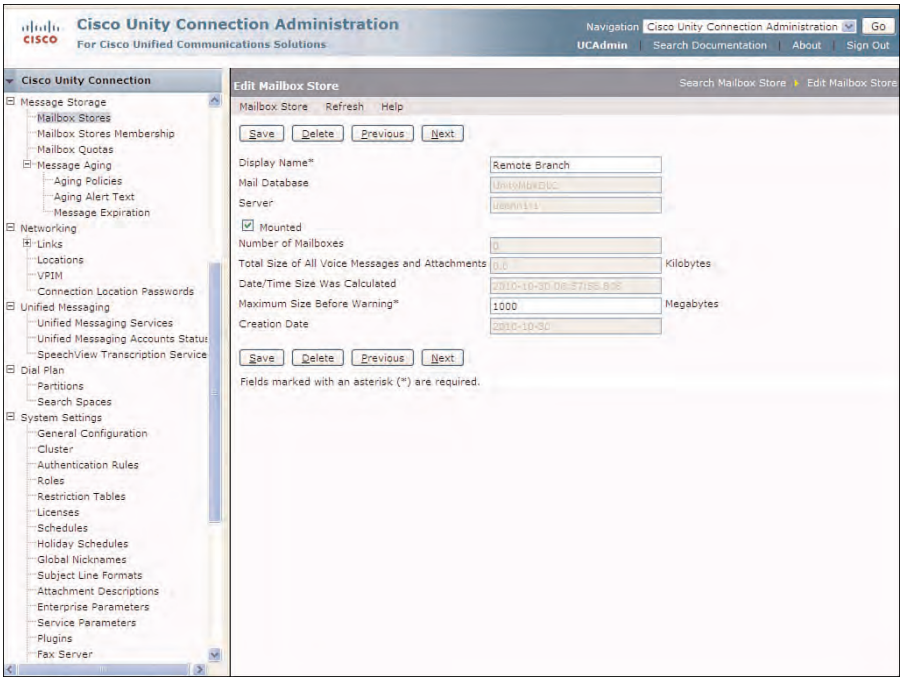

Figure 7-6 *Edit Mailbox Store Page for the New UnityMbxDb2 Mailbox Store*

In the next section, you understand how to move users between message stores and create new users in specific message stores using templates and the user pages in Cisco Unity Connection Administration.

Mailbox Stores Membership

The Mailbox Stores Membership enables the administrator to view and modify the assignments of users to the various mailbox stores. This is also the only option that an administrator has to move an existing user to a new mailbox store. To view the current mailbox stores membership, from the navigation pane on the left portion of the page in Cisco Unity Connection Administration, select **Message Storage > Mailbox Stores Membership**. The Search Mailbox Stores Membership page displays.

From this page, the administrator moves a user from the default mailbox store to the newly created message store, as shown in Figure 7-7. The following selection is made:

Step 1. To find user mailboxes, from the drop-down, select **In** and **Corporate Users**.

Step 2. Select the check box next to the user or users that you want to move to the mailbox store. In this example, the user Tiffany Davis is selected.

Step 3. Under the Move Selected Mailboxes option, from the drop-down, select the target message store. In this case, the **Remote Branch** message store is selected.

www.it-ebooks.info

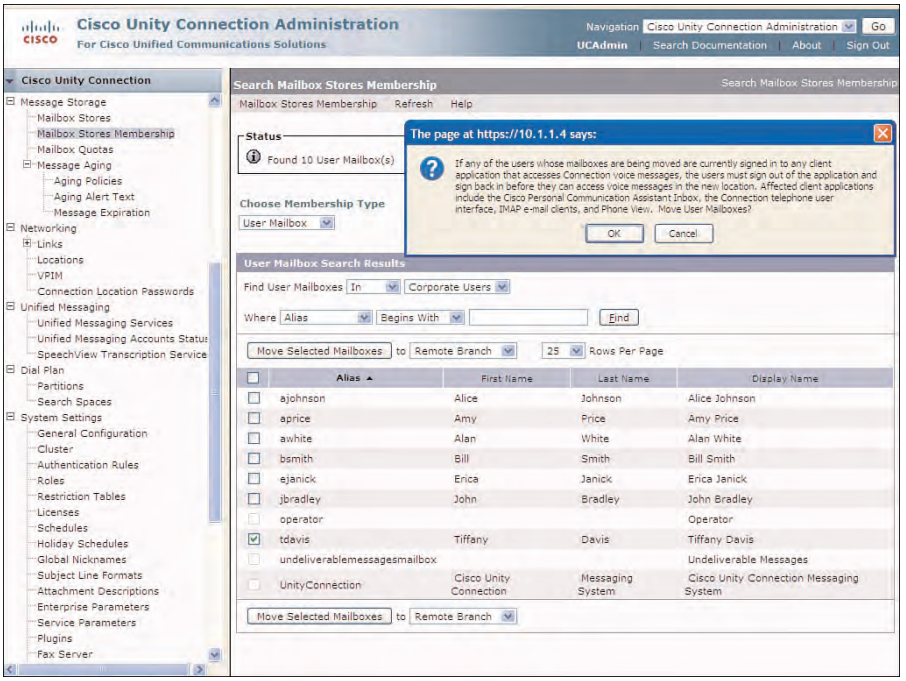

Figure 7-7 *Search Mailbox Stores Membership Page for Corporate Users*

Finally, select the **Move Selected Mailboxes** button. A warning pop-up message for the administrator appears:

```
If any of the users whose mailboxes are being moved are currently signed in to
 any client application that accesses Connection voice messages, the users must
 sign out of the application and sign back in before they can access voice
 messages in the new location. Affected client applications include the Cisco
 Personal Communication Assistant Inbox, the Connection telephone user
 interface, IMAP email clients, and Phone View. Move User Mailboxes?
```

Select **OK** to complete the move operation. The Status section of the Search Mailbox Stores displays the move status as the move operation is completed.

You need want to ensure that the move was successful and no failures occurred by reviewing the Status section on this page. The Corporate Users mailbox store membership now displays the remaining members, as shown in Figure 7-8.

From the Search Mailbox Stores Membership page, select **Remote Branch** from the Find User Mailboxes In drop-down, and click **Find**. The user mailbox search for the Remote Branch message store now displays the user, Tiffany Davis, as a member of this new message store, as shown in Figure 7-9.

www.it-ebooks.info

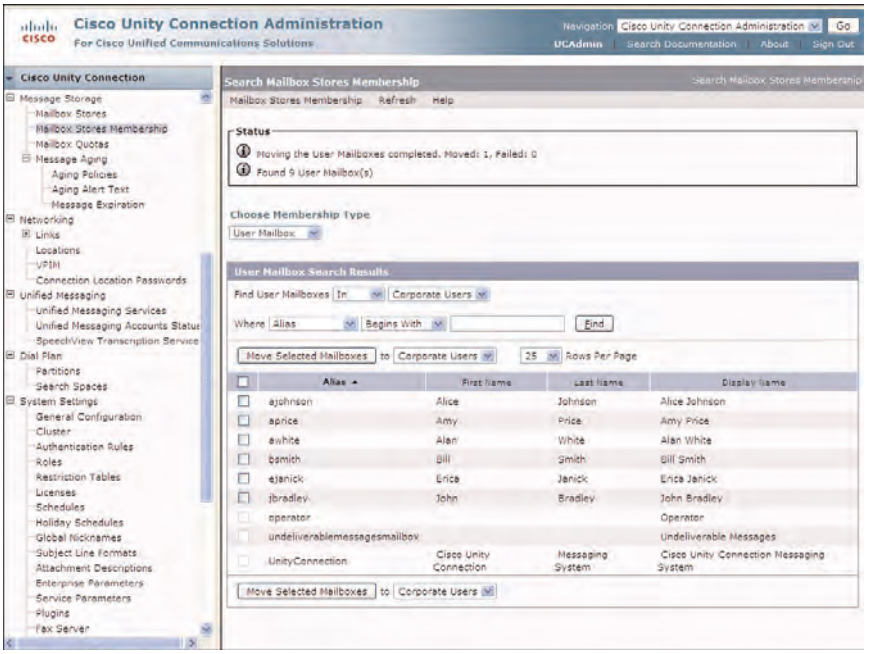

Figure 7-8 *Moving Users to a New Message Store*

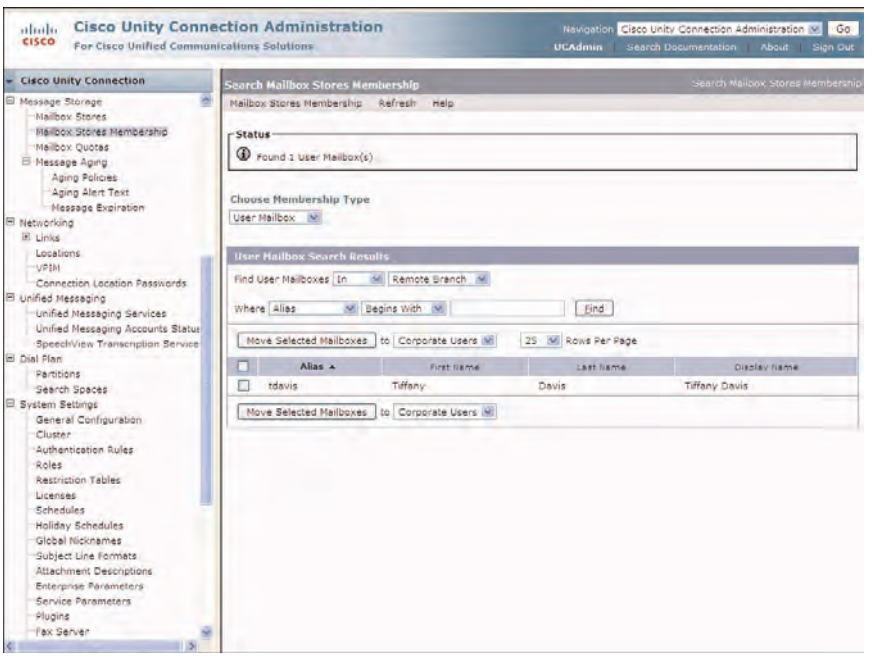

Figure 7-9 *User Moved to the New Message Store*

www.it-ebooks.info

To verify the mailbox store and the current messages, select **Message Storage > Mailbox Stores**, and select the **UnityMbxDb2** mailbox store. The Edit Mailbox Store page for this message store displays and indicates that there is one mailbox with a current size of all messages of 3.294 Megabytes, as shown in Figure 7-10.

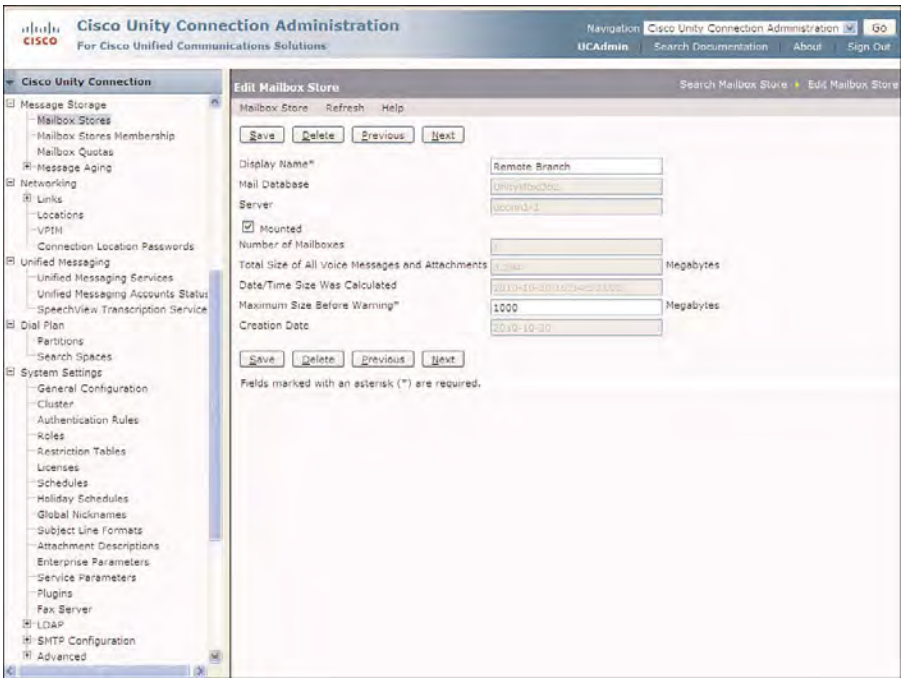

Figure 7-10 *Edit Mailbox Store Page for User Moved to the New Message Store*

The author left a 1-minute message for this user. Figure 7-11 displays the Edit Mailbox Store after this message was delivered.

The field for the Total Size of All Voice Messages and Attachments has now increased to 3.785 Megabytes. The difference of the calculation between the message store before and after the 1-minute message was delivered as follows:

3.785 Megabytes – 3.294 Megabytes = 491 Kilobytes

Therefore, the size of this 1-minute message was 491 Kilobytes. This is inline with the current default recording codec of G.711, which accounts for approximately 480 K of disk space for each 1-minute message according to standard documentation. Table 7-1 displays the approximate disk space usage for a 1-minute message according to the recording codecs. Refer to Chapter 2 for further discussions about codecs.

www.it-ebooks.info

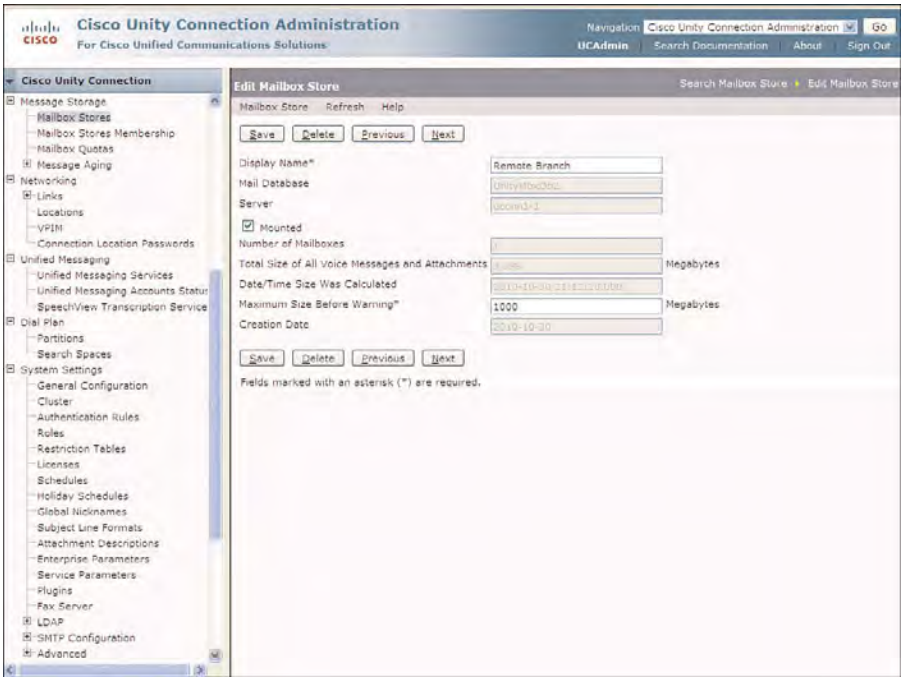

Figure 7-11 *Edit Mailbox Store After a One-Minute Message Was Delivered*

Table 7-1 *Disk Space Usage per Codec (Per 1-Minute Recorded Message)*

Codec	Disk Space Usage
	480 Kilobytes
G.726	240 Kilobytes
GSM 6.10	98 Kilobytes
G.729a	60 Kilobytes

Voice-Message Directory

All voice messages are stored as .WAV files in the voice-message directory, which is the associated directory with the message store. This directory includes .WAV files and any attachments currently saved for each user located in the message store.

The mailbox store and voice-message database is replicated between servers in a cluster pair. Therefore, within a cluster pair, the message store and voice-message database exists in both the publisher and subscriber servers providing complete redundancy.

www.it-ebooks.info

Creating Users in a Mailbox Stores

The Mailbox Stores Membership page enables the administrator to change the message store assignments to one or more user templates. This is accomplished by simply selecting **Message Storage > Mailbox Stores Membership** from the navigation pane in Cisco Unity Connection Administration. On the Search Mailbox Stores Membership page, from the Choose Membership Type drop-down, select **User Template**. From this page, select the check box next to the template name. Then, select the desired message store from the **Assign Selected Templates** drop-down. Click the **Assign Select Templates** button to complete the operation, as displayed in Figure 7-12.

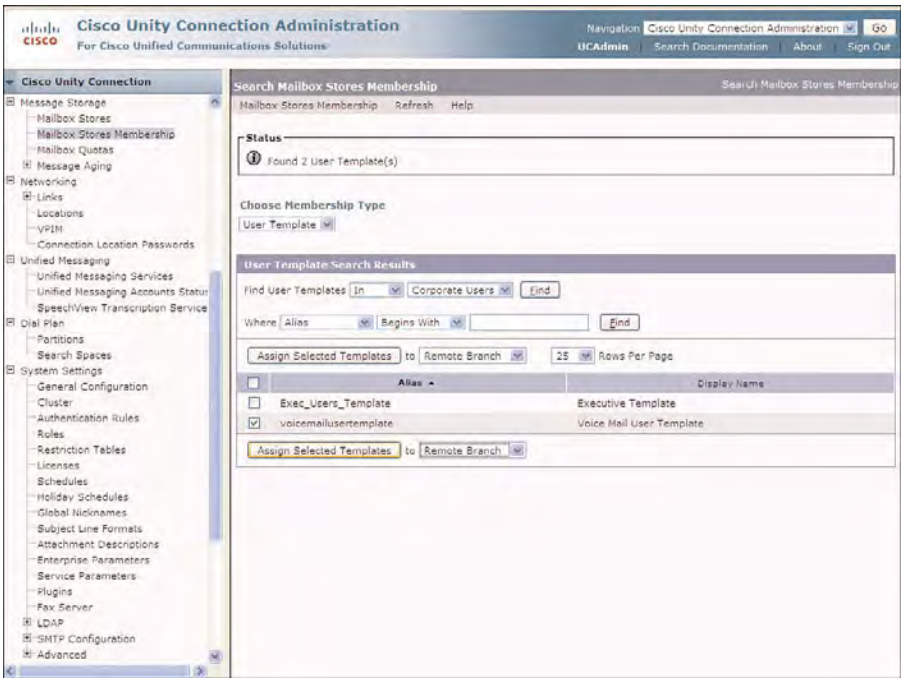

Figure 7-12 *Assign the User Template to a Different Message Store*

To create a new user with a specific mailbox store, from the navigation pane, select **Users > Users**. Select the **Add New** button to create the new user. The New User page displays. From this page, you can select the desired message store from the Mailbox Store drop-down. A new user, Bill Evan, is created and assigned to the Remote Branch message store, as shown in Figure 7-13.

Message Aging Policy

Use Message Aging Policies to determine how long messages should be retained in a user's voice mailbox. You can configure policies to move messages to saved or deleted items folders after a specific time and whether to permanently delete message after a

www.it-ebooks.info

defined number of days. Secure messages can also be treated differently based the message status, either being untouched or retrieved by the user.

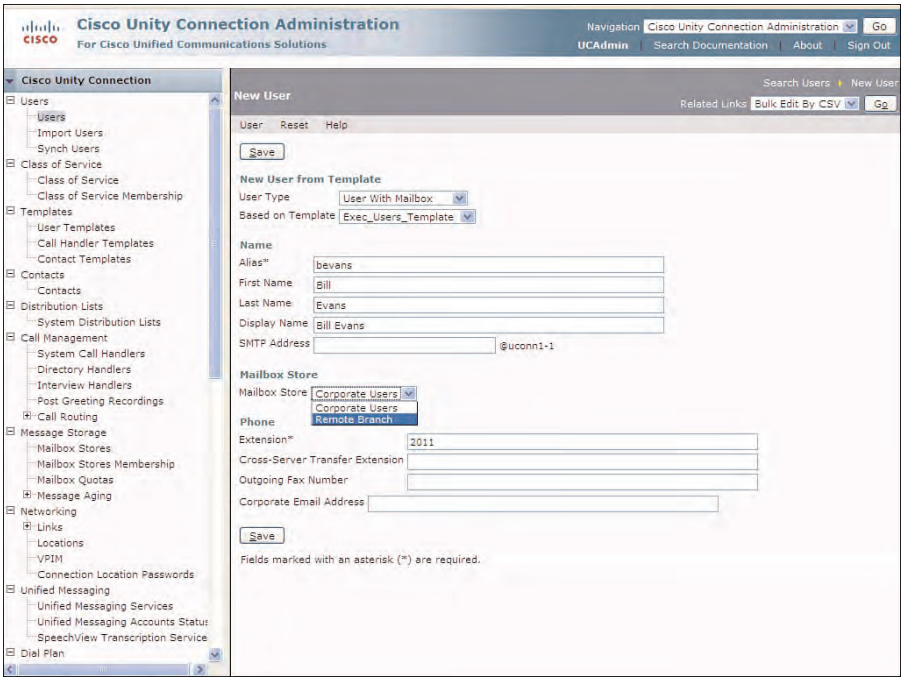

Figure 7-13 *New User Mailbox Store Selection*

Currently, two Message Aging Policies are defined in Cisco Unity Connection at the time of installation. These can be viewed by selecting **Message Storage > Message Aging > Aging Policy** from the navigation pane on the left portion of the Cisco Unity Connection Administration page. The Search Message Aging Policy displays, as shown in Figure 7-14.

There are currently two default message aging policies defined: Default System Policy and Do Not Age Messages policies. The Default System Policy is optimized and enabled for all users that are created with the default Voice Mail User Template (**voicemailusertemplate**). The Do Not Age Messages policy is currently not enabled, and all options are unselected.

To review the message aging policy, from the Display Name column, select the Default System Policy. The Message Aging Policy (Default System Policy) page displays, as shown in Figure 7-15.

By reviewing this policy, the administrator can notice that all messages are permanently deleted in the deleted items folder after 15 days. This action ensures that any unwanted messages do not use disk space needlessly.

www.it-ebooks.info

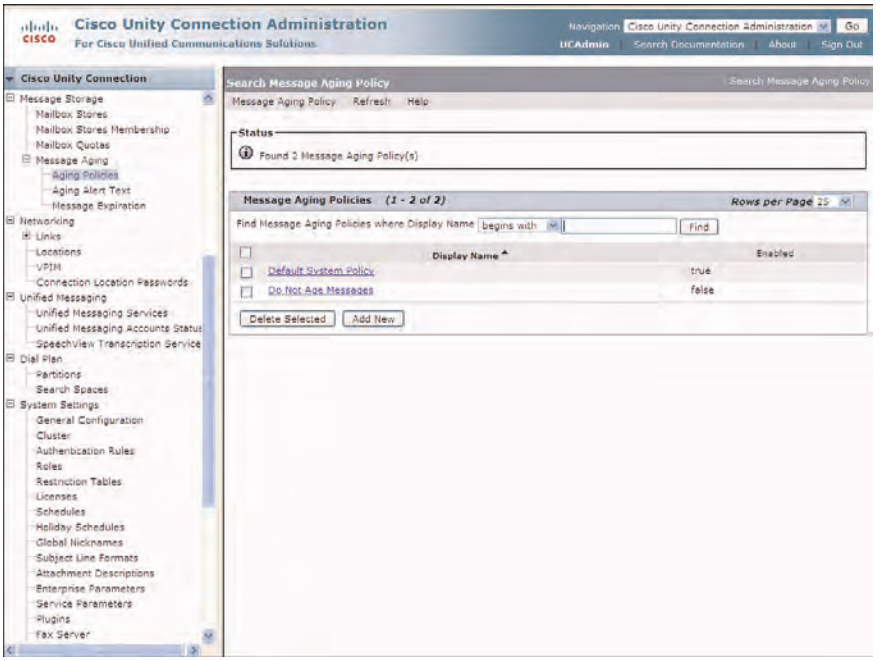

Figure 7-14 *Search Message Aging Policy Page*

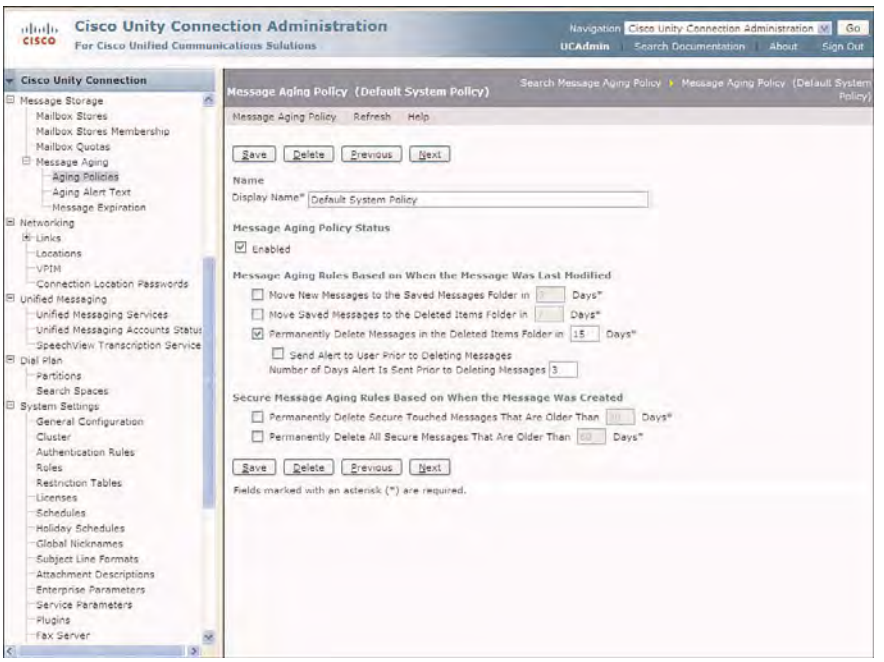

Figure 7-15 *Default System Policy Defined for Message Aging*

www.it-ebooks.info

The default policy can be tailored to further optimize disk space by clearing the message folders after a set number of days, such as 7 days instead of 15. Additional message aging policies can be created as needed. Cisco Unity Connection version 8.5 adds a few new options to automatically send alerts to users before moving or deleting messages based on the message aging policy. The alert is sent to the user's mailbox and is selectable for the number of days in which the alert is sent prior to each specific event.

To create a new message aging policy, from the Search Message Aging Policy page, select **Add New**. On the New Message Aging Policy page, enter the name for the new policy, and click **Save**. The Message Aging Policy page for the new policy is now displayed, as shown in Figure 7-16.

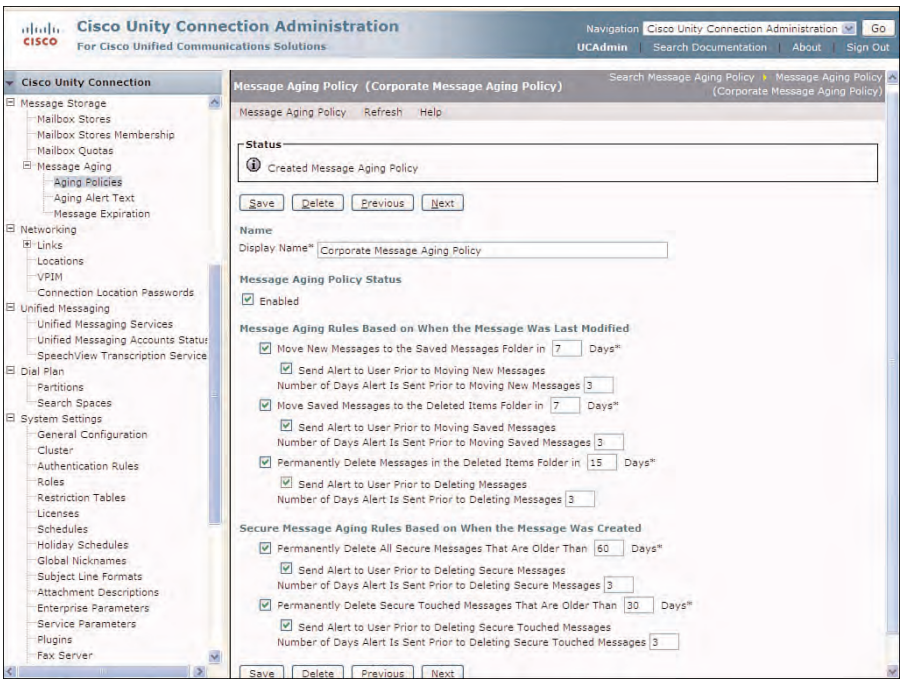

Figure 7-16 *Message Aging Policy Optimized for Corporate Policies*

In this example, the policy was optimized according to management's corporate policy for user mailboxes, which are as follows:

- Move New Messages to the Saved Messages Folder in 7 Days
- Move Saved Messages to the Deleted Items Folder in 7 Days
- Permanently Delete Messages in the Deleted Items Folder in 15 Days
- Permanently Delete Secure Touched Messages That Are Older Than 30 Days
- Permanently Delete All Secure Messages That Are Older Than 60 Days

www.it-ebooks.info

The message aging policy should be optimized according to the organization's policies for users to maintain their mailbox. This policy might not be optimized for your company or organization and is used here as an example for discussion purposes only.

In this example, if a user does not check messages for more than 7 days, these messages will be moved to the saved folder. However, an alert gives the users advanced warning, to act on the messages in their mailbox. At the time of deletion, the MWI light will be turned off if there are no further messages in their inbox. After 7 days, these messages are then moved to the deleted items folder, after which time they are permanently deleted in 15 days. In all cases, the users are notified 3 days prior to each event.

To ensure that messages are archived when using this type of policy, the administrator can select the **Accept and Relay the Message** voice-messages option in the user's Message Actions. An SMTP Smart Host might be required for the relay feature depending on your network installation. Chapter 9, "Understanding Cisco Unity Connection Networking," covers the SMTP Smart Host in more detail. Under the SMTP field of the Message Actions page, select the user's email to forward voice message to this location to ensure proper archiving. The Message Actions configuration options are discussed in Chapter 6.

Message Archiving

Cisco Unity Connection should not be used as an archive for users to store voice messages. If storage of voicemails is required, it is suggested that users use an IMAP client and save the messages to their local workstation as needed. This can also be accomplished by using the Messaging Inbox within the Personal Communications Assistant. Select the **Save Recording As** option on the Options selection of the Media Master, as shown in Figure 7-17.

The administrator can also configure the user's mailbox to deliver the message to the user's voicemail in Cisco Unity Connection, and relay a copy of this message for remote access or archiving purposes. Cisco Unity Connection 8.5 has expanded this capability to enable *Single Inbox*. This is a type of unified messaging, where the voicemail is delivered to the user's voicemail, after which a copy of the message is replicated to user's Exchange inbox. In this case, the user can retrieve the message from either location. The message status (read, unread, or deleted) is synchronized between the storage locations. The Single Inbox feature is explored later in this chapter in the section, "Unified Messaging Service."

If users continue to store messages without aging, disk space usage continues to increase and backup takes longer to complete. If the corporate policy (depending on the business practices and industry type, or government standards, such as Sarbanes-Oxley) might dictate that voice messages be archived, this should be accomplished through one of the various aforementioned means described. Any policy about message retention should be communicated to all users and enforced by the corporate message aging policy. The message aging policy can be changed on an existing user or applied to a new user using the user template configuration option.

www.it-ebooks.info

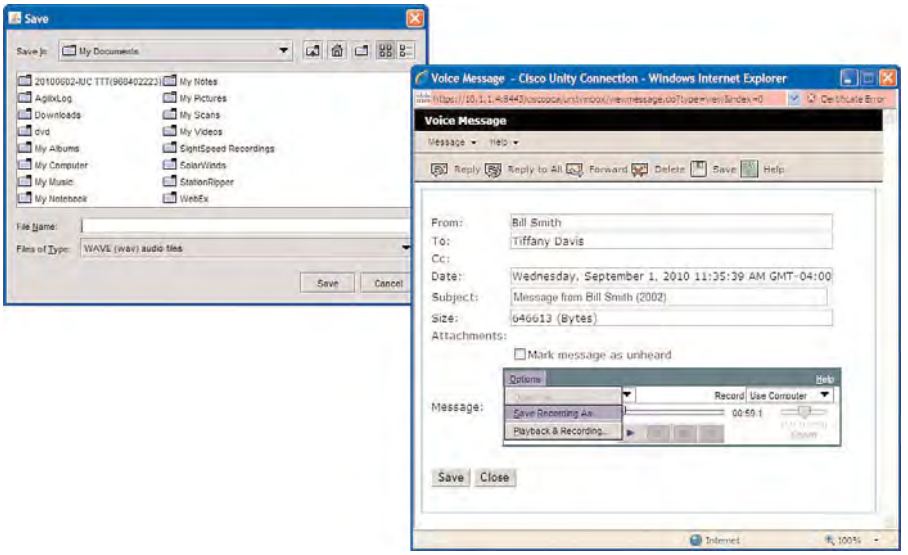

Figure 7-17 *Message Archiving Using the Messaging Inbox*

Apply Message Aging to User

To change the message aging policy for a user, from the Search Users page, select the specific user. Then, from the Edit User Basics page, select **Edit > Mailbox**. Figure 7-18 shows the Edit Mailbox page for this user. Select the desired message aging policy from the **Message Aging Policy** drop-down, and click **Save**. The new policy is now applied to all messages in this user's mailbox.

You can use this same procedure to change the message aging policies for a user template. To complete this action, do the following:

Step 1. From the navigation pane on the left portion of the page in Cisco Unity Connection Administration, select **Templates > User Templates**.

Step 2. From the Search User Templates page, select the desired template to modify.

Step 3. From the toolbar on the Edit User Template Basics page, select **Edit > Mailbox**.

Step 4. The Edit Mailbox page for this user template displays enabling the user to modify the message aging policy, as shown in Figure 7-19.

Aging Alert Text

Cisco Unity Connection 8.5 adds the option to send alerts to the user's mailbox when a specific message is to be removed based on the currently applied message aging policy. You can view and modify the text for these alerts in Cisco Unity Connection Administration by selecting **Message Storage > Message Aging > Aging Alert Text.** The Edit Message Aging Alert Text page displays providing access to the specific text options for each five alerts, as shown in Figure 7-20.

www.it-ebooks.info

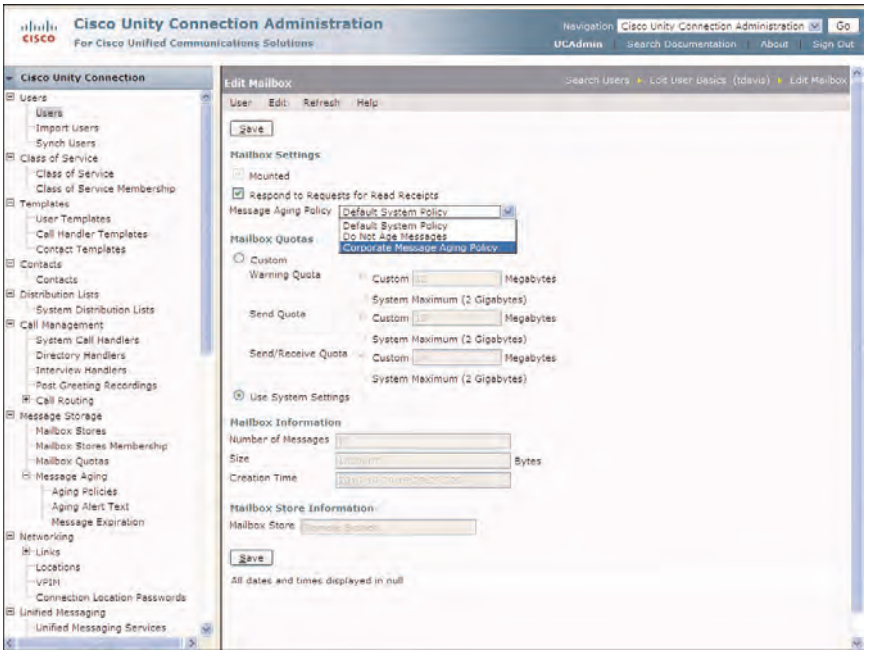

Figure 7-18 *Applying a New Message Aging Policy to an Existing User*

Figure 7-19 *Edit Mailbox Page*

www.it-ebooks.info

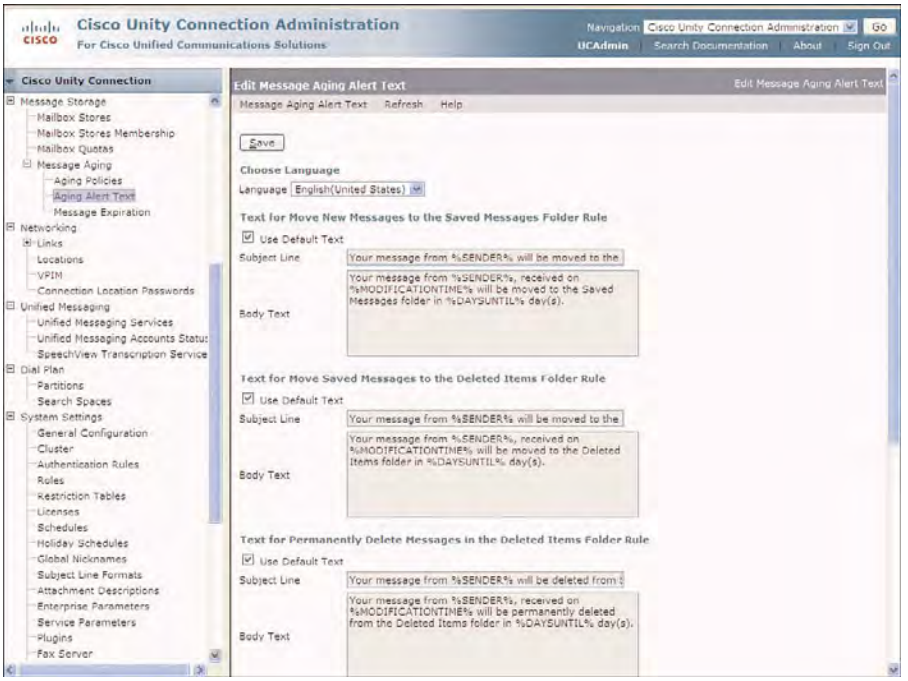

Figure 7-20 *Edit Message Aging Alert Text Page*

You can use special characters to customize the alerts as follows:

- %SENDER%
- %MODIFICATIONTIME%
- %DAYSUNTIL%
- %ARRIVALTIME%

Message Recording Expiration

Cisco Unity Connection 8.5 also adds the option for message expiration. The default for message expiration is 180 days. This option prevents a user from saving messages that have been received beyond a defined number of days. The users cannot circumvent this counter by forwarding the message to their mailbox because the counter does not get reset on the forwarding operation.

To view or modify the message recording expiration, in Cisco Unity Connection Administration, select **Message Storage > Message Aging > Message Expiration.** The Edit Message Recording Expiration page displays, as shown in Figure 7-21.

www.it-ebooks.info

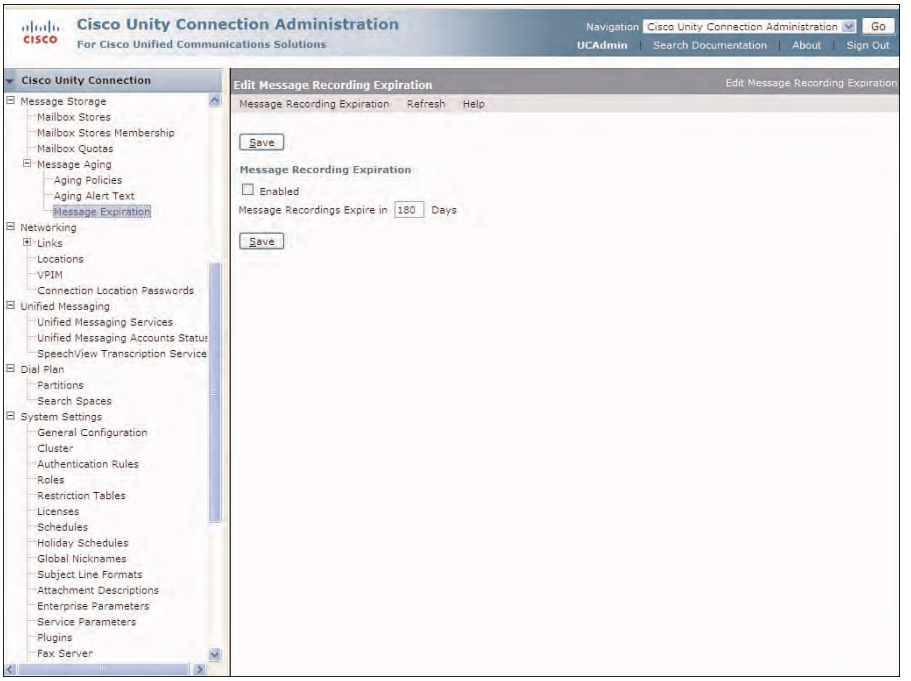

Figure 7-21 *Edit Message Recording Expiration Page*

To further ensure that users manage their mailbox and pay closer attention to the amount of stored voice messages, Cisco Unity Connection enforces mailbox quotas. Mailbox quotas provide a level of control based on the amount of voice messages stored in a user's voicemail.

Mailbox Quotas

Mailbox quotas are applied to every user's mailbox. There is a System-wide Mailbox Quota enforced by default; although each user's quota can be customized in the mailbox option in each user's configuration. To view or modify the System-wide Mailbox Quotas, from the navigation pane on the left portion of the Cisco Unity Connection Administration page, select **Message Storage > Mailbox Quotas**. The Edit System-wide Mailbox Quota page displays, as shown in Figure 7-22.

The Mailbox Quotas provides three levels of control, which can be changed from the system default or set at the system maximum of 2 Gigabytes:

- **Warning Quota:** Provides a warning to the users, informing them that their mailbox is reaching the maximum size. The default configuration for the warning quota is configured to 12 Megabytes. At the default recording codec of G.711, this accounts for

www.it-ebooks.info

approximately 25 minutes of recorded messages (12,000 Kbytes / 480 Kbytes = 25 minutes of recording time). If this setting is customized from the system default, it should always be configured to be less than the Send and Send/Receive Quota.

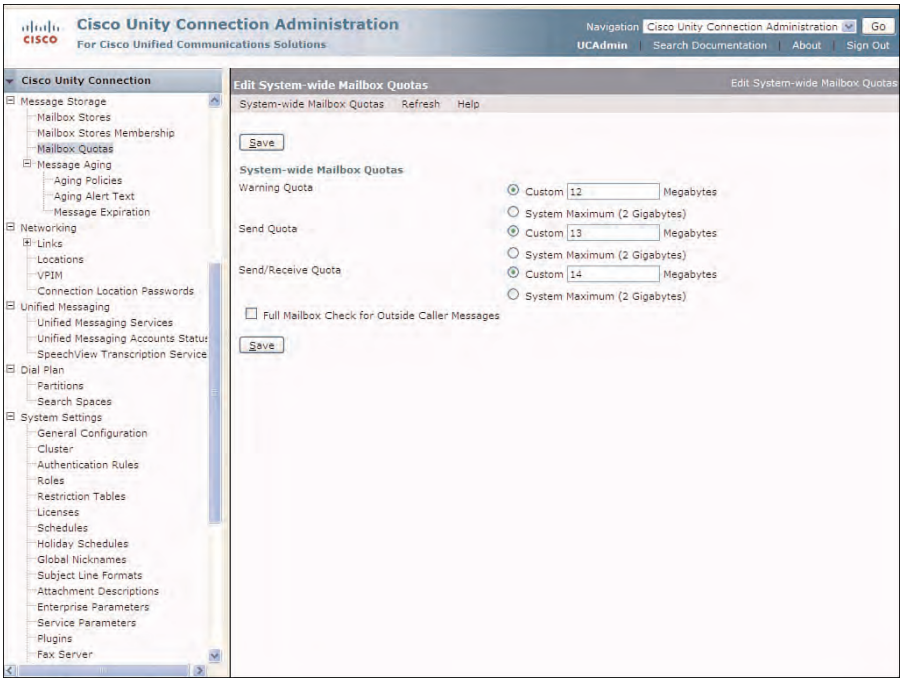

Figure 7-22 *Edit System-Wide Mailbox Quotas*

- **Send Quota:** Prevents the users from sending, forwarding, or replying to messages from their mailbox when this quota is reached. However, callers can still leave messages, and the users can retrieve their messages. The default quota setting for this parameter is 13 Megabytes. At the default recording codec of G.711, this accounts for approximately 29 minutes of recorded messages (13,000 Kbytes / 480 Kbytes = 29 minutes of recording time). If this setting is customized, it should be configured to be less than the Send/Receive Quota. When this quota is reached, a new warning message plays for the users letting them know they cannot send messages. The message instructs the user to delete messages. The warning message continues to be played when they access their mailbox until the messages in the mailbox are below the quota.
- **Send/Receive Quota:** Prevents the user from sending and receiving messages from their mailbox when this quota is reached. Internal callers cannot leave messages for the user, and a nondeliverable receipt (NDR) is returned to the internal caller. External

www.it-ebooks.info

callers cannot receive an NDR; therefore, the message from external callers is still delivered to the user. The default setting for this parameter is 14 Megabytes. At the default recording codec of G.711, this accounts for approximately 27 minutes of recorded messages (14,000 Kbytes / 480 Kbytes = 27 minutes of recording time). When this quota is reached, a new warning message plays for the user, informing them that they cannot send and receive messages. The message instructs the users to delete messages. The warning message continues to play when they access their mailbox until the messages in the mailbox are below the configured quota. In all instances, warning messages cannot be skipped and must be listened to in their entirety before the users can make any selections within their mailbox.

The **Full Mailbox Check for Outside Caller Messages** check box in the Edit System-wide Mailbox Quota page enables the administrator to disallow the recorded messages for outside callers if the user's mailbox is full. In these cases, the Send/Receive Quota has been reached. This option affects only outside callers directed to the user's mailbox.

If this option is selected and Send/Receive Quota has been reached, the caller receives a message stating that the user's mailbox is full and therefore the caller cannot leave a message.

Internal callers are not affected by this option. When an internal caller leaves a message for the same user, the message is recorded and attempted to be delivered; however, the message is returned to the caller with a receipt of undeliverable, or Non-Deliverable Receipt, or NDR (error code 422).

If the **Full Mailbox Check for Outside Caller Messages** check box is not selected, outside callers can record and send messages and the user's mailbox continues to fill beyond the Send/Receive Quota. For this reason, this practice is strongly discouraged because users might not properly retrieve their messages and manage their voicemails. In these cases, disk space continues to be consumed for voice messages. It is advisable to provide adequate training and communicate company policies about voicemail and proper voice-message management.

In many voice-messaging systems, these types of undeliverable messages might be delivered to a system mailbox for undeliverable messages. Cisco Unity Connection provides a similar feature called the undeliverablemessages distribution list. However, this option is not used for messages that exceed the mailbox quotas. The undeliverablemessages distribution list is used for messages that cannot be delivered because the user cannot be found or has been deleted. This issue will be less common because the act of deleting users also removes them from the directories. Also, internal users attempting to send messages to nonexistent users receive an NDR. Outside callers who cannot receive this notification after they address and send the message have their message delivered to this undeliverablemessages distribution list. Care must be taken for administration to monitor, review, and handle these messages properly; otherwise, voice messages might continue to collect in this location without the knowledge or attention of administration. Distribution lists are discussed later, and in Chapter 8, "Understanding Call Handlers and System Features."

www.it-ebooks.info

In addition to the System-Wide Mailbox Quotas, the individual users and user templates can be customized to override the systemwide quotas. To customize a user's mailbox quota, select the specific user to be configured from the Search Users page in Cisco Unity Connection Administration. Then, from the Edit User Basics page, select **Edit > Mailbox**. Figure 7-23 shows the resulting Edit Mailbox page.

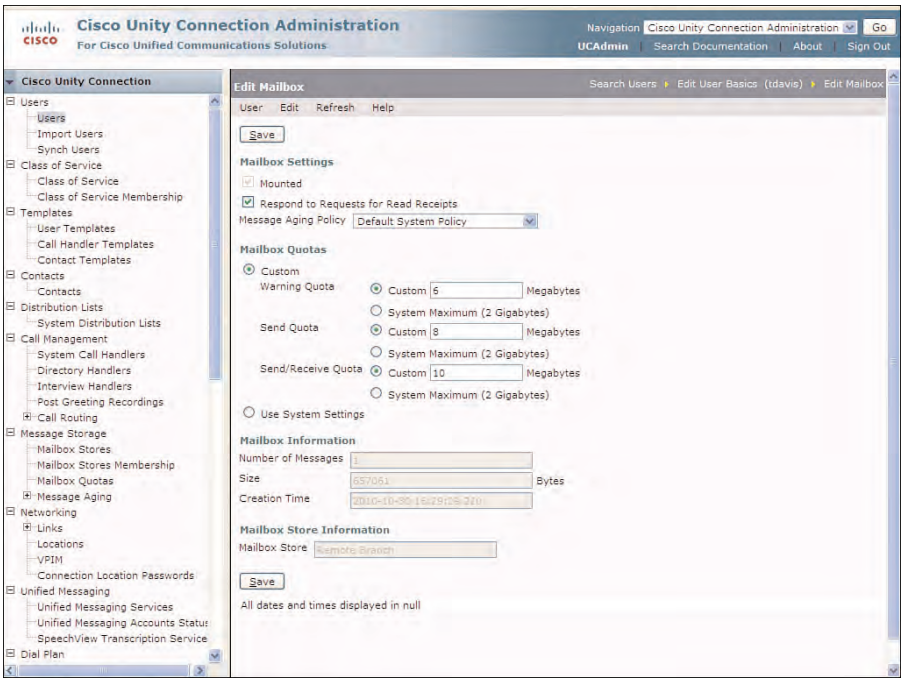

Figure 7-23 *Customized User Mailbox Quotas*

In this case, the quota has been customized from the systemwide quota to enable for a **Warning Quota** of 6 Megabytes, a **Send Quota** of 8 Megabytes, and a **Send/Receive Quota** of 10 Megabytes. The **Full Mailbox Check for Outside Caller Messages** check is still used, if selected in the System-wide Mailbox Quotas page.

Case Study: Message Aging and Archiving

Tiferam Corporation is concerned about the amount of disk space consumed for voice messages. Users continually save and accumulate voice messages in their mailbox. Currently, users have access to email using Outlook configured on their workstation. Executive management is concerned about deleting messages because specific employees are required to archive voice messages.

To resolve these issues, administration has enacted a new policy that educates users in the use and archiving of messages. With this new policy, users are notified that all

www.it-ebooks.info

voicemails will automatically be removed from their mailbox after 10 days. This is accomplished by applying an appropriate message aging policy to all users. To ensure that valuable messages are not entirely deleted (before archiving), the Message Actions have been configured to Accept and Relay the message to the users' email account. Users are instructed to archive message from their email account to the corporate file share that is configured for this purpose.

To ensure that the users take action sooner on messages in their account, the System-Wide Mailbox Quota settings have been reduced to notify the users of their messages and to ensure that they delete and remove messages from their mailbox in a timely basis.

Greetings and Caller Input

The Greetings and Caller Input options configured for the user's voicemail determine what the caller hears and how they interact with Cisco Unity Connection as the caller is directed to the user's voicemail when the user is not available or busy. Greetings can be customized by the administrator using Cisco Unity Connection Administration, or configured by the user using the phone interface, or the Messaging Assistant from the Personal Communications Assistant web pages.

Cisco Unity Connection version 8.x provides a new option to enable the administrator to implement a post greeting recording. This feature is implemented by the administrator, where a prerecorded announcement or .WAV file is played to the caller after the users' greeting and before they record their message. These announcements are then applied to a users' configuration by the administrator. Post greeting recordings can be used to provide the caller with specific instructions about the user's availability, company information, or further instructions that might be important to the caller.

Caller Input is a programmed menu of key stroke options (1–9, *, 0, #) from which a caller can select. The programmed logic instructs Cisco Unity Connection how to further process the call. If programmed through the Caller Input pages, these actions can consist of directing the caller to an assistant, call handler, directory, or another user as needed.

Greetings

All users configured on the Cisco Unity Connection server should personalize their recorded name and standard greeting to inform callers of the specific mailbox they have reached before they leave a message. As mentioned previously, if the users do not record a name, the Display Name is spoken to announce the user's mailbox.

If an outside caller is forwarded to a phone user's voicemail because the user is busy or not available, the recorded greeting plays. If the user does not record the greeting, the caller hears the system recording stating that the user is not available along with the user's recorded name. For example:

> Sorry... <recorded name played here, or, Display Name> ...is not available. Record your message at the tone. When you finish, hang up or the press pound sign for more options. <tone>

www.it-ebooks.info

After the greeting plays, the caller can record their message. This greeting is defined as the System Default Recording, which is applied to all users' voice mailboxes using the default user template, **voicemailusertemplate**. Of course, this template can be changed, or a new template can be created to be used for creating users with a different greetings configuration.

A number of greetings can be defined for users. Each greeting (with the exception of the Error and Standard Greeting) can be enabled indefinitely, enabled for a specific time, or disabled. If using the default **voicemailusertemplate** user template to create users, the Standard and Error Greetings are enabled with no end date. The Greeting for a user and a user template include the same options and are configured in a similar fashion. Therefore, the greetings selection on the user configuration pages is reviewed in this section.

The Standard Greeting is configured to play the System Default Recording by default. If the user records a greeting, this new greeting will be used. Greetings can be configured for individual users or applied to a user's configuration through the user templates at the time the user is created in Cisco Unity Connection. Each greeting depends on the user's schedule (Closed/Holiday greeting) and availability (Busy/Internal/Alternate) configured. Only the Standard and Error greetings are enabled for each user. Therefore, to use the greetings, they need to be enabled by the user or administrator. These greetings and their interaction are defined as follows:

- **Standard:** Enabled by default (set as the System Default Recording, previously defined). This greeting is enabled to play indefinitely.
- **Closed::** This greeting overrides the Standard greeting when the configured schedule for the user is off-hours, or closed hours.
- **Holiday:** This greeting overrides the Standard and Closed greetings when the specific holidays occur. Holiday greetings follow the configured holiday configuration for the user's defined schedule.
- **Internal:** This greeting overrides the Standard, Closed, and Holiday greetings but only for internal callers or users defined in Cisco Unity Connection.
- **Busy:** This greeting overrides the Standard, Closed, Holiday, and Internal greetings. When this greeting is enabled, it plays only when the caller reaches the user's voicemail because of the forwarded Routing Rule, and the reason for forwarding was because of the user being busy.
- **Alternate:** This greeting overrides all greetings. The greeting can be used for circumstances where a user is unavailable for extended periods of time, leave of absence, or seasonal employees.
- **Error:** This greeting is always enable with no end date and cannot be disabled. This greeting provides feedback when the caller dials an invalid key or sequence of key strokes. This greeting defaults at the system recording, which provides the following information to the caller: I Did Not Recognize That as a Valid Entry. The administrator can still personalize this recording through the user template or the individual user greeting pages.

www.it-ebooks.info

To begin the configuration of greeting in Cisco Unity Connection Administration, select the specific user from the Search Users page. Then, select **Edit > Greetings** from the Edit User Basics toolbar to result in the Greeting page, as shown in Figure 7-24.

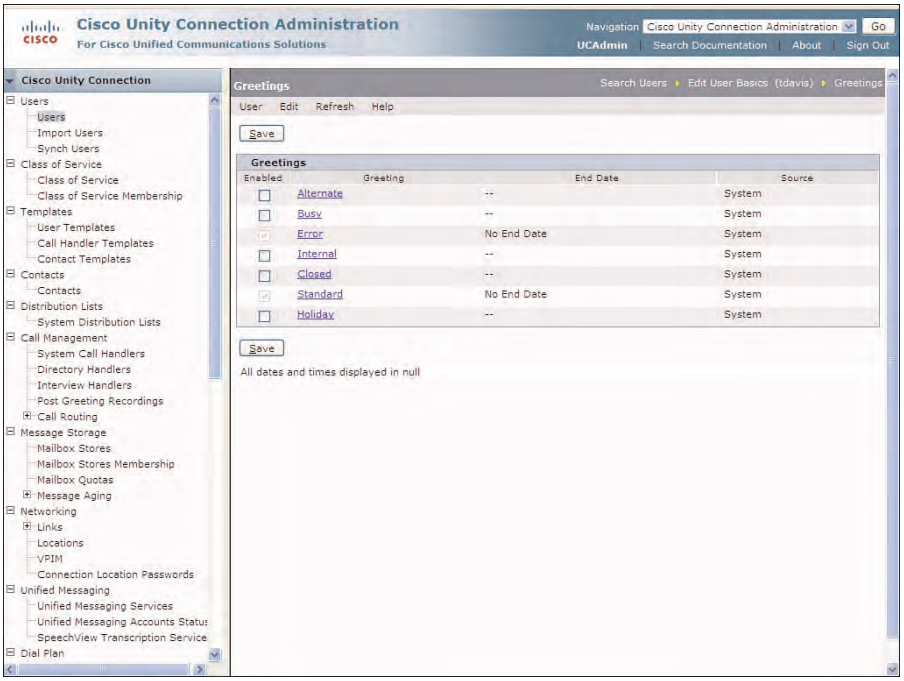

Figure 7-24 *User Greetings Page in Cisco Unity Connection Administration*

From this page, you can select each greeting to review or modify the existing configuration. If you want to enable a specific greeting, select the check box to the left of the greeting. Finally, select **Save** to commit this change to the database. Only the Standard and Error greetings are enabled by default. Each greeting page includes the same configuration options. Therefore, only the Standard greeting option will be discussed here because these can be applied to any of the aforementioned greetings.

To review or modify the greeting configuration options, select the specific greeting from the Greetings page. The Edit Greeting page for the Standard greeting now displays, as shown in Figure 7-25.

The Standard greeting cannot be disabled but can be overridden by the other greetings if these other greetings are enabled. The options on the Edit Greeting page included the Status, Callers Hear, During Greeting, After Greeting, and the Recordings sections. The purpose of the greetings can be varied, but in most cases they communicate to the callers whose mailbox they have reached and enable them to record their message. In other cases, the greetings might provide further information as to how to forward to a

www.it-ebooks.info

live operator or attendant, or even skip the greeting, which uses the caller input selections. In either case, greeting configurations define the caller's experience during the greeting and after the greeting.

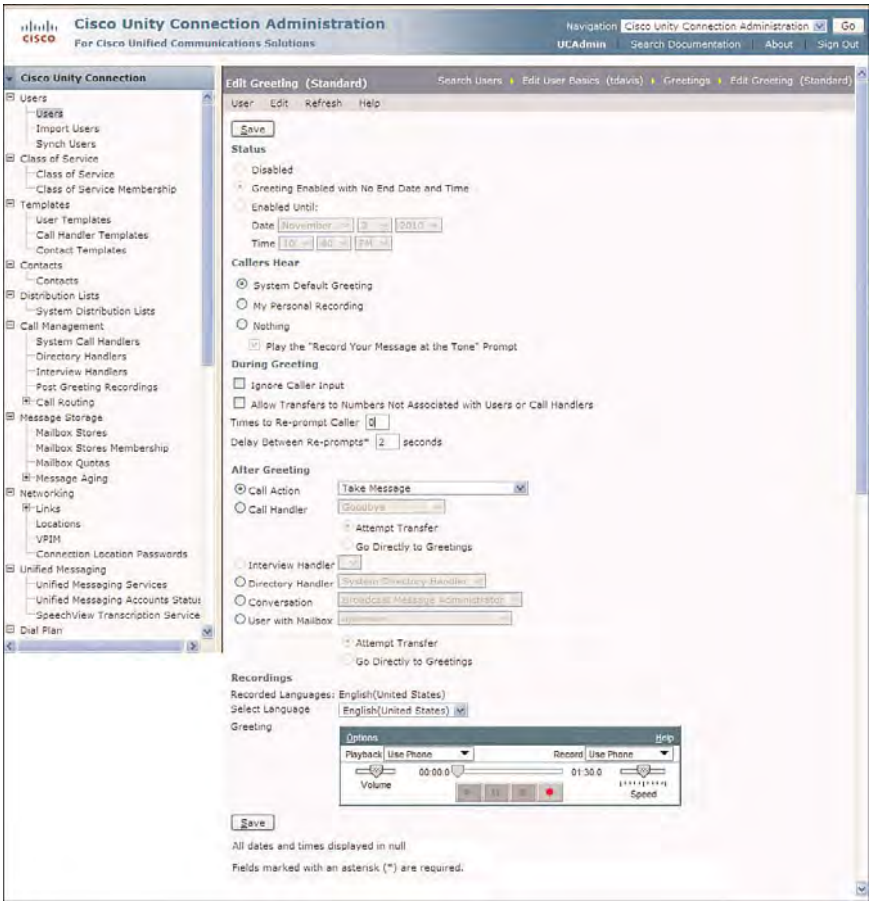

Figure 7-25 *Edit Greeting Page*

The Status section is grayed-out for the Standard greeting because it cannot be changed; however, the other greetings (with the exception of the Error Greeting) can be disabled or enabled indefinitely, or enabled for a period of time (until a configured date/time), depending on the needs of the user.

The Caller Hear section of the Edit Greetings pages defines what greeting is heard when the caller reaches the user's mailbox. By default, the System Default Greeting plays. However, when the users record their personal greeting using the Cisco Unity Connection phone interface or the Messaging Assistant in the Personal Communications Assistant application, this option automatically changes to the My Personal Recording radio button. At this point, the user's recording plays for all callers. Additionally, the

www.it-ebooks.info

administrator can record the greeting for the caller by selecting the Play/Record button in the Recording section at the bottom of the Edit Greetings page.

When the Play/Record button is selected, the Media Master displays enabling the administrator to review the current recording, rerecord the current recording, or add to the current recording. The Media Master requires the proper Java Runtime Environment (JRE) to be installed on the administrator workstation. When the Media Master displays, the Options included in the Media Master enables the administrator to use a .WAV file for the greetings, record and play the greetings using the PC speakers/microphone, or have Cisco Unity Connection use TRAP to dial out to an extension to allow real-time recording, as shown in Figure 7-26. If multiple languages are installed, different recordings can be added for various languages.

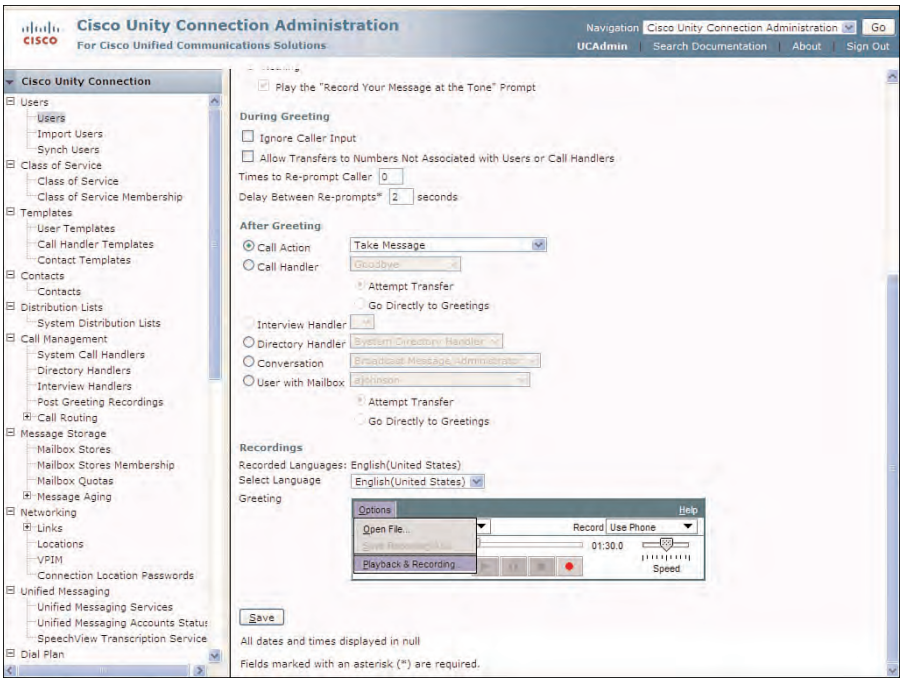

Figure 7-26 *Media Master Options for the User's Greeting*

When recording a greeting with the Media Master, you can terminate the recording using the Stop button on the Media Master, or simply hang up. To avoid any extraneous disconnect noise at the end of the recording; select the Stop button. By using the Stop button, the recording terminates cleanly without any further background noise.

One last option under the Callers Hear section is the Nothing radio button. With this option, the users are left with no information as to who they are leaving their message for, which in most cases might not be optimal. A check box is included for this option to

www.it-ebooks.info

at least instruct the callers to leave a message, which displays as Play the "Record Your Message at the Tone" Prompt check box.

The During Greeting section enables the administrator to configure options for the callers as they are listening to the user's greeting. The Ignore Caller Input check box is unchecked by default, meaning that callers can select various options configured for Caller Input. If the Ignore Caller Input check box is selected, the callers are forced to listen to the entire message before making a selection.

If the Allow Transfers to Numbers Not Associated with Users or Call Handlers check box is selected, callers are allowed to transfer to other numbers, as long as they are not blocked by the restrictions table. The restrictions table is discussed later in the section, "Alternative Extension Features and Restriction Tables." This option is unchecked by default, and care must be taken with this selection. If configured incorrectly; callers can transfer out of the user's mailbox and make calls using the organization's phone system.

The last two options, Times to Re-prompt Caller and Delay Between Re-prompts, should be used only when the mailbox is not used for callers' recordings. In these cases, you expect caller actions using the Caller Input selection options. Otherwise, the Times to Re-prompt Caller option continually replays the greeting for the number of times that the administrator selects the option box if the caller does not respond.

The After Greeting section is the one of the most important sections on the greeting page because this dictates the callers' experience after the user's greeting plays. In most cases, the Take Message option will be selected from the Call Action drop-down, which is the default action. This enables the callers to leave their message after the tone. However, these options could be configured to play the greeting and simply hang up, restart the greeting, or route from the next the call routing rule, whether the call was received from the forwarded or direct routing rules table. Optionally, the caller could be routed to a specific call handler, directory handler, conversation, or a specific user. This last option might be useful when someone is on vacation, or for an extended leave of absence and someone else, such as an administrative assistant, needs to intercept the call. This feature can be configured using the alternative greeting because this greeting overrides all other greetings.

The user can edit and enable greetings through the Cisco Unity Connection phone interface options or from the Messaging Assistant option in the Personal Communications Assistant web pages. To use the Messaging Assistant, the user must be a member of a Class of Service (CoS) that provides access to this feature.

To view and modify the greetings, the user selects the Messaging Assistant option from the Navigation drop-down within the Personal Communications Assistant web pages. Then, select **Greetings > View Greetings** from the toolbar. The Greetings page displays, as shown in Figure 7-27.

From the Greeting page in the Messaging Assistant, the user can review, modify, or enable any recordings. By selecting the greeting type from the Greetings column, the user can configure the specific options for the greeting.

www.it-ebooks.info

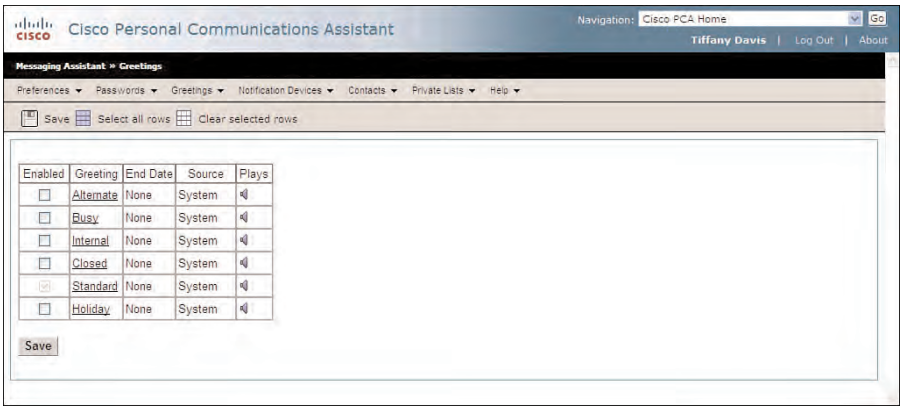

Figure 7-27 *Messaging Assistant Greetings Page*

In Figure 7-28, the Alternate greeting is selected. From this page, the users can record their personal greeting using the Media Master controls, in the same manner as an administrator. The Status section also displays the various enable functions; however, only the administrator has access to the During Greeting and After Greeting configuration options.

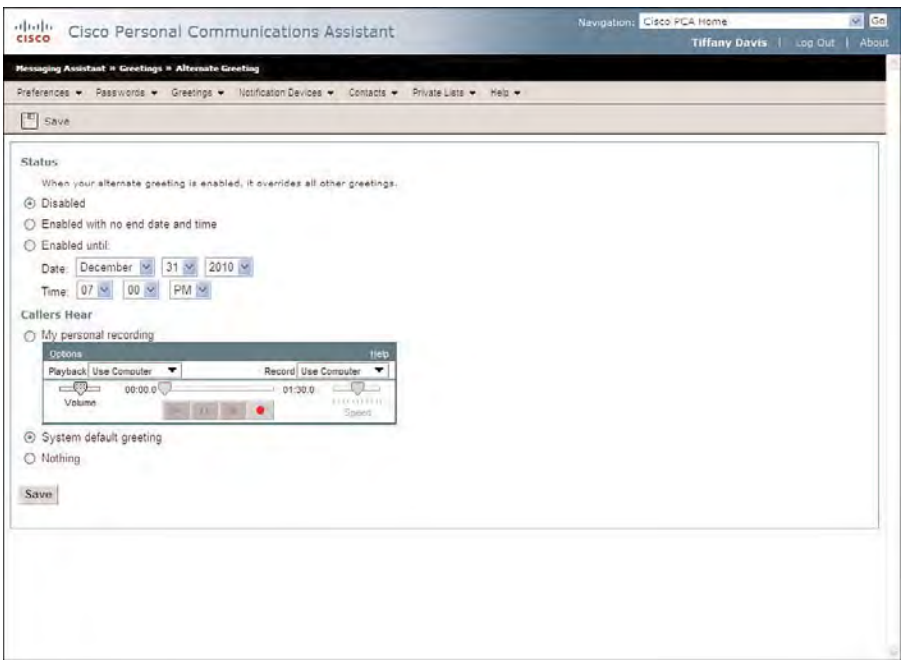

Figure 7-28 *Alternate Greeting Page in the Messaging Assistant*

www.it-ebooks.info

Note When using the Media Master, consider using computer speakers and microphone, as opposed to using the phone. When the phone is selected for this operation, a port is used for the Telephone Record and Playback (TRaP) operation. There must also be ports configured for TRaP in the phone system integration. If port usage is a concern in the organization, from the toolbar for Playback and Record, select the **Use Computer** option. This option is also selectable under the Option page, as discussed in the previous chapter. However, some companies might also have a policy that prevents the usage of speakers because of workspace compliance and privacy.

Caller Input

Caller Input settings can be configured for the user mailbox to determine how the caller interacts with the users voice mailbox. Caller input settings can be applied individually on the user configuration pages or through the user template at the time the user is created. In some cases, you might want the callers to hear the entire message before they leave a message or exit out of voicemail. In these cases, select the Ignore Additional Input checkbox under the greetings page. At other times, you might want to let the users know that they could save time by pressing a specific key to skip the greeting and record their message. The caller input can be programmed to complete this function. Keep in mind that any changes to these features need to be communicated to the caller through the user's greeting.

To add caller input settings to the user pages, select **Edit > Caller Input** from the Edit User Basics page for the selected user. Figure 7-29 shows the Caller Input page.

From this page, three default options for caller input are available:

- ***:** Sends the caller to the Sign-In conversation
- **#:** Enables the caller to skip the users' greeting and start the recording process
- **0:** Sends the caller to the operator

To configure a new caller input option, select the desired number from the Key column. For example, to configure the **3** key to enable callers to reach the directory, begin by selecting the **3** option from the Key column. The Edit Caller Input (3) page displays, as shown in Figure 7-30. Then, select the Directory Handler radio button from the Action section. The System Directory Handler is the current directory displayed.

From this page, the administrator can configure a number of different actions based on the caller input selection. These options can be a call action, call handler, directory handler, conversation option, or a specific user with a mailbox. The Call Actions can consist of a number of features, including options to take message, hang up, restart the greeting, route from the next call routing rule, skip the greeting, or transfer to an alternate contact.

www.it-ebooks.info

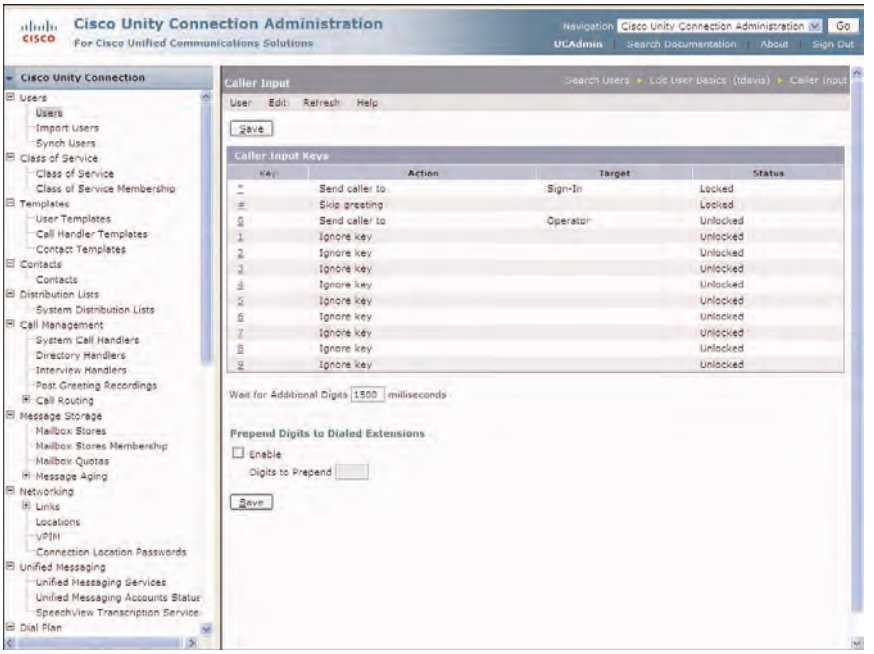

Figure 7-29 *Caller Input Page for a Defined User*

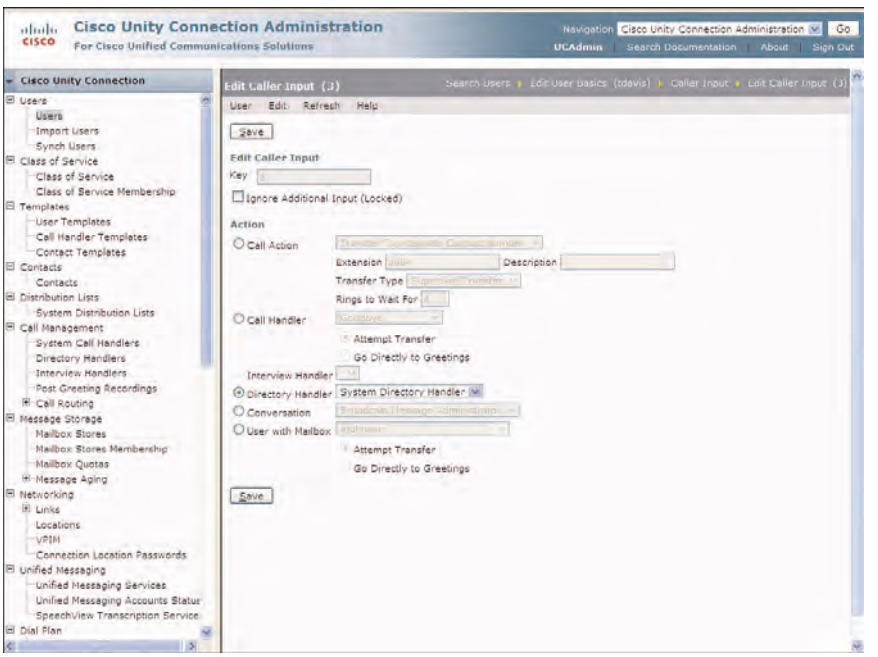

Figure 7-30 *Edit Caller Input Page*

www.it-ebooks.info

Transfer options can be configured to enable the various transfer types, extensions, and rings to wait. If you plan to transfer calls to remote extensions, outside calls, or cell phones, it would be advisable to increase the number of rings in the **Rings to Wait For** option box. This ensures that the target extension has adequate time to answer the call. The **Supervise Transfer** option from the Transfer Type dropdown enables the administrator to implement call screening capabilities for the target extension, provided that the Class of Service enables this feature.

If the Ignore Additional Input (Locked) check box is selected, the configured option is taken immediately as soon as the keystroke is selected. If unchecked, there will be a short delay before the action is taken. For system efficiency and best practices, select this option for all keystrokes, except those that begin with numbering that is the same as any configured extensions on your system. For example, if you have users with extensions 2000 through 4999, select the Ignore Additional Input (Locked) check box for all keystrokes except for 2, 3, and 4. If this is selected for these options, callers cannot dial another extension while listening to the greeting page. After all options are selected, click **Save**.

From the Edit Caller Input toolbar, select **User > Caller Input**. The Caller Input page is now displayed showing the new key configuration, as shown in Figure 7-31.

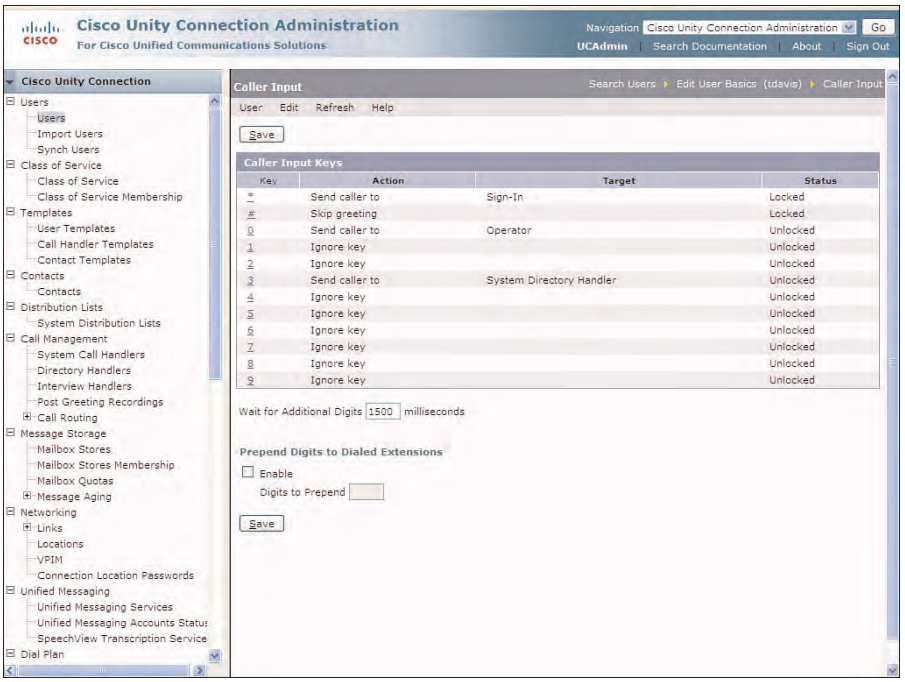

Figure 7-31 *Caller Input Selection with Key Configured for Caller Selection of the Directory*

www.it-ebooks.info

Case Study: Alternate Greetings

Micam-Lyn University has a number of professors located at its main campus in Southern California. These professors might need to travel abroad doing research sabbaticals for extended lengths of time. However, graduate students might need to contact these professors for information related to their thesis projects. The professors currently on sabbatical want to ensure that students get the information and help they need from their administrative assistants.

The university has configured each professor's mailbox with an alternative greeting that instructs the callers of their unavailability, while informing them of several options. One of these options is that they can be transferred to the administrative assistant by pressing **6** at any time during the greeting. A Caller Input selection is configured for this option in each professor's voicemail configuration.

Each professor can enable or disable the alternative greeting without the administrator's involvement through the use of the Cisco Unity Connection phone interface or by using the Messaging Assistant web pages.

Additional options enable the administrator to configure the Message Actions to relay the message, or transfer the call directly to the administrative assistant, depending on the specific needs of each professor.

Post-Greeting Recordings

A new feature available in Cisco Unity Connection version 8.x software is the post-greeting recording. This feature is administratively configured and enables the administrator to record any number of recordings and apply them to specific users or user templates.

When applied to a user's voicemail, they can be used for all callers or just unidentified callers (outside callers). There are no caller input options, and the post greeting recording is informational only, presented to the caller after the system or personal recording and before the After Greeting actions. Any caller input selections configured for this user must be selected by the caller during the user's personal greeting. After the post greeting recording begins, the caller input options can no longer be selected.

An application for this feature might be to inform callers they are transferred to a different department or user, without affecting the user's actual greeting. In this case, the post greeting recording can be configured to play after the user's greeting to notify the callers of the transfer before the actual transfer occurs.

To begin the configuration of Post Greeting Recordings, from the navigation pane on the left portion of the Cisco Unity Connection Administration page, select **Call Management > Post Greeting Recordings**. The Search Post Greeting Recording page displays. No post greeting recordings configure by default. To configure a new recording, select **Add New** to configure a new Post Greeting Recording. The New Post Greeting Recording page displays, as shown in Figure 7-32.

www.it-ebooks.info

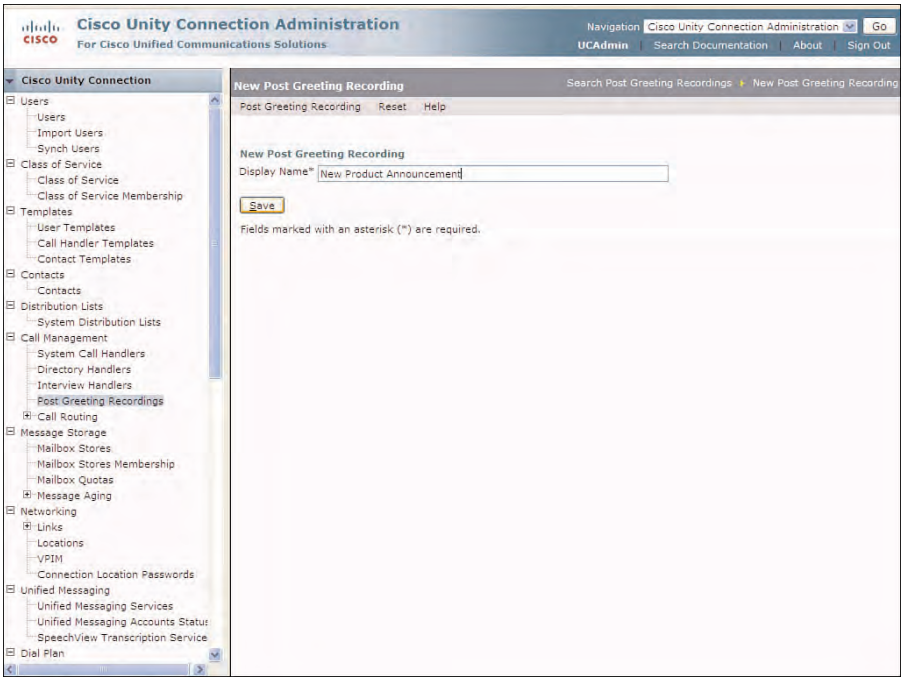

Figure 7-32 *New Post Greeting Recording*

In this example, a short post greeting recording for the sales team is configured informing the caller of a new product release. Enter a descriptive name for the greeting in the Display Name field. Click **Save** to begin editing the recording.

The Edit Post Greeting Recording will be presented enabling the administrator to record the new greeting. Select **Play/Record** to display the Media Master, and click **Record** (in red) to begin the recording process. Optionally, you can use the Options selection from the toolbar and use a .WAV file as the recording. Click **Save** to complete the operation. Figure 7-33 illustrates the completed Edit Post Greeting Recording page.

Note When using the Media Master, consider the options of using computer speakers and microphone, as opposed to using the phone. When the phone is selected for this operation, a port is used for the TRaP operation. There must also be ports configured for TRaP in the phone system integration. If port usage is a concern in the organization, select the **Use Computer** option from the toolbar for Playback and Record. This option is also selectable under the **Options** page, as discussed in the previous chapter.

After the post greeting recording is created by the administrator, the recording needs to be applied to the user's configuration or to an existing user template. The user and user template configurations are similar in their configuration. Therefore, the user configuration for the post greeting recording configuration will be explored.

www.it-ebooks.info

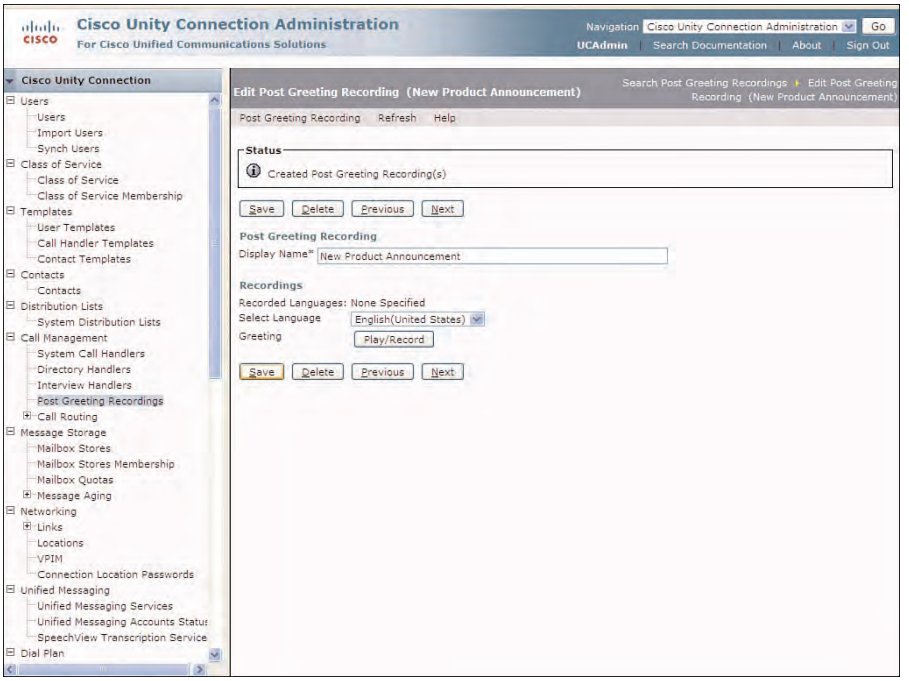

Figure 7-33 *Edit Post Greeting Recording Page*

From the Edit User Basics page of the selected user, select **Edit > Post Greeting Recording** from the toolbar. The Edit Post Greeting Recording Settings page displays. The administrator has the option to play the post greeting recording for all callers, unidentified callers only, or not play the recording, which is the default option. Select the desired post greeting from the Post Greeting Recording Selection drop-down under the Post Greeting Recording section. Finally, select **Save** to complete the operation.

In Figure 7-34, the administrator has configured this user to play the New Product Announcement post greeting to all unidentified callers, or outside callers. In this case, the intention is to play the post greeting for all new and existing customers as they reach the user's mailbox.

Message Notification

Message notification enables a users or a group of users to be notified of specific messages as they arrive to a user's mailbox or distribution list. The notification parameters and devices can be configured by the administrator and modified by the user. For example, if an executive or manager might need to be informed of all urgent messages, the administrator can configure a series of notification devices for this user to receive a notification. These devices might consist of the users' cell phone, home/work phone, pager, or SMTP message. When the users receive the notification, they can retrieve their message by responding to the notification.

www.it-ebooks.info

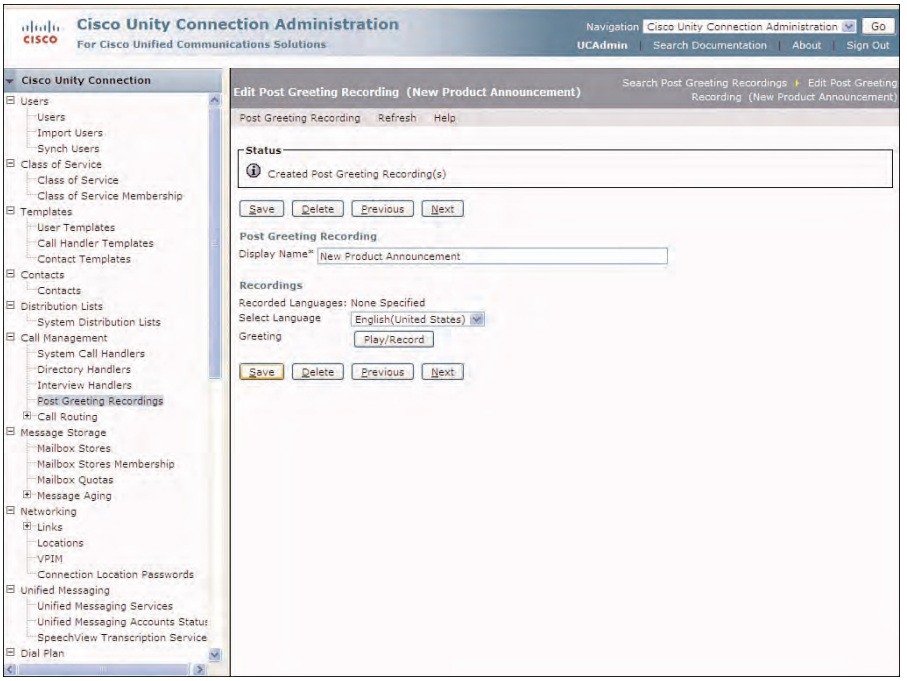

Figure 7-34 *Edit Post Greeting Recording Settings for a User*

This message notification configuration can be applied to a user or user template. In both cases, the configuration of message notification is similar. To configure message notification for the user, select **Edit > Notification Devices** from the Edit User Basics page. The Notification Devices page displays, as shown in Figure 7-35.

By default, message notification is disabled for the five default notification devices. Additional notification devices can be created as required based on the three device types; phone, pager, or SMTP device. The default devices can be modified and enabled as required but cannot be deleted. Click **Add New** to create a new notification device, or select a pre-existing device from the Display Name column to begin the configuration of an existing device.

In this example, the Mobile Phone is selected to provide notification of urgent messages for this user. After the Mobile Phone has been selected, the Edit Notification Device page displays for this device. Under the Notification Device section, check the **Enabled** check box. Also, select the **Urgent Only** check box for the All Voice Messages option under the Notify Me Of section.

Under the Phone Settings, enter the phone number as required in the Phone Number field. The *and # keys can be used as required in this field. Also, a comma inserts a 1-second period of silence. Some phone systems might require a delay between the access code and the presentation of the phone number to be dialed.

www.it-ebooks.info

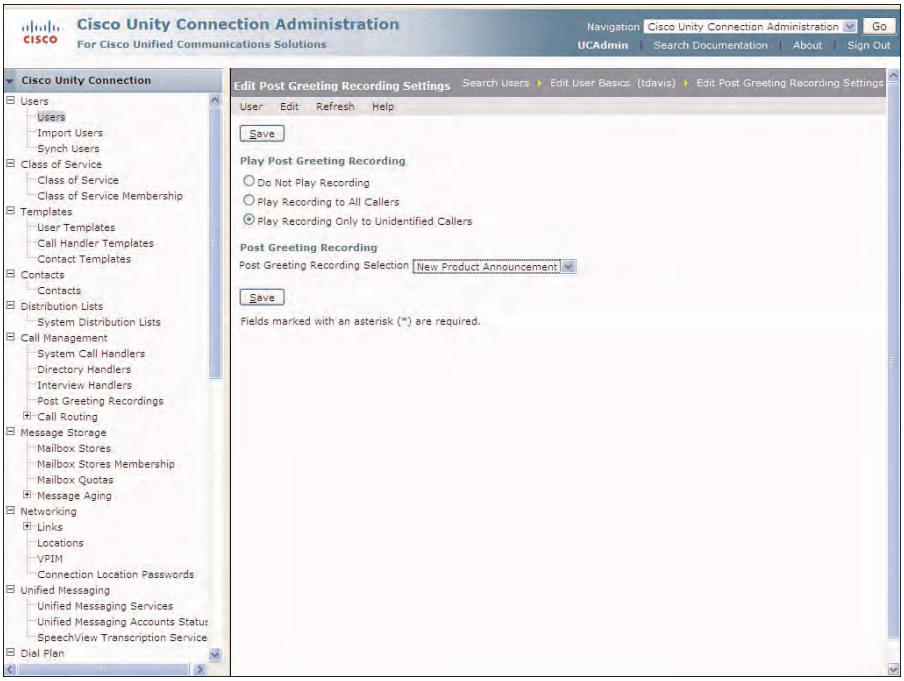

Figure 7-35 *Notification Devices Page of a User in Cisco Unity Connection Administration*

In Figure 7-36, Cisco Unity Connection is configured to send a message notification of urgent messages to the user's cell phone (555-0179). The access code (9) will be preceded by two seconds of silence before the number is dialed. Additional configuration options enable the administrator to configure extra digits after the phone number, busy and ring no answer (RNA) retries, and interval. In this example, the user's cell phone will be retried up to four times every 15 minutes if she does not answer. If the user is busy, the number will be attempted four times, every 5 minutes.

Additionally, notification devices can be concatenated using various timing and delay options. The On Notification Failure option enables the administrator to configure notification on the second device, as displayed in Figure 7-36. Each notification device can be configured with a separate timing and delay.

Note Take care to understand how message notification is used in the organization. Every notification requires the use of a port configured for message notification.

After the devices are configured by the administrator, users can change the numbers and enable or disable message notification using the Cisco Unity Connection phone interface, by selecting the **Setup Options > Message Settings > Message Notification** from the phone interface main menu.

www.it-ebooks.info

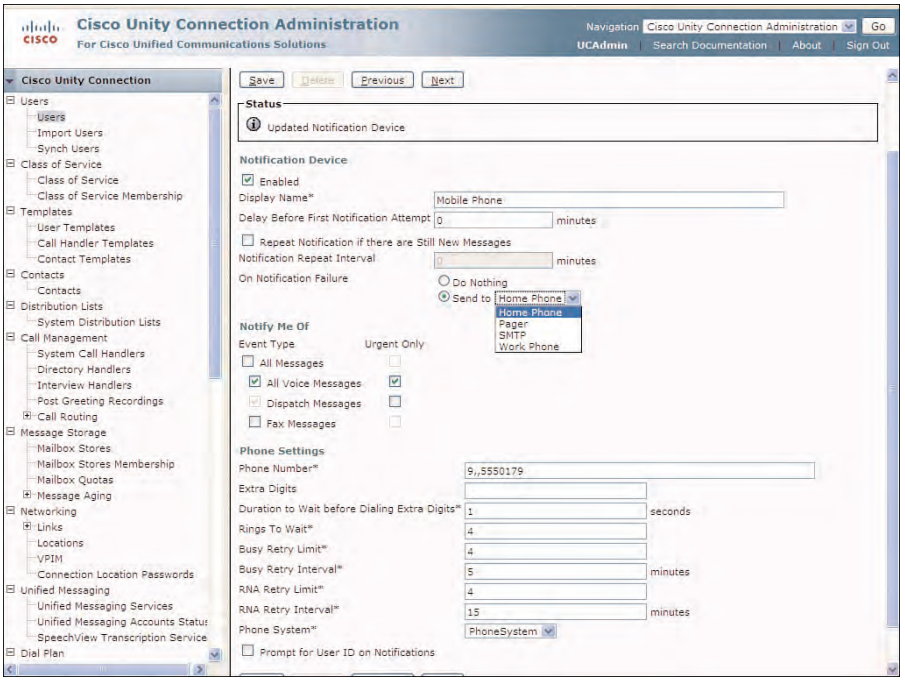

Figure 7-36 *Edit Notification Device Page*

A user with the CoS that enables access to the Messaging Assistant can use this interface to modify message notification. When logged into Cisco Personal Communications Assistant, select **Notification Devices > View Notification Devices** from the toolbar to display the Notification Devices page, as shown in Figure 7-37.

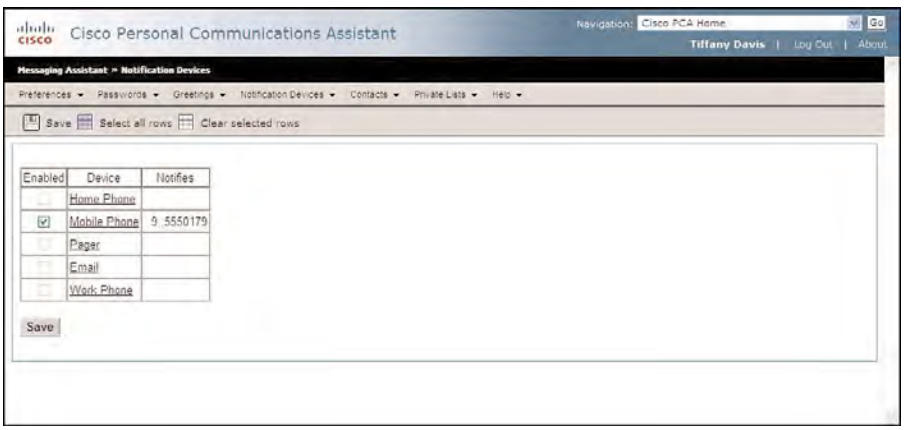

Figure 7-37 *Notification Devices in the Messaging Assistant*

www.it-ebooks.info

Select a notification device from the Device column to configure and enable the device. In the example in Figure 7-38, the Home Phone was selected and configured to notify the users at their home as to any voice messages from Bill Smith. The configuration on this page provides the users with the ability to configure message notification from a user or a specific number pattern and to enable or disable the notification as required.

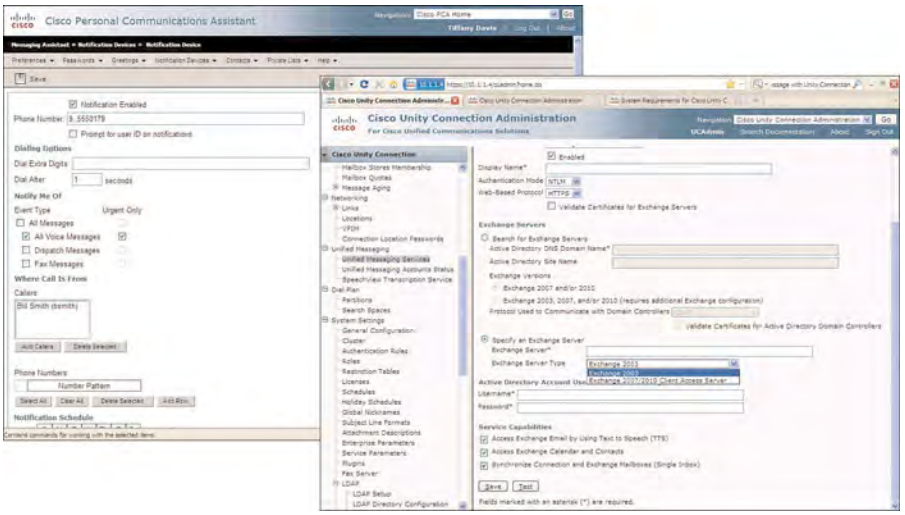

Figure 7-38 *Message Notification Device Modifications in the Messaging Assistant*

Additional options on this page enable the user to configure a notification schedule as required. In this example, the schedule was cleared by selecting the **Clear Schedule** button on the Notification Schedule. Then, the Quick Add option was used to add a notification schedule of 9 a.m. to 5 p.m. for Monday through Friday.

The options on the Messaging Assistant enable the users to administrate many of the features of their own voicemail, which would otherwise need to be managed by the system administrator. This empowers the users and saves the administrator's time having to manage all message notifications.

Alternative Extension Features and Restriction Tables

Alternative extension enables the users to perform Easy Message Access to their messages from other locations, or outside extensions. When configured, users can have their cell phones and home phones configured as an alternative extension. This feature enables the users to automatically access their voicemail from other phones when calling to Cisco Unity Connection, as discussed in Chapter 6. An additional feature of alternative extensions is that they can be added automatically as the users access their voicemail repeatedly from the same phone number.

www.it-ebooks.info

Cisco Unity Connection keeps a history of the Caller ID when user access their voicemail from a remote location. By default, if the users call in to Cisco Unity Connection five times within a 30-day period, this number is offered as an alternative extension. The users must acknowledge the addition of this phone number; otherwise, the extension is not added. If the user declines this action, this specific number is never offered again to be added as an alternative extension. However, after the number is added as an alternative extension, the users need to enter only their voicemail password to access their voicemail. From this point forward, the users can access voicemail in much the same way they do from their desk phone. Removing an alternative extension must be performed manually because there is no option to automatically remove an alternative extension that has been added automatically.

The configuration for the automatically added alternative extension can be modified in the advanced settings of Cisco Unity Connection Administration. The Conversation Configuration page displays, as shown in Figure 7-39. To view or modify the default options, select **System Settings > Advanced > Conversations** in the navigation pane. There are two options that define the alternative extension feature. The first option, Sign-In Count for a Number Before It Is Offered as an Alternate Extension, has a default configuration of five, which sets the number count, or history, before the number is offered to the user as an alternative extension. The second option, Consecutive Days to Count Sign-In for a Number, defaults for 30 days. This sets the number of days before the history counter is reset. Both options can be modified from their default configuration.

For a user to automatically add alternative extensions, they must belong to a CoS that provides this feature. Their specific Cos must have the option Allow Users to Manage Their User-Defined Alternate Extensions selected under the Alternate Extensions section. Otherwise, this feature will be unavailable to the user.

In certain case, there might be a need to restrict specific phones or numbers from being automatically added as alternative extensions. For example, you might want to restrict internal extensions or phones in public areas of the organization from being added as a user's alternative extension. In these cases, the restriction table includes a listing of numbers that will not be added to the alternative extension list. To view and modify these features, select **System Settings > Restriction Table** from the navigation pane on the left. The Search Restriction Tables page displays, as shown in Figure 7-40.

This listing includes a number of different restriction tables:

- **Default Fax:** Restricts dialing capabilities for faxes
- **Default Outdial:** Restricts dialing out for message notification
- **Default System Transfer:** Restricts system transfer dialing
- **Default Transfer:** Restricts user-defined transfer dialing
- **Excluded Extensions for Automatically Added Alternate Extensions:** Restricts specifically configured extensions and ranges from being added as alternative extensions

www.it-ebooks.info

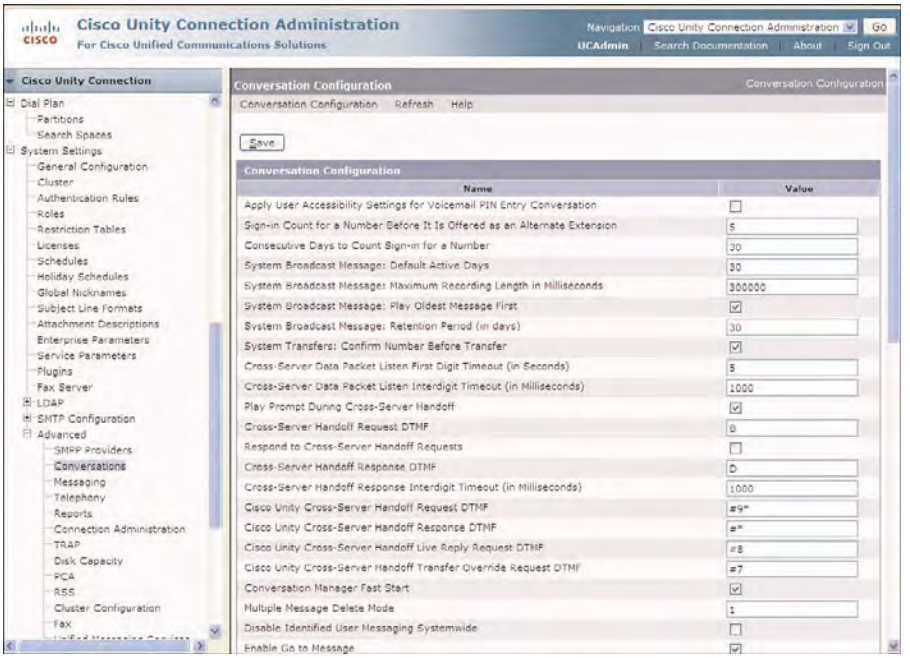

Figure 7-39 *Conversation Configuration Options That Affect Alternative Extensions*

Each restriction table is used for each specific purpose: to restrict faxes, message notifications, transfers, or alternative extensions. The first four options provide security by controlling toll charges; disallowing users to make long distance or international calls from Cisco Unity Connection for faxes, message notification, or transfers. By default, each of these restriction tables is configured identically. Therefore, the alternative extension restriction tables will be discussed next because they apply to the automatic addition of alternative extensions.

To begin, select the **Excluded Extensions for Automatically Added Alternate Extensions** option from the Display Name column on the Search Restriction Tables page. Figure 7-41 shows the Edit Restriction Table Basics page.

By default, the restriction tables restrict all long distance, international, 900 numbers, or any number that is 11 digits or more. To review the special characters used in the restriction table, the **?** character designates any digits (0 through 9), whereas the * character designates one or more of any digits.

All pattern restrictions are acted on in a top-down fashion, where the final pattern is defined as an "explicit allow," meaning that everything remaining is allowed. The Blocked check box determines whether the pattern is allowed or blocked. When the pattern is matched, any other restriction patterns will not be used or acted on for that pattern. Therefore, as a best practice you should always configure the more specific rules to be a

www.it-ebooks.info

higher order (lower order number). The order is viewed in the Order column of the Edit Restriction Table, as shown in Figure 7-41. The final explicit allow pattern matches any number (one or more digits), where the Blocked check box is unchecked. All other patterns above are blocked according to their order.

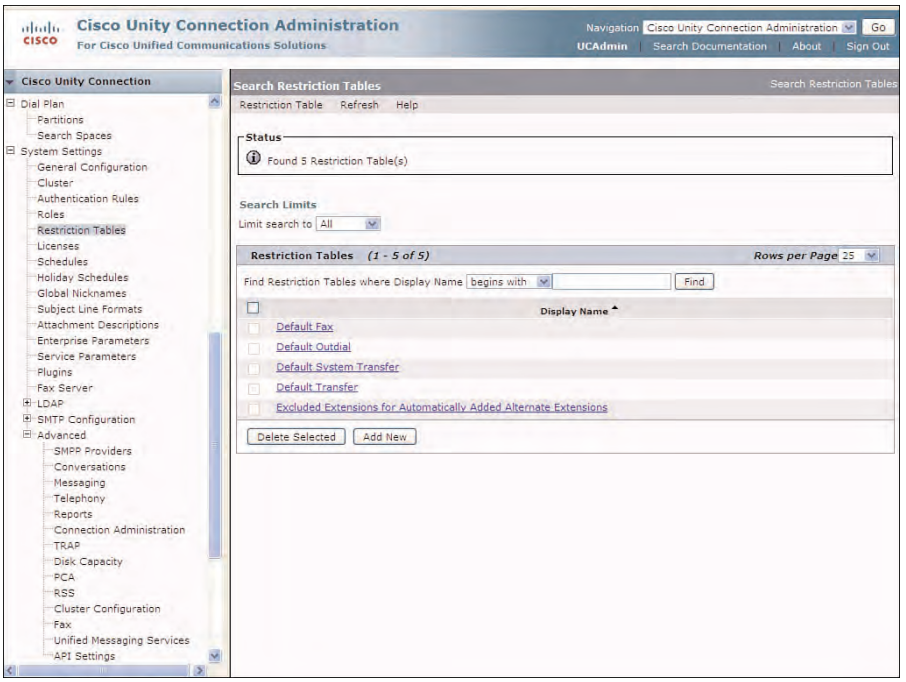

Figure 7-40 *Search Restriction Tables*

The explicit allow pattern is the only pattern that cannot be removed or edited because this enables all remaining patterns that do not match the previous restriction patterns. If the administrator desires to make the restriction table completely unrestricted, all patterns could be removed, except for this final explicit allow pattern.

The administrator can add new pattern to the table by clicking **Add New**. The new pattern is added to the top of the restriction table, enabling the administrator to configure the specific pattern.

If required, the order of the patterns can be changed by selecting the Change Order button. The Change Restriction Pattern Order page displays, as shown in Figure 7-42. At this point, the administrator can change the order of the new and existing patterns as needed.

In this example, two restriction patterns have been added for internal extension of 3000 through 4999, preventing users from automatically adding these numbers to their existing alternative extensions. These two new restriction patterns have been moved to the bottom of the list, after the 900 restriction pattern, though this action is not required.

www.it-ebooks.info

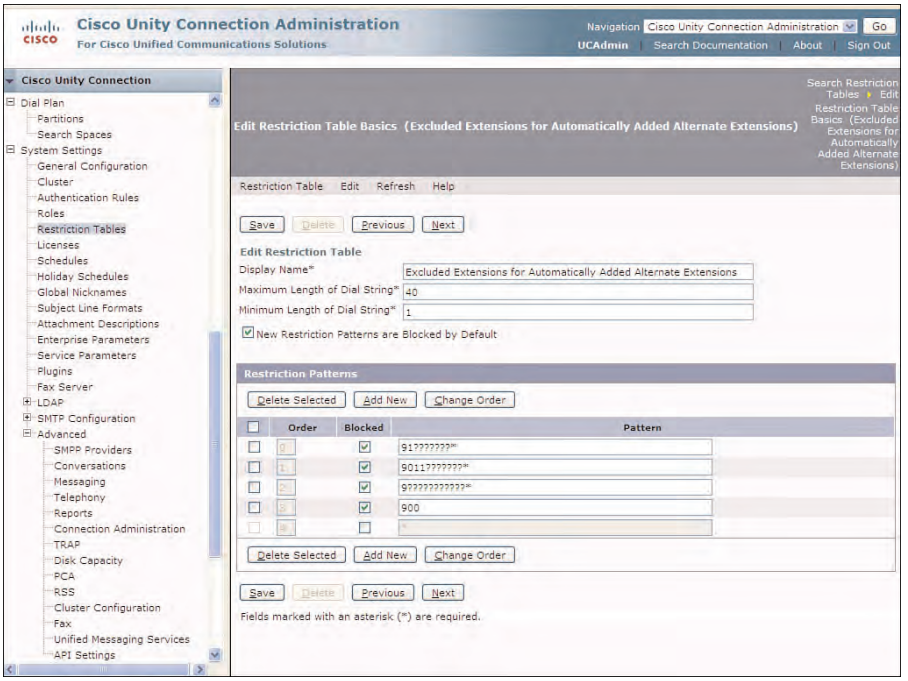

Figure 7-41 *Edit Restriction Table Basics*

Caution Take care while making changes to restriction patterns. Any changes made to any pattern or additional pattern configured in the Restriction Tables affect all users.

Distribution Lists: System and Private

Distribution Lists provides users with the ability to send or forward voice messages to a group of users without having to address the message to each individual user. In the case of System distribution lists, they can be made available to users and selected through the directory. Distribution Lists could be created for specific groups of users according to location or job function. For example, All Phoenix Employees or All Software Engineers Distribution Lists could be used to send messages to these users that are part of these groups.

System distribution lists can be made available to all users, whereas Private distribution lists or Private Lists are available only to a specific user.

System Distribution Lists

System distribution lists enable users to send and forward voice messages to users in much the same fashion that distribution lists are used for email. In this case, the user can search the directory for a distribution list to send or forward a voice message to a group

www.it-ebooks.info

of users who are members of the distribution lists. All distribution lists are created specifically by the administrator in Cisco Unity Connection Administration.

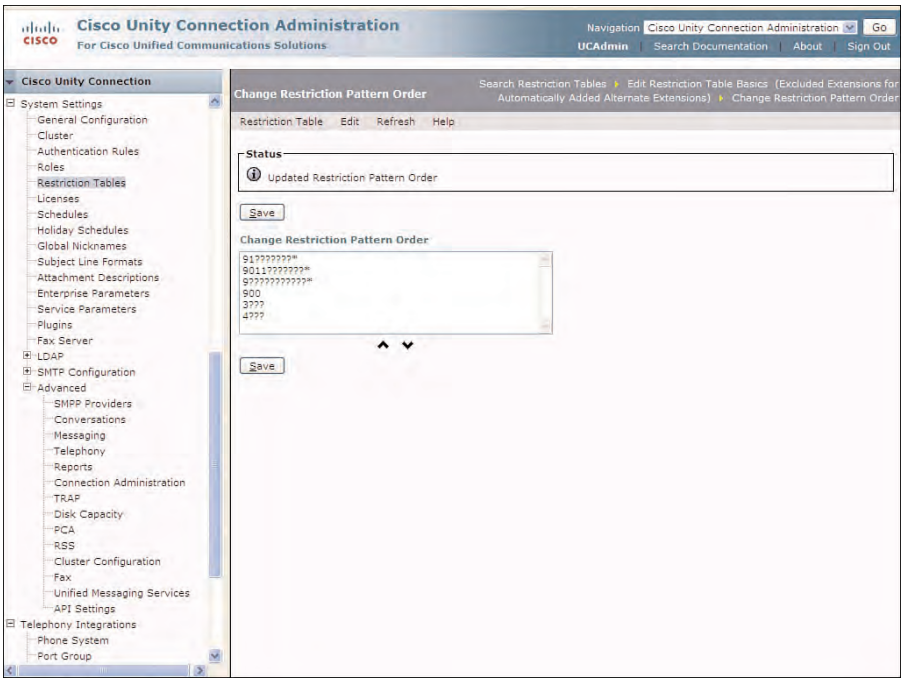

Figure 7-42 *Change Restriction Pattern Order*

To view, create, or modify the distribution lists, from the navigation pane in Cisco Unity Connection Administration, select **Distribution Lists > System Distribution Lists**. Figure 7-43 shows the Search Distribution Lists page.

Three System distribution lists are created by default at the time of installation:

- **undeliverablemessages:** This distribution list receives any messages from outside callers that cannot be delivered because the user has either been deleted or is not found. These messages are forwarded to all members of this distribution list.
- **allvoicemailusers:** This distribution list contains all users and templates created as Users with Mailboxes.
- **allvoicemailenabledcontacts:** This distribution list can be used to send messages to VPIM contacts. You explore VPIM contacts in Chapter 10, "Implementing Voice Profile for Internet Mail (VPIM)." There are currently no members included in this distribution list.

These three distribution lists are protected by the system and cannot be deleted; however, they can be modified as needed, and users can be added. The **allvoicemailusers** and **allvoicemailenabledcontacts** distribution lists are configured specifically with extension

www.it-ebooks.info

99991 and 99992, respectively. This enables users to address messages to these lists by using number dialing. Number dialing can be accomplished when a user is addressing messages via the Cisco Unity Connection phone interface. To switch between name and number dialing, a user can select **##** on the phone.

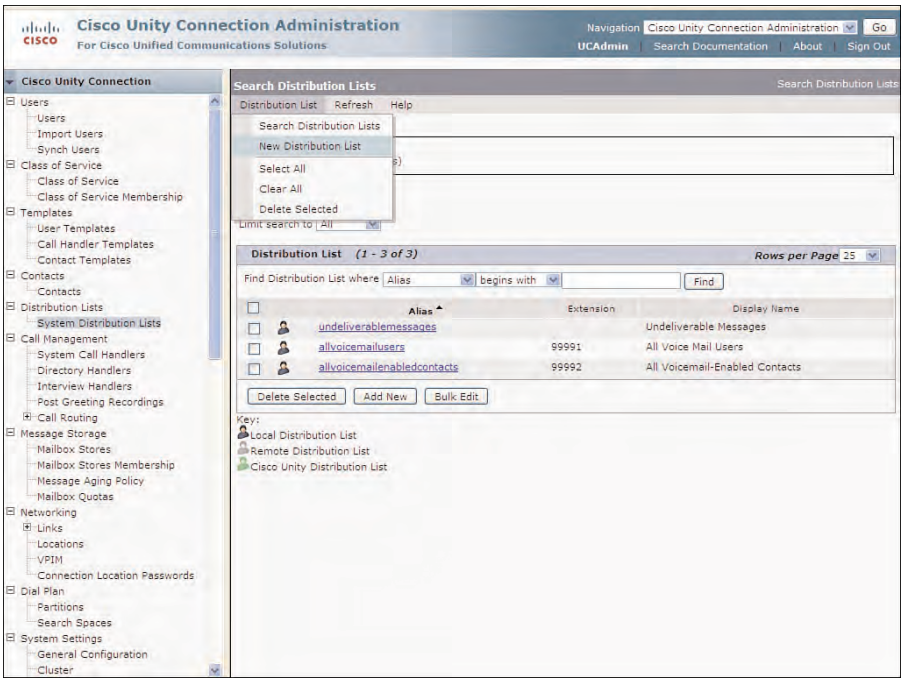

Figure 7-43 *Search Distribution Lists Page in Cisco Unity Connection Administration*

To create a new distribution list, either from the toolbar on the Search Distribution List page, click **Add New** or select **Distribution Lists > New Distribution List**, as displayed in Figure 7-44. The New Distribution page displays.

Enter a name for the new distribution list in the **Alias** field. The **Alias** is the unique identifier that will be used by users to address messages by using name dialing. The Display Name is the name Cisco Unity Connection uses to notify the users to whom they are addressing their message.

The **Replicate to Remote Sites Over Intersite Links** check box enables this distribution list to be replicated to other server in the digital network. In Chapter 9 you discover these capabilities in the digital networking chapter. By default, this feature is enabled.

The **Allow Contact** check box enables for VPIM contacts to be included as members of the new distribution list. By default, contacts are not allowed to be members of the distribution list. If VPIM contacts are allowed, this distribution list cannot accept messages from other messaging systems configured to use VPIM.

www.it-ebooks.info

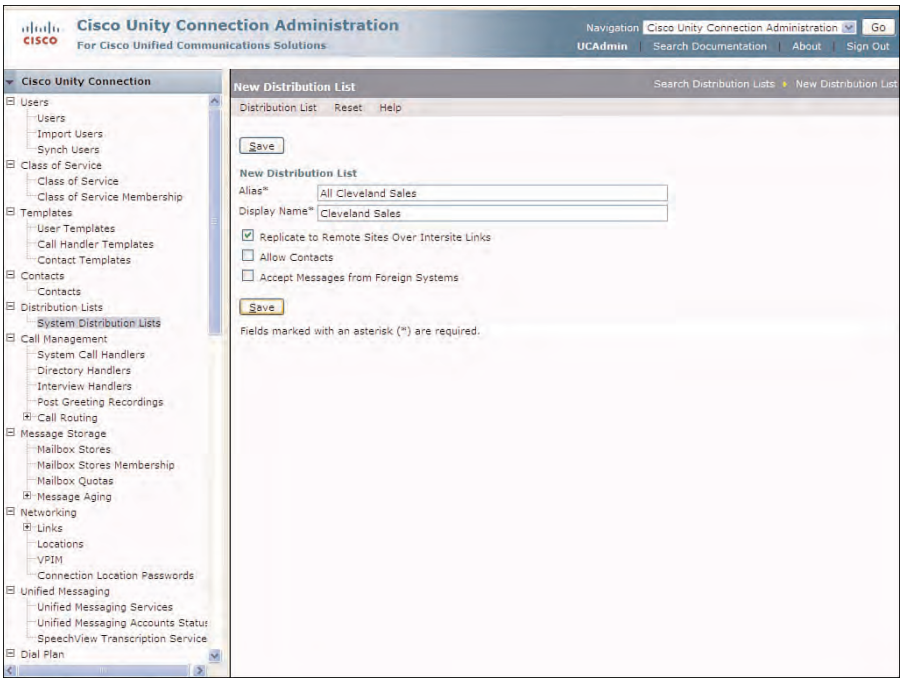

Figure 7-44 *New System Distribution List*

The **Accept Messages from Foreign Systems** check box enables for remote systems configured using VPIM to send messages to this distribution list.

In Figure 7-44, a new distribution list is created for All Cleveland Sales. Users address messages by entering the Alias of All Cleveland Sales. Voice Recognition users could simply speak the Alias when addressing their message.

When the administrator clicks **Save** to save the new distribution list, the Edit Distribution List Basics page displays. From this page, the administrator could enter a unique extension or record a name. The recorded name and extension are entirely optional. If you include an extension, users can address messages to this distribution list using number dialing. Otherwise, name dialing must be used to address or forward messages. If you click **Play/Record** and decide to record a name, this recorded name will be used to identify the list. If a name is not recorded, the Display Name will be used as the name of the distribution list.

The new distribution list needs to include the desired users as members. Users are automatically added to the default **allvoicemailusers** distribution list. However, any other distribution list membership needs to be configured in Cisco Unity Connection Administration.

Users can automatically be added to a specific distribution list by adding the User Template that is used to create the user to be a member of the distribution list. Also,

www.it-ebooks.info

other distribution lists can be added to other distribution lists. For example, a distribution list for All Cleveland Sales might be included in a distribution list called All Cleveland Employees.

To assign membership to a new or existing distribution list, from the toolbar on the Edit Distribution List Basics page, select **Edit > Distribution List Members**. The Distribution List Members page displays as in Figure 7-45.

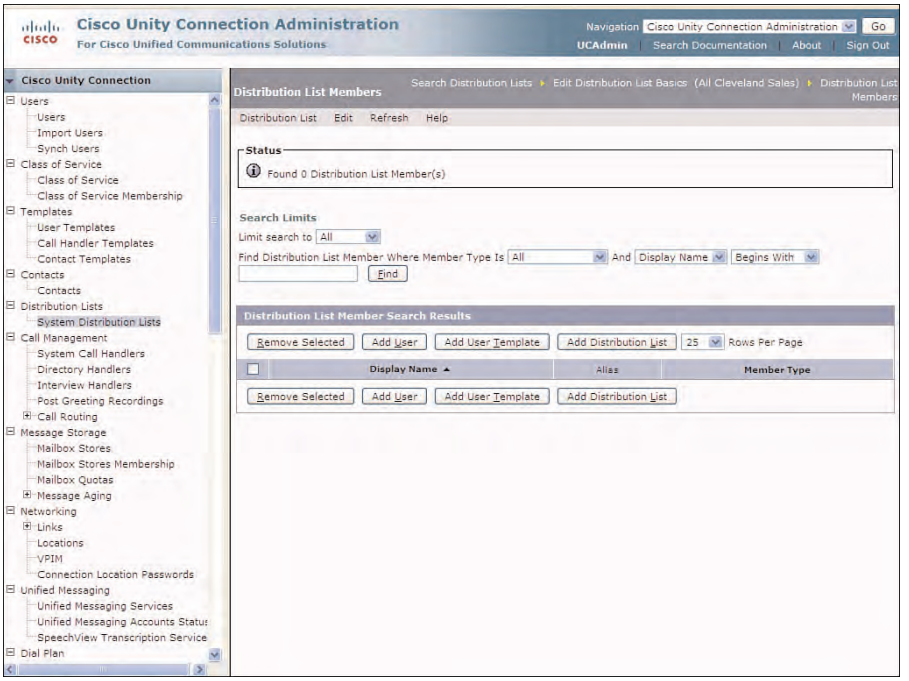

Figure 7-45 *Distribution List Members Page*

Select the **Add User** button to add new users to this distribution list. The Available Users Search Results page displays in a pop-up window, as displayed in Figure 7-46. If VPIM contacts are allowed as part of this distribution list, these will be listed as well. Next, select the specific users to be added to the list, and click **Add Selected** followed by the **Close** button to complete the operation.

After closing the pop-up window, The Distribution List Members page displays as in Figure 7-47. From this location, the administrator can remove members, add new users, add user templates, or add other distribution lists.

In this example, two users, Alan White and Bill Smith, were added to the All Cleveland Sales distribution list. The Executive Template (**Exec_Users_Template**) was also added to this distribution list.

www.it-ebooks.info

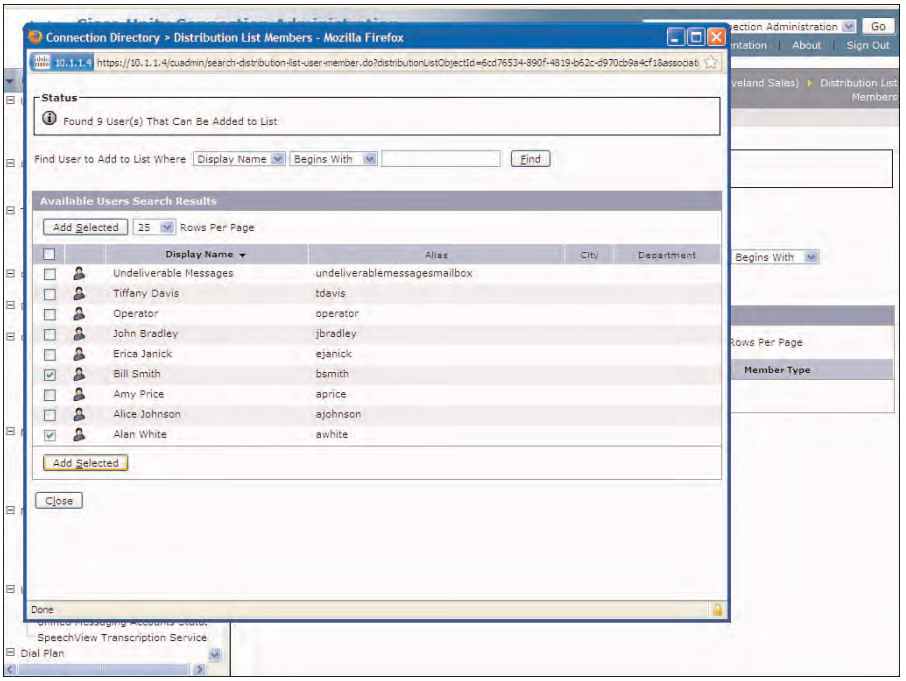

Figure 7-46 *Distribution List Membership: Add Members*

Then, a new user, Bob Johnson, was created with this template. Because the template, Executive Template, used to create the user was a member of the distribution list at the time the user was created, this user is automatically assigned as a member of this list.

You can also configure alternative names for distribution lists. In some cases, users might know a location by a different name or spelling. For example, the Cleveland office might be known as Corporate or Headquarters. If users address messages using these names, the list can be located by these names. To configure the alternative names for system distribution lists, from the toolbar of the Distribution List Members page, select **Edit > Alternate Names**. The configuration of the alternative names for distribution lists is similar to the alternative name configuration for users.

Cisco Unity Connection version 8.x also adds the capability to create a system distribution list access list to provide further granularity for a user to send messages to any specific distribution list. In this case, you create a second distribution list that includes the defined suffix. This changes the list from a distribution list to a distribution list access list. The members of this list are the defined users that are allowed to send messages to the corresponding distribution list. However, these users must also be assigned to a search space that includes the partition of the distribution list.

www.it-ebooks.info

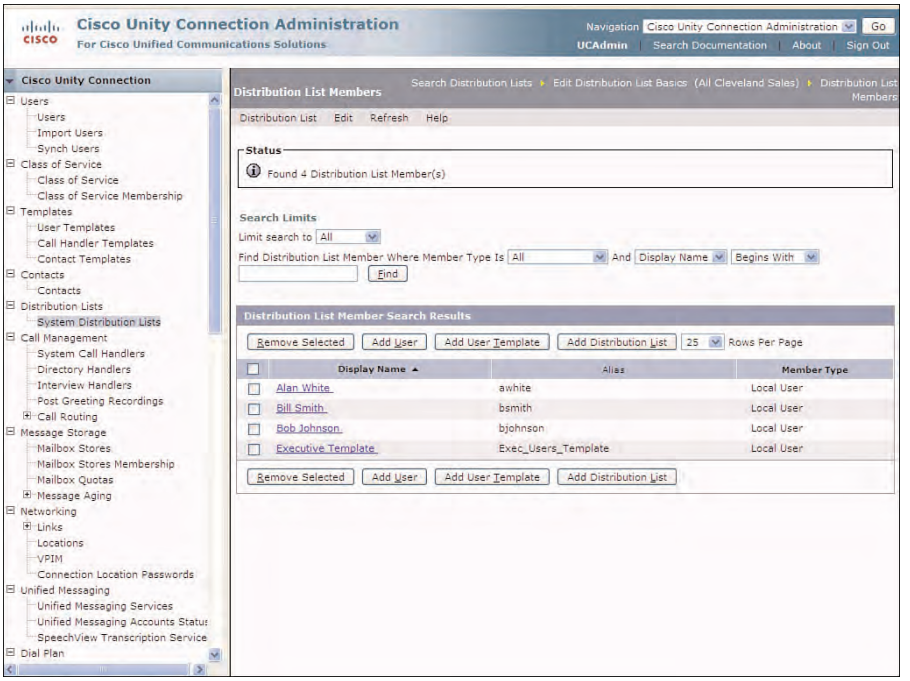

Figure 7-47 *Distribution List Members Page Configured for a New Distribution List*

Case Study: Configuring System Distribution List Access Lists

Tiferam has a large number of system distribution lists throughout its organization. It has a need to further limit access to the **Allsales_DL**. This access needs to be more granular than what search spaces and partitions provide. Therefore, the organization has decided to enable the distribution list access list feature to provide this access. First, it enabled the feature by selecting the Use Access Lists to Control Who Can Send to System Distribution Lists option under the **System Settings > Advanced > Messaging** page in Cisco Unity Connection Administration, as shown in Figure 7-48.

Then, administration created a new system distribution list with the same name, Allsales_DL, followed by the suffix configured in the Secure Messaging Configuration page for the System Distribution List Alias Suffix for Access Lists option.

In this case, the access list for this system distribution list will be **Allsales_DL-accesslist**. The membership of this list determines who can send message to the corresponding access list, **Allsales_DL**. Figure 7-49 illustrates the System Distribution Access List for the Allsales_DL.

www.it-ebooks.info

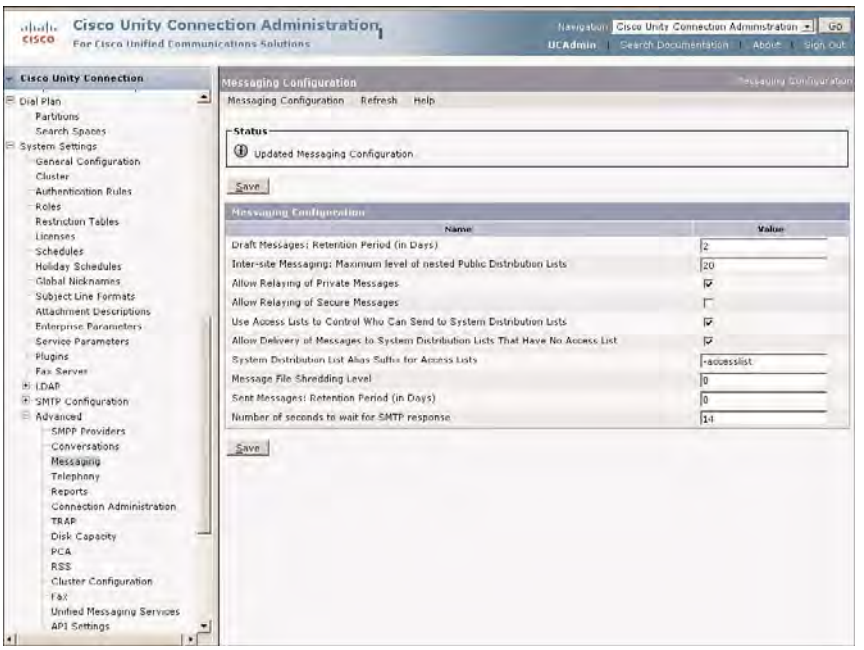

Figure 7-48 *Secure Messaging Configuration Page*

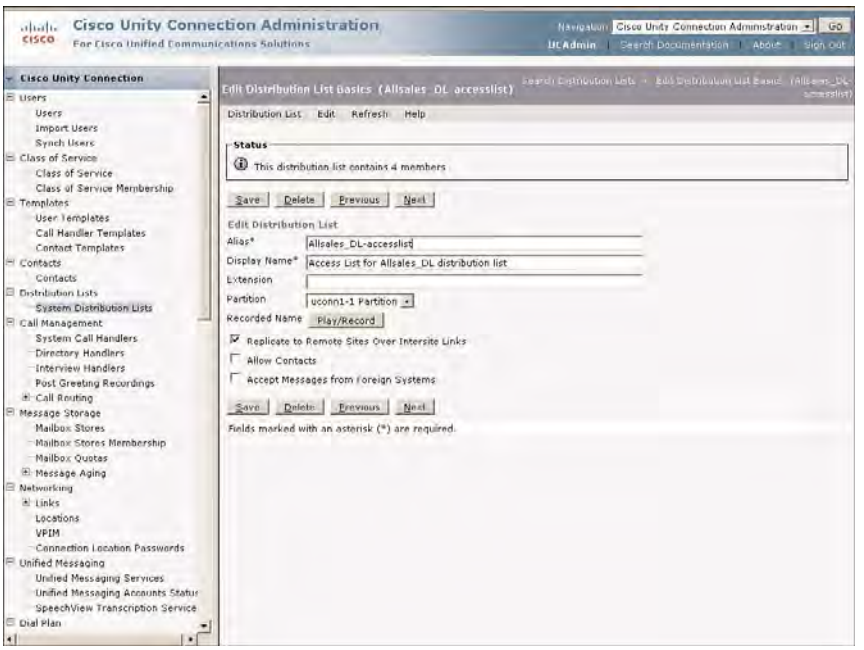

Figure 7-49 *System Distribution List Access List Configuration*

www.it-ebooks.info

Private Distribution Lists

Private distribution lists, or Private Lists, are configured by either the administrator or user, if their CoS enables this feature. The default CoS enables the user to have up to 25 lists with as many as 99 members each, as displayed in Figure 7-50. To disallow the use of private lists, the administrator would need to create a new from the toolbar of the Distribution List Members page, or modify an existing from the toolbar of the Distribution List Members page and not allow the user access to the Messaging Assistant. Additionally, the administrator can modify the from the toolbar of the Distribution List Members page configuration for maximum private lists per user to 1 and maximum members per list to 1. This would enable the user to create only a single private list with one member, rendering the private lists feature useless. The maximum number of private lists that can be allowed is 99 lists with up to 999 members each.

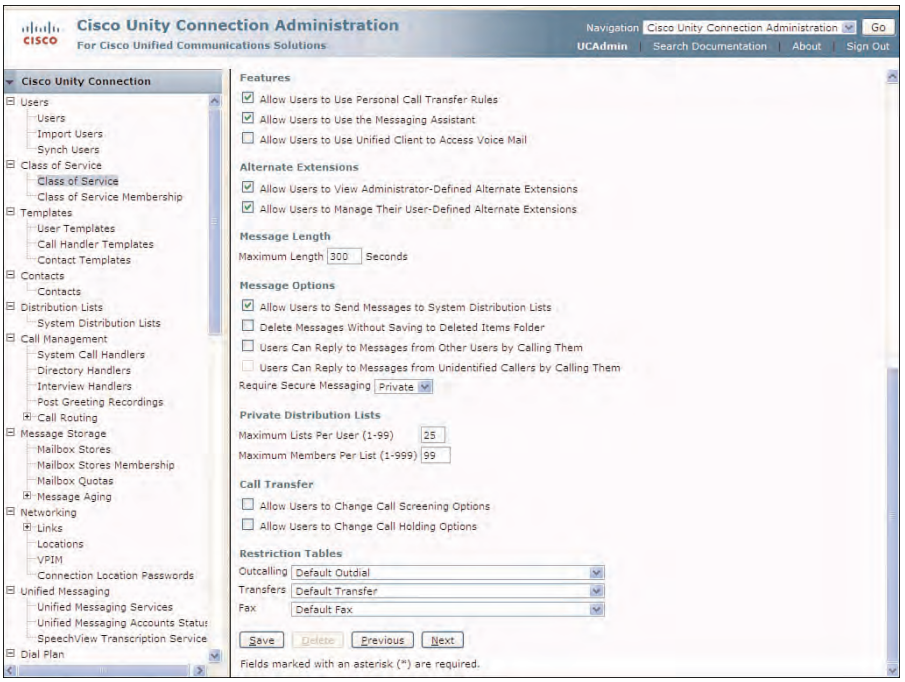

Figure 7-50 *Class of Service Configuration for Private Distribution Lists*

The administrator could create private lists for the user through Cisco Unity Connection Administration, or the user can create the private lists through the Messaging Assistant. To create a private distribution list, the administrator would select **Edit > Private Distribution Lists** from the Edit User Basics page. The private list configuration for the user within the Messaging Assistant page is opened, as shown in Figure 7-51. This will be the same page that displays for the user when they create a private list in the Messaging Assistant.

www.it-ebooks.info

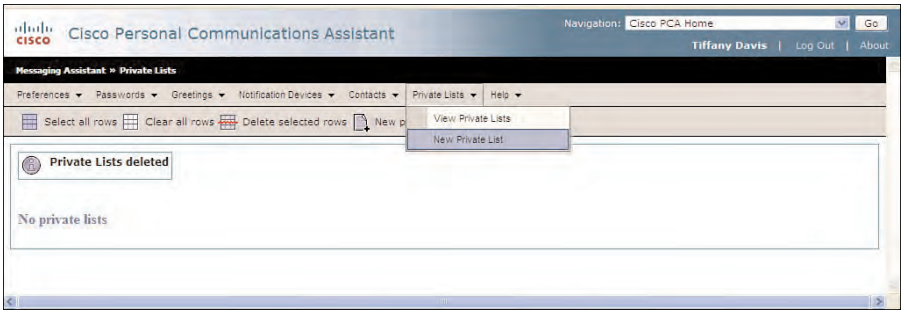

Figure 7-51 *Private Distribution Lists Using the Messaging Assistant*

From this page, the administrator could select the **New Private List** option, or select **Private Lists > New Private List** to create a new list. Enter a name for the new list in the Name field. To add members to the new private list, click **Add Members**. A pop-up window displays enabling the administrator to search for users, contacts, distribution lists, or other private lists. From this page, the administrator can select users as needed. Finally, click **Add Members** to complete the configuration of the new private distribution list. The private list page now displays reflecting the new lists with the selected member, as shown in Figure 7-52.

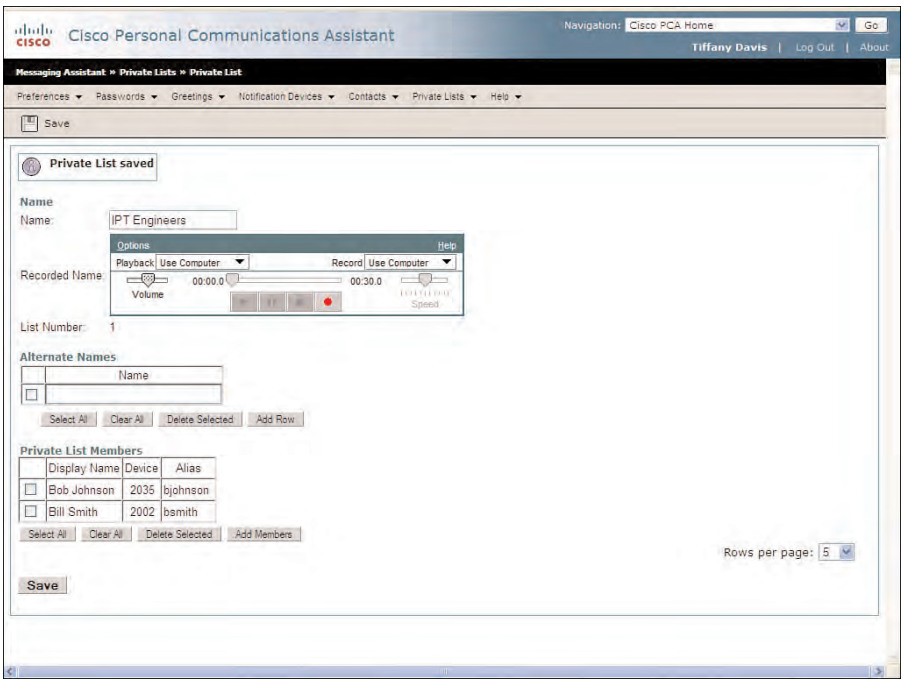

Figure 7-52 *New Private Distribution List Created in the Messaging Assistant*

www.it-ebooks.info

You can also add a recorded name to the private list to inform the users of the addressing of their message. If a recorded name is not included for the list, the Name field will be used.

In this example, a private list for IPT Engineers was created with two members, Bill Smith and Bob Johnson. After all configuration details are entered, click **Save** to complete the configuration of the new private list.

The user configuration of private lists is identical to the procedures mentioned previously. In a user's case, they log in to Cisco Personal Communications Assistant to complete the same configuration steps. For security reasons, the administrator has access to the Messaging Assistant and Personal Call Transfer Rules for the user but is prevented from accessing the Messaging Inbox.

The Private distribution lists created for a specific user are available for use only by that user. Unlike system distribution lists, private lists cannot be used, shared, or exported to other users.

A user can address messages to private lists from the phone interface, or using the Messaging Inbox in Cisco Personal Communication Assistant, as shown in Figure 7-53. In this example, Tiffany Davis is addressing a message to the IPT Engineers about the Engineer Work Schedule. The message sent is 20 seconds in length as shown on the display of the Media Master. The user simply clicks **Send** to send the message.

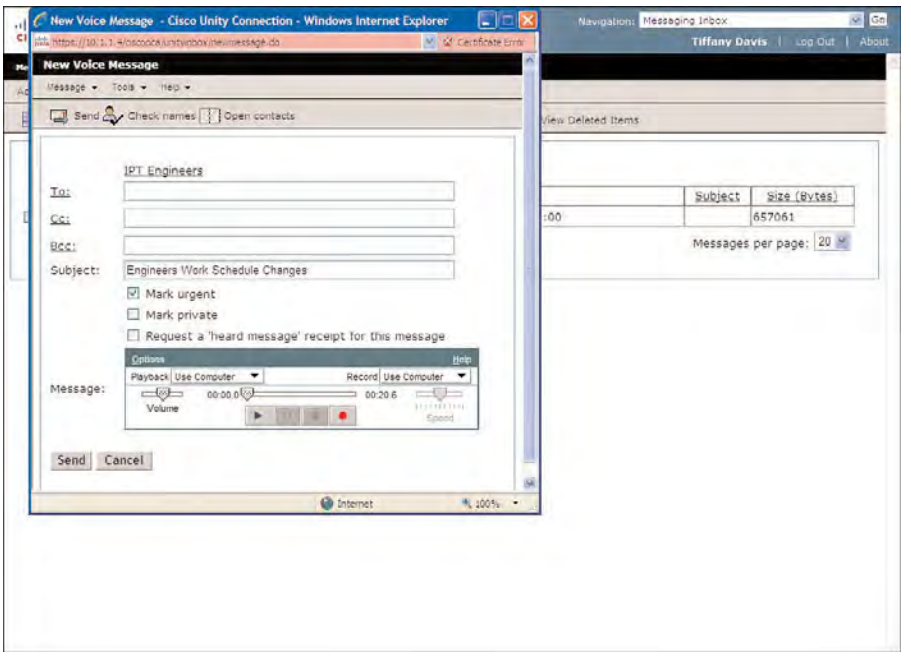

Figure 7-53 *Messaging Inbox: Addressing Messages to Private List*

www.it-ebooks.info

Tip When using distribution lists, both private and public distribution lists, administrators must be aware of the port activity that can occur. Unlike broadcast messages, the MWI light is turned on for all users that receive a message sent to a distribution list. If these users are currently working in the office, and notice the MWI light on their phone, an abnormal amount of port activity might occur as they attempt to retrieve their messages.

External Service Accounts

Cisco Unity Connection version 8.0 and earlier releases enabled integration with various calendar applications including Microsoft Exchange 2003 and 2007 and Cisco Unified MeetingPlace and MeetingPlace Express.

In this case, users can use the Cisco Unity Connection phone interface to send, accept, join, or cancel meetings depending on the application and their rights within the meeting. If using Exchange 2003 and 2007, users can import contacts by using the Messaging Assistant and use these contacts when using the Personal Call Transfer Rules, depending on their configuration and assigned CoS.

The configuration of Microsoft Exchange 2003, 2007, and Cisco Unified MeetingPlace is beyond the scope of this book. Refer to the proper documentation at Cisco.com. The configuration of Cisco Unity Connection to prepare and enable users to access the calendaring integrations is discussed here, however.

To create calendar integrations for a user, an external service account must first be created in Cisco Unity Connection. From the navigation pane on the left in Cisco Unity Connection Administration, select **System Settings > External Service > Email, Calendar, Contacts**. The Search External Services page displays. Click **Add New** to create a new external service account. On the New External Service page, select the type of service from the **Type** drop-down. This Type could be selected as either Microsoft Exchange 2003, 2007, or MeetingPlace 7.0/8.0, or MeetingPlace Express 2.0.

In Figure 7-54, Exchange calendar integration is created for users with Microsoft Exchange 2003. The alias used for the Service Credentials must be a privileged account in Exchange to enable the integration. The Test button on the External Service Account page enables the administrator to test the authentication and configuration. Select the desired Service capabilities for user access. These options enable access to calendar and personal contacts and email in third-party stores. Click **Save** to complete this step.

Finally, each user must be configured to allow access to the service account configured in the previous step. From the Edit User Basics page, select **Edit > External Service Accounts**. The External Service Accounts page displays for this user. Click **Add New** to add a service account. The New External Service Accounts page displays, as shown in Figure 7-55.

www.it-ebooks.info

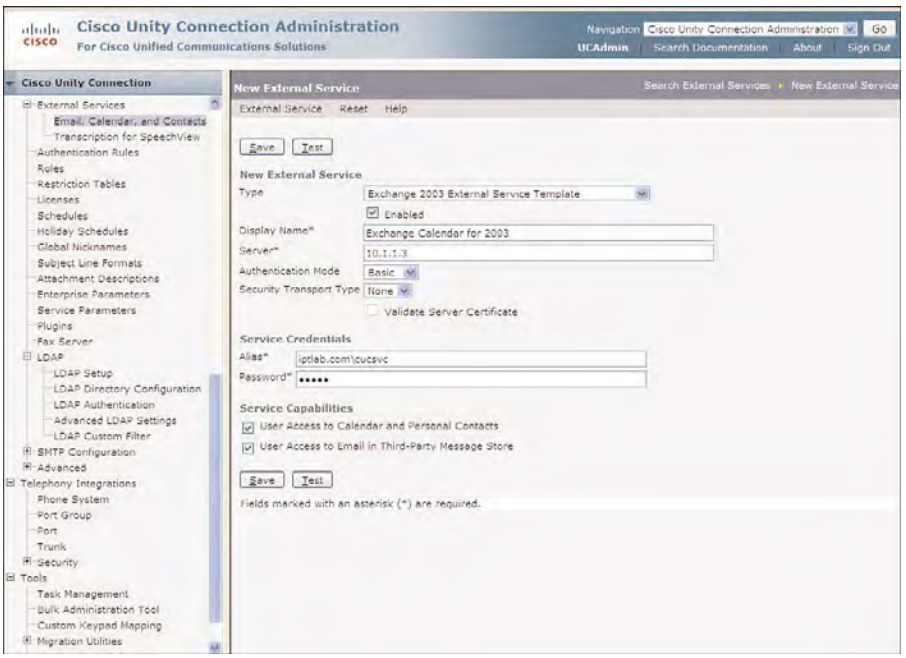

Figure 7-54 *Edit External Service Account Page for Exchange 2003 Integration*

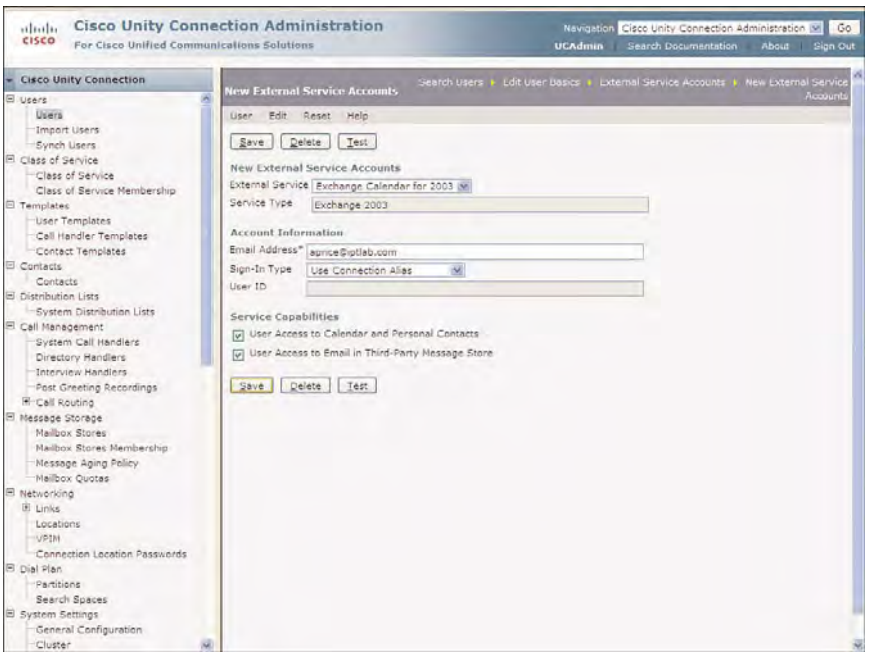

Figure 7-55 *Edit External Service Account Created for a Specific User*

www.it-ebooks.info

In this example, the user, Amy Price, is configured to use the Microsoft Exchange 2003 External Service Account. The email address here should be configured with the primary SMTP address in Active Directory for this specific user.

From this point, the users can receive a list of upcoming meetings when they are logged into their voice mailbox using the phone. They can also accept or decline meeting invitations. If their CoS provides access to the Cisco Personal Communications Assistant applications, these users can view their upcoming meetings and use the Personal Call Transfer Rules to allow or disallow transfers, or call forwarding based on meetings and current availability.

Unified Messaging Service

Cisco Unity Connection version 8.5 changes the external service accounts section to the Unified Messaging section, where the installer would configure similar options under the Unified Messaging Services section. In the current deployment, this is not exactly what would be defined as *unified messaging* in the purest sense of the term.

The meaning of unified messaging is defined here as a single message store for both email and voice messaging. Integrated messaging is defined as a separate message stores for email and voice messaging. (For example, emails are stored on Exchange, whereas voicemails are stored on Cisco Unity Connection.) From a user's perspective with unified messaging, the user would see both their email and voicemails in the same inbox. However, the user's perspective with integrated messaging means that the user would manage their emails and voice messages in separate mailboxes or clients.

With the current deployment of Cisco Unity Connection version 8.5, you can configure access to Exchange, MeetingPlace, or MeetingPlace Express to access emails and calendar information for text to speech. Users can hear the voice messages and calendar events.

Cisco also introduced unified messaging to the Cisco Unity Connection in version 8.5. This new feature is referred to as *Single Inbox*. With this feature enabled, voice messages are first delivered to the user's voicemail on Cisco Unity Connection and replicated immediately to the user's mailbox on Exchange. The user's voice messages are then available to the user from Cisco Unity Connection or the user's Inbox on the Exchange server. Users can then retrieve their messages using the various methods that Cisco Unity provides: phone (Cisco Unity Connection) or ViewMail for Outlook (Exchange).

In essence, this *Single Inbox* type of unified messaging would be more correctly termed *Synchronized Unified Messaging*. In this case, a message updated in one delivery location is updated in the other; however, not all messages are synchronized between the two systems. For example, broadcast, sent, draft, and unaccepted dispatch messages are exceptions and are not synchronized with Exchange.

www.it-ebooks.info

Using ViewMail for Outlook with Single Inbox

Voice messages are handled differently depending on whether the user uses (or doesn't use) ViewMail for Outlook. When a user listens to messages using ViewMail for Outlook, the message condition (read, unread, and deleted) is synchronized with Cisco Unity Connection. If ViewMail is not installed, Outlook handles any voice messages as an email with a .WAV attachment. Therefore, Cisco Unity Connection treats any forwarded voice messages to other users as emails. In this case, the message routing is handled entirely by Exchange and thereby never sent (or synchronized) to the recipient's mailbox on Cisco Unity Connection.

ViewMail for Outlook also enables the user to listen to secure messages and prevent the forwarding of private messages. Without ViewMail, the user cannot listen to secure messages, and might forward private messages because voice messages will be forwarded as emails with .WAV attachments.

Secure messages are never stored on the Exchange server. A secure message is replicated only as a "decoy" message, where the user chooses to play the secure message. The secure message is then retrieved from the user's mailbox on Cisco Unity Connection.

Configuring Single Inbox

To configure the service, select **Unified Messaging > Unified Messaging Service** in Cisco Unity Connection Administration. Click **Add New** on the Search Unified Messaging Service page to create a new service. Select the service type from the Type drop-down. The currently supported types follows:

- Exchange 2003, 2007, and 2010 (for Single Inbox)
- MeetingPlace 7.0
- MeetingPlace 8.0
- MeetingPlace Express 2.0

Figure 7-56 illustrates this configuration for the Exchange server. Cisco Unity Connection can be configured to search for an Exchange server in a domain or be statically configured. In this example, the configuration displays with the corporate Exchange server. Also, you must configure an SMTP Smart Host before completing the configuration settings on this page; otherwise, the options on the Unified Messaging Service page will not be saved.

The Unified Messaging section also includes the SpeechView, which is discussed in Part III.

www.it-ebooks.info

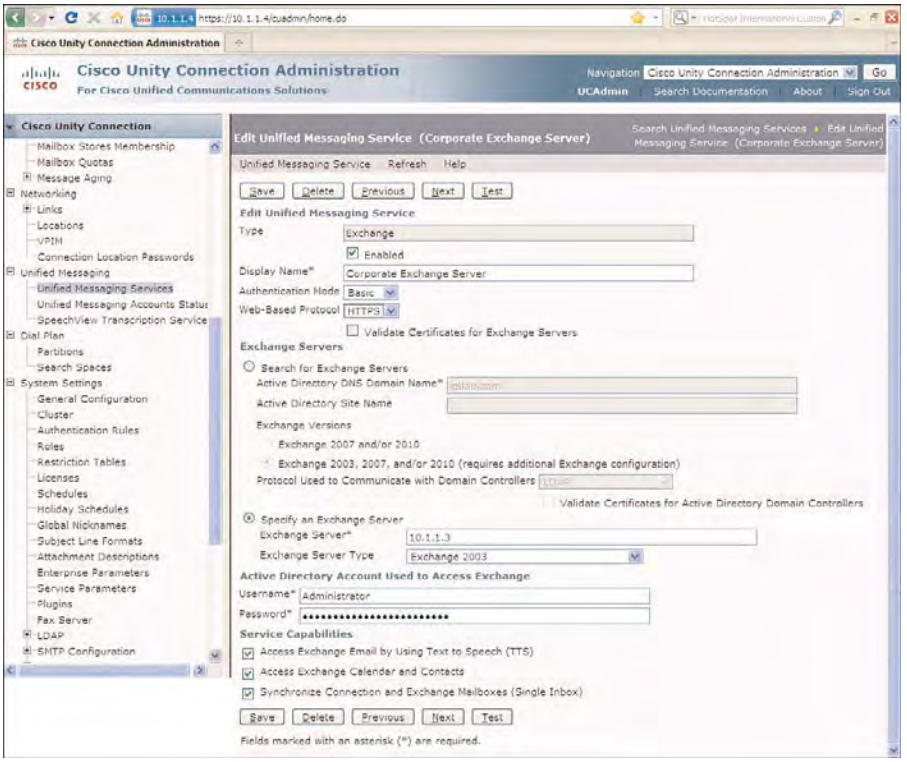

Figure 7-56 *Unified Messaging Service Configuration*

User Configuration for Single Inbox

After the Unified Messaging Service is complete, you need to enable users to use the Single Inbox feature. To begin, select the user from the Search Users page in Cisco Unity Connection Administration, followed by selecting **Edit > Unified Messaging Accounts** from the toolbar. The Unified Messaging Accounts page displays, as shown in Figure 7-57. Select the **Add New** button to configure a new unified messaging account for this user.

For the Single Inbox, you want to specify the proper Exchange service, SMTP address, and corporate email (Exchange) address. The Unified Messaging Account settings enable the administrator to select a different email address if it is different from the corporate account. You also have the option to change this option on the Edit User Basics page under the option called Corporate Email Address. In most cases, you want to ensure that the SMTP proxy address for the user is the same as the user's corporate email account.

www.it-ebooks.info

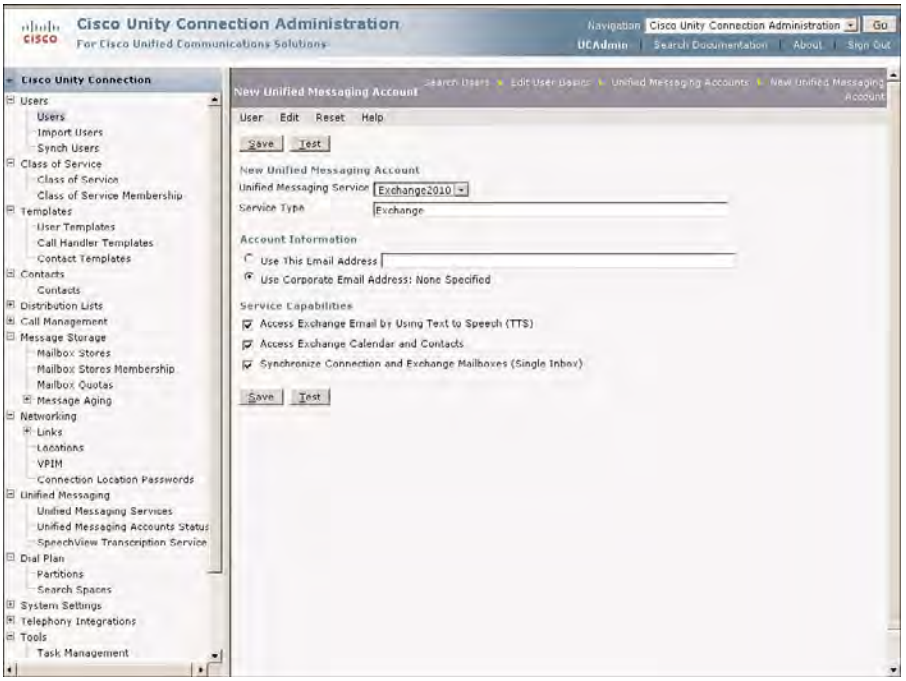

Figure 7-57 *Unified Messaging Account Configuration Page*

SMTP Proxy Addresses

The final configuration option about user configuration that you explore in this chapter is the SMTP Proxy Address. Simple Mail Transfer Protocol (SMTP) is the protocol that sends and receives messages when using the IMAP client. If a user uses an IMAP client, such as ViewMail, to record, send, and forward voice messages to a user defined on Cisco Unity Connection, the system uses the SMTP proxy addresses to map the sender and the recipient of the message to the correct user. The SMTP proxy address should be configured to map to the user's corporate email account to ensure the proper delivery of messages to the user's account.

To configure the SMTP Proxy Address for a user, from the Edit User Basics page for the specific user, select **Edit > SMTP Proxy Addresses**. Click **Add New** to enter the SMTP proxy address. Click **Save** to complete the operation.

The SMTP Proxy Addresses page displays, as shown in Figure 7-58. The Bulk Administration Tool can configure the SMTP proxy addresses for multiple users.

www.it-ebooks.info

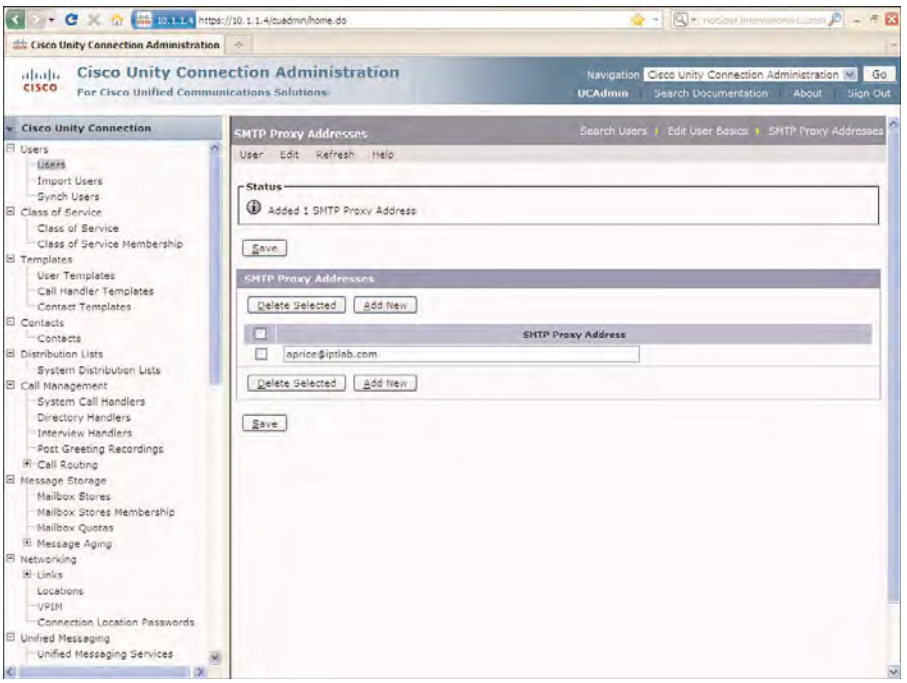

Figure 7-58 *SMTP Proxy Addresses Configured for a Defined User*

Summary

This chapter explored various user features and applications, building on the previous chapter about users' access to voice messaging. You learned to

- Configure and customize mailbox stores in Cisco Unity Connection and understand the design of mailbox storage for voice messaging.
- Understand the various parameters of mailbox storage including configuring mailbox quotas, message aging policies, mailbox stores membership, and managing voicemail storage.
- Understand the configuration and purpose of the various greeting and caller input setting for a users' voice mailbox.
- Configure alternative extensions to provide easy message access for users in Cisco Unity Connection.

www.it-ebooks.info

- Understand how to customize a user's ability to automatically add alternative extensions and disallow this feature using the Class of Service and Restriction Tables.
- Configure System and Private distribution list from an administrator and users' perspective.
- Discover the use of External Service Account and the new Unified Messaging Service for Cisco Unity Connection version 8.5 for the contact and calendar integration with Cisco Unity Connection and Microsoft Exchange, Cisco Unified MeetingPlace, or MeetingPlace Express.
- Explore the configuration of the SMTP Proxy Addresses for defined users in Cisco Unity Connection.

www.it-ebooks.info

Chapter 8

Understanding Call Handlers and System Features

This chapter covers the following subjects:

- **System Call Handlers:** Provide an understanding of the function and configuration of system call handler. Explore the different types of call handlers and their purpose to provide direction and information for callers.
- **System Directory Handlers:** Understand system directory handlers and how directory handlers can segment users by location or job function to simplify access.
- **Interview Handlers:** Describe the purpose, function, and features of interview handlers. Understand the configuration of questions and the sending of responses to the proper user or group of users.
- **Audiotext Applications:** Understand the design and configuration of an audiotext application, and how it can be customized to meet the needs of the organization to direct callers to the proper location and resources.
- **Dial Plan Components:** Understand partitions and search spaces, and how they define accessibility and reachability in Cisco Unity Connection.

In the previous chapters of this part, you explore the callers' experience as they contact a user and are directed to the user's voicemail. You also discovered the various features, functions, and control that users have available to retrieve these messages.

You learned how the caller's experience is controlled by the routing rules, depending on a number of factors. These factors are determined by whether the caller is identified as a user, where they are calling from (ANI, or callerID), or where they are calling to (DNIS, or dialed number).

In some cases, a call might be directed to Cisco Unity Connection from the organization's main number, where an audiotext application provides for an automated attendant functionality. This feature expands Cisco Unity Connection beyond the purposes of voice messaging, enabling callers to select from a menu of options presented as their call is answered by Cisco Unity Connection.

www.it-ebooks.info

An audiotext application provides a full-featured application configured by the administrator to provide the caller with direction and accessibility to users, directories, resources, or company information as needed. The application is built using the various call handlers, which are defined as follows:

- System call handlers
- Directory handlers
- Interview handlers

Finally, an organization might want to allow users to address messages and have the capability to dial other users from voicemail, while disallowing other users with this capability. All system objects, consisting of call handlers and users, can be accessed through the use of dial plan components. The dial plan in Cisco Unity Connection provides flexibility and access to resources, users, and features though the use of partitions and calling search spaces. Partitions enable an organization to segment resources in Cisco Unity Connection for the purpose of dialing, transfers, messaging, addressing, or multitenant functionality.

In this chapter, you become familiar with the following:

- The purpose, functions, and configuration of system call handlers. Explore the default system call handlers, and understand how to create additional call handlers.
- The default system directory handlers, and understand the configuration and purpose for creating additional directory handlers.
- The interview handler, and its use, function, and configuration. You also learn how the interview handler can record the responses to a defined list of questions and deliver the responses to a user or group of users.
- The design, features, and configuration of an audiotext application in Cisco Unity Connection.
- The dial plan components in Cisco Unity Connection, and understand how partitions and search spaces control addressing and dialing from within Cisco Unity Connection.

Call Handler Components

You can configure a number of different types of call handlers in Cisco Unity Connection, which are defined as system call handlers, directory handlers, and interview handlers. Call handlers define the experience of callers as they are directed to Cisco Unity Connection. This experience might be in the form of presenting information, enabling the caller to select from a menu of options, or enabling the caller to locate a user within a directory. These call handlers can be designed and built together to provide an audiotext application, providing a flexible and efficient caller experience within Cisco Unity Connection.

www.it-ebooks.info

Understanding System Call Handlers

System call handlers provide caller direction through a customized set of configurable features. These features consist of greetings, caller input, transfer, and message settings. The various options included in these features provide an organization with the tools required to design and build an audiotext application to support their unique business needs and requirements.

Default System Call Handlers

At the time of installation, three system call handlers are created by default:

- Opening Greeting
- Operator
- Goodbye

All three call handlers use the same basic building blocks but are configured for different purposes. The following sections investigate these purposes and explore how to create additional system call handlers.

The three default call handlers can be modified as needed, but they cannot be deleted. Only new system call handlers that were created by the administrator can be deleted. These default system call handlers can be viewed by selecting **Call Management > System Call Handlers** in the navigation pane on the left portion of the page in Cisco Unity Connection Administration. Figure 8-1 shows the Search Call Handlers page.

As you learned in Chapter 4, "Integrating Cisco Unity Connection," the direct routing rules define the caller's experience when they are directed to Cisco Unity Connection. By default, if the caller's extension or phone number is not defined as a user in the system, the direct routing rules send the caller to the Opening Greeting call handler. Figure 4-41 in Chapter 4 shows the direct routing rules.

The Opening Greeting system call handler plays the standard system opening greeting announcement, followed by a number of options. These options enable the user to select between a user's extension, the system directory, or the operator. If the caller does not make a selection, they are directed to the operator. This action is accomplished through the default configuration, which directs the caller to the Operator call handler.

By default, the Operator call handler enables the caller to dial "0" to contact the user defined as an operator. This action automatically forwards the call to the operator extension programmed under the transfer section. By default, there is not an extension configured for this transfer, meaning the operator is not be available. At this point, the Operator call handler is configured to take a message. After the caller has recorded a message for the operator, the user is directed to the Goodbye call handler, which simply says goodbye and disconnects the call.

www.it-ebooks.info

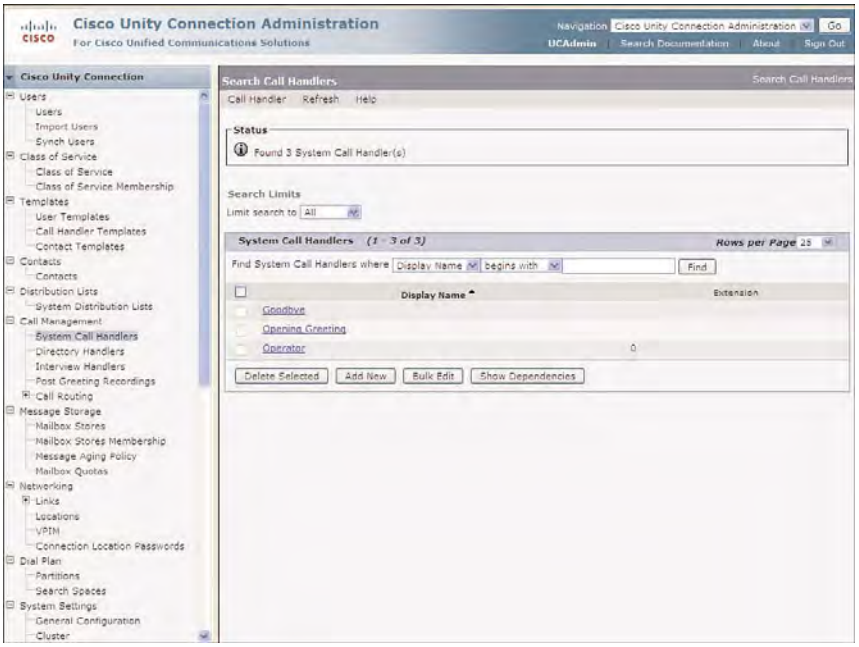

Figure 8-1 *Default System Call Handlers*

Each call handler provides a unique experience to the caller. All default call handlers can be modified, or new call handlers can be created to define this experience. To better understand these call handlers, you need to explore the default call handlers, and how they can be modified to meet the needs of each organization. In most cases, these default call handlers will be used and modified to provide access to users and resources.

Configuring Call Handlers

The Opening Greeting system call handler has a system recording announcement, informing the callers that they have reached the Cisco Unity Connection messaging system. This greeting can be customized to meet the needs of the organization. In many cases, a company might have a recording professionally recorded to provide specific information to the caller, about the organization's products and services. Another business might have someone in the company with a good speaking voice record its announcement from a script.

To review and modify the Opening Greeting, select the Opening Greeting from the Search Call Handlers display. Figure 8-2 shows the Edit Call Handler Basics page.

The Edit Call Handler Basics page provides a number of features and options, including the configuration of the following:

- **Display Name:** Descriptive name for the call handler.
- **Creation Time:** Read-only field that defines the date/time stamp of when the call handler was created.

www.it-ebooks.info

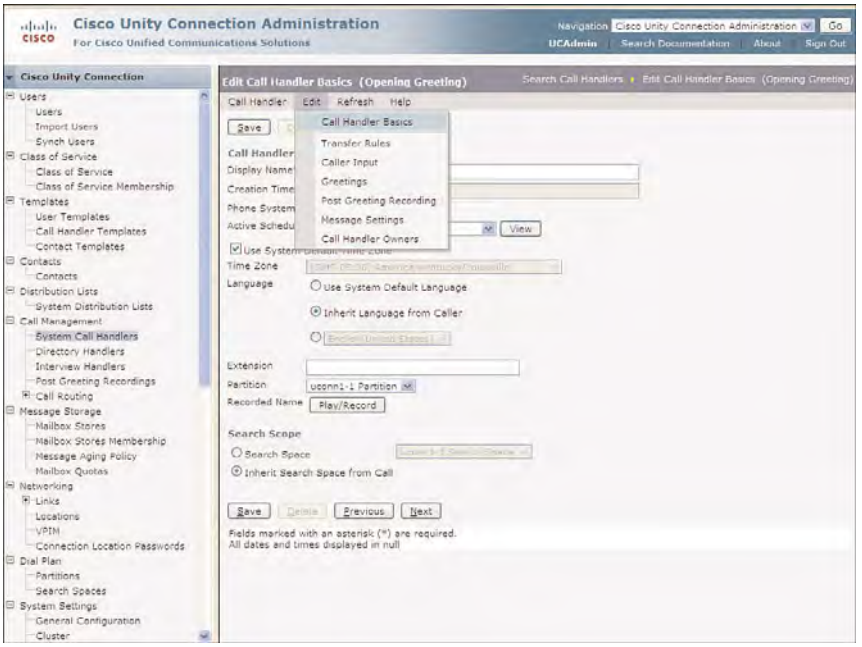

Figure 8-2 *Edit Call Handler Basics Page for the Opening Greeting*

- **Phone System:** Assignment of the call to the phone system integration
- **Active Schedule:** Defined schedule for the call handler. The schedule enables the various greetings (Standard, Closed, and Holiday) and transfers (Standard, Closed, or Alternate) to be enabled.
- **Time Zone:** Defined timezone or system timezone that controls the greetings and transfers in coordination with the Active Schedule.
- **Language:** Defines the language type to be used for the call handler. This depends on the installed languages. The call handler can be configured to use the system default, or to inherit the language as it was learned from a routing rule or previous call handler, if the caller were transferred to this call handler by the caller input or an after greeting option. The installation of addition language files is accomplished through the Install/Upgrade features in Cisco Unified Operating System web pages. Part III discusses this operation.
- **Extension:** Enables the caller to reach the specific call handler by dialing the extension. This field is optional but required if using the greeting administrator to select this call handler.

www.it-ebooks.info

- **Partition:** Defines the dial plan configuration in Cisco Unity Connection. Allows or disallows reachability within Cisco Unity Connection. Partitions and search spaces are part of the dial plan, which are discussed at the end of this chapter.
- **Recorded Name:** Enables the administrator to record the name for this call handler. If a name is not recorded, the Display Name informs the caller of the call handler. This option is important when using the greeting administrator because users need to know which call handler they are recording a greeting for.
- **Search Scope:** Defines the dial plan configuration in Cisco Unity Connection. Allows or disallows dialing or addressing within Cisco Unity Connection. Partitions and search spaces are part of the dial plan, which are discussed later in this chapter.

On the Edit Call Handler page, from the toolbar, select **Edit**. Six options are on the drop-down (refer to Figure 8-2):

- **Transfer Rules:** Enables the administrator to configure a Standard, Closed, or Alternate Greeting. The Standard transfer is enabled with no end date and cannot be deleted. The Closed transfer, if enabled, overrides the Standard transfer according to the schedule. The Alternate transfer is currently disabled. If enabled, the alternate transfer can override the standard and closed transfer.
- **Caller Input:** Provides various caller input selections during the greeting. The caller needs to be informed of the selection options within the greeting. Similar to the configuration under the user setting, the Ignore Caller Input option should be unchecked in the During Greeting section of the Greeting page, or ensure that the callers have sufficient time to make their selection.
- **Greetings:** Similar to the user configuration settings, call handlers can be configured with various greetings: Standard, Holiday, Closed, Internal, Error, Busy, or Alternate. The same rules apply to the greetings, as discussed in the user configuration from the previous chapter.
- **Post Greeting Recordings:** Enables the administrator to apply a post greeting recording, which plays after the selected greeting. The same rules apply to the post greeting recordings, as discussed in the user configuration from the previous chapter.
- **Message Settings:** Apply only to call handlers that record messages from callers. In these cases, the message length, urgency, security, and recipient can be configured. In the latter case, the recipient of the message can be an individual user or distribution list.
- **Call Handler Owners:** Enables the defined user to record the greetings using the Greeting Administrator.

www.it-ebooks.info

Transfer Rules

From the Edit Call Handler Basics toolbar, select **Edit > Transfer Rules**. The Transfer Rules page displays the three available transfer rules: Alternate, Closed, and Standard. Only the Standard and Closed transfer rules are enabled. The closed transfer rule follows the closed hours as applied to the defined schedule on the Edit Call Handler Basics page. From the Rule Name column, select the **Standard** transfer rule. The Edit Transfer Rule page displays, as shown in Figure 8-3.

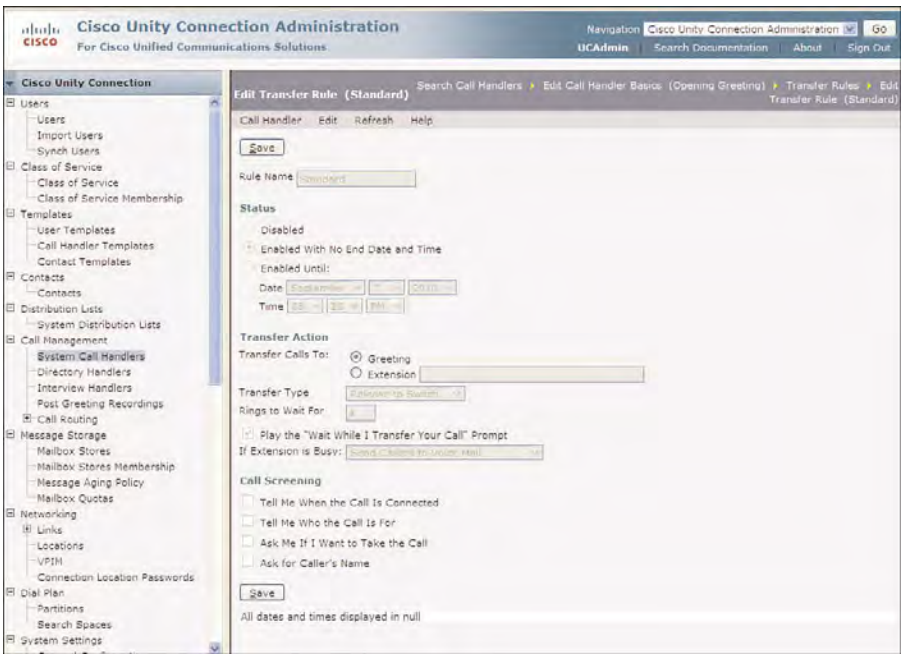

Figure 8-3 *Transfer Rules for a System Call Handler*

From the Edit Transfer Rule page, the administrator can configure a number of options, including the various call screening features. In this case, the Transfer Action is selected to send the caller to the greeting. However, a call handler can be selected to send the caller to a specific extension directly, or use the supervise transfer and call screening options. Because the **Greeting** radio button is selected, the caller hears the recorded greeting. By default, the default greeting plays. You need to re-record this greeting to meet the needs of your organization.

Greetings

To review and modify the greeting, from the Edit Call Handler Basics page, select **Edit > Greetings**. The Greetings page appears displaying the seven greetings: Alternate, Busy, Error, Internal, Closed, Standard, and Holiday. The behavior of the various greetings that were discussed in the last chapter for users are the same as applied to system call handlers.

To begin editing the greeting, from the Greeting column, select the specific greeting. In Figure 8-4, the Standard greeting is selected displaying the Edit Greeting page.

www.it-ebooks.info

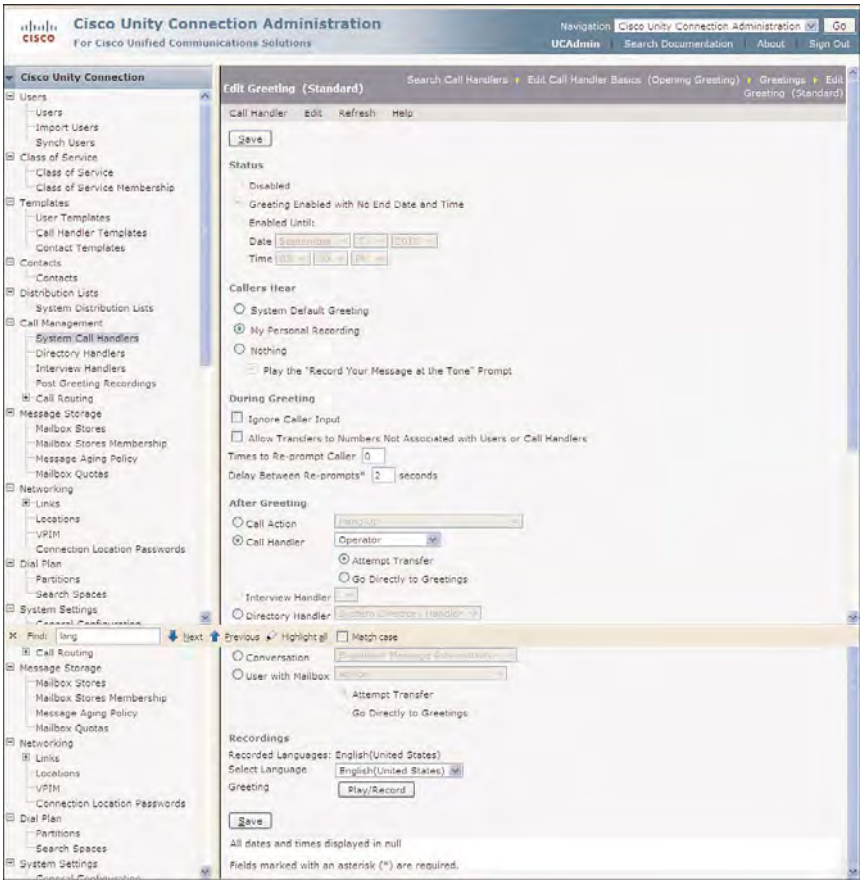

Figure 8-4 *Edit Greeting Page for a System Call Handler*

By default, the greeting is configured to play the system default greeting. Click **Play/Record** near the bottom of the greetings page to display the Media Master to begin recording a new greeting. The Media Master is used in a number of locations in Cisco Unity Connection. It is used to record names and the greetings in Cisco Unity Connection and the Cisco Personal Communications Assistant. As mentioned previously, ensure that the JAVA on your workstation is up-to-date because the Media Master is JAVA-centric. Ensure that you record the greeting under the Edit Greeting page. This is what the callers hear when they reach this call handler.

Two important sections of this page enable the administrator to define the caller experience during and after the greeting finishes; therefore, you need to understand the **During Greeting** and **After Greeting** options on the Greeting page.

www.it-ebooks.info

In the During Greeting section, the **Ignore Caller Input** option forces the caller to listen to the entire greeting before making a selection. The **Allow Transfers to Numbers Not Associated with Users or Call Handlers** option enables callers to transfer out of voicemail and make a call or transfer to an undefined number using the configured phone system integration. The Default Outdial restriction table disallows the abuse of long distance, toll, and international calling. If you plan to modify the restriction table, ensure that toll fraud and security features are considered in your design. These two options are not selected by default.

The **Times to Re-prompt Caller** option defaults to **0**. If the call handler is expecting input from the caller, this option, along with the **Delay Between Re-prompts** repeats the greeting the configured number of times with the delay between each re-prompt until the caller makes a selection. If the caller does not make a selection, the selected option from the After Greeting section is chosen.

The After Greeting section enables the administrator to direct the caller to one of the following:

- **Call Action:** Can be selected to restart the greeting, route for the next call routing rule, take a message, or simply hang up.
- **Call Handler:** Enables the administrator to send the caller automatically to another defined call handler.
- **Interview Handler:** Forwards the caller to a configured interview handler. The interview handler will be discussed later in this chapter.
- **Directory Handler:** Forwards the caller to a directory handler, either the system directory handler, or another administratively defined directory handler.
- **Conversation:** Directs the caller to a specific system conversation. The conversation options can consist of the Broadcast Message Administrator, Greeting Administrator, Sign-In, or System Transfers, as required.
- **User with Mailbox:** Forwards the caller directly to a user with a mailbox, defined by the drop-down selection.

Figure 8-4 shows the Standard Greeting page. While the Standard Greeting is playing, the caller can make a specific selection as instructed during the greeting because the **Ignore Caller Input** option is unchecked. If the caller does not make a selection, then he or she will be forwarded to the Operator call handler.

However, during this greeting, the caller could make a number of selections:

- Dial another user's extension.
- Dial an option configured under the **Caller Input** section.
- Dial a different number if the Allow Transfer to Numbers Not Associated with Users or Call Handlers is checked.

www.it-ebooks.info

If a user dials an option configured for the Caller Input section, that option interrupts the After Greeting action, and the caller will be directed to the specific selection accordingly.

Caller Input

The Caller Input selection functions the same as discussed in the previous chapter for user configuration settings; however, these might be more specific to the needs of the organization.

To review or modify the Caller Input selection of a system call handler, from the Edit Call Handler Basics page, select **Edit > Caller Input**. Figure 8-5 shows the Caller Input.

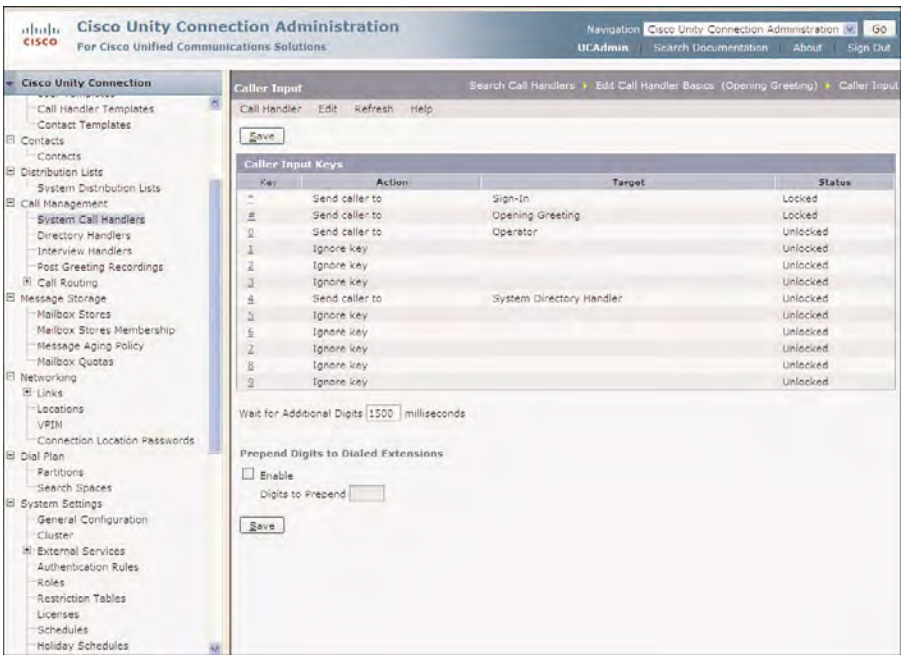

Figure 8-5 *Caller Input Selection for a System Call Handler*

The default options for Caller Input within the system call handler provide the following options to callers:

- Send caller to the Sign-in Conversation (if they are a user) by dialing the * key. This option shows as "locked," meaning that the action will be taken immediately without waiting for any further input.
- Send caller to the Opening Greeting by dialing the **#** key. This option shows as "locked," meaning that the action will be taken immediately without waiting for any further input.

www.it-ebooks.info

- Send caller to the Operator if they dial a **0**.
- Send caller to the System Directory Handler if they dial a **4**.

All default configurations can be modified as necessary to meet the organizations' business requirements.

Post Greeting Recordings

Post Greeting Recordings were discussed in the previous chapter and should be reviewed in the corresponding "Post Greeting Recordings" section of that chapter. The administrator can apply a post greeting recording to a call handler greeting, similar to how it is applied to a user. The post greeting recording will be played directly after the call handler greeting is completed. The user cannot make a selection during the post greeting recording. Any caller input selections must be selected by the caller during the normal greeting. To apply a post greeting recording to a system call handler, from the Edit Call Handler Basics page, select **Edit > Post Greeting Recording**, as shown in Figure 8-6.

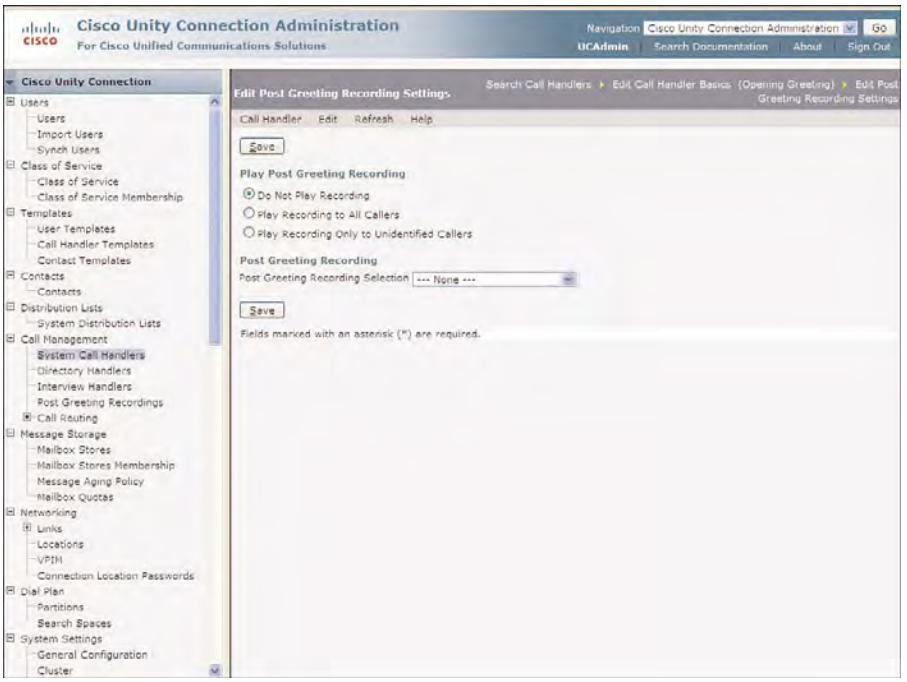

Figure 8-6 *Edit Post Greeting Recording Settings Page for a System Call Handler*

The Post Greeting Recording Settings page enables the administrator to select a specific post greeting recording and play it after the normal greeting for all callers or unidentified

www.it-ebooks.info

callers. The default for this option is disabled. The Post Greeting Recordings must be created first before they can be selected here.

In some cases, call handler might need to record messages from a caller and send these messages to a user or group of users. The message settings for this option need to be configured in these cases.

Message Settings

The Message Settings section determines the handling of any messages recorded by callers because of either a Caller Input selection or After Greeting call action. Because the call handler is not a user with a mailbox, the message settings section determines the handling of these recorded messages. If the call handler is not intended to record a message, these options are not used.

Within this section, the administrator can determine the maximum message length and whether the callers are allowed to edit their recorded message. Also, the message urgency and security can be selected. These messages can be marked urgent or normal (which is the default), or the system can be configured to ask the caller. In the latter case, the caller's selection decides how the message is marked before it is delivered to the recipient.

Additionally, the caller's messages can be marked as secure, meaning that these messages can be forwarded only to other users on the system and cannot be retrieved by certain methods, such as the RSS readers and IMAP clients (with the exception of ViewMail). The secure messaging feature also enables the administrator to apply specific message aging policies to messages received by the user. Chapter 7, "Understanding User Features and Applications," discussed the message aging policy in greater detail.

The message recipient section determines who receives the caller's message. Cisco Unity Connection provides the option to forward the recorded message to a specific user with a mailbox, or a distribution list. In the latter case, the distribution list enables the forwarding of messages to multiple users. This type of call handler can provide special purpose call handlers that forward urgent messages to multiple recipients.

A call handler can be specifically designed for an emergency support line or a technical job/work orders message box. For example, callers might select the option to record a message for a support team (distribution list). The message is then delivered to each team member as an urgent message. Each user is configured with message notification, so team members get immediate notification of the message and can respond to the caller in a timely manner.

Finally, the After Message section determines the caller's experience after the caller completes the recording of a message. In most cases, the option is to send the callers to the Goodbye handler, which says goodbye and disconnects the call.

To review and modify the message setting for a system call handler, from the Edit Call Handler Basics page, select **Edit > Message Settings**. The Edit Message Settings page displays as shown in Figure 8-7. The default options are reflected in the example here. If

www.it-ebooks.info

any options are selected or changed, however, you need to select **Save** to commit any changes to the database.

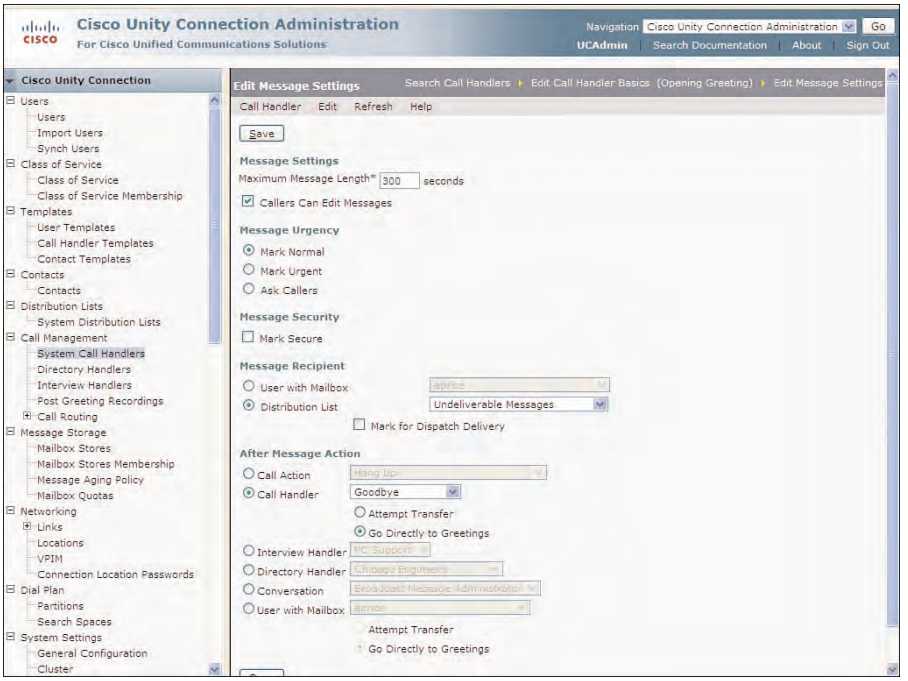

Figure 8-7 *Edit Message Settings Page*

Call Handler Owners

By default, only users that have a role of system administrator can create or modify call handler greetings. Greetings might need to be dynamic in many organizations, however, sometimes changing daily. This might be the case with product information, service announcements, or company news. In these cases, the administrator might want to offload this function to someone that has the job responsibility that relates to the specific call handler. For example, a company's product news call handler greeting might need to be recorded by the marketing department. A job opening call handler greeting might need to be recorded by the human resource department.

To offload the recording of greetings, the administrator needs to configure a user as a call handler owner. Multiple users can be assigned to one or more call handler owners, enabling them to use the greeting administrator to create, change, and record greetings for the specific call handlers.

To assign the call handler owners to a specific call handler, from the Edit Call Handler Basics page, select **Edit > Call Handler Owners**. Click **Add Users** to add one or more users as call handler owners. A pop-up window, the Call Handler Potential Owner Search

www.it-ebooks.info

Results appears. Select one or more of the users with mailboxes on the pop-up, and click **Add Selected User**; then click **Close**. The Call Handler Owner page is presented displaying the assigned call handler owners, as shown in Figure 8-8. The user, **tdavis**, has been added as a call handler owner to this call handler.

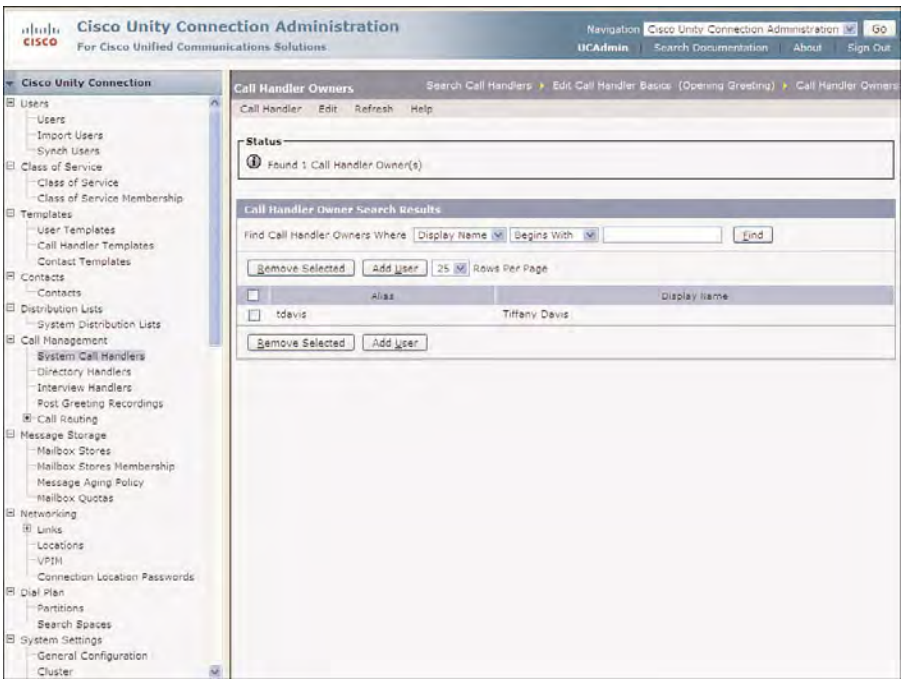

Figure 8-8 *Call Handler Owners Page for a System Call Handler*

Configuring New Call Handlers

New call handlers can be created in Cisco Unity Connection Administration by clicking **Add New** on Search Call Handlers page. The New Call Handler page displays, as shown in Figure 8-9.

From this page, the administrator can enter a unique Display Name. Optionally, an extension can be entered. The extension must be a unique number that will be dialed to select this call handler. If this call handler is to be maintained using the Greeting Administrator, the extension is required. The final selection on this page is the Call Handler Template drop-down. The Call Handler Template page enables the administrator to apply a series of options to a new call handler at the time of creation. Click **Save** to complete the operation. The Edit Call Handler Basics page displays for the new call handler. The administrator can now customize the options as needed.

In this example, the Call Handler is created for the IT Department, based on the System Call Handler Template configuration elements.

www.it-ebooks.info

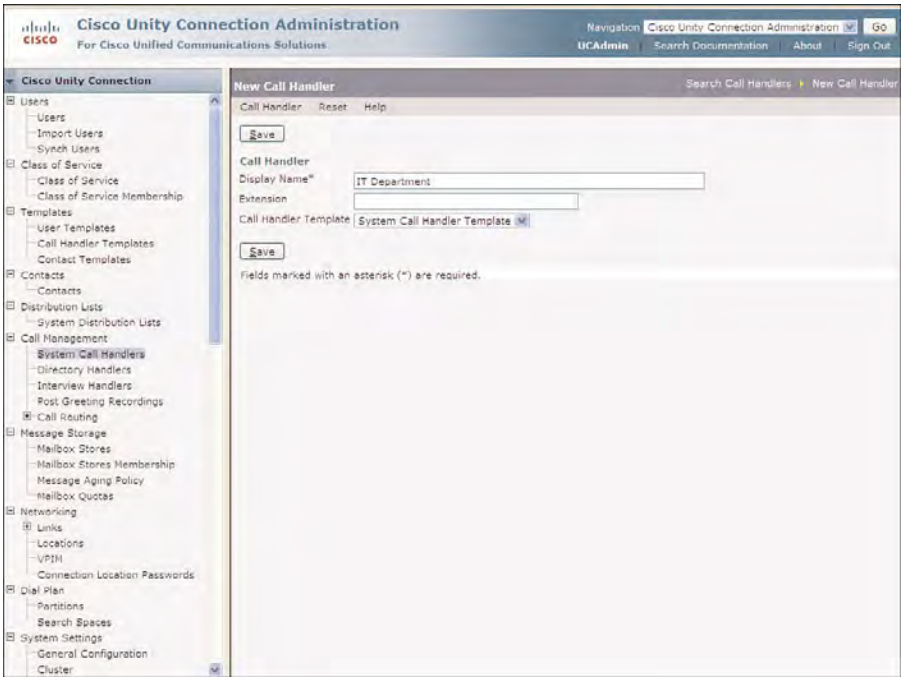

Figure 8-9 *New Call Handler Page in Cisco Unity Connection*

Call Handler Templates

By default, there is one call handler template, the System Call Handler Template, created at the time of installation. In most cases, this template will suffice to create call handlers in most organizations. As an administrator of Cisco Unity Connection, you can create new call handler templates or modify the existing template to meet the needs of your organization. The purpose of the template is to apply a desired set of configurations (Transfer Rules, Caller Input, Greetings, Message Settings, and Post Greeting Recordings) to new call handlers. After the call handlers are created, they can be modified as needed. The template that was used to create the call handler, with the exception of the System Call Handler Template, can be deleted if it is no longer needed. All templates in Cisco Unity Connection are used only at the time of creation of the object. Therefore, deleting a template does not affect any call handlers that were created with that specific template.

To review, modify, or create a new call handler template, from the navigation pane in Cisco Unity Connection Administration, select **Templates > Call Handler Templates**. The Search Call Handler Templates page displays, as shown in Figure 8-10. The default System Call Handler Template displays. This template can be modified as needed, or additional templates can be created as needed by clicking **Add New**.

www.it-ebooks.info

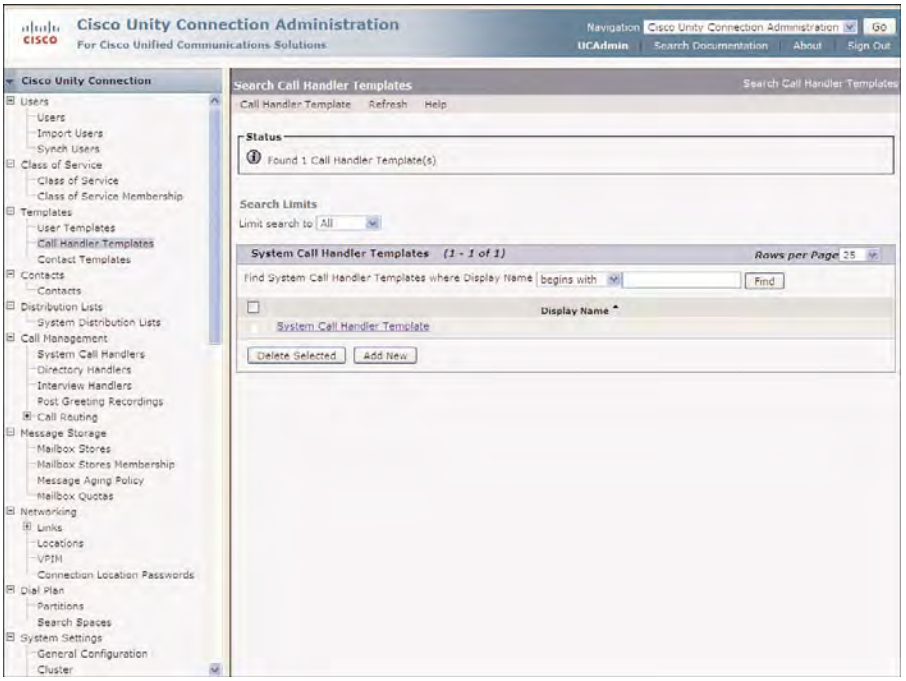

Figure 8-10 *Call Handler Templates in Cisco Unity Connection Administration*

Create a new call handler template by clicking **Add New**. A New Handler page displays to enable the administrator to provide a customized set of configurations for the creation of new call handlers. The call handler owners are the only configuration elements that cannot be applied through the template.

Understanding Directory Handlers

Directory handlers are special call handlers that enable a caller to locate users by using defined criteria (last name/first name, first name/last name, or extension). There is a single default directory handler to which all users are assigned. This is the System Directory Call Handler. Additional directory handlers can be created as required by the organization.

Some organization might decide to create specific directory handlers for each location (Chicago, Cleveland, or Detroit) or job function (Sales, Exec, or Admin). In these cases, directory handlers might be segmented, rather than forcing callers to search across the entire organization. This assists the caller by narrowing the search, where large directories might consist of multiple users with similar names.

The administrator might want to configure existing and new directory handlers to present the directory search results in a number of formats. The administrator can configure the search to

- Route Automatically on a Unique Match
- Always Request Caller Input

www.it-ebooks.info

- Announce Matched Names Using Extension Format
- Announce Matched Names Using Menu Format (additionally, present the extension with the menu option)

The various options provide flexibility in creating directory handlers, while simplifying the caller's selection, and possibly hiding the user's extension, if required.

To view or modify the directory handlers, from the navigation pane in Cisco Unity Connection Administration, select **Call Management > Directory Handlers**. The Search Directory page displays. To view or modify existing directory handlers, select the name of the directory handler from the Display Name column.

As an administrator, you need to understand how to add a new directory handler. To begin, on the Search Directory page, click **Add New**. The New Directory Handler page displays. On this page, enter the name for the new directory handler, extension, and partition. The extension is optional and only required if the directory handler is to be dialed by extension.

The last option on the New Directory Handler page enables the directory handler to be configured for voice recognition. In this case, voice recognition users can locate names by saying the first name followed by the last name. Finally, click **Save** when completed with all configurations. The Edit Directory Handler page displays as in Figure 8-11.

In this example, a new directory handler has been created for Chicago Engineers. The caller can search the directory by entering the last name, followed by the first name. The matches found will be presented in a menu format with up to eight possible options, with no user extension advertised to the caller.

Understanding Interview Handlers

In the previous section, you understood how a call handler defines the caller experience in Cisco Unity Connection. The call handler configuration defines this experience by playing a greeting, defining what the caller can do during the greeting, and what happens after the greeting finishes. In some cases, a caller might record a message for a single user or a group of users using a distribution list. The process of recording and delivering messages is entirely optional for system call handlers.

Interview handlers, however, are intended primarily for recording the caller's message and delivering these messages to a single user or group of users. Voice messaging in an interview handler presents a series of questions, records the caller's responses, and delivers these responses to a message recipient. In this way, an organization can ensure that the proper information is queried and recorded from the caller. The interview handler configuration enables the organization to control the length of the response because each recorded response can have different maximum message lengths.

You an use interview handlers in the organization where the responses to a series of questions can be delivered to the proper individuals. For example, interview handlers might be used for technical support, job interviews, or operator-assisted messages.

www.it-ebooks.info

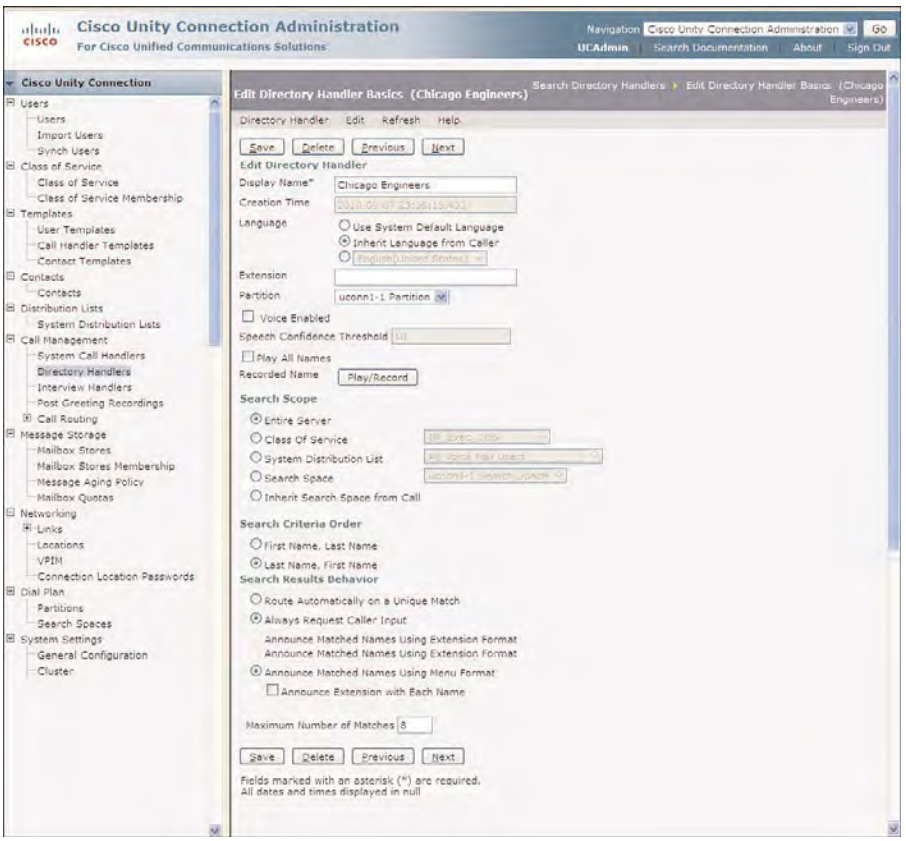

Figure 8-11 *New Directory Handler Configured in Cisco Unity Connection Administration*

A technical support organization might use the interview handler for support. In this case, a series of questions are presented to the call regarding their contract number, type/model of equipment, description of the problem, and contact information. This information is then delivered to the support team. If the call is urgent, message notification can be used to notify the individuals for expedited response.

An organization might use an interview handler to qualify a prospective applicant for employment. In this case, the questions asked might apply to their past experience and reasons for applying for the job. The responses from these interview handlers are then delivered to the human resources director.

In other cases, the interview handler might be used for an operator-assisted messaging. If callers do not know who they need to speak to, they might be queried as to the nature of their call. The interview handler records their responses and delivers them to an administrative assistant, where the messages are then forwarded to the proper individual.

www.it-ebooks.info

Configuring Interview Handlers

To configure an interview handler, from the navigation pane in Cisco Unity Connection Administration, select **Call Management > Interview Handlers**. The Search Interview Handler page displays, enabling the administrator to create a new interview handler, edit existing call handlers, or use the Bulk Edit feature to edit multiple interview handlers.

To begin, click **Add New** to create a new call handler. Figure 8-12 shows the resulting New Interview Handler page.

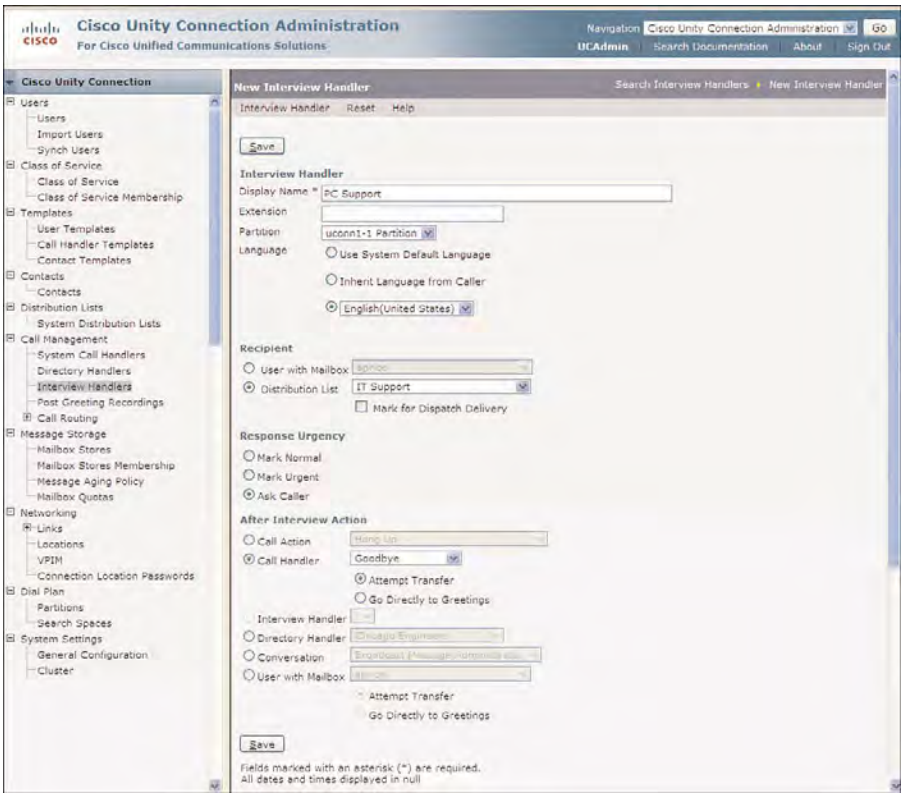

Figure 8-12 *New Interview Handler Page in Cisco Unity Connection Administration*

In this example, an interview handler has been created for PC Support presenting a series of questions to the callers. The callers are asked if their message is urgent. The responses are then delivered to the IT Support distribution list. After the call is completed, Cisco Unity Connection plays the Goodbye call handler, which says goodbye to the caller and terminates the call. Finally, click **Save** to complete the operation.

Next, the questions need to be formulated and recorded. To begin this configuration, from the toolbar on the Edit Interview Handler Basics page, select **Edit > Interview**

www.it-ebooks.info

Questions. The Interview Question page is presented, enabling the administrator to select each question. You need to begin by adding each question in the order to be presented to the caller. Select the first question from the Question Number column. The Edit Interview Question page displays, as shown in Figure 8-13.

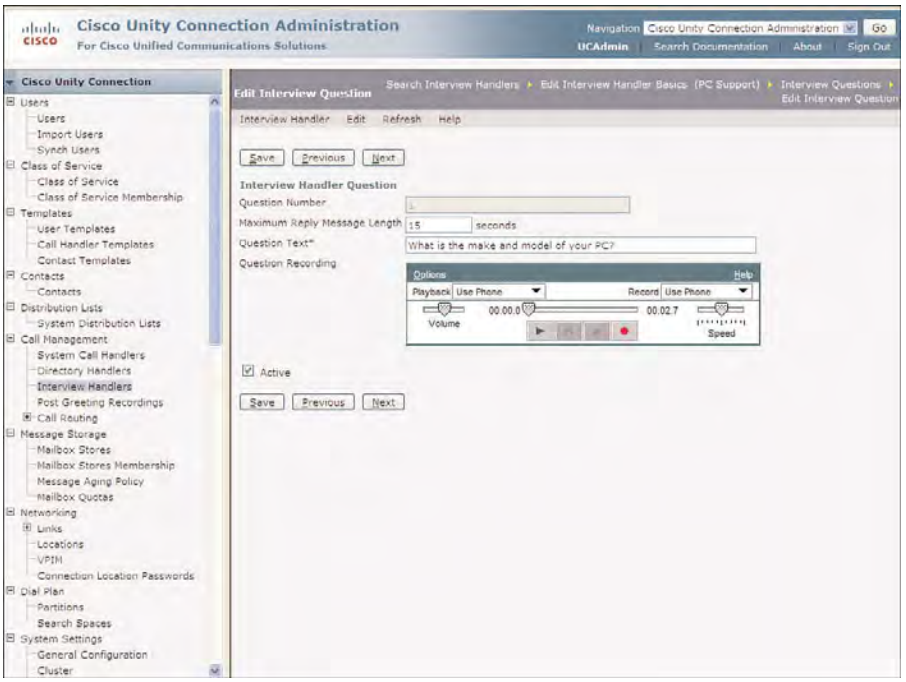

Figure 8-13 *Edit Interview Questions Page in Cisco Unity Connection Administration*

In this example, the first question asks the callers for the make and model of their PC. From this page, the administrator can specify the maximum reply message length and record the question. The administrator has chosen to change the default of 30 seconds to a maximum reply time of 15 seconds. This time should be configured with enough time for the callers to state the information required in the question.

The Question Text is used as a guide to let the administrator know the recorded question. This information is not used to play the question to the caller. If the message length is too long, the caller can skip a question or move to the next question by selecting the **#** key, or by not answering.

The administrator needs to record each question using the Media Master, as shown in the example. The total recording time for this question is 2.7 seconds.

Each question must be configured and recorded inside the interview handler. The completed interview questions appears similar to the Interview Questions page shown in Figure 8-14.

www.it-ebooks.info

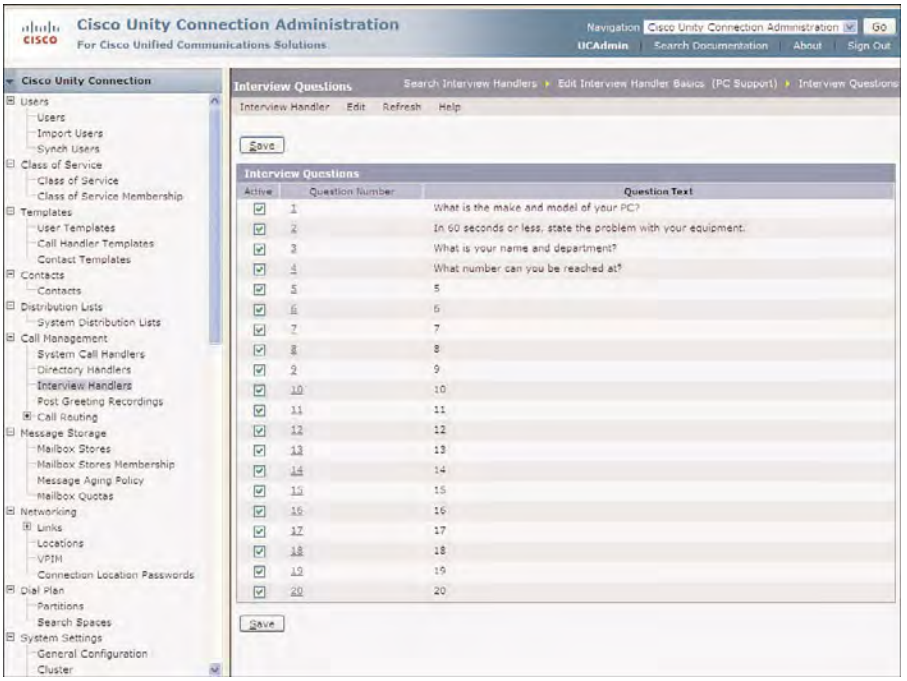

Figure 8-14 *Interview Questions for PC Support*

In Figure 8-14, four questions are asked of the callers about their equipment, problem, and contact information. The responses are delivered to the distribution list as illustrated in the Recipient section of the New Interview Handler page, as shown in Figure 8-12. Only the responses are delivered in the message, so the message recipient needs to know the specific questions that were presented to the caller.

Building an Audiotext Application

The various call handlers and directory handlers now need to be made available to the callers through a cohesive series of menus, greetings, and selections called an *audiotext application*. This application needs to be designed, discussed, and configured to provide an acceptable user experience. Before beginning any configuration, you must determine the design and flow of the audiotext application.

Audiotext Application Design

The design of the audio of the audiotext application use a series of greetings that informs the callers to make selections based on an audiotext menu of options. The Caller Input configurations of the various call handlers and the flow is important to ensure that the callers are directed to the correct resources, applications, or users.

www.it-ebooks.info

Figure 8-15 details an example of an audiotext application that might be used for an organization. In this example, a simple opening greeting enables the callers to select between different options. The call handlers can be concatenated to provide multiple layers of options. As a rule of thumb, it is best to keep the number of choices to approximately four options, while allowing no more than four levels for a single call. This can help to avoid caller frustration. Also, it is best to always give callers the option to speak to a live operator or agent. For example, this can be accomplished by letting the callers know they can dial "0" at any time to directly speak to someone.

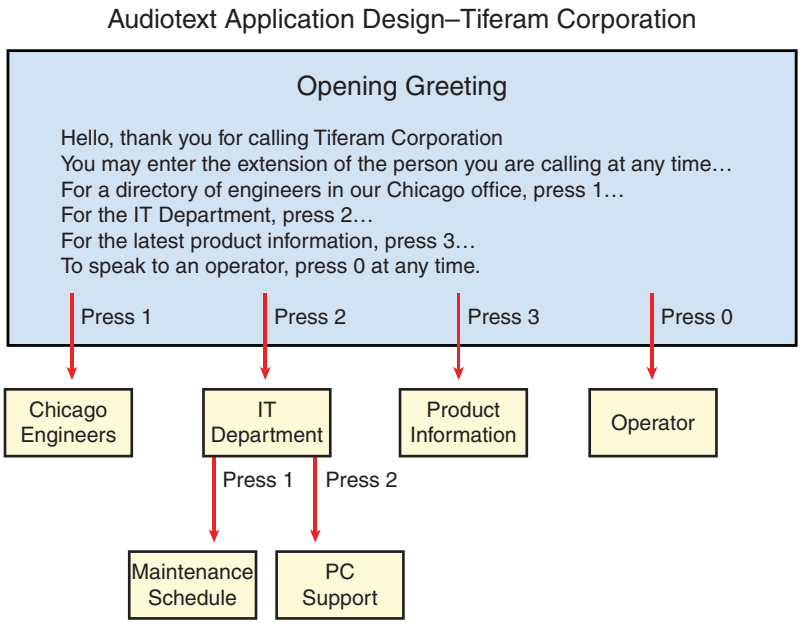

Figure 8-15 *Audiotext Application Design*

The audiotext application design in Figure 8-15 for Tiferam Corporation is a simple example of using the various call handlers that were explored in this chapter. Of course, the design of an audiotext application can vary greatly between organizations. As an administrator of the system, however, you always need to design the audiotext application and build a complete script in its entirety. Then, you need to have a meeting with the various department managers and executives in the organization to ensure that the needs of each department are considered before beginning any configuration.

When you begin the configuration of the audiotext application, this process must be completed in the reverse order from the bottom of the audiotext application to the opening greeting. The reason is that the selections of the call handlers in the caller input section are selected from a drop-down list. Therefore, the call handlers selected in the call input section must already exist.

www.it-ebooks.info

In the example, the opening greeting has been created enabling the caller to make one of four choices. These choices consist of the following options:

- **Option 1:** Sends the caller directly to the Chicago engineers directory handler, where the caller can search for a specific user in that department.
- **Option 2:** Sends the caller to the IT Department. There are two choices, enabling the caller to hear the current maintenance schedule (option 1), or report a PC problem, using the PC Support interview handler (option 2). The IT director is configured as the greeting administrator for the Maintenance Schedule call handler, enabling this person to change the greeting as required.
- **Option 3:** Sends the callers to the latest product information. The marketing manager is configured as the greeting administrator, enabling this person to change the greeting information as needed.
- **Option 0:** Sends the caller to the operator. The callers are informed that they can make this selection at any time during the greeting. Therefore, all call handlers have a default configuration enabling this selection. This option is configured within the System Call Handler Template.

Cisco Unity Connection Dial Plan Components

At this point in the configuration, all callers can address messages and dial all other users from Cisco Unity Connection. However, most organization might not want to provide callers with the ability to send voice messages to the president and executive team. It might also not be desirable for callers to have access to distribution lists to avoid solicitation to groups of users.

The dial plan components, including partitions and search spaces, are used to segregate users, distribution lists, and call handlers for the purpose of addressing message and dialing from Cisco Unity Connection.

Partitions

By default, all dialable extensions, call handlers, and distribution lists are assigned to the system partition. This name is based on the name of the server, followed by **Partition**. For example:

```
<server name> Partition
```

The partition is a logical grouping of objects that have the same reachability. The following objects belong to a specific partition:

- Users
- Contacts
- Distribution Lists
- Call Handlers (system call handlers, directory handlers, and interview handlers)

www.it-ebooks.info

To review the default dial plan in Cisco Unity Connection, from the navigation pane in Cisco Unity Connection Administration, select **Dial Plan > Partitions**. Figure 8-16 shows the resulting Search Partitions. The default system partition displays. From this page, the administrator can click **Add New** to create a new partition.

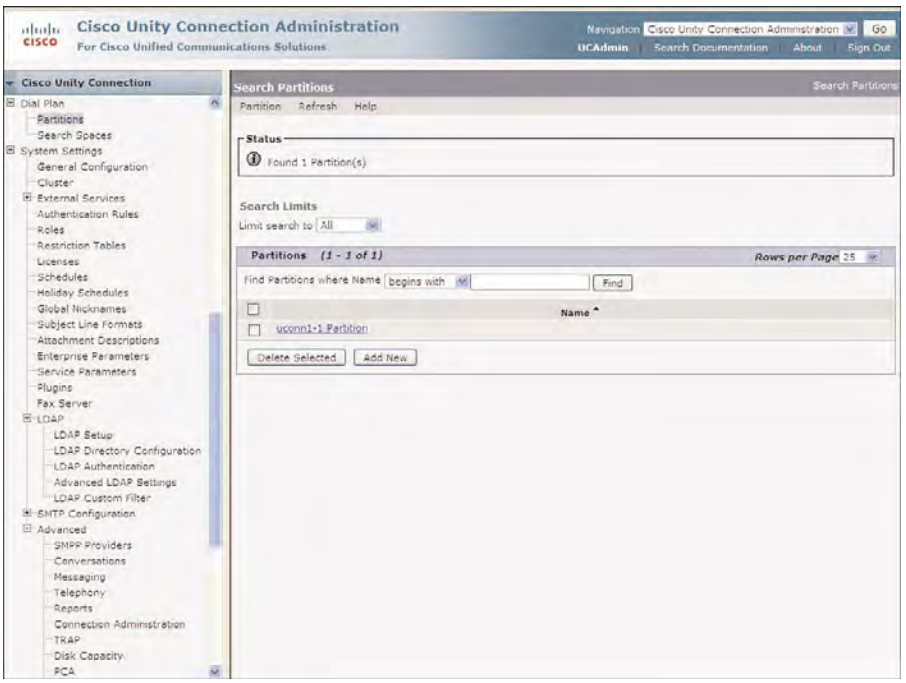

Figure 8-16 *Search Partition Page in Cisco Unity Connection Administration*

Search Spaces

Any object that can address messages or dial from Cisco Unity Connection will be assigned a search space. The default system search space is assigned to all dialing or addressing entities at the time of installation and includes the default system partition.

Search spaces are assigned to any object or user that can initiate a call or address a message to another entity. These search spaces determine the accessibility of the various objects in Cisco Unity Connection. This accessibility is determined by the partitions assigned to the search space. In other words, the search space assigned to an object determines the search scope, or the objects that can be dialed or addressed, based on the assigned partitions.

www.it-ebooks.info

The default system search space is based on the name of the server, followed by **Search Space**. For example:

```
<server_name> Search Space
```

The following objects will be assigned to a search space:

- Users
- Call handlers (system call handlers and directory handlers)
- Routing rules

To view the system search space, select **Dial Plan > Search Space** from the navigation pane to display the Search Search Spaces page, as shown in Figure 8-17.

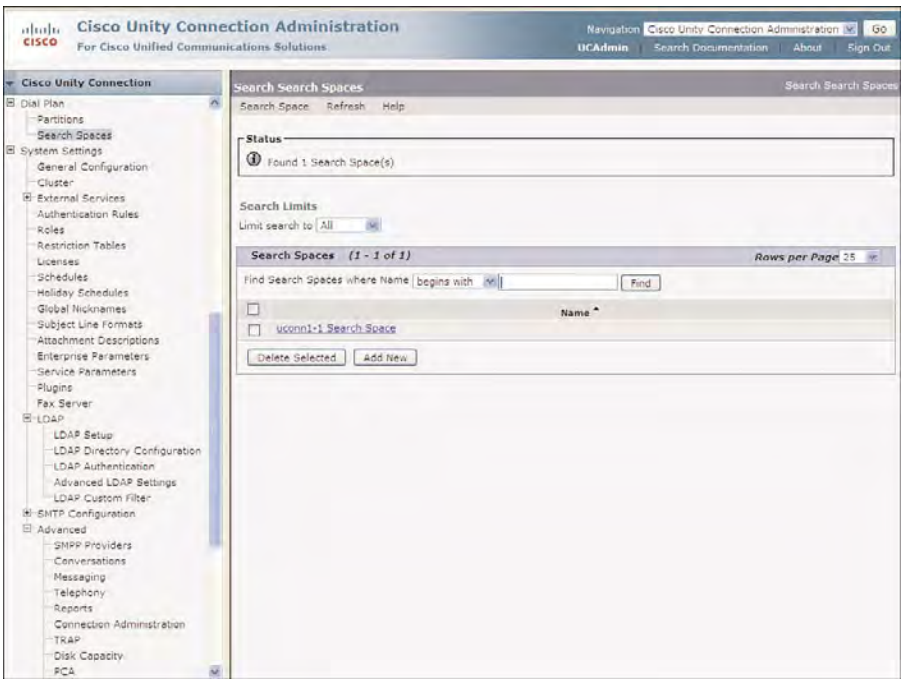

Figure 8-17 *Default Search Space in Cisco Unity Connection Administration*

Partitions and Search Spaces can sometimes be confusing and is best understood with an example using the various dial plan components.

www.it-ebooks.info

Case Study: Configuring The Dial Plan

Tiferam Corporation has a number of different groups of users within their corporate office. These groups are divided into four specific areas, where all users in the same group should have the same capabilities when dialing from voicemail or addressing messages. These four groups are defined as follows:

- Administration
- Finance
- Sales
- Executive

Each group of users has their own call handlers and distribution list that they use on a daily basis. Each group of users has their own needs and capabilities, depending on their job function. Therefore, because each of the four groups of users have the same capabilities, Tiferam has decided to create four unique partitions. Also, the executive team should have access to all resources in Cisco Unity Connection. The other groups, however, should not have access to any resources assigned to the executive partition. Administration should have access to all resources in administration and sales but not finance and executive resources. Sales personnel should have access only to sales resources, whereas financial personnel have access to all resources, except the executive.

Because all groups are going to be unique in their accessibility, Tiferam Corporation has decided to create four different search spaces. To complete the configuration of the search spaces, partitions need to be assigned to each search spaces to provide this accessibility. The assignment follows:

- **Exec Search Space:** Includes the Admin, Sales, Finance, and Exec partitions
- **Sales Search Space:** Includes only the Sales partition
- **Finance Search Space:** Include the Admin, Sales, and Finance partitions
- **Admin Search Space:** Includes the Admin and Sales partitions

Figure 8-18 illustrates the relationship of the various objects in Cisco Unity Connection for Tiferam Corporation. Each of the four groups (Admin, Sales, Finance, and Exec) are assigned to their respective search spaces and partitions. The individual partitions assigned to each search space define each object's reachability.

In this example, the Executive search space includes all partitions. Therefore, any user or resource assigned to this search scope can address messages or dial from voicemail to all other resources. The Admin search space includes only the Admin and Sales partitions; therefore, users assigned to this search space can address messages or dial only to other users and resource within these two partitions.

www.it-ebooks.info

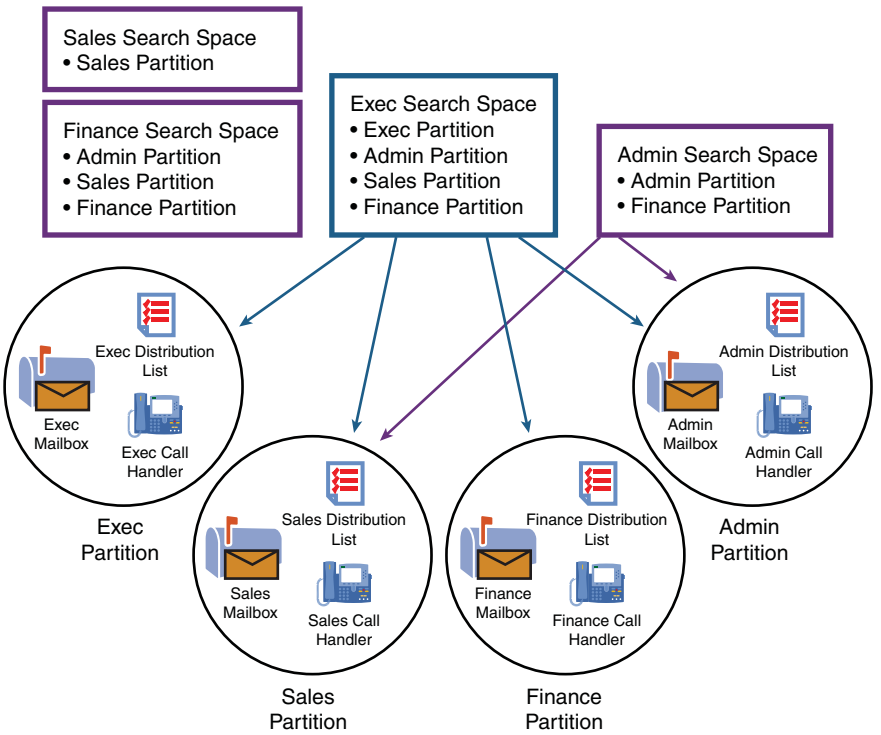

Figure 8-18 *Partition and Search Space Relationship*

Configuring Partitions

To begin the configuration of the dial plan, you must first define the partitions. In Cisco Unity Connection Administration, select **Dial Plan > Partitions**. The Search Partitions page displays. Click **Add New** to create a new partition.

Figure 8-19 shows the New Partition page. Enter the name for the New Partition in the Name field. In this example, the Admin partition has been created. Click **Save** when finished to create the partition. The Edit Partition page displays enabling the administrator to enter a description for the partition. Select **Partition > New Partition** from the Edit Partition page to repeat this procedure, adding all partitions to be used in the organization.

After you complete adding all partitions, select **Partition > Search Partitions** from the toolbar on the Edit Partition page. The Search Partition page displays showing all configured partitions, as shown in Figure 8-20.

www.it-ebooks.info

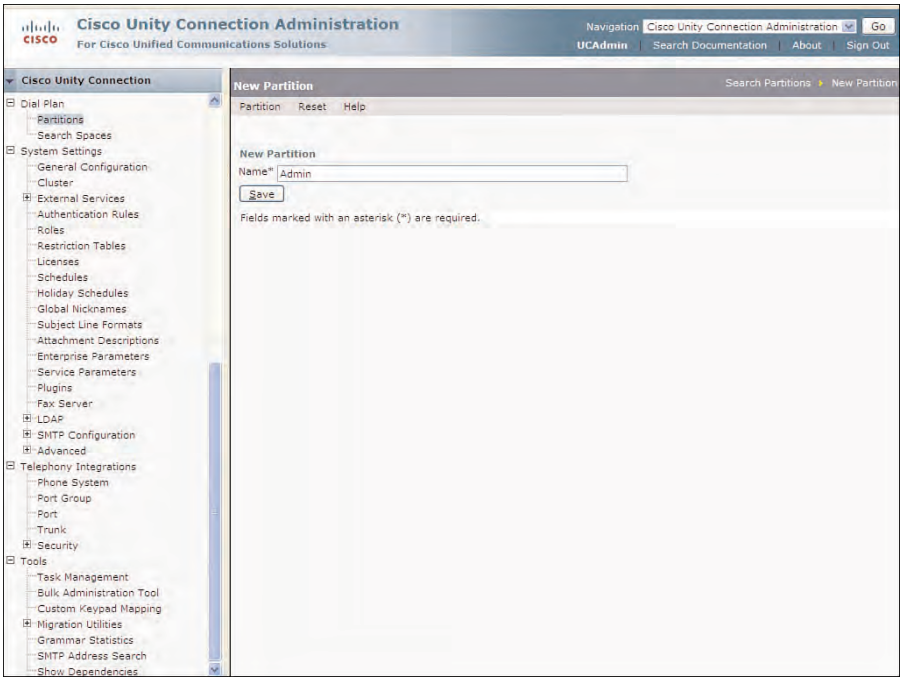

Figure 8-19 *New Partition Configuration in Cisco Unity Connection*

Configuring Search Spaces

The next step in the dial plan configuration is to create the search spaces and assign the proper partitions. To complete this operation, select **Dial Plan > Search Spaces** from the navigation pane. The Search Search Spaces page appears. Click **Add New** to create a new search space.

The New Search Space page appears. Enter the name for the new search space as displayed in Figure 8-21, and click **Save**.

Assigning Partitions to Search Spaces

After clicking **Save** on the New Search Space page, the Edit Search Space page displays enabling the administrator to assign partitions to the new search space. In the Unassigned Partitions pane, highlight the partition to be assigned, and click the Up Arrow to move the partition to the Assigned Partitions pane. Repeat this step for each partition that is to be assigned. Optionally, you can enter a descriptive name in the Description field. Click **Save** to complete the operation.

www.it-ebooks.info

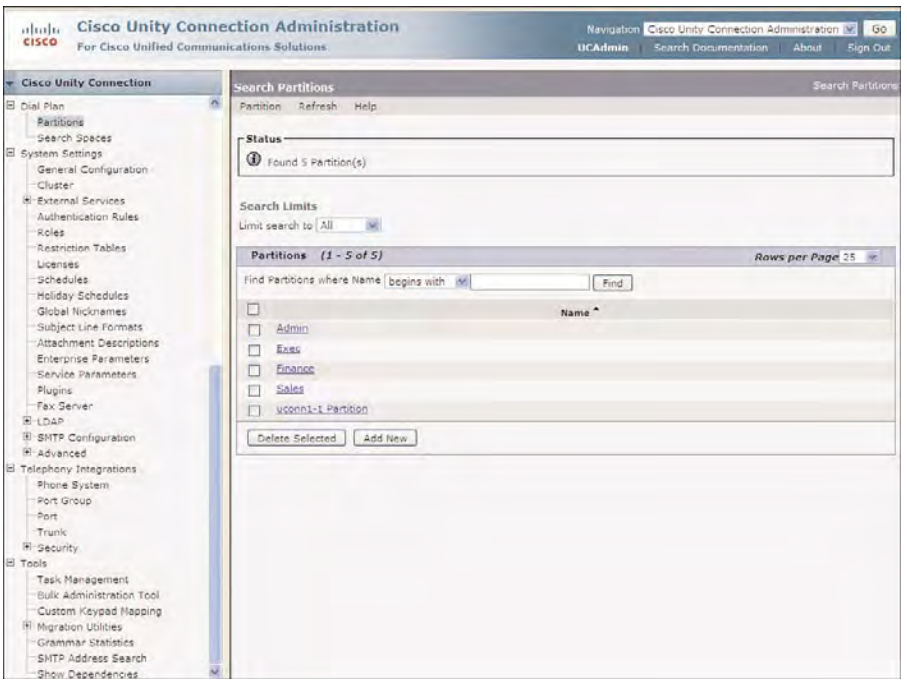

Figure 8-20 *Search Partition Page Displaying the New Partitions*

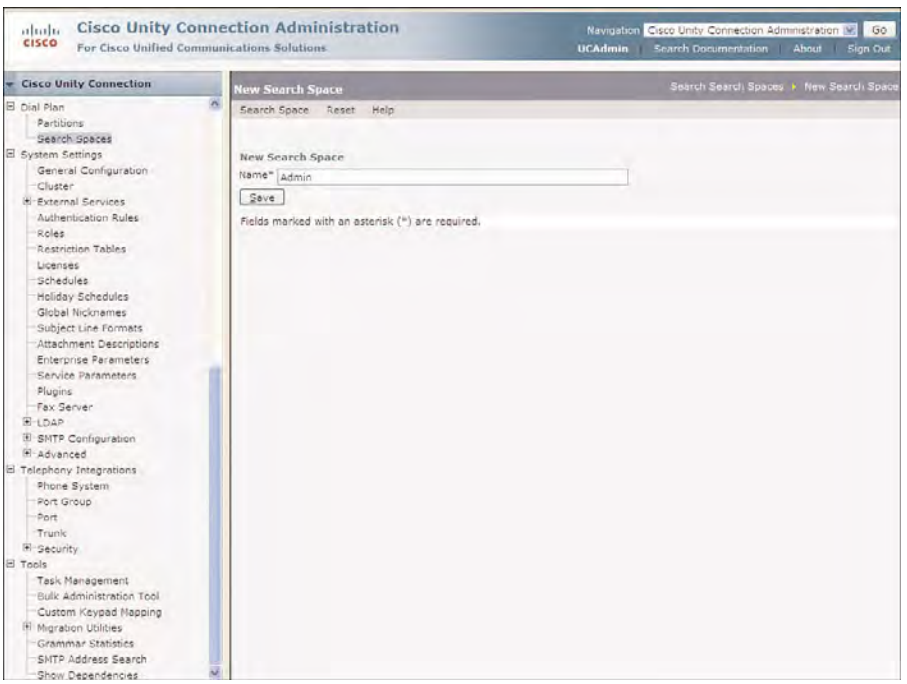

Figure 8-21 *New Search Space Configuration in Cisco Unity Connection*

www.it-ebooks.info

In Figure 8-22, the Admin search space is configured with two partitions, the Admin and Sales partitions. As the administrator, you need to repeat this configuration for the remaining search spaces, assigning the proper partitions accordingly.

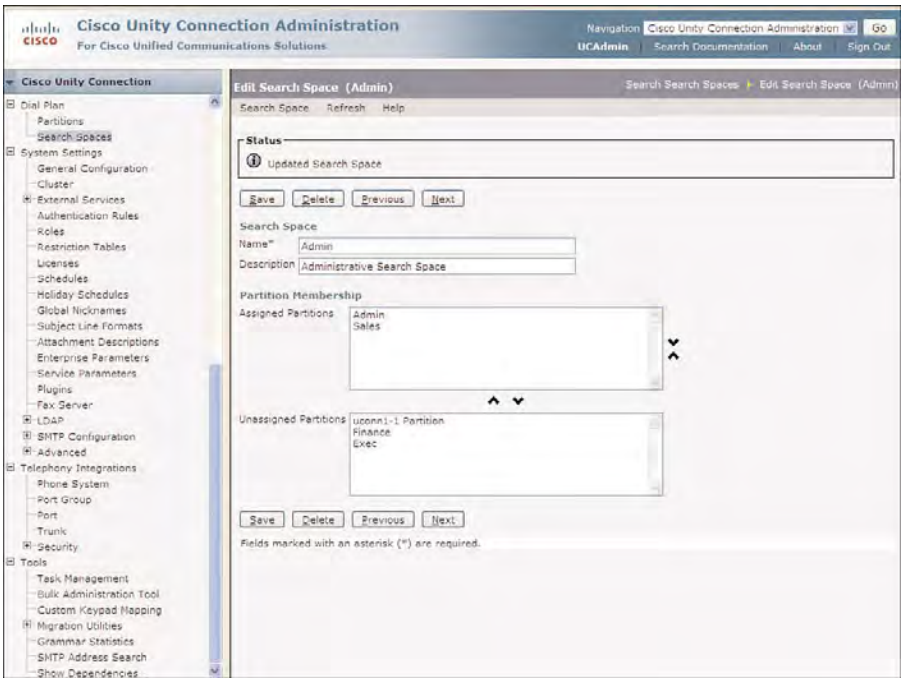

Figure 8-22 *Assigned Partition to Search Spaces*

Select **Search Space > New Search Space** from the toolbar on the Edit Search Space page to create a new search space and repeat this procedure for all remaining search spaces.

After all the Search Spaces have been configured with the proper partitions, select **Search Space > Search Search Spaces** from the toolbar on the Edit Search Space page. The Search Search Space page now displays all configured Search Spaces, as shown in Figure 8-23.

Applying Partitions and Search Spaces

Finally, the respective objects are placed into the partitions, and the search space is assigned accordingly. Figure 8-24 illustrates the configuration of an executive user. In this case, Tiffany Davis is assigned to the Exec search space and the Exec partition. Only users that have the Exec partition in their search space can address message or dial Tiffany's number from Cisco Unity Connection. Also, Tiffany can use all resources assigned to the partitions included in her search space. In this case, she has access to all resources in Cisco Unity Connection.

www.it-ebooks.info

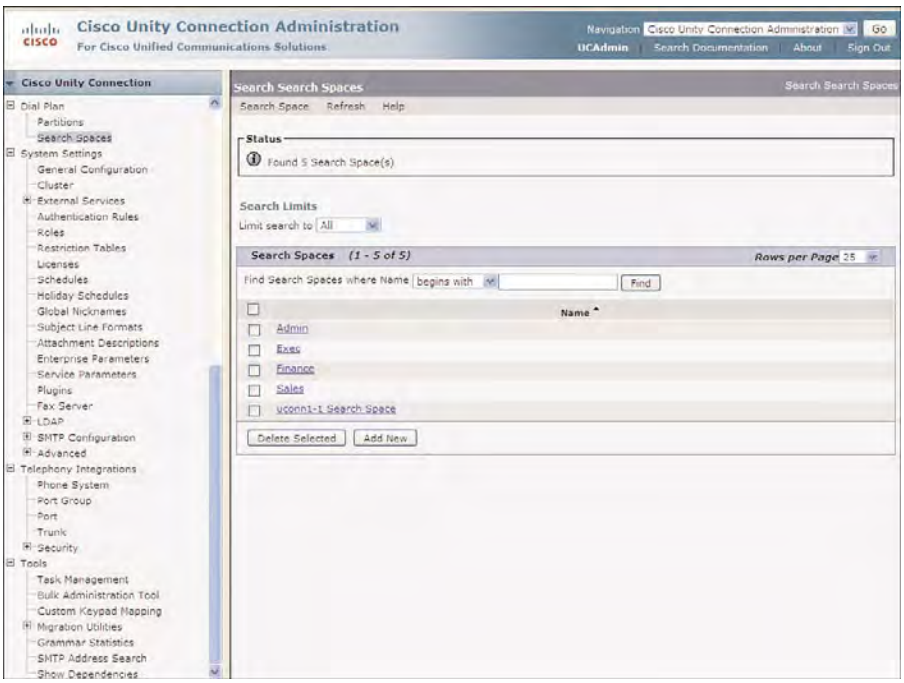

Figure 8-23 *Search Search Spaces Page Displaying the New Search Space Configurations*

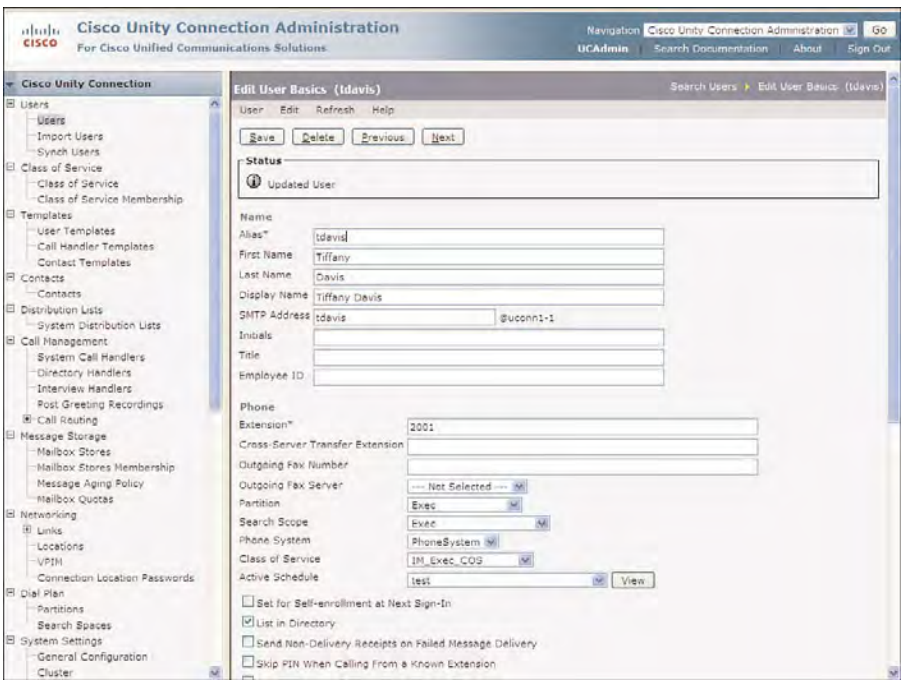

Figure 8-24 *Assignment of Search Spaces and Partitions to a User*

www.it-ebooks.info

Users assigned to the Finance, Admin, and Sales search space cannot address messages or dial Tiffany's extension from Cisco Unity Connection because their search space does not include the Exec partition. Also, these users cannot access any resources (distribution lists and call handlers) assigned to the Exec partition.

Changing the Default Search Space and Partition

Search spaces and partitions are assigned to the default search space and partitions for objects created without using a template. Because most objects will be used by the administrative team, the defaults will be changed to the Admin search space and partition.

To review and modify the defaults, from the navigation pane, select **System Settings > General Configuration**. The Edit General Configuration page displays. From the Default Partition and Default Search Scope drop-down, select the Admin partition and search space, as shown in Figure 8-25.

Figure 8-25 *Edit General Configuration Options of the Default Partition and Default Search Scope*

Removing Search Spaces and Partitions

Partitions and search spaces can be removed only if they are not assigned to an object. A search space, however, can be reassigned when you attempt to delete the search space.

www.it-ebooks.info

To remove a search space, select **Dial Plan > Search Spaces** to display the Search Search Space page. Select the check box next to the search space to be removed and click **Delete Selected**, as shown in Figure 8-26.

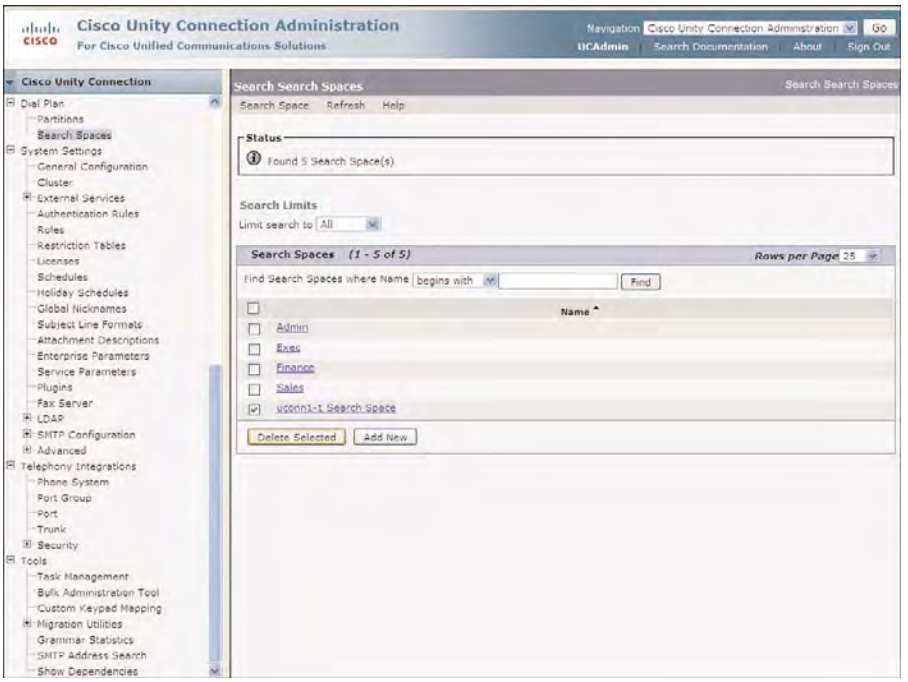

Figure 8-26 *Remove the System Search Space*

In this example, the organization determined that the system search space and partition are not going to be used and are to be removed. Therefore, the default system search space is checked.

Currently, the default system search space cannot be deleted because it is assigned to specific objects. When you click **Delete Selected**, however, a pop-up menu is presented for the Replacement Search Space, enabling the administrator to reassign all objects assigned to this search scope.

In Figure 8-27, the system search space is to be reassigned to the Admin search space, by clicking the radio button next to the Admin search space and clicking **Select Search Space**.

The unwanted search space is then deleted after reassigning all objects to the selected search space. The Search Search Space page is now displayed showing the remaining four search spaces, as shown in Figure 8-28. In this example, the system search space has now been deleted from the system, and all objects previously assigned to the system search scope have been reassigned to the Admin search space.

www.it-ebooks.info

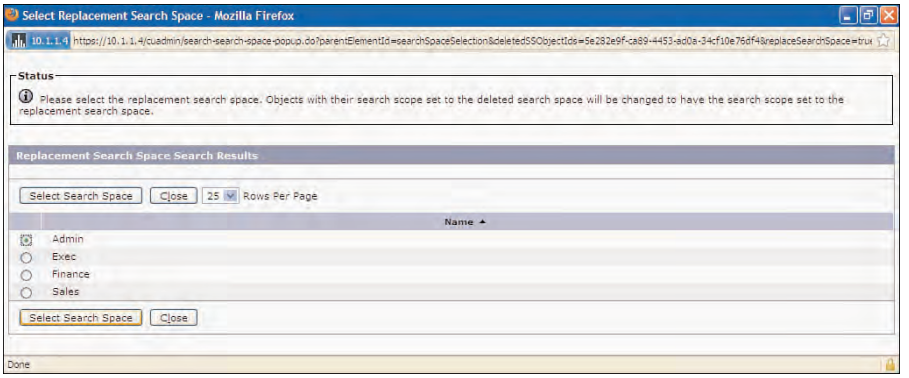

Figure 8-27 *Replacement Search SpaceAssigned to a Search Space*

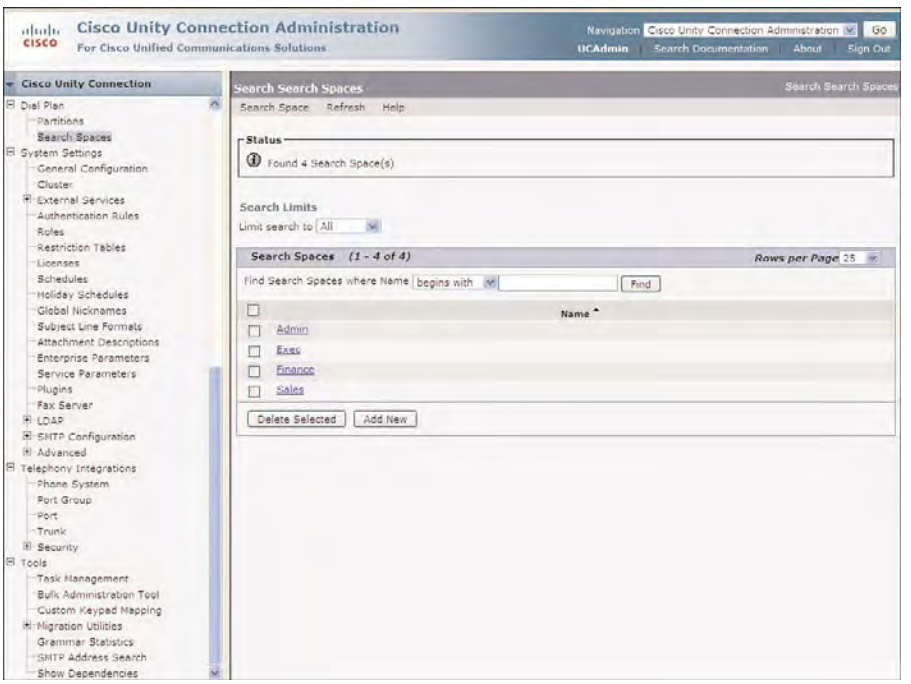

Figure 8-28 *Search Search Spaces Displaying the Remaining Search Spaces*

www.it-ebooks.info

There is not currently a mechanism to automatically reassign a partition before a deletion. You could use the Bulk Edit or Bulk Administration Tool, but this will still be a lengthy process if there are large amount of users, call handlers, and other system objects. Even though a partition cannot be deleted that has been assigned to any object, it can be renamed. For example, the default system partition can be renamed to a standard partition used in the organization and assigned to a search scope.

In Figure 8-29, the system partition was changed to the Exec partition, which is then assigned to the Executive search scope to meet the requirements of this organization.

Note The default system partition and search scope must be understood entirely before attempting to delete these components because they are used by default for all objects created in Cisco Unity Connection. The process discussed here is not intended to be a discussion of best practices for every organization, but intended for discussion of the process and procedures for deleting these components. The application of this process can vary between organizations.

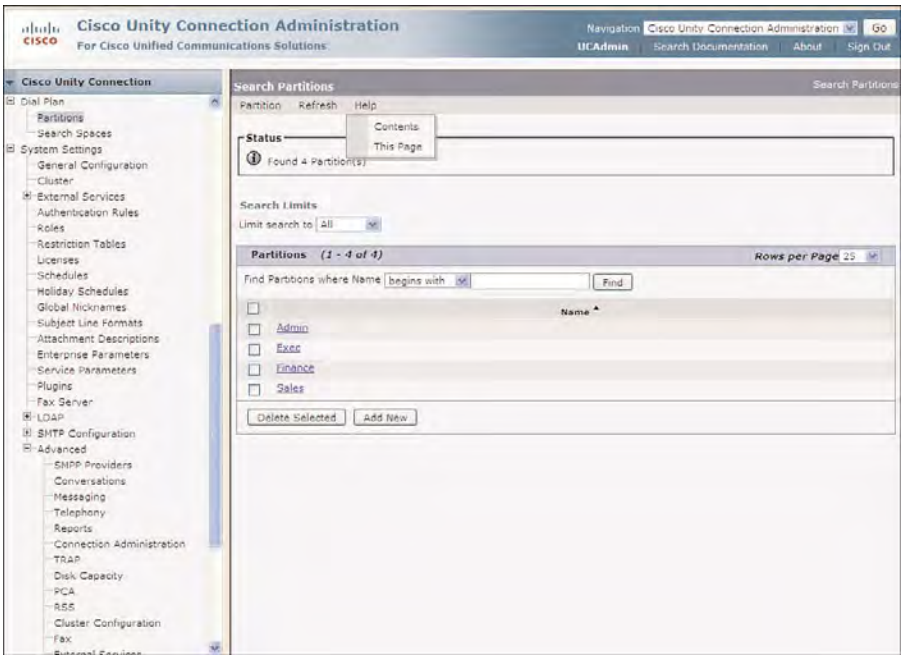

Figure 8-29 *Search Partitions Page Showing the Reconfigured System Partition*

www.it-ebooks.info

To confirm the new assignment and naming for the system partition and search scope, select an object and review the dial plan components assigned. In Figure 8-30, the **voicemailusertemplate** user template in Cisco Unity Connection displays the partition and search scope assignment. This template has a partition of **Exec**, which is the new name for the system partition. The **Admin** search space was reassigned from the system search space during the deletion of the system search space.

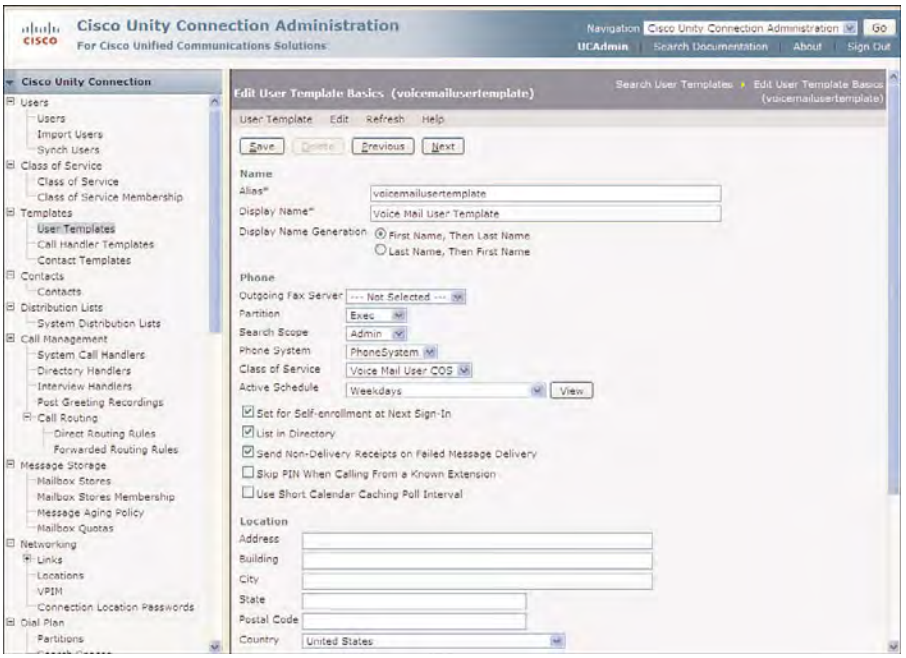

Figure 8-30 *System User Template with Reassigned Search Space and Partition*

There are a number of different approaches and purposes when configuring partitions and search spaces. The approach you decide in your organization depends on the level of accessibility required, locations, and your corporate division of labor. In some cases, everyone might be required to have access to all resources and users, whereas others might be more restrictive.

Case Study: Troubleshooting Dial Plan Issues

Tiferam Corporation has designed its dial plan according to the division of labor discussed in this chapter. Everything internally is operating as designed. The executives can address message and dial all other extension. Sales can call only sales, whereas Admin can contact Admin and Sales. Finance can call all other groups except for the executive team.

www.it-ebooks.info

Customers call the main number, which plays the company's opening greeting in Cisco Unity Connection. While listening to this greeting, the customers need to dial by extension or use the main directory to call users. During the pilot installation, it was discovered that customers could perform both functions when they were calling administration and sales. Customers could not contact finance or executive personnel, however, which is a requirement.

The solution was quickly located in the Direct Routing Rules. When an outside caller contacts the company, the direct routing rules determine who they can contact. In this case, the partitions included in the search space makes this determination. Based on this rule unknown callers can access the companies opening greeting,. This applies to all outside callers or customers. Their accessibility to users and resources is based on the search space assigned to the matched routing rule. The issue was located in the default routing rule, as shown in Figure 8-31.

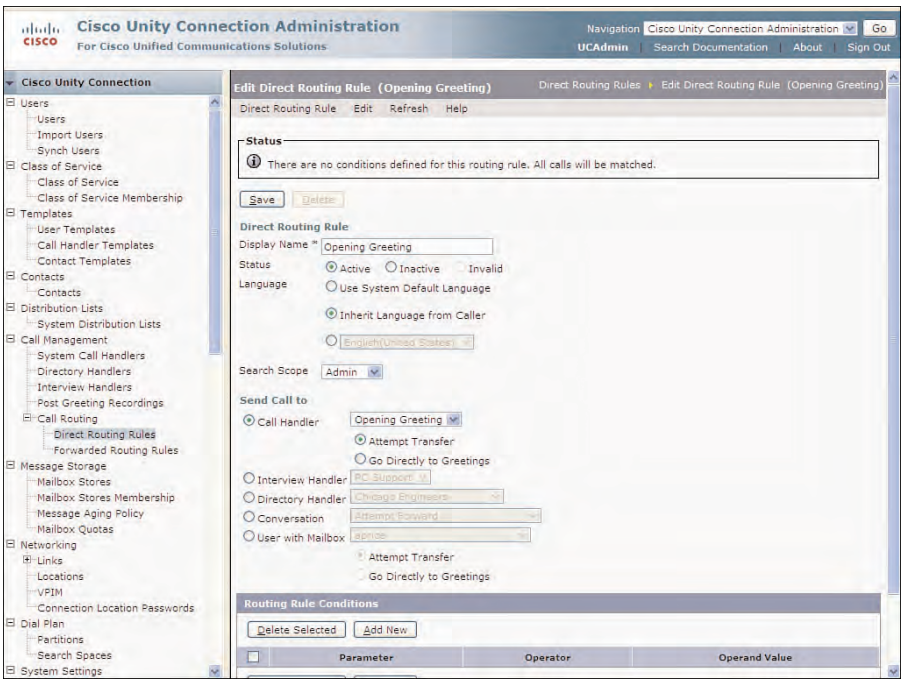

Figure 8-31 *Default Direct Routing Rule for Tiferam Corporation*

This direct routing rule is configured with the Admin search scope. This enables outside, or unidentified, callers to dial administrative and sales personnel from Cisco Unity Connection because the Admin and Sales partitions are assigned to this search space. These same callers, however, cannot place calls from the opening greeting to the executive and finance personnel.

www.it-ebooks.info

The issue was quickly resolved by assigning the above direct routing rule to the Exec search scope. At that point, customers could contact all users in all four partitions as needed.

Case Study: Configuring The Greeting Administrator

Mag's Motorcycle Corporation has many customers worldwide that call to get updates on the new product availability. Many of these requests arrive off-hours. To better assist these customers, the organization decided to use an audiotext application, enabling the customers to select from a menu of options. One of these options would be the marketing information available in a marketing call handler. A greeting would be recorded as needed to provide timely information to customers when they call and make the proper selection.

This was easily accomplished through the configuration of the proper call handlers and caller input select on these system objects; however, the IT department is busy and understaffed. The continual recording of new greetings always appears to get delayed. To eliminate the delay and ensure that these customers get the information required in a timely basis, the marketing manager was configured to be a call handler owner for the marketing call handler.

A new hunt pilot with the unique number of 2880 was added to Cisco Unified CM for access to the Greeting Administrator conversation. This hunt pilot would use the same hunt list and voicemail port as the integration. A new direct routing rule is created that sends all calls that dialed 2880 to the Greeting Administrator conversation. The marketing manager can now access Cisco Unity Connection from any location as required to record the new greetings for the marketing information.

In this case, the marketing manager dials 2880, the direct routing rule is matched, and the Greeting Administrator conversation is accessed. Figure 8-32 shows the direct rule configuration.

When the marketing manager dials 2880, the following conversation occurs:

1. **Cisco Unity Connection Greeting Administrator, enter your ID followed by pound:** The callers enter their assigned extension, followed by pound sign.
2. **Enter your PIN, followed by pound sign:** The caller enters their voicemail password, followed by pound sign.
3. **Enter the extension of the caller handler, followed by pound sign:** The caller enters the extension of the call handler, followed by pound sign.

www.it-ebooks.info

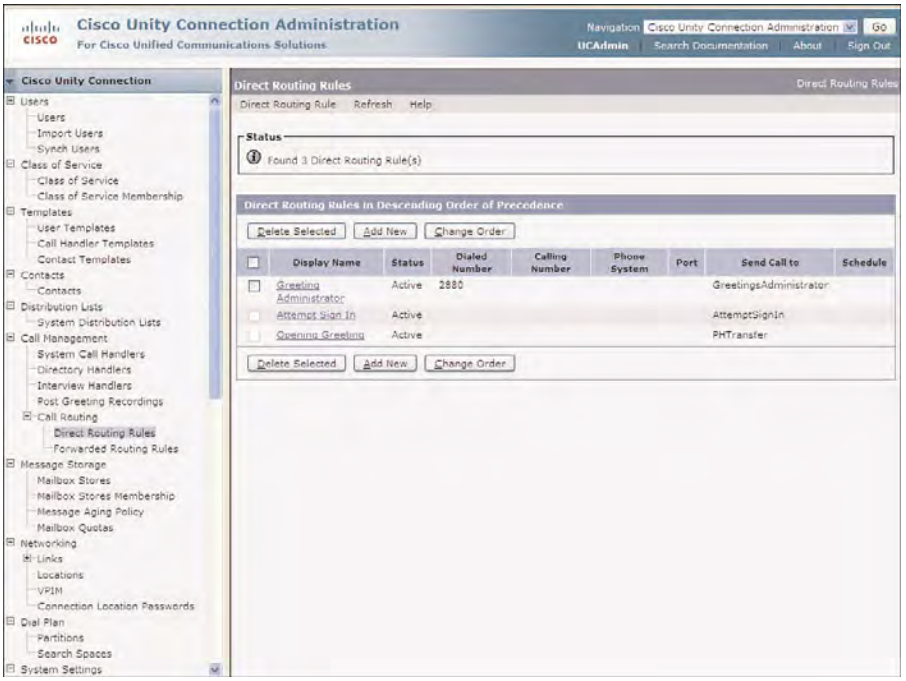

Figure 8-32 *Direct Routing Rules to Provide the Greeting Administrator Conversation*

From this point, the caller is authorized to record greetings or enable other greetings. For example, an Alternate greeting might be enabled to override the Standard Greeting during certain times. The marketing manager, who is responsible for this information, can now ensure that this information is available to customers in a timely basis.

Security for the Greeting Administrator is ensured because anyone contacting the Greeting Administrator conversation cannot access greetings that they are not listed as a call handler owner. When they attempt to contact this number and sign-in with their ID and PIN, they hear an announcement stating that they are not listed as a call handler owner for any call handlers on this system. Or if they are listed as a call handler for call handlers other than the one they are trying to access, they hear the announcement that they are not listed as a call owner for this call handler. A user who has authorization to use the Greeting Administrator to record greetings is limited to this function. They cannot change of options and features of call handlers.

www.it-ebooks.info

Summary

This chapter explored the various components and objects in Cisco Unity Connection that enable the design and configuration of an audiotext application. These consist of system call handlers and templates, directory handlers, interview handlers, and dial plan components. You learned how to do the following:

- Explore the function, features, and configuration of system call handlers and the use of templates to create these call handlers.
- Understand the features of directory handlers, and how they can provide accessibility to locate callers in Cisco Unity Connection.
- Explain the function and configuration of interview handlers, and how they can collect the responses to specific questions from a caller and deliver the responses to a user or group of users.
- Understand the design and configuration of the audiotext application in Cisco Unity Connection.
- Describe the various dial plan components, consisting of partitions and search spaces, and how they allow or restrict accessibility and reachability to users and resources.

www.it-ebooks.info

Chapter 9

Understanding Cisco Unity Connection Networking

This chapter covers the following subjects:

- **Simple Mail Transfer Protocol:** This section describes the function and purpose SMTP and how it delivers voice messaging between networked servers and cluster pairs.
- **Cisco Unity Connection Networking:** This section describes Cisco Unity Connection networking concepts and terminology, including the various elements: locations, sites, and SMTP domains.
- **Preparation for Networking:** You understand the steps to be considered before beginning the configuration of networking Cisco Unity Connection servers and cluster pairs.
- **Configuration of Network:** Explore the automatic and manual methods of configuring networking using intrasite and intersite links, and the various post-networking tasks.
- **Verification of Locations:** Understand the proper steps to verify the networking and synchronization of server in a Cisco Unity Connection network.
- **SMTP Smart Host Function and Configuration:** Explore the configuration, function, and purpose of the SMTP Smart Host between Cisco Unity Connection locations.
- **Interlocation Options and Features:** This section describes the features and configuration of cross-server sign-in, transfers, and live replay.

Cisco Unity Connection version 8.x software supports up to 20,000 users with mailboxes on a single server or cluster pair. This specification, of course, depends on the server platform, as discussed in Chapter 1, "Cisco Unity Connection Overview." When more users are required in the organization, multiple servers can be networked to form a *site*, enabling up to 10 servers to be networked together to support up to 200,000 users. A site is two more locations joined together by intrasite links. If more locations or servers are

www.it-ebooks.info

required in the network, two sites can also be joined together to form a *Voicemail Organization*. The Voicemail Organization concept increases these limitations.

If an organization needs to support multiple voicemail systems and must network with Cisco Unity, Cisco Unity Express, or other manufacturer server, Voice Profile for Internet Mail (VPIM) might need to be implemented. VPIM provides an industry standard protocol to enable the exchange of the voicemails between different voice-messaging systems. Chapter 10, "Implementing Voice Profile for Internet Mail (VPIM)," covers the VPIM networking concepts, features, and configuration in greater detail.

The concept of networking in voice-messaging system was first discussed in Chapter 2, "Designing Voicemail Systems with Cisco Unity Connection;" however, in this chapter, you specifically learn the various concepts, configuration, and troubleshooting involved with voicemail networking. If you are still unclear about these concepts, review Chapter 2 before you begin any configuration in Cisco Unity Connection.

The exchange of the messages and information between networked systems is accomplished through Simple Mail Transfer Protocol (SMTP), which is a standards-based TCP/IP protocol using port 25 for message transfer.

In this chapter, you understand the following:

- SMTP and its implementation in voice messaging
- The implementation and configuration of locations and sites using intrasite and intersite links to form a Cisco Voicemail Organization
- VPIM implementation between different voice-messaging systems
- The various features and networked objects, such as partitions, search spaces, contacts, and various addressing methods
- Directory synchronization methods in Cisco Unity Connection version 8.x
- The purpose and function of the SMTP smart host between locations
- The various cross-server features, including cross-server sing-in, transfers, and live reply

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is a standard-based protocol using port 25 to exchange messages and information between voice-messaging systems. The protocol is defined in RFC 821, published in 1982. This standard grew out of the number of earlier protocols, where a need to communicate electronically between various systems existed and was continuing to grow. In these cases, SMTP provided the protocol and mechanism for transferring information, and it continues to be used and implemented in today's modern voicemail systems.

SMTP provided the transfer of email in these earlier systems, especially for text-based messaging; however, the protocol was ASCII-based and could not handle other types of

www.it-ebooks.info

formats, such as binary file transfers. The transfer mechanisms of SMTP worked well because it provided the addressing and envelope information for the transfer of the outgoing and incoming messages. Other standards were developed to provide the delivery mechanism of the content, while SMTP was used for message transfer. The other standards that were developed that handled the encoding of content are referred to as the Multipurpose Internet Mail Extensions (MIME), which is specifically designed to encode the content of messaging, while using SMTP to deliver this content. SMTP uses TCP as the transport and therefore lends itself well to networking over the WAN.

SMTP and MIME is the standard used in Cisco Unity Connection networking to provide the transfer of voice messages to networked servers. VPIM networking also uses the SMTP and MIME standard to provide networking between dissimilar voice-messaging systems. In Chapter 10, you explore VPIM networking concepts and configuration.

An SMTP server, sometimes referred to as a Mail Transfer Agent (MTA) or mail relay is responsible for the transfer of messages from one system to another. Each system has its own implementation of the MTA. The transfer of messages between systems uses a Domain Name System (DNS) to locate the domain of the target host, using Mail Exchange (MX) Records. In other words, the MX records specify how messages are transferred or routed. When the domain is located for the message, the actual host or IP address must be determined. The MTA uses DNS to locate the address using Address (A) Records of the target host. These records resolve the IP address of the server. When this information is known, the MTA can transfer the message to the remote MTA server.

Messages can be routed and transferred between intermediate MTA servers acting as a mail relay agent. In these cases, messages are forwarded using MX and A records between the two systems using a Smart Host. Cisco Unity Connection supports the SMTP Smart Host implementation between networked Cisco Unity Connection servers. An SMTP Smart Host can also be used between VPIM networked voice-messaging systems.

The complete discussion of Simple Mail Transfer Protocol is beyond the scope of this text. However, the understanding of SMTP as it is related to Cisco Unity Connection networking is discussed throughout this chapter.

Cisco Unity Connection Networking

Digital networking in Cisco Unity Connection was first introduced with version 7.x software. In this version, up to five servers or cluster pairs could be digitally networked. In version 7.1, this limit was increased to ten servers. However, the maximum number of users is limited to 10,000 users with mailboxes, depending on the server platform. Even though the maximum number of digitally networked servers has increased, the amount of combined users and contacts cannot exceed 50,000. This limit has been increased in version 8.x software. The number of users per server is increased to 20,000 users, and the limitation of the total number of networked users and contacts has been increased to 100,000.

www.it-ebooks.info

Locations, Sites, and Intrasite Links

The Cisco Unity Connection version 8.x software uses different implementations and terms for referring to the various elements compared to the earlier version 7.x implementation of networking. Each server or cluster pair in the network is referenced as a *location*. Up to ten servers or locations can be networked together to form a *site*.

The location is determined at the time of installation and cannot be removed from the server configuration. A single location can be a member of only one site. Locations are interconnected to other locations in the site using *intrasite links*, as shown in Figure 9-1.

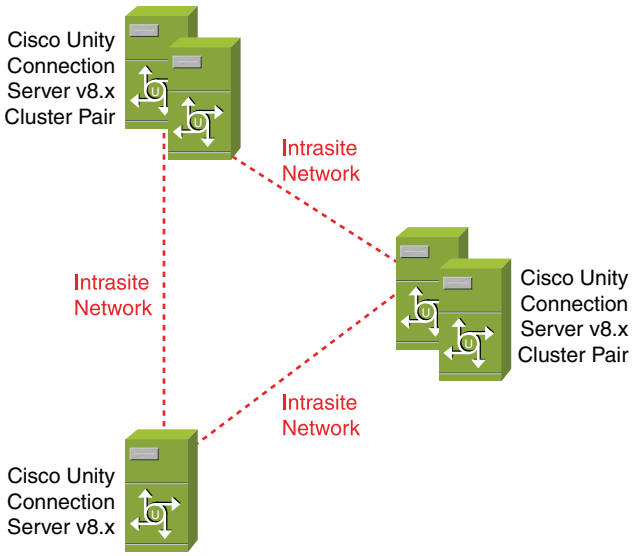

Figure 9-1 *Three Locations Networked to Form a Site Using Intrasite Links*

In this example, there are three locations, represented by a single server and two cluster pairs, which are interconnected using the intrasite links to form a site.

Networking between locations within a site uses SMTP for message transfer; therefore, the various locations can be interconnected between various corporate offices, as shown in Figure 9-2. This design architecture enables the flexibility of server placement according to the business requirements. In this illustration, three locations are networked across the WAN.

SMTP is also used for directory synchronization between locations. Within the site, all directory information, updates, and messages are transferred between each location, whether the Cisco Unity Connection servers are located on the corporate LAN or interconnected across the WAN to the various branch offices. In this manner, all locations have complete interconnectivity to all other locations within the site.

www.it-ebooks.info

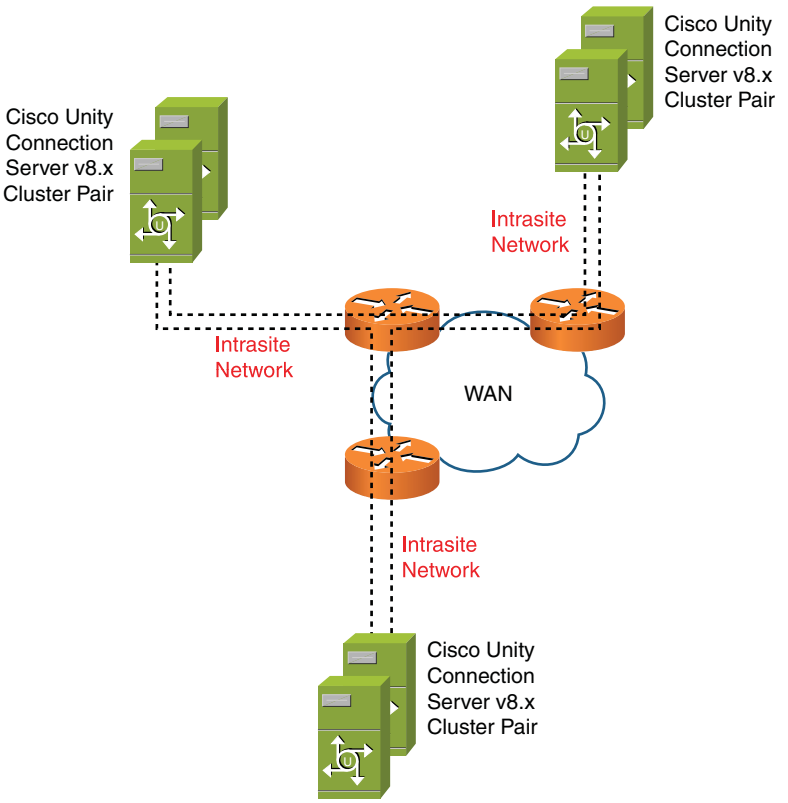

Figure 9-2 *Three Locations Networked Across the WAN to Form a Site*

Intersite Links and Cisco Voicemail Organization

Two sites, each consisting of up to ten locations, can be interconnected using an intersite link to form a Cisco Voicemail Organization, as shown in Figure 9-3. The intersite links are connected between two location servers, described as gateways (one in each site), to provide this interconnectivity. Only one intersite link can be used between two sites. In addition, the servers used within the Cisco Voicemail Organization must consist of Cisco Unity Connection or Cisco Unity version 8.x servers.

A Cisco Voicemail Organization can be configured between a single Cisco Unity Connection server (or site) and a single Cisco Unity server (or a digital network of Cisco Unity servers). However, the Cisco Unity Connection servers or site must consist of version 8.x server, whereas the Cisco Unity server that functions as the site gateway must be a version 8.x server.

www.it-ebooks.info

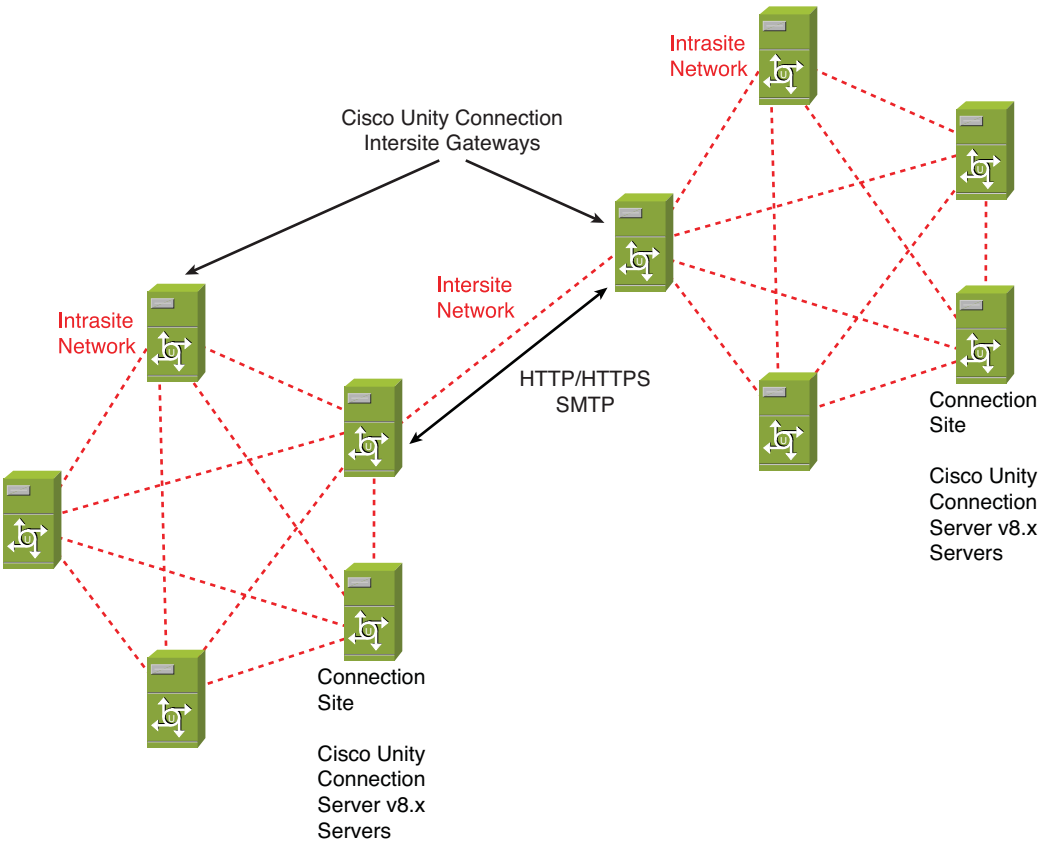

Figure 9-3 *Two Sites Joined by an Intersite Link to Form a Cisco Voicemail Organization*

If you use a Cisco Unity version 5.x server within the digital network, the appropriate engineering special must be installed on the Unity server to provide support for networking with Cisco Unity Connection servers. Also, the site gateway of Cisco Unity digital network must be a version 8.x server.

Directory synchronization and updates occur periodically between the two site gateways using the intersite link. The directory synchronization and updates uses HTTP or HTTPS protocols for this exchange. These gateways are also responsible for sending messages between sites using SMTP. If you install a cluster pair as the site gateway, only the publisher participates in the directory synchronization over the intersite link, even though the subscriber continues to perform message transfer using SMTP.

When configuring a Cisco Voicemail Organization, a global directory of all local and replicated objects is formed between the sites; however, there are limitations on the number of combined system objects. One of these limitations concerns the number of users, contacts, and distribution lists. That is, for the intersite link to be successfully created to

www.it-ebooks.info

form the Cisco Voicemail Organization, there is a limitation of a 100,000 users and contacts in the global directory and 100,000 distribution lists between the two sites.

Preparations for Networking Cisco Unity Connection Servers

Before networking is configured on the Cisco Unity Connection servers, a number of preparation tasks must be considered:

- Review the current network design and software.
- Ensure connectivity between locations.
- Configure display names and SMTP domains.
- Configuring intrasite links (Automatic versus Manual Method).
- Verify the network.
- Verify directory synchronization.
- Verify users and system objects.

Review the Current Network Design and Software

It is imperative that your network planning includes the proper placement, location, and addressing of all Cisco Unity Connection servers to be joined to the site. If you plan for a Cisco Voicemail Organization, one version 8.x server must be designated as a bridgehead server that will be configured with the intersite link.

Ensure Connectivity Between Locations

Verify that there is connectivity between servers to be joined to the network in the site. This connectivity includes SMTP port 25, for directory synchronization and message transfer. In some cases, an SMTP Smart Host might need to be configured, where firewalls prevent access to port 25. Also, an SMTP Smart Host needs to be configured where cluster pairs are deployed. This provides transfer of messages to the subscriber servers. SMTP Smart Hosts will be discussed later in the section, "SMTP Smart Host Function and Configuration."

Configure Display Names and SMTP Domains

Any server or cluster pair to be networked within the site must have a unique display name and SMTP domain. By default, the display name is configured to be the hostname of the server, and the default SMTP domain is configured to include this hostname. In this way, all new installations should have a unique SMTP domain name by design. If you upgrade from a previous version of software, however, you must ensure this uniqueness.

www.it-ebooks.info

To review the display name of the server, from the navigation pane on the left in Cisco Unity Connection Administration, select **Networking > Locations**. The Search Locations page displays, as shown in Figure 9-4.

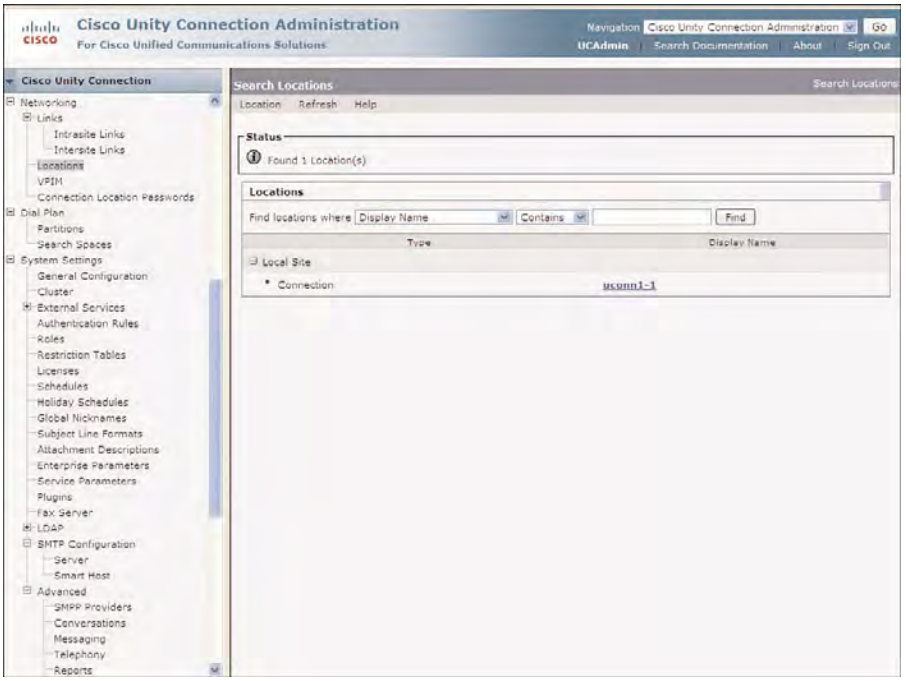

Figure 9-4 *Review the Display Name in Search Locations*

On the Search Locations page, each location consisting of a server or cluster pair is visible. In this case, the **uconn1-1** server references a cluster pair associated with a single location showing a display name of **uconn1-1**. The display name is based on the name of the publisher because the publisher is responsible for networking and directory synchronization between locations. When using cluster pairs, an SMTP Smart Host is required to resolve the domain name for communication to the subscriber server.

Select the link for the local server, **uconn1-1**. The Edit Location page displays as in Figure 9-5. This page enables the administrator to change the Display Name as necessary. The main reason to change this option is to assure uniqueness and also provide a meaningful naming convention.

The SMTP domain name is the same name as the display name and the server hostname. As stated previously, the display name must also be unique; however, it cannot be changed here on the Edit Location page. This must be completed under the SMTP configuration.

www.it-ebooks.info

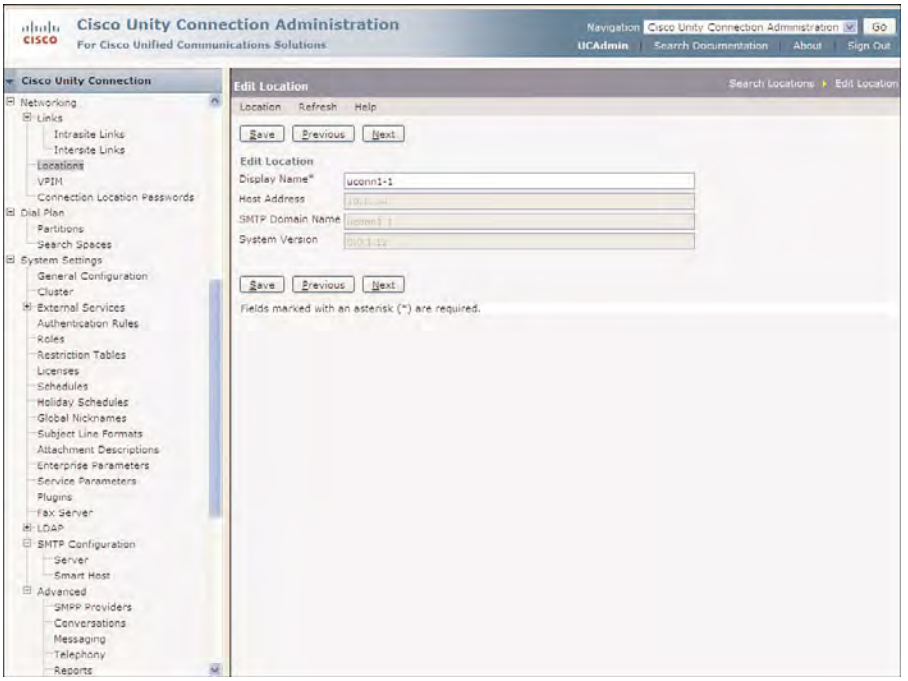

Figure 9-5 *Edit Location Page for the Local Server*

Case Study: Configuring Display Names

In this scenario, the Tiferam Corporation requires that the display names should match the departments and the users hosted on each server. This directive was decided in the design and planning phase.

For this solution, this server's display name will be renamed from **uconn1-1** to **Admin_Bldg5**, as shown in Figure 9-6. On the Edit Location page, the host address, SMTP domain name, and software version also displays. After all the changes have been made, select **Save** to commit the changes to the database.

Again, from the navigation pane, select **Networking > Locations**, verify that the new Display Name is listed correctly, as shown in Figure 9-7.

Changing the SMTP Domain

To review or modify the SMTP domain, from the navigation pane on the left in Cisco Unity Connection Administration, select **SMTP Configuration > Server**. The SMTP Server Configuration page displays, as shown in Figure 9-8.

From this page, you can change numerous SMTP parameters, including the number of simultaneous connections, message size, limits, and timeouts. Two options listed are read only, however: SMTP port and domain.

www.it-ebooks.info

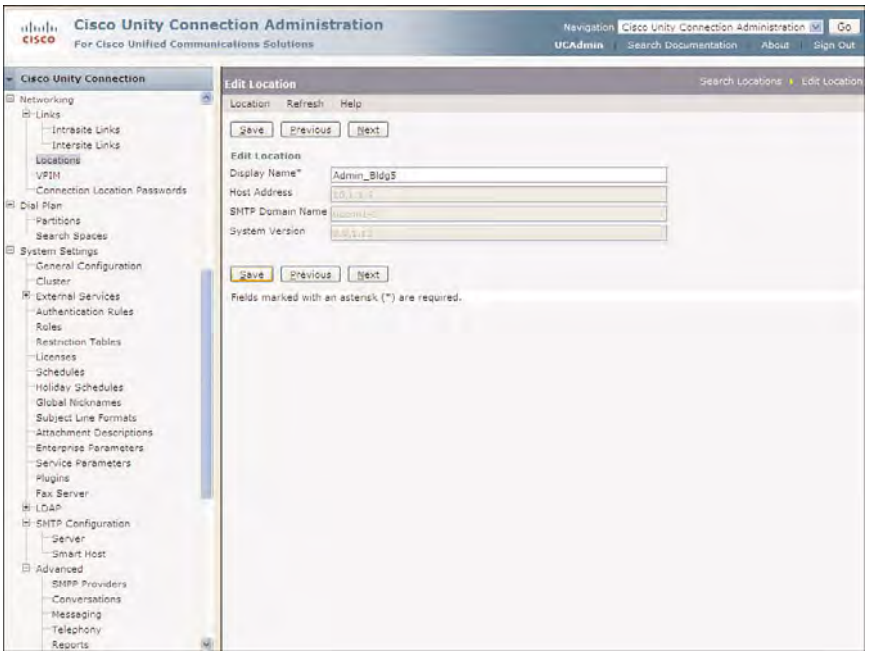

Figure 9-6 *Edit Location Page for the Admin_Bldg5 Location*

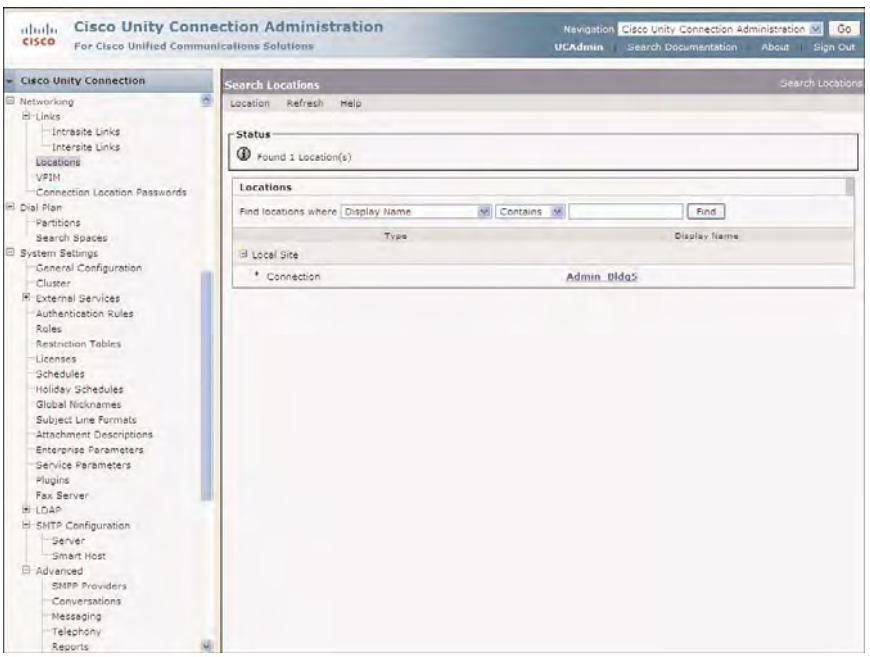

Figure 9-7 *Search Location Page Showing the New Display Name*

www.it-ebooks.info

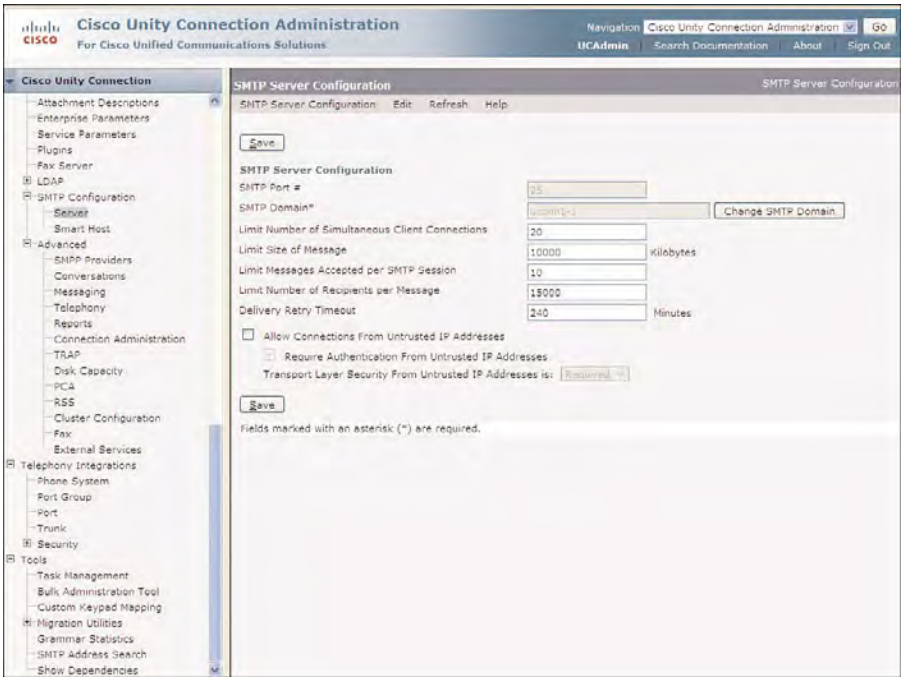

Figure 9-8 *SMTP Server Configuration in Cisco Unity Connection*

SMTP uses port 25 as a standard port and should not be changed. In a previous verification step, it was mentioned to ensure connectivity, which includes verifying that port 25 is not blocked by firewalls, router access lists, or any other networking elements. The SMTP domain name must be unique; change it clicking **Change SMTP Domain** to the right of the domain check box.

Case Study: Configuring SMTP Domains

Tiferam Corporation is using the domain name of tiferam.com; however, within the organization, it was determined that each SMTP domain must be configured according to the job function of the hosted users with a specific naming convention.

For this part of the solution, the SMTP domain is changed to **admin**. This change was made to assist administration in management of servers. The SMTP domain is associated with the display name, **Admin_Bldg5**, which was configured in the previous step.

When the administrator selects the **Save** button, a pop-up window displays a message stating the following:

```
Changing the SMTP server domain name will cascade to all associated
users referencing this server. Press Ok to continue with this operation.
```

www.it-ebooks.info

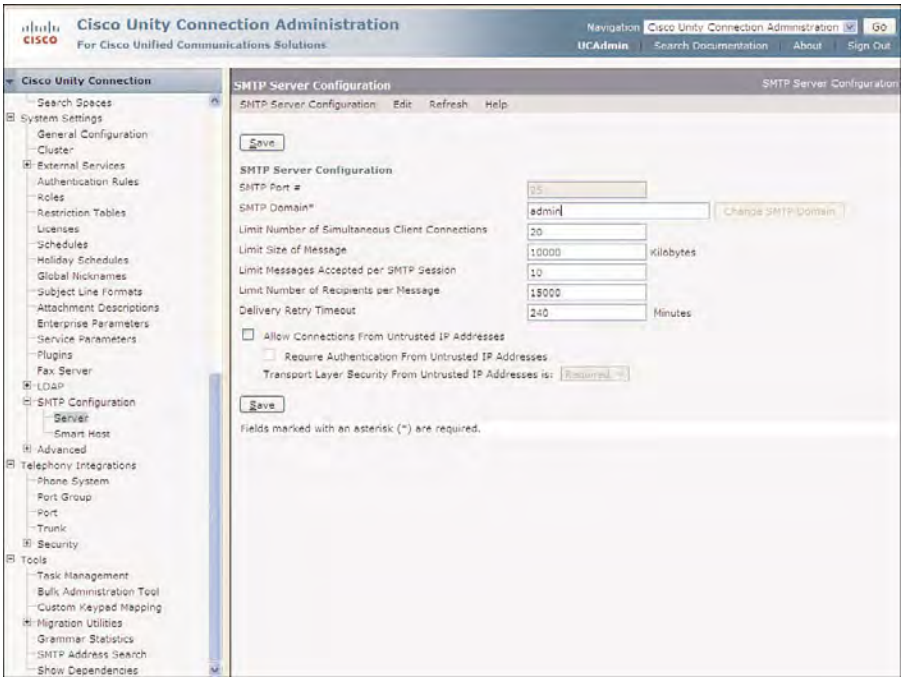

Figure 9-9 *Changing the SMTP Domain Name in Cisco Unity Connection*

Click **OK** to complete the operation. The SMTP server is now updated, as can be seen in the Status section of the SMTP Server Configuration page, as shown in Figure 9-10.

In Figure 9-10, the status section also indicates that the Connection Conversation Manager service must be restarted for the new domain name to be applied. This is necessary because all objects and users homed on this server need to be referenced to this new SMTP domain.

To restart the Connection Conversation Manager service, select Cisco Unity Connection Serviceability from the Navigation drop-down on the upper portion of the screen, and click **Go**. The Cisco Unity Connection Serviceability page displays.

On the Cisco Unity Connection Serviceability page, select **Tools > Service Management** from the toolbar. You need to locate the Connection Conversation Manager service listed under the Critical Services section. Click **Stop** under the Change Service Status column for this service, as shown in Figure 9-11.

At this point, a pop-up warning displays saying that the roles of servers will change. Of course, this applies only to cluster pairs, in which the subscriber can now become the primary server. You review these changes in the cluster management section after restarting the Connection Conversation Manager service.

www.it-ebooks.info

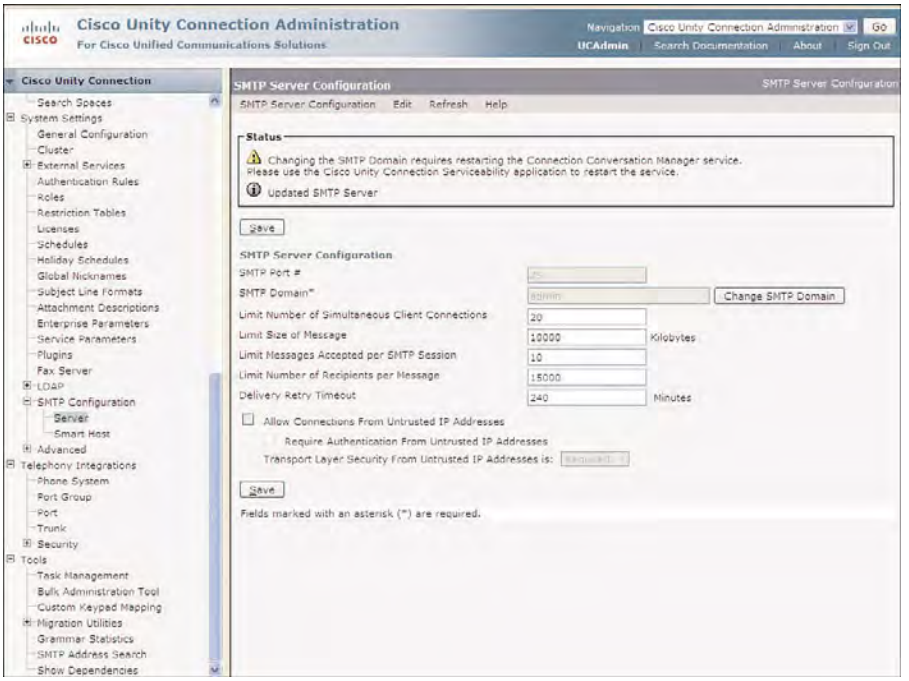

Figure 9-10 *SMTP Server Configuration Illustrating the SMTP Domain Change*

After the screen refreshes, under the Service Status column, the Connection Conversation Manager service indicates **Stopped**. Click **Start** to restart the Connection Conversation Manager service. Then, you need to ensure that the service indicates **Started** in the Service Status column before continuing on to the next steps.

If this location is a cluster pair, the subscriber server will have assumed the Primary role. Therefore, you need to navigate to Cluster Management and manually make the publisher the Primary server in the cluster. If the location is a single server, this next step can be skipped, because it applies only to a cluster pair.

Cluster Management

Cluster Management enables the administrator to manage each server in the cluster pair and provide a view of their current status. This ensures that both the publisher and subscriber function properly with the correct status.

From Cisco Unity Connection Serviceability, from the toolbar, select **Tools > Cluster Management**, as shown in Figure 9-12. The Server Manager section displays the server

www.it-ebooks.info

status of the publisher and subscriber, where you can notice that the Subscriber server shows a status of Primary. This occurred when Connection Conversation Manager service was restarted on the publisher. In this situation, the subscriber operates as the Primary; however, you need to ensure that the publisher is the Primary for normal operations.

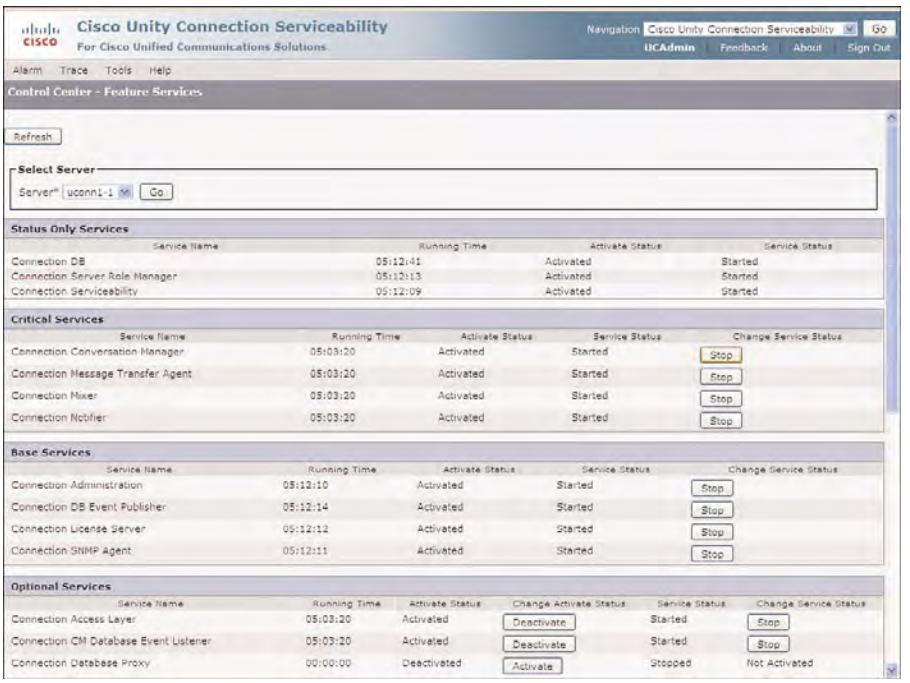

Figure 9-11 *Restart the Connection Conversation Manager Service After Domain Changes*

The server that has the Primary status is responsible for publishing the database and message store and sending message notification, MWI requests, and SMTP notifications. All critical services will be active on the server that has the Primary status.

To ensure that the publisher server operates as the Primary, under the Change Server Status column, click **Make Primary**. The Status section displays the change and the Pending Change column.

In this case, the publisher sends a request to the subscriber to make the change. Then, the subscriber enters a pending task, which is the request from the publisher server to **MakePrimary**, as shown in Figure 9-13.

Finally, after a few moments, the subscriber can honor the request from the publisher and change its status to Secondary. At this point, the publisher now assumes the Primary status of the cluster, as shown in Figure 9-14. The subscriber server logs the last status change under the Last Change Request column. This will be important information to the administrator, informing that a change occurred at some point.

www.it-ebooks.info

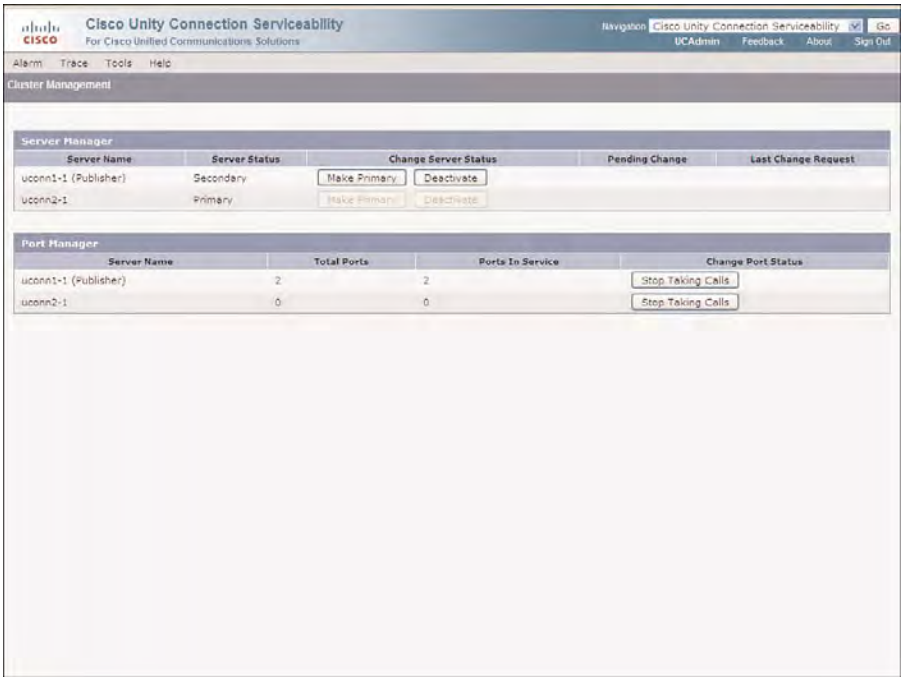

Figure 9-12 *Cluster Management Showing the Subscriber with Primary Status*

The preceding steps should be completed on all servers and cluster pairs that are to be joined in the network and where the SMTP domain must be changed. Of course, this step is not required if the default SMTP domain is to be used.

Under the Last Change Request column, select the link called **Srm.MakePrimary**. The pop-up window displays the Task Execution Results of the event, as shown in Figure 9-15. This change was a manual failback initiated by the administrator.

Review the Naming Conventions of System Objects

Finally, you need to review the network names for all objects to be replicated between locations, especially the system generated objects. In some cases, these objects might be renamed. In other cases, they might be removed or possibly made unreachable.

For example, you can understand the confusion that might occur with a user sending a message to the system distribution list. If you do not rename the default objects, these objects will exist in the multiple locations and have the same name. So, when a user selects the distribution list, there could actually be multiple distribution lists with the same name. Therefore, because you are replicating information between locations, you must think globally, rather than locally concerning these system objects.

www.it-ebooks.info

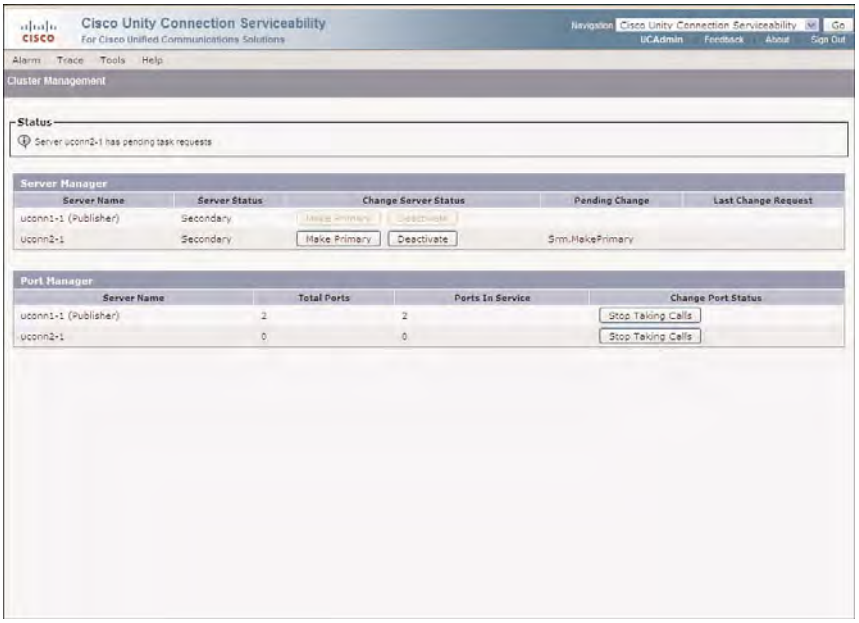

Figure 9-13 *Cluster Management: Providing the Publisher Server with Primary Status*

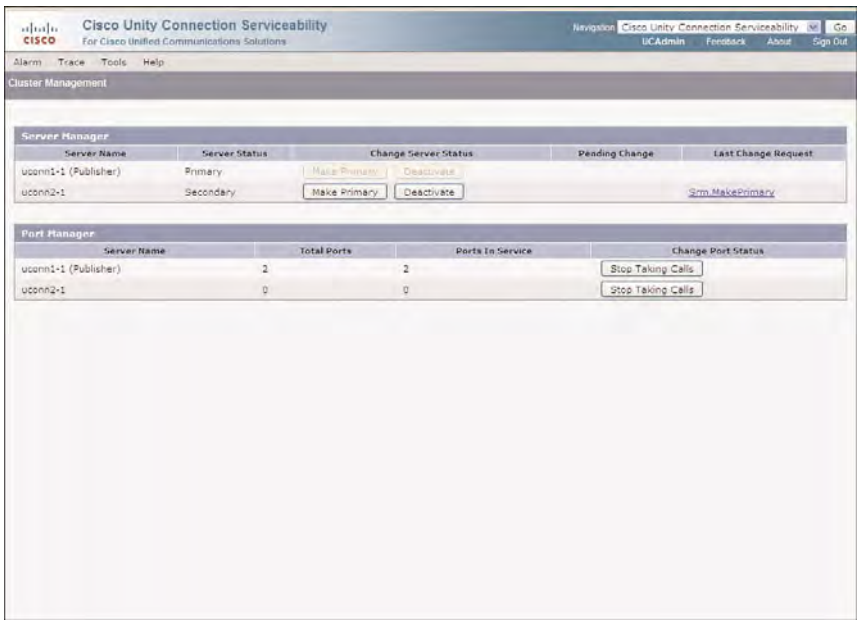

Figure 9-14 *Cluster Management Displaying the Proper Status of a Cluster Pair*

www.it-ebooks.info

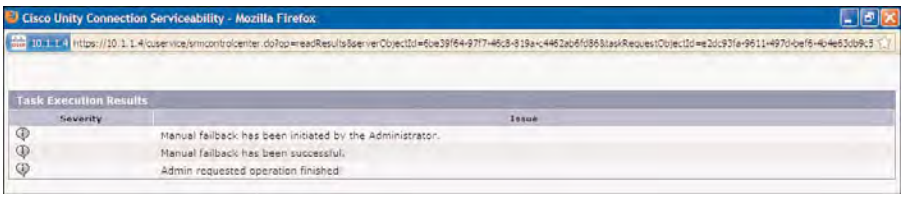

Figure 9-15 *Task Execution Results for the Manual Failback Event*

In the last section, you learned how the system-generated partitions and search spaces were renamed and changed to provide accessibility and reachability to users and resources. Partitions and search spaces once more need to be considered when understanding the networked objects because these objects are synchronized between locations.

Following are the various objects that need to be considered:

- Users
- Contacts
- Partitions
- Search Space
- Distribution Lists
- VPIM Locations

Case Study: Managing Distribution Lists

Tiferam Corporation decided to use the system distribution list for the users homed on each location in the organization. The distribution lists will then be made available to all users in the network.

To accomplish this task, the default system distribution list (**allvoicemailusers**) is changed to **All Admin** and assigned to the Admin partition, as shown in Figure 9-16. This configuration enables all users on this server that have the Admin partition in their search space to address messages to this distribution list. This distribution list can then be replicated to all other locations automatically; however, the distribution list membership is not propagated as part of this replication.

www.it-ebooks.info

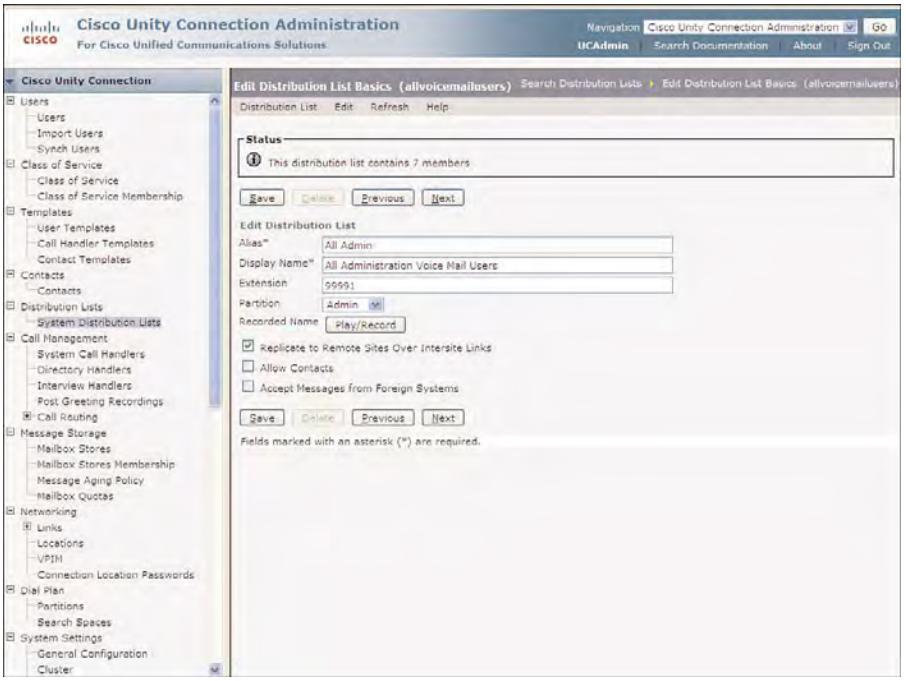

Figure 9-16 *Changing the Naming Convention of Distribution Lists*

If the organization uses the intersite link to form a Cisco Voicemail Organization, you can make this distribution list available to the other site, by selecting the **Replicate to Remote Sites over Intersite Links** check box. The organization also has the option to allow VPIM contacts to be included in the distribution list by selecting the **Allow Contacts** check box. You can also make this distribution available to accept messages from other voice-messaging system defined as VPIM locations. This later option is not available if you allow VPIM contacts to be included in the distribution list. Also, the distribution list cannot be replicated across the intersite link, if the **Allow Contacts** option is selected.

Any message addressed to this distribution list throughout the network will be sent to all the admin users that are homed on this server.

The configuration of the system distribution lists for Tiferam Corporation follows the same naming conventions. In the following example, you explore networking this server with another in the organizations' engineering department. The same distribution list on that server will be configured in a similar manner, but named **All Engineers**. If this configuration was not done, you would have multiple distribution lists with the same name

www.it-ebooks.info

replicated throughout the network. After the configuration is complete, you need to ensure that users are aware of the changes to their distribution lists and how to address messages to these distribution lists.

Configuring Intrasite Links

When the servers are installed, configured, and properly prepared as discussed in the previous steps, the network configuration can begin. It is advisable to use a phased approach when first beginning to network Cisco Unity Connection servers and cluster pairs. In most cases, you want to start with two locations, ensuring the results are exactly as designed. As the network engineer, you need to become comfortable with the various networking procedures, methods, and verification steps. Finally, after the networking configuration is complete, users need to be informed and trained on the various features and message addressing between servers.

After you choose the locations to be networked, the first step is to create intrasite links between the two locations. In essence, the formation of an intrasite link between two or more locations constitutes a site, or a digital network of Cisco Unity Connection servers and cluster pairs. Because digital networking was first introduced in Cisco Unity Connection version 7.x servers, you can also configure intrasite links between version 7.x and version 8.x servers.

The next step is to understand the various methods that can be used to create these links. You need to understand the various methods and procedures before beginning any configuration.

Automatic Versus Manual

The following are two different methods that can configure intrasite links:

- **Automatic:** The automatic method to join two servers with an intrasite link is the easier of the two methods; however, both servers must be reachable at the time of configuration.
- **Manual:** The manual method requires the download and upload of each server's location configuration file between all servers to be joined to the site.

Figure 9-17 illustrates an overview of these two methods.

In this example, two locations (Admin_Bldg5 and Eng_Bldg9) will be joined to form a site for the Tiferam Corporation. Both automatic and manual methods can be used to complete this procedure. The final result will be identical with two networked locations consisting of a cluster pair and a single server for the administration and engineering departments, respectively. Both methods are explored in the next section.

www.it-ebooks.info

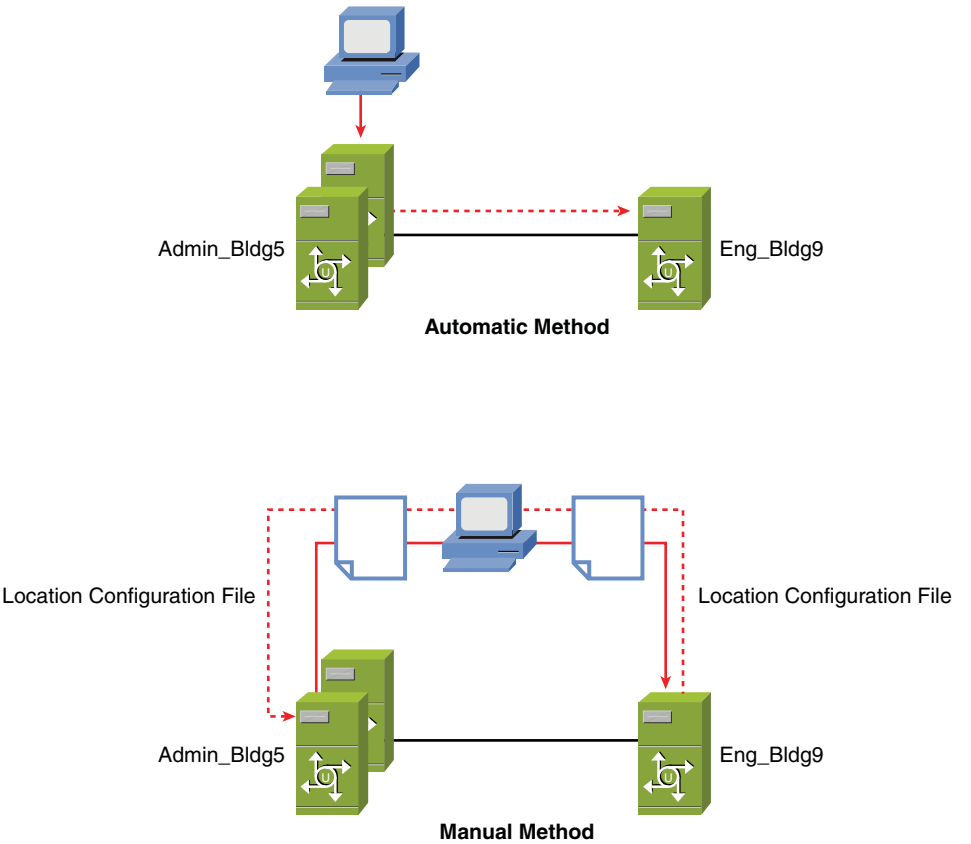

Figure 9-17 *Automatic Versus Manual Method of Joining Two Locations to a Site*

Automatically Join Two Locations to a Site

To configure two locations (single server or cluster pair) to form a site, select **Networking > Links > Intrasite Links** on one of the servers. If you perform this procedure on a cluster pair, ensure that you connect to the publisher server. The Search Intrasite Links page displays, as shown in Figure 9-18.

From the Search Intrasite Links page, select the **Join Site** button. The Join Site page displays, as shown in Figure 9-19. From this page, you first need to select the method to join the site. Select the **Automatically Join the Site** radio button to use the automatic method.

In the Join Site section, select the remote location by either IP address or its fully qualified domain name (FQDN). If you decide to use the FQDN, ensure that DNS is

www.it-ebooks.info

configured and accessible to the Cisco Unity Connection server. Finally, in the Remote Username and Remote Password field, enter the proper authentication credentials. The authentication credentials chosen here must be a user on the remote location assigned to the System Administrator role. In this example, an intrasite link is configured with the server located at 10.2.1.4 using the specific system administrator credentials. After all information has been entered, click **Auto Join Site** to create the intrasite link. A pop-up window confirms that you want to join the site. Click **OK** to complete the operation.

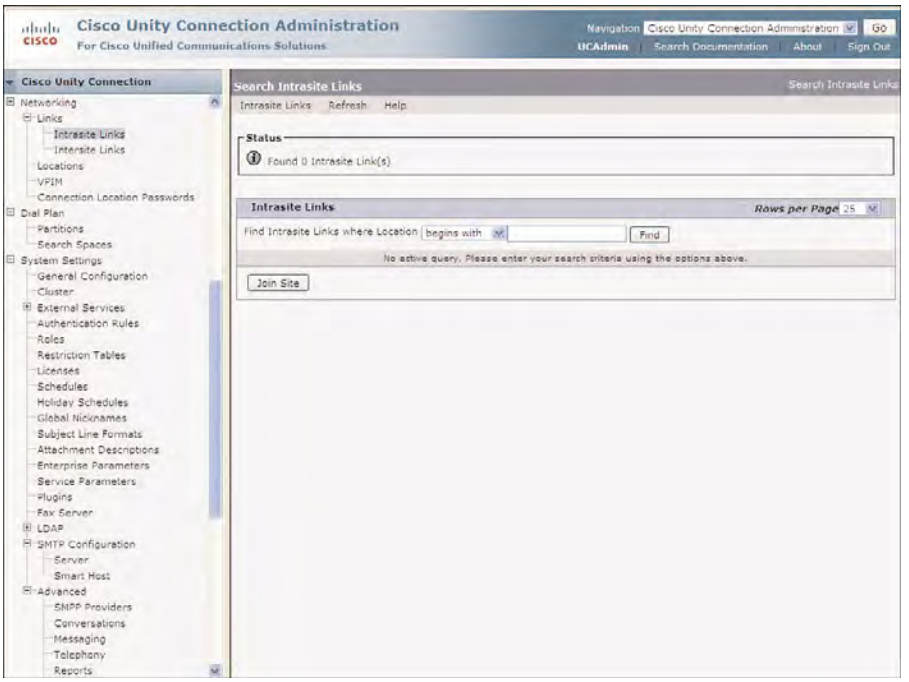

Figure 9-18 *Search Intrasite Links in Cisco Unity Connection*

In Figure 9-20, the Search Intrasite Links page now displays showing the remote location that has been joined to the site. The status section at the top of the page informs the administrator that the Connection Digital Networking Replication Agent service must be activated on all servers participating in the network. If you join a cluster pair to the site, this service needs to be activated only on the publisher server because only the publisher in a cluster pair participates in the networking between locations. You need to activate this service on both locations that form the intrasite link.

The Connection Digital Networking Replication Agent service is responsible for all networking functions between locations. This service is deactivated when a server is removed from the site, and again, needs to be activated when a server joins a site.

www.it-ebooks.info

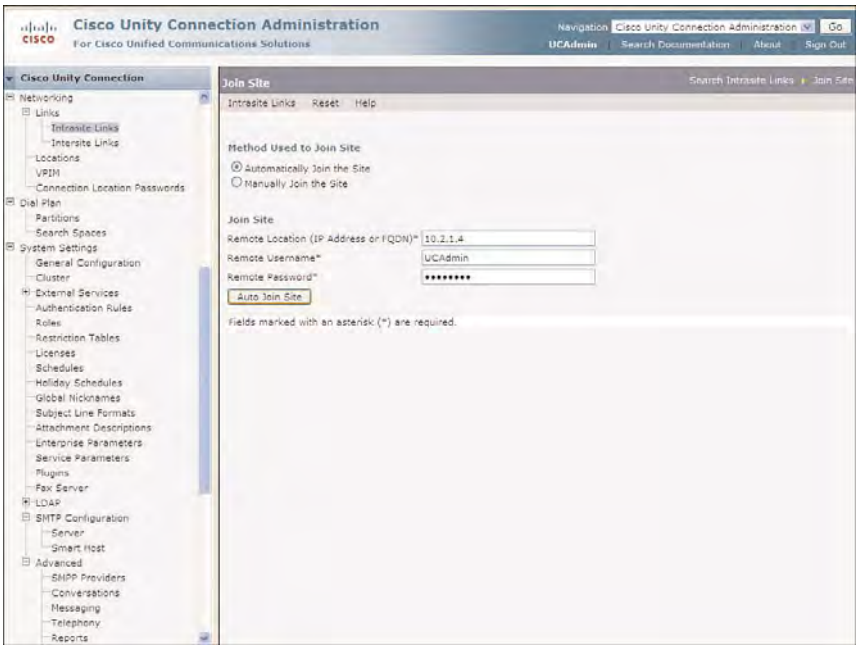

Figure 9-19 *Join Site Page to Automatically Join Two Locations to Form a Site*

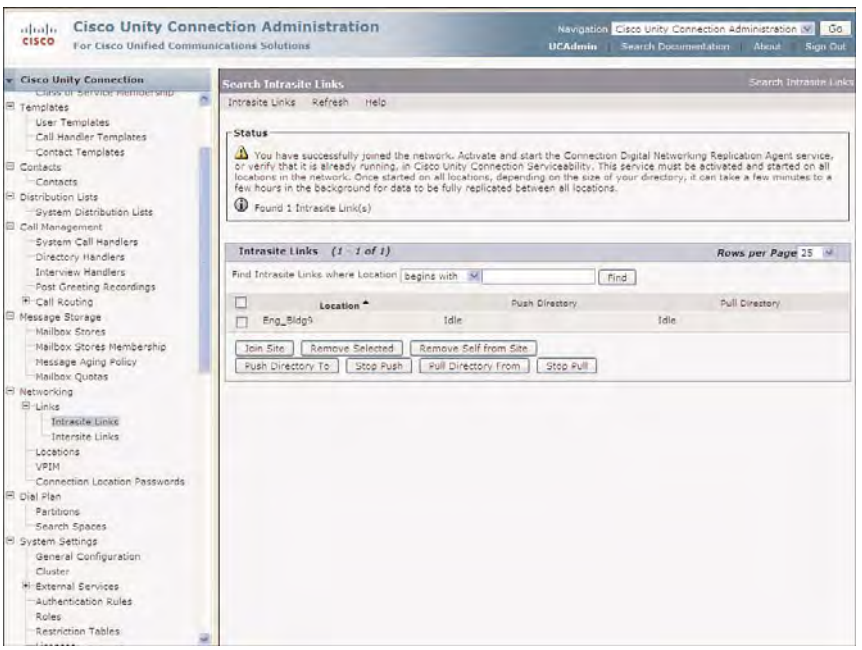

Figure 9-20 *Search Intrasite Links: Remote Location (Eng_Bldg9) Joined to the Site*

www.it-ebooks.info

To activate this service, from the Navigation drop-down, select Cisco Unity Connection Serviceability, and click **Go**. Select **Tools > Service Management** from the toolbar to view the **Control Center - Feature Services**. Under the Optional Services, click **Start** from the Change Service Status column for the Connection Digital Networking Replication Agent service, as shown in Figure 9-21.

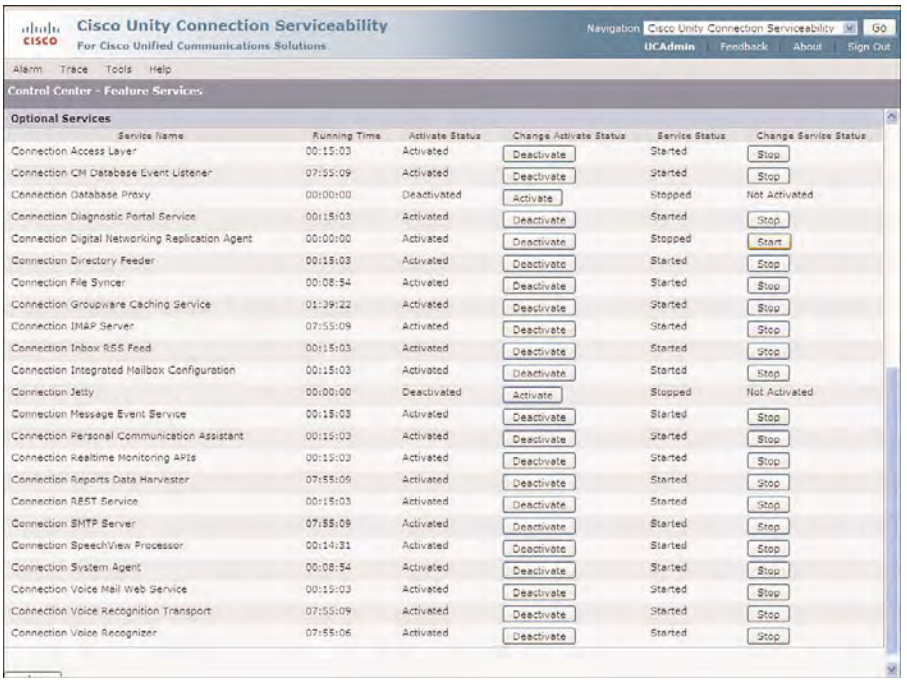

Figure 9-21 *Starting the Connection Digital Networking Replication Agent Service*

The Connection Digital Networking Replication Agent is responsible for the replication of all objects between locations in the site. It is active only when intrasite and intersite links are used. As mentioned previously, if a location is removed from the site, this service is automatically deactivated.

Manually Join Two Locations to a Site

The automatic method of joining locations to a site is the easiest method when networking servers. The manual method accomplishes the same results; however, it enables the complete configuration of networking to be completed without the remote server being readily available. For example, if an engineer needs to preconfigure a server at the headquarters site and have it shipped to a remote site, this procedure might be more preferable. In this way, the configuration can be completed and shipped to a remote location for installation at a later time. Using this method, the servers can be added to the network without administrator intervention.

www.it-ebooks.info

The manual method involves downloading a file, called a location configuration file, from each server, and uploading it to the other servers in the site. You then need to repeat this procedure for each server, so each server has the remote location configuration file of all other servers to be networked. You need to complete this procedure for every location to be joined to the site. Figure 9-17 illustrates the manual method to join two locations to the site.

To manually configure two locations (single server or cluster pair) to form a site, select **Networking > Links > Intrasite Links** on the first server. If you perform this procedure on a cluster pair, ensure that you connect to the publisher server. The Search Intrasite Links page displays.

On the Search Intrasite Links page, click **Join Site**. The Join Site page displays. Under the Method Used to Join Site section, select the **Manually Join the Site** radio button. The page refreshes, providing access to the download and upload sections, as shown in Figure 9-22.

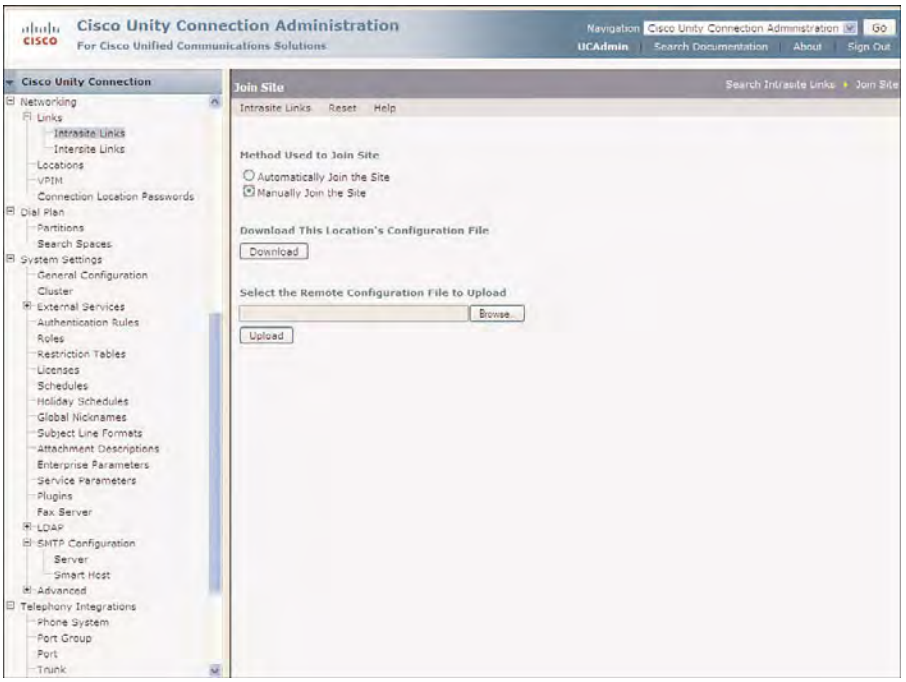

Figure 9-22 *Join Site Page for Manually Joining a Location to a Site*

The first step to manually join the site is to download the server's location configuration file. To complete this step, under the Download This Location's Configuration File section, click **Download**. A pop-up window opens enabling the engineer to view this file or save it to a workstation. Save this file, which will be used in the next step to import it to

www.it-ebooks.info

the other location to be joined. The default name of this file is called **LocationConfigurationFile**. You can change the name, if you want.

For illustration purposes, the author has chosen to open this file to view the contents for discussion purposes. This file displays in Figure 9-23.

Figure 9-23 *Location Configuration File*

The contents of this file include the location ID, display name, IP address, and replication user alias, followed by the certificate information.

After this file is saved to your workstation, you need to upload it to each server that is be joined to the site. To do this, on the next server or cluster pair, select **Networking > Links > Intrasite Links**. If you perform this procedure on a cluster pair, ensure that you connect to the publisher server. The Search Intrasite Links page displays.

On the Search Intrasite Links page, click **Join Site**. The Join Site page displays. Under the Method Used to Join Site section, select the **Manually Join the Site** radio button. The page refreshes, providing access to the download and upload sections.

Then, under the Select the Remote Configuration File to Upload section, click **Browse**, and browse to find the **LocationConfigurationFile** that was downloaded from the first server. Then, click **Upload**, as shown in Figure 9-24.

www.it-ebooks.info

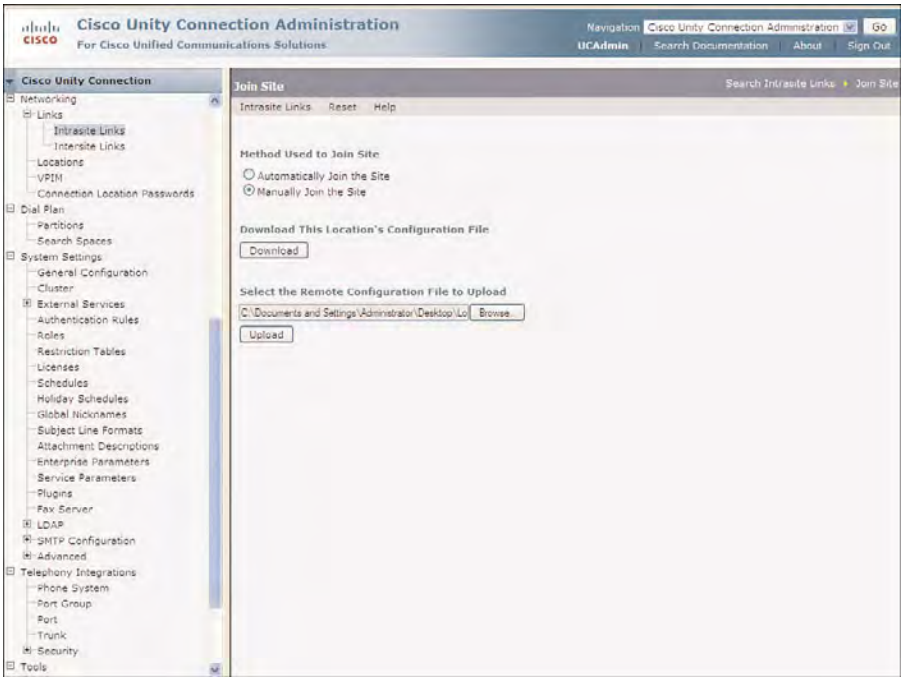

Figure 9-24 *Upload of the Location Configuration File*

After the upload procedure on the next server is complete, the Search Intrasite Links displays showing the new link created in Figure 9-25. The Status section indicates that the Connection Digital Networking Replication Agent service must be activated.

The procedure for starting this service must be completed on all servers to be joined to the site. For cluster pairs, this procedure should be performed only on the publisher server. This is identical to the procedure completed when using the automatic method of joining locations to a site. Figure 9-21 shows this process.

This completes the procedure for joining this location to the site; however, the same process must be successfully repeated for all other servers to be joined to the site. From the second server, download the **LocationConfigurationFile** and upload it to the first server using the same aforementioned procedures. Similar to the automatic method, you need to activate the Connection Digital Networking Replication Agent service after the upload is complete.

The manual method requires the download and upload of files at both servers, where the automatic method requires the configuration to be completed only on a single server. However, the Connection Digital Networking Replication Agent service must still be activated on all locations that participate in the site.

www.it-ebooks.info

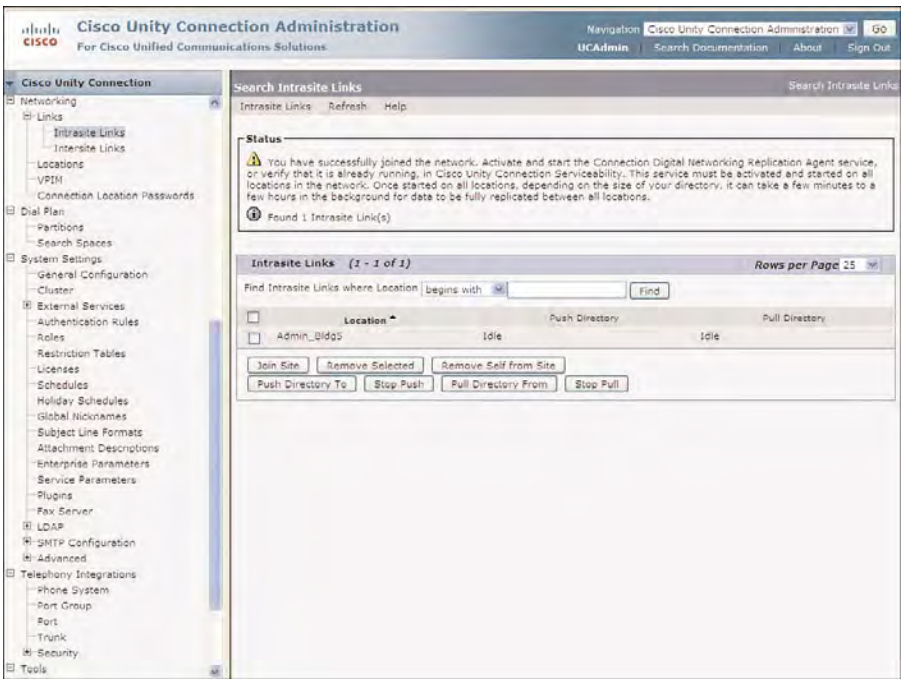

Figure 9-25 *Search Intrasite Links Displaying the New Location (Admin_Bldg5)*

Networking Verification

After the configuration has been completed and the locations have been properly joined to the site, each server can begin to replicate users and objects to all other locations joined to the Site. This is referred to as *directory synchronization* and occurs automatically without the engineers' or administrators' interaction after the location joins the site.

Verify Directory Synchronization

To verify the directory synchronization and networking between locations in the site, from the navigation pane in Cisco Unity Connection Administration, select **Networking > Locations**. The Search Location page displays showing the various locations joined to the site, as shown in Figure 9-26. The highlighted location is the local location. All others listed are remote locations.

The display names are used to select each location. Select the remote location **Eng_Bdlg9** that was joined to the site. The Edit Location page for the Eng_Bldg9 location displays, as shown in Figure 9-27.

The Edit Location section on this page is the section that the engineer can use to verify the proper networking and directory replication. From this page, you can view the remote location's display name, address, SMTP domain name, and software version. The last

www.it-ebooks.info

three fields (Last USN Sent, Last USN Received, and Last USN Acknowledged) verify the directory synchronization.

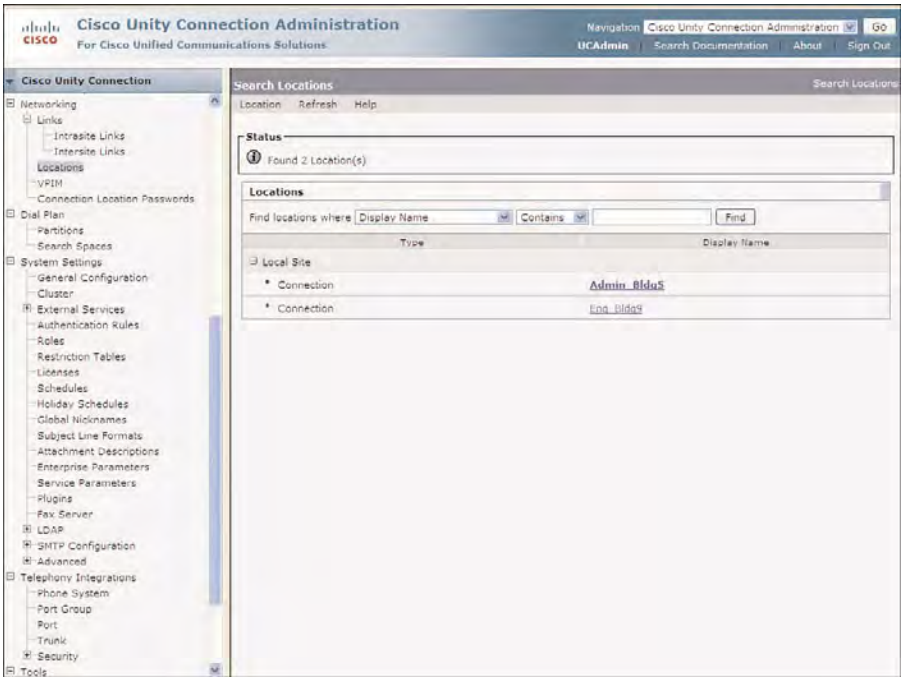

Figure 9-26 *Search Locations Page Displaying the Locations Joined to the Site*

When synchronization is performed between locations, all synchronization is tracked by Unique Sequence Numbers (USN). These USNs are part of a replication set. A replication set can track the most current information between locations to ensure that each server is using the most current configurations. If a location is upgraded or restored from a previous configuration, the replication set is incremented. Therefore, all locations use the most current replication set and acknowledge the corresponding USNs received from the remote locations' most current replication set.

In Figure 9-27, the Last USN Sent to this remote location is the same as the Last USN Acknowledged. Compare this information with the same information at the remote location. This means that from the perspective of the remote server it was sent USNs up to 36 and acknowledged 36 USNs back to the local server.

On the Eng_Bldg9 location, from the navigation pane in Cisco Unity Connection Administration, select **Networking > Locations**. On the Search Location page, select the remote location, Admin_Bldg5. The Edit Location page for this location displays, as shown in Figure 9-28.

www.it-ebooks.info

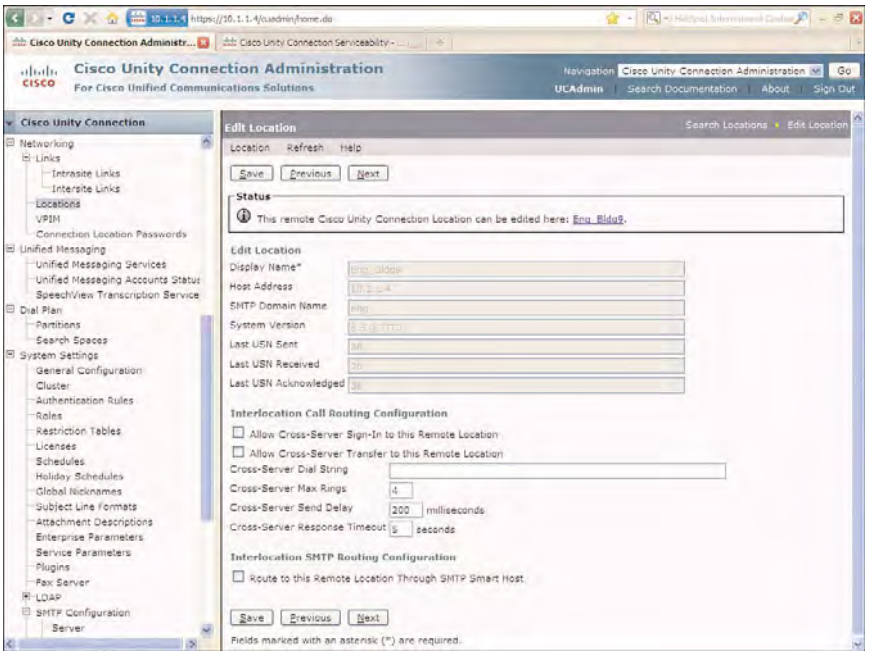

Figure 9-27 *Edit Location for Eng_Bldg9 Location Joined to the Site*

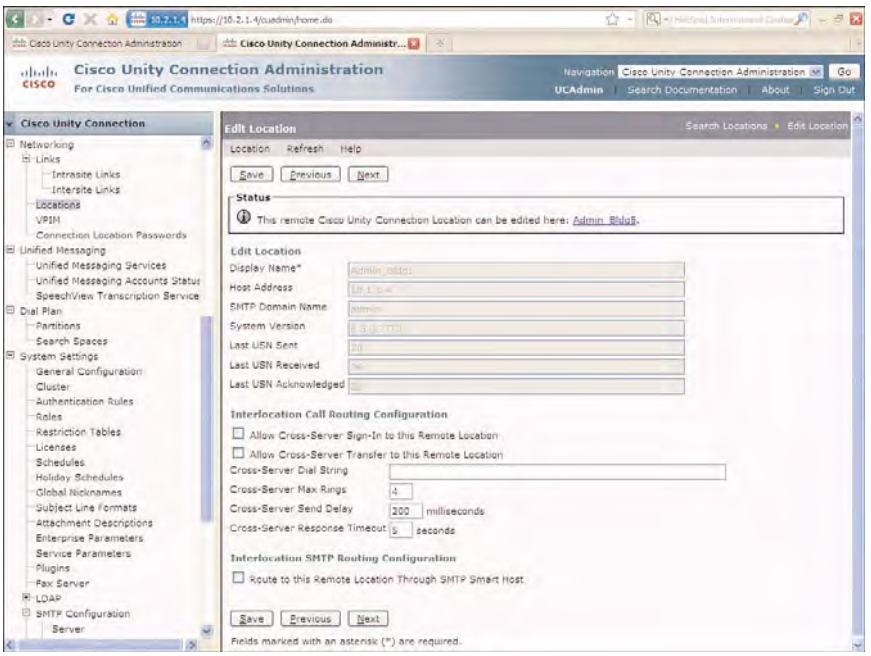

Figure 9-28 *Edit Location for Admin_Bldg5 Location (from the Perspective of Eng_Bldg5)*

www.it-ebooks.info

The Last USN Received is 36, which is the same as the Last USN Sent and Acknowledged on the Admin_Bldg5 location (refer to Figure 9-27) for this remote location. Consequently, this server shows the Last USN Sent and Acknowledged of 20 for the Admin_Bldg5 location, where this matches the Last USN Received on the Admin_Bldg5 location for this remote location (refer to Figure 9-27). In other words, from the perspective of the Eng_Bldg5 location, it received up to USN 36. This verifies proper synchronization between both servers that are now considered to be in sync.

The USN numbers sent will be different between servers and are tracked independently; however, for proper synchronization, each server tracks their USNs beginning with 0. The larger the configuration and database on the server means larger USN numbers and longer synchronization times.

The synchronization process proceeds as follows for a single location:

1. Admin_Bldg5 begins directory synchronization and sends USN 1 to Eng_Bldg9. This information is viewed from **Admin_Bldg5**; select the Eng_Bldg9 remote location and review the **Last USN Sent**.
2. Eng_Bldg9 acknowledges USN 1 from Admin_Bldg5. This information is viewed from Admin_Bldg5; select the Eng_Bldg9 remote location and review the **Last USN Acknowledged**.
3. Admin_Bldg5 receives the USN 1 acknowledgment from Eng_Bldg9. This information is viewed from Eng_Bldg9; select the Admin_Bldg5 remote location and review the **Last USN Received**.

The directory synchronization could take up to 5 minutes. Therefore, there might be moments when the Last USN Acknowledged might lag slightly but should continue to increase during the time of complete synchronization. When synchronization is complete, the three numbers (the remote Last USN Sent and Acknowledged with the local Last USN Received) should be equal.

You can also view the synchronization status from the Search Intrasite Links page. The Push Directory and Pull Directory columns display as **In Progress** while directory synchronization occurs. Synchronization can be manually initiated by the administrator, however, by selecting the check box next to the location and clicking **Push Directory To** or **Pull Directory From**, as shown in Figure 9-29. This page also enables the option to remove a location from the site, or remove the local location, as needed.

In this example, the check box next to the Admin_Bldg5 location was selected. Then, **Push Directory To** was clicked. The Push Directory column now displays the synchronization process as **In Progress** for the selected remote location. During this time of synchronization, the USN sequence is reset and starts again from 0. Depending on the size of the directory and configured objects on the server, this synchronization process might take up to 5 minutes or more to complete.

www.it-ebooks.info

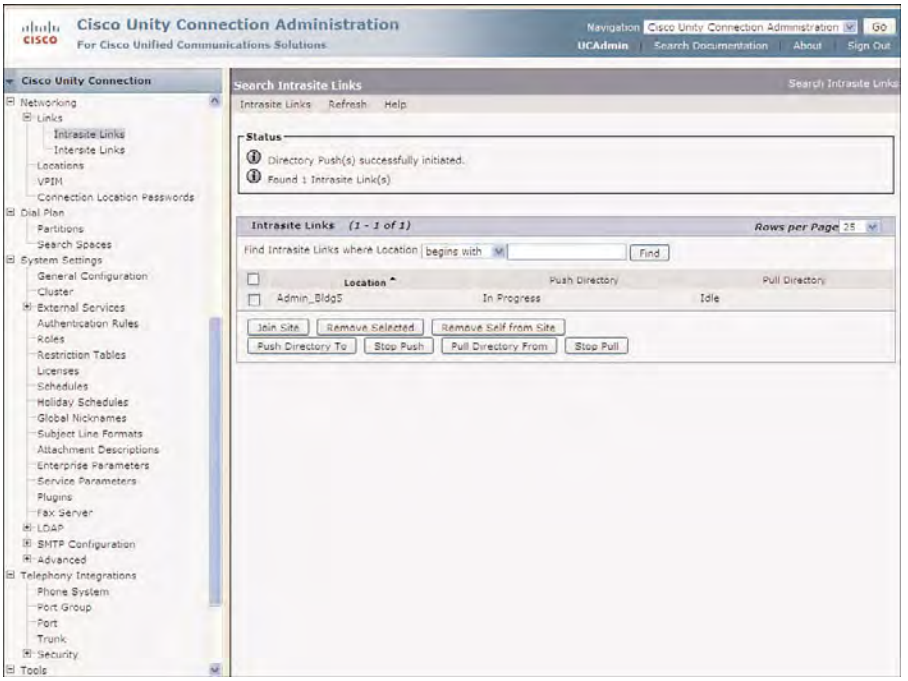

Figure 9-29 *Manual Push Directory to a Remote Location*

In Figure 9-30, the Edit Location page for the remote location shows the progress during this time of synchronization. In this illustration, synchronization information was sent to Admin_Bldg5 in 20 USN messages. This remote location is in the process of acknowledging these messages. At this point, none of these USN messages have been acknowledged. After all messages have been acknowledged and received, the locations are then in sync, and the Search Intrasite Links page changes to Idle for both the Push Directory and Pull Directory columns.

Verify Users and System Objects

In the next steps, you need to verify the users, distribution lists, and the various system objects. All this information is included in the replication sets exchanged as part of the directory synchronization. To verify the users, from the navigation pane on the left, select **Users > Users**. The Search Users page displays, as shown in Figure 9-31.

The remote users, Doug Engle and Dan Weis, display as grayish icons next to the Alias. The legend at the bottom of this page indicates that these are remote users. If you select these users to view their configuration, all options display as view only; therefore all changes must be completed on the local server where these users are located, or considered to be homed.

www.it-ebooks.info

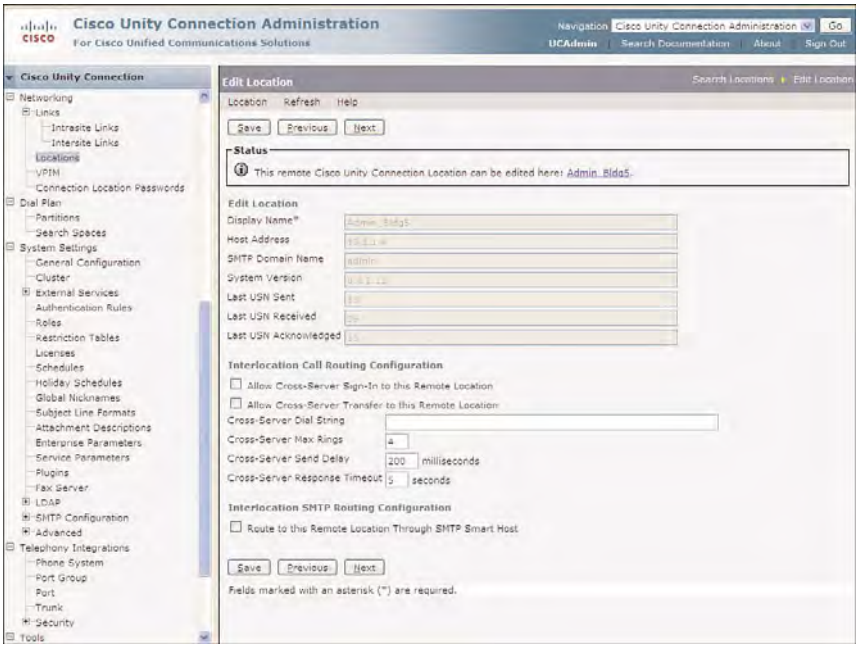

Figure 9-30 *Edit Location Page Displaying Directory Synchronization in Progress*

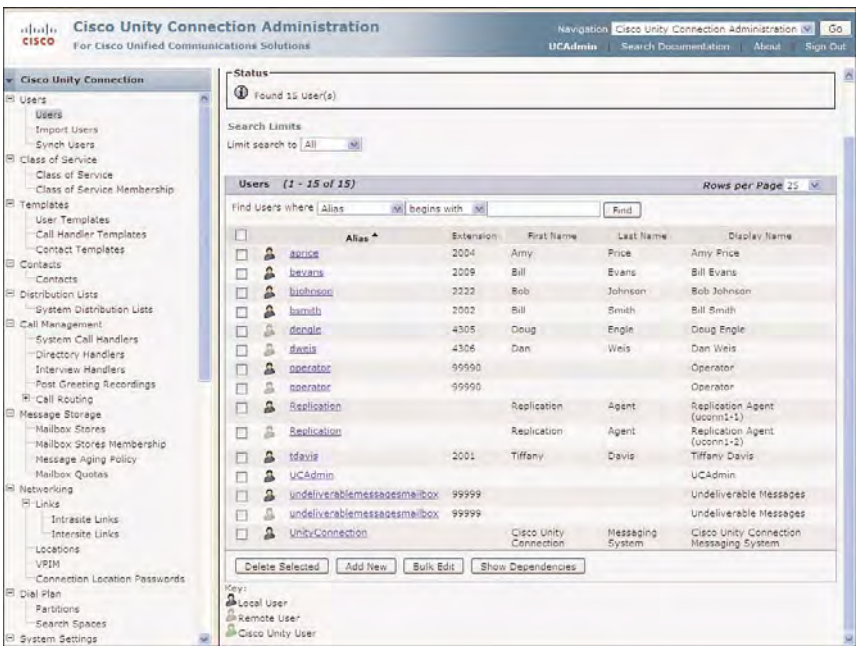

Figure 9-31 *Search Users Page Displaying Local and Remote Users*

www.it-ebooks.info

There are multiple names for the operator, replication, and undeliverable message mailbox. This was intentional to show that multiple names can exist between servers. This was discussed previously, where system objects were changed to identify their function, as configured earlier for distribution lists.

From the navigation pane, select **Distribution Lists > System Distribution Lists** to view the Search Distribution Lists page, as shown in Figure 9-32.

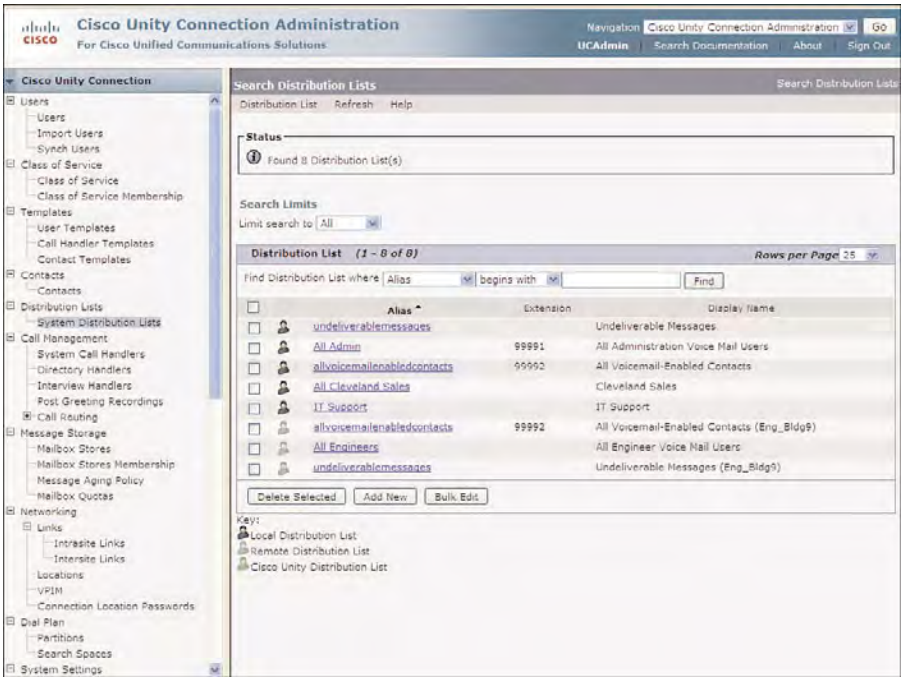

Figure 9-32 *Search Distribution Lists Page Displaying Local and Remote Distribution Lists*

The **All Admin** and **All Engineers** that were changed previously now display; however, the All Engineers distribution list was assigned to the All Engineers partition. If administrative users need to send messages to either distribution list, you need to assign this partition their search space on the Admin_Bldg5 location. Likewise, the same approach must be applied for engineering users to allow access to the **All Admin** distribution list.

This is one approach to show how one organization might use distribution lists. Another approach that might be used is to hide the default system distribution lists by assigning them to a partition that is not assigned to any search space. The result of this approach makes these distribution lists completely inaccessible to all users. Then, a new master distribution list is created and assigned to a partition, which is then assigned to the search space for all users. Finally, the default system distribution lists are then assigned as

www.it-ebooks.info

members to this new master distribution list. This creates a global directory available for all users in the site.

However, this example uses the earlier approach using the **All Engineers** and **All Admin** partitions. To complete this configuration, from the navigation pane, select **Dial Plan > Partitions**. The Search Partitions page displays, as shown, in Figure 9-33. The remote partition, **All Engineers**, has been replicated to this location.

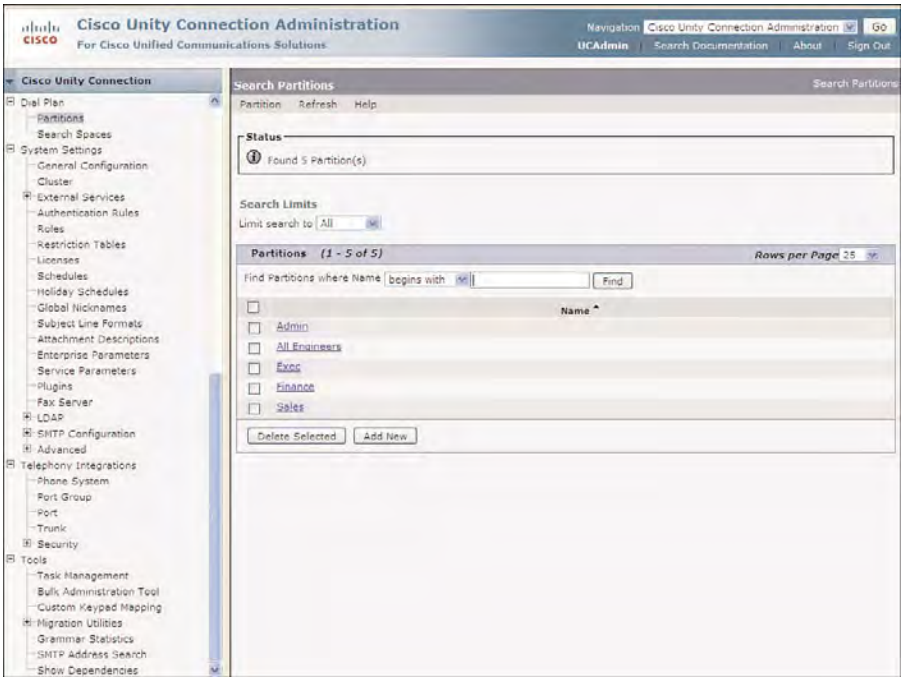

Figure 9-33 *Search Partitions Page Displaying Local and Remote Partitions*

To review the Search Spaces, from the navigation pane, select **Dial Plan > Search Spaces**. The Search Search Spaces page displays showing the local and remote search spaces that were replicated to this location, as shown in Figure 9-34.

In this case, the **All Engineer SS** search space displays as a remote search space and can be edited only from the location from where it was created.

Case Study: Performing Post-Networking Tasks (Dial Plan)

Tiferam Corporation has completed the initial networking of its administration and engineering locations; however, administrative users need to send address messages to engineers at the remote location. Currently, they cannot perform this task.

www.it-ebooks.info

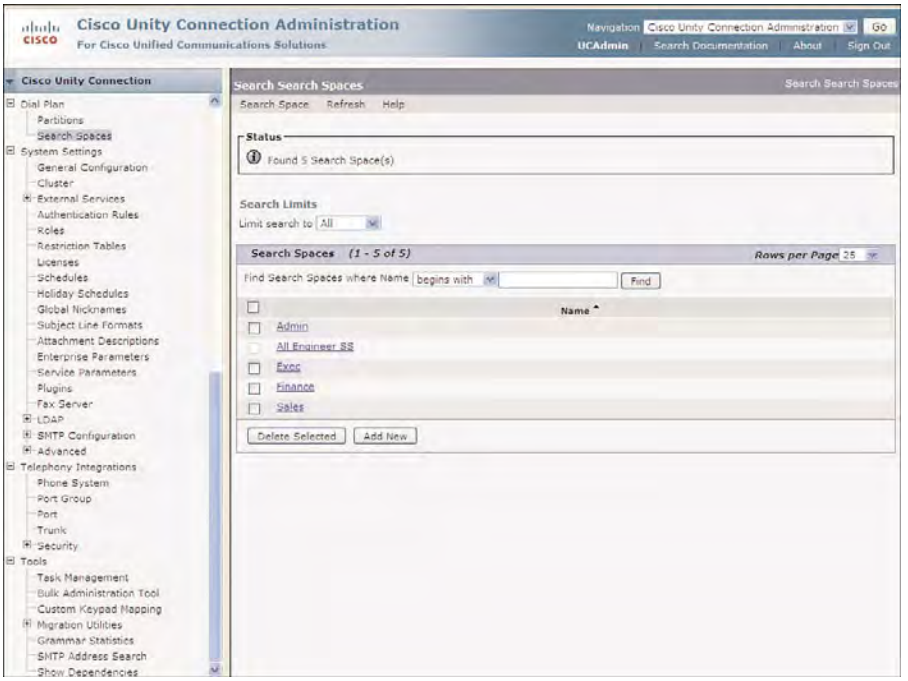

Figure 9-34 *Search Search Spaces Page Displaying Local and Remote Search Spaces*

It was discovered that all administrative users belong to the **Admin** search space. After further investigation, it was discovered that the **All Engineers** partition is not included in their search space.

To resolve this issue, the administrator for the Admin_Bldg5 location accessed Cisco Unity Connection Administration and from the Search Search Spaces page selected the **Admin** search space from the Search Search Spaces page. The problem was quickly resolved by moving the **All Engineers** partition from the Unassigned Partitions to the Assigned Partitions pane, as shown in Figure 9-35.

This procedure will then be completed for all local search spaces to provide access to the remote objects as necessary. Partitions are not automatically assigned to search spaces and therefore need to be manually added to the existing search spaces as required.

Voice Network Map

The last verification step requires that the administrator reviews the Voice Network Map. This is a new option for Cisco Unity Connection version 8.x software that enables engineers and administrators to get a visual display and details of the various locations within the site.

www.it-ebooks.info

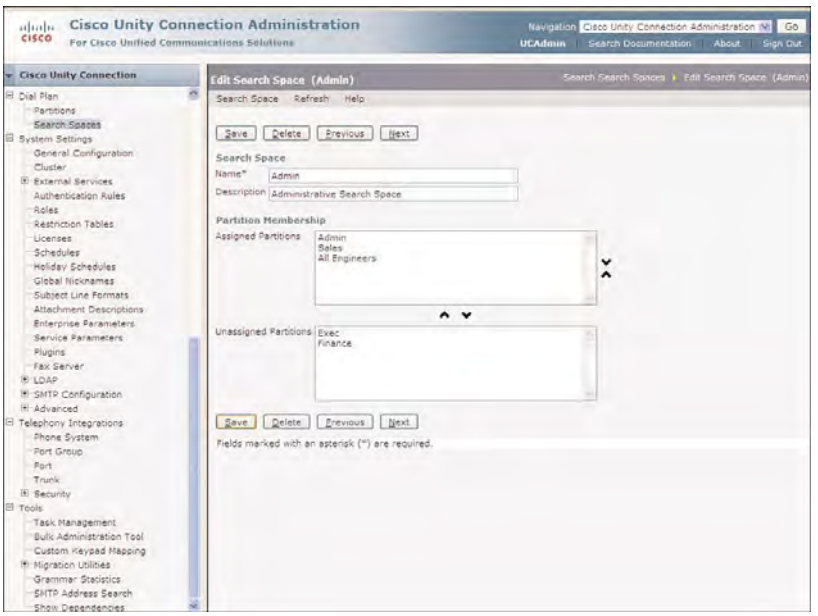

Figure 9-35 *Assigning the Remote Partition to the Local Search Space*

To view the Voice Network Map, select Cisco Unity Connection Serviceability from the Navigation drop-down, and click **Go**. Then, from the toolbar in Cisco Unity Connection Serviceability, select **Tools > Voice Network Map**. The Voice Network Map displays showing the various locations, as shown in Figure 9-36.

Figure 9-36 *Voice Network Map in Cisco Unity Connection Serviceability*

On the Voice Network Map, the display names, addresses, and synchronization status display for the current topology. If you place the mouse over each server listed, the information on the left portion of the page changes accordingly and provides the specific details for that location. This information displays from the perspective of the selected server.

www.it-ebooks.info

In this example, the Voice Network Map is selected from the Admin_Bldg5 server location. Then, in the Voice Network Map, the administrator clicked the **Eng_Bldg9** location, showing that this location (Eng_Bldg9) acknowledged up to USN 36. Also, when the cursor is placed over the local Admin_Bldg5 location, the data displays for this location, showing that Admin_Bldg5 sent and received acknowledgments for up to USN 36. However, there is no information available from the remote location, Eng_Bldg9 on the map, as No Data Available displays for this location. However, Admin_Bldg5 acknowledged up to USN 20. Therefore, the proper credentials need to be configured to provide access to the network health at this location.

The legend at the top of the page lists a number of options, depending on the status of the location:

- **No errors:** Indicates the normal status for locations in the Site.
- **Gateway:** Indicates a Cisco Unity Gateway, when using Cisco Unity version 8.x servers.
- **Syncing:** Indicates that Directory Synchronization is currently in progress.
- **Sync Error:** Indicates a problem with synchronization. The location has lost communication with the Site.
- **No password:** Authentication credentials have not been configured in Cisco Unity Connection Administration.

The Eng_Bldg9 location indicates a status of No Password. If you place the cursor over this site, no information is available because the server cannot gain access to this information. Therefore, the authentication credentials must be configured on the local server for access to these remote server details. Remote access is configured in Cisco Unity Connection Administration under the Networking options.

To complete this task, return to Cisco Unity Connection Administration and from the navigation pane, select **Networking > Links > Connection Location Passwords**. The Search Enterprise Administration Passwords page displays, as shown in Figure 9-37. Enter the proper credentials for each specified location from the Connection Location drop-down.

The username and password selected must be assigned to the System Administrator role because this is required for remote servers to gain access to configuration and status information at this specific location.

In this example, the Eng_Bldg9 location is chosen from the Connection Location drop-down. Then, the proper credentials are entered for the Alias and Password for the user assigned to the System Administrator role on the remote location selected. When all information is entered, click **Add New** x. The selected information displays in the Stored Enterprise Administration Passwords section; however, for security purposes, the password does not display on this page.

www.it-ebooks.info

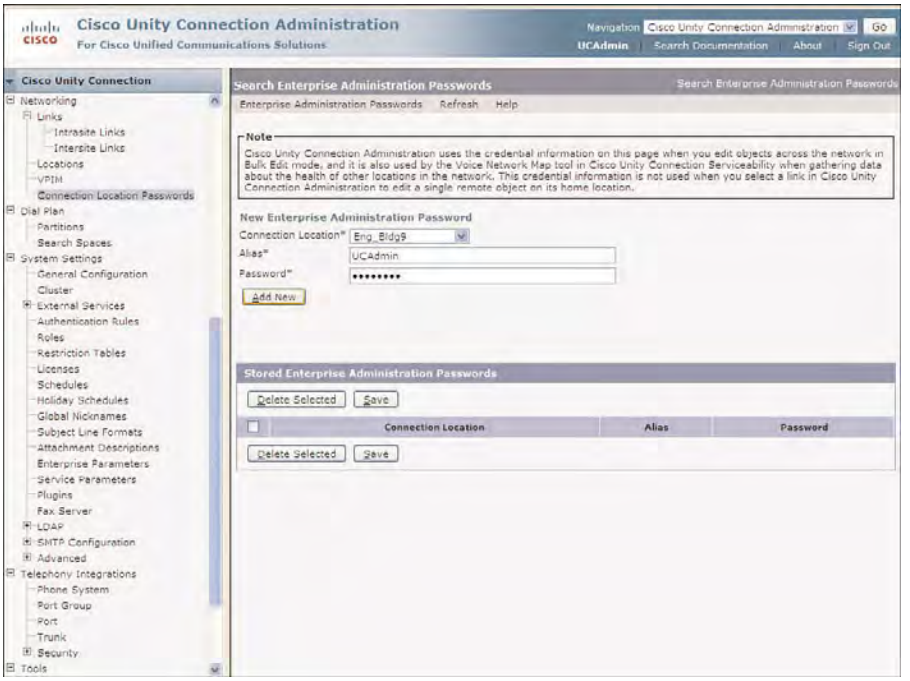

Figure 9-37 *Search Enterprise Administration Passwords*

Review the information listed at the top of this page, which explains how these credentials are used. Specifically, these credentials are used for the Voice Network Map tool and also for Bulk Edit features.

When you return to the Voice Network map, the information for the remote location is now available. This procedure must be completed on all servers in the site.

In Figure 9-38, the Voice Network Map was selected on the Admin_Bldg5 location. Information for both locations now displays. This is the same information displayed on the location page in Cisco Unity Connection Administration for the remote locations; however, all information is visible without having to access each location.

In this example for the Admin_Bldg5 location, notice the following:

- **Info for:** Admin_Bldg5 section provides the servers IP address, Display Name, and current USN number that have been acknowledged, which is currently USN 45.
- **Perspective info for:** Eng_Bldg9 provides the information from the perspective of the Eng_Bldg9. In this case, EngBldg9 received up to USN 45.
- **Perspective info for:** Admin_Bldg5 provides the information from the perspective of the Admin_Bldg5. In this case, Admin_Bldg5 sent and received an acknowledgment of up to USN 45 from Eng_Bldg9 location, which is the same as the USN number acknowledged in the **Info for: Admin_Bldg5** section.

www.it-ebooks.info

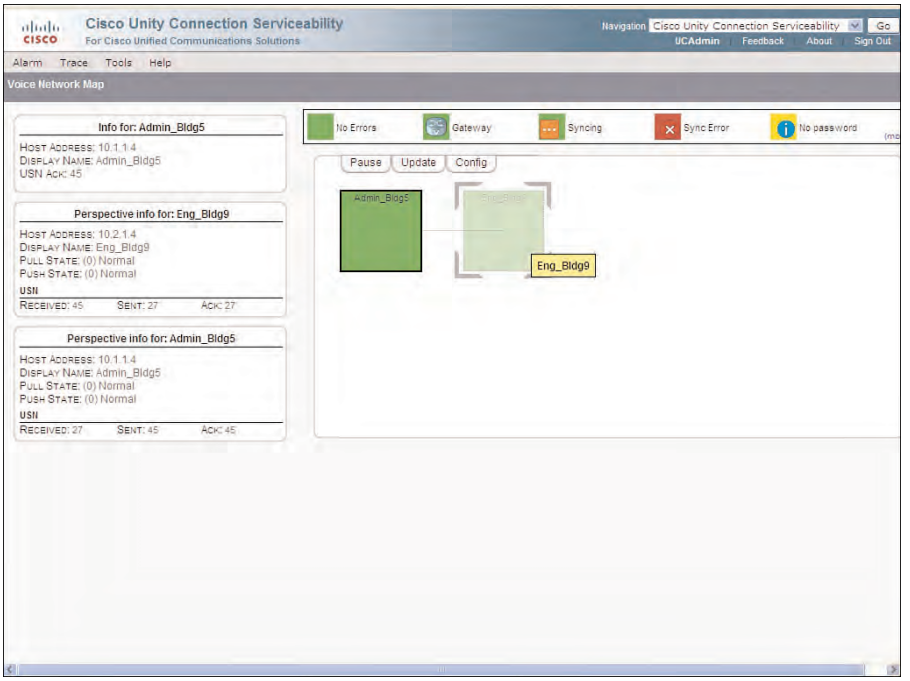

Figure 9-38 *Voice Network Map for the Eng_Bldg9 Location*

SMTP Smart Host Function and Configuration

Multiple locations consisting of servers and cluster pairs are joined to the site using intra-site links. Directory replication and message transfer is performed between all servers joined to the site using SMTP. However, only the publisher of the cluster pair is responsible for joining the network and performing directory synchronization because it runs the networking replication agent. In this case, the various locations in the network must be configured to route to the subscriber of the cluster pair through an SMTP Smart Host. This enables traffic to reach the subscriber if the publisher is unreachable. In this case, the SMTP Smart Host also performs SMTP resolution of the cluster for both publisher and subscriber because the SMTP domain name is configured for the publisher server and there is not a separate SMTP domain name for the subscriber. Therefore, the SMTP Smart Host performs this resolution.

Also, an SMTP Smart Host is required if any locations in the network cannot communicate directly because SMTP traffic is blocked by a firewall or an access list. An SMTP Smart Host must be configured between these locations to provide this access.

The SMTP Smart Host is a separate product from Cisco Unity Connection. The configuration of the Smart Host is beyond the scope of this text, though the capabilities of this device are explored. This section of the chapter covers the configuration in Cisco Unity Connection Administration to provide the SMTP Smart Host integration.

www.it-ebooks.info

The SMTP Smart Host and all remote location subscribers must be configured to be trusted entities in Cisco Unity Connection. This is accomplished by adding the IP address of this device to the IP address access list in the SMTP configuration.

To complete this task, from the navigation pane in Cisco Unity Connection Administration, select **System Settings > SMTP Configuration > Server**. Then, from the toolbar, select **Edit > Search IP Address Access List**. On the Search IP Address Access List page, select the **Add New** button, where the New Access IP Address page displays.

On the New Access IP Address page, enter the IP address of the SMTP Smart Host. This is the address that Cisco Unity Connection sends all SMTP traffic through to all locations. Finally, click **Save** to complete the configuration.

For each remote cluster pair, you need to add the IP address of all remote subscriber servers to this access list. The reason for this is that only the publisher server of the cluster pair participates in the directory synchronization. If the publisher is unavailable, the subscriber must be trusted to allow message transfer and directory synchronization with the other remote locations. Therefore, all remote subscribers need to be considered as trusted.

The SMTP Server Configuration page provides an option to enable connection from untrusted IP addresses. This means that all connections will be allowed, regardless of whether they are configured in the access list. For security purposes, this option is not recommended.

When the save operation finishes, from the toolbar select **Edit > Search IP Address Access List** to display all entries on the Search IP Address Access List page, as shown in Figure 9-39.

On the Search IP Address Access List page, verify the proper IP addresses of the remote subscribers and the SMTP Smart Host. These IP addresses are now considered to be trusted.

After the access list is configured, configure the SMTP Smart Host on each server and publisher of every cluster pair in the Site by selecting **SMTP Configuration > Smart Host** from the navigation pane and configuring the IP address of the SMTP Smart Host, as displayed in Figure 9-40. Only one SMTP Smart Host can be configured for each location.

Finally, each location must be configured to use the SMTP Smart Host when communicating to each remote location. To complete this configuration, from the navigation pane, select **Networking > Locations**. Then, select the Display Name of the location that will be communicating through the SMTP Smart Host from the Search Locations page.

On the Edit Location page, select the **Route to this Remote Location Through SMTP Smart Host** check box, as shown in Figure 9-41. This option is located under the Interlocation SMTP Routing Configuration section. Finally, click **Save** to complete the configuration. Not all locations need to be configured to use the Smart Host for routing traffic because this configuration depends entirely on the remote location and the network path to this location.

www.it-ebooks.info

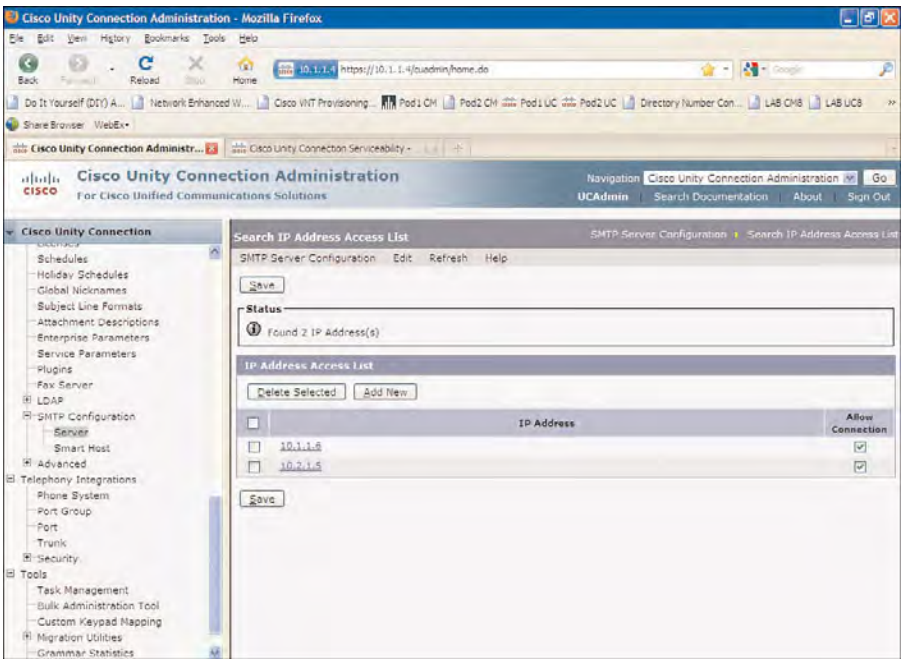

Figure 9-39 *Search IP Address Access List Configuration*

If you did not previously configure the SMTP Smart Host, you are prompted to complete this configuration in the Status section, by offering an option to complete this task. In this case, select this option, which directs you to the SMTP Smart Host configuration page.

Configuring Intersite Links

A Cisco Unity Connection site can consist of up to ten locations, consisting of Cisco Unity Connection servers or cluster pairs. Cisco Unity Connection version 8.x software provides the ability to expand this limitation by linking two sites to create a Cisco Voicemail Organization. You can accomplish this by configuring an intersite link between the sites; although you can link only *one* intersite link between any two sites. The intersite link is used for all directory synchronization and updates between sites.

The servers configured with the intersite links are responsible to send messages between sites using SMTP; however, all directory synchronization between sites communicates using either HTTP or HTTPS. Intersite links also support the configuration of using an SMTP Smart Host for communication between sites. This would be required when the location configured with the intersite link is a cluster pair.

www.it-ebooks.info

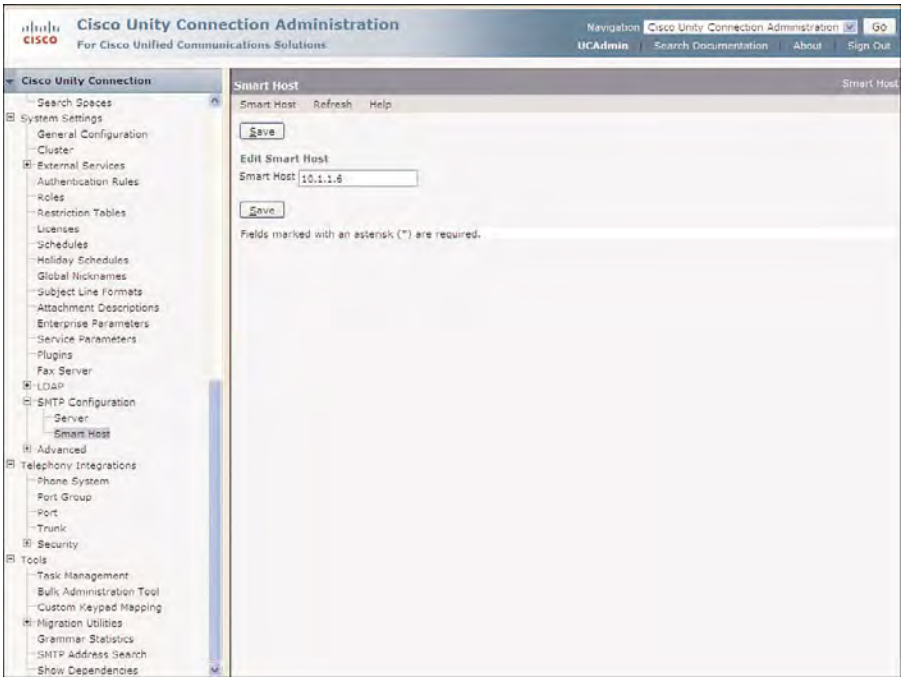

Figure 9-40 *SMTP Smart Host Configuration in Cisco Unity Connection Administration*

Similar to the configuration of intrasite links, the intersite links can be created automatically or manually. In this case, the manual method is accomplished by downloading and uploading site configuration files between servers, as opposed to the location configuration file, used with the intrasite links. A Cisco Unity Connection server or cluster pair is referred as a remote site gateway configured with the intersite link. Before beginning the configuration of the intersite link on the server or cluster pair, you need to verify that the location and networking is operational on both servers in each site that are to be configured as the remote site gateway.

To configure the intersite links, from the navigation pane in Cisco Unity Connection Administration, select **Networking > Links > Intersite Links**. Then, click **Add New** to create a new intersite link. On the New Intersite Links page, select the **Link to Cisco Unity Connection Site by Using Automatic Configuration Exchange Between Servers**. Note the pop-up warning, and click **OK**.

Enter the Hostname of the remote server for the remote site gateway on the New Intersite Link page. Complete the authentication credentials, as displayed in Figure 9-42. The user account selected for the automatic configuration must be assigned to the System Administrator role for the intersite link to be created.

www.it-ebooks.info

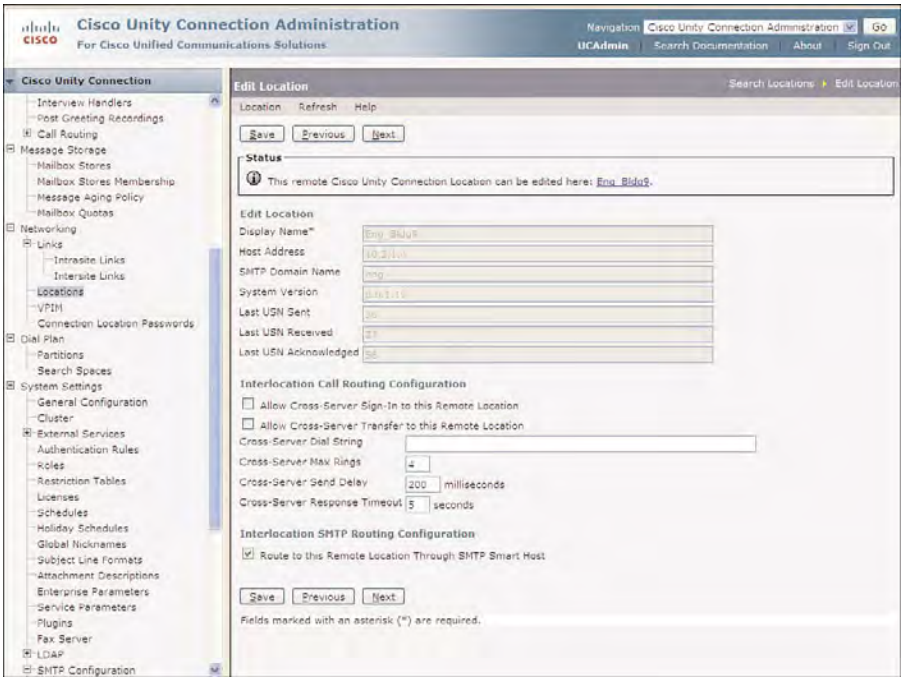

Figure 9-41 *Edit Location Page Configured to Route Through an SMTP Smart Host*

Finally, select the various options as required for synchronization, and click **Link**. The Status section indicates the current status of the linking procedure while the intersite link is created. After the link is configured, a Cisco Voicemail Organization is now created, which consists of two sites linked with a single intersite link between the two sites through the remote site gateways.

Interlocation Options and Features

The networking of Cisco Unity Connection servers has now been properly completed. You have also verified the directory synchronization and ensured that all objects are available as required. The next step is to configure, test, and verify the interlocation options, or cross-server features. These interlocation options and features consist of cross-server login, transfer, and live reply. In essence, these options are performed by configuring an originating location or server to transfer functionality to the caller's home location. The home location is defined as the receiving location. In this way, all capabilities and features provided to a user are essentially the same from all locations in the site, as if users were connected to their home server.

www.it-ebooks.info

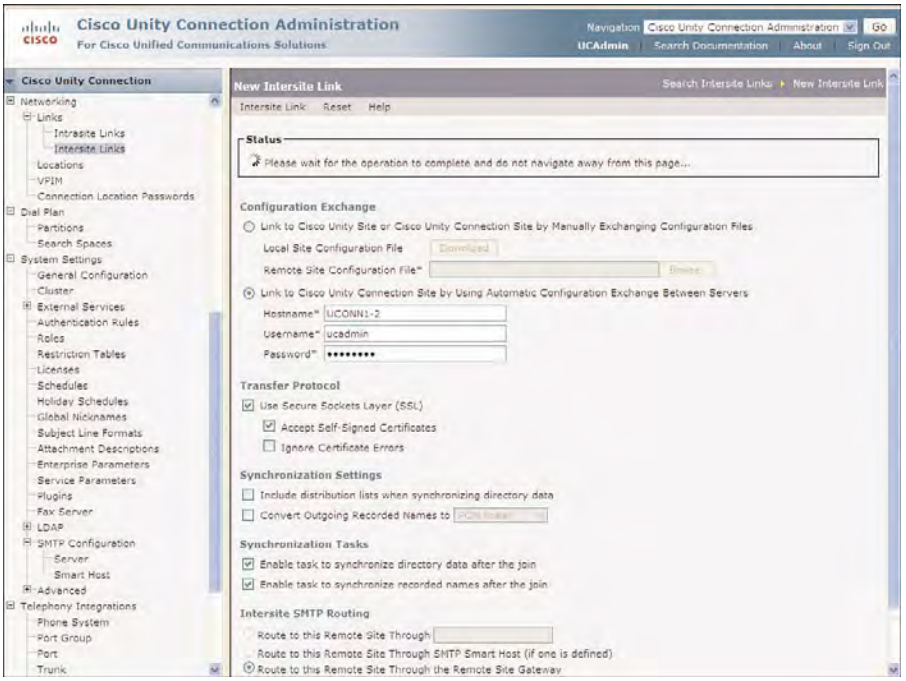

Figure 9-42 *New Intersite Link page for a Remote Site Gateway*

These features provide users with the following capabilities:

- **Cross-Server Sign-In:** Enables users to login to their voicemail from any server within the network.
- **Cross-Server Transfer:** Provides the capability of transferring to a user or object located or homed on another server or cluster pair within the network.
- **Cross-Server Live Reply:** Provides the capability of a user to transfer to a user located in the network, while listening to a voice message from that user.

All cross-server features are subject to the search space and configuration as discussed in the previous section. A user trying to perform a cross-server transfer cannot perform this function if the user does not have access to that specific partition.

All cross-server features use DTMF requests and responses configured under the Conversation Configuration page. The requests and responses must agree between the originating and receiving location. Additionally, the **Respond to Cross-Server Handoff Requests** option must be selected on the receiving location. The default configuration is unselected, meaning the server will not respond to cross-server sign-in or transfer.

www.it-ebooks.info

Cross-Server Sign-In

In many cases, organizations provide a single number for login to voicemail, regardless of where the users are located. Typically, this number is located at the headquarter location. When users attempts to sign-in with their extension, Cisco Unity Connection transfers the call to their home location for authentication.

Cross-server sign-in provides this feature by enabling users to call a single number to access Cisco Unity Connection and be transferred to the server where their voice mailbox is homed. Without this option, users would need to access voicemail by contacting their specific home server. This feature requires multiple ports on the originating location; therefore, the planning and design specifications for the number of required ports should considered.

Take care in designing and configuring extensions and partitions. Cisco Unity Connection uses the search scope of the incoming call for the Attempt Sign-In conversation. This identifies the user. For example, if the user is calling from a phone that is not identified on the system, the opening greeting will be used to accept the call according to the direct routing rules.

If the extension of a user overlaps with an extension in a partition from another location and partitions are in the search space for the routing rules, the user might reach the incorrect extension. The call is identified by the order of partitions in the search space of this rule.

The search space for direct routing rules under the Attempt Sign-in conversation need to include the users and extensions at the receiving locations to allow for the cross-server sign-in. The search space considerations extend from the originating location to the receiving location that accepts the transfer. Cisco recommends that the same search scope be used on both originating and receiving locations to avoid conflicts with extensions and partitions. Figure 9-43 illustrates cross-server sign-in in two different scenarios.

The first scenario displays a configuration using separate Cisco Unified CM (CUCM) clusters, whereas the second scenario uses the same CUCM cluster. The sign-in is accomplished by the users calling the originating location and attempting to sign-in with their user ID, or extension. The server locates the users in its database, which was learned through the networking directory synchronization process. After the users are located, the originating server attempts a cross-server handoff to the receiving location, which is the home location of the users. During this time, the caller hears the response “one moment please” from the originating location. As shown in Figure 9-43, two ports are required at the originating location, which are the incoming port that users use to access the server, and an outgoing port that the originating location uses for the cross-server handoff. When using cross-server features, the originating location will “handoff” the call to the receiving location. The ports on the originating location are no longer used for the transfer and the call goes directly to the receiving location.

www.it-ebooks.info

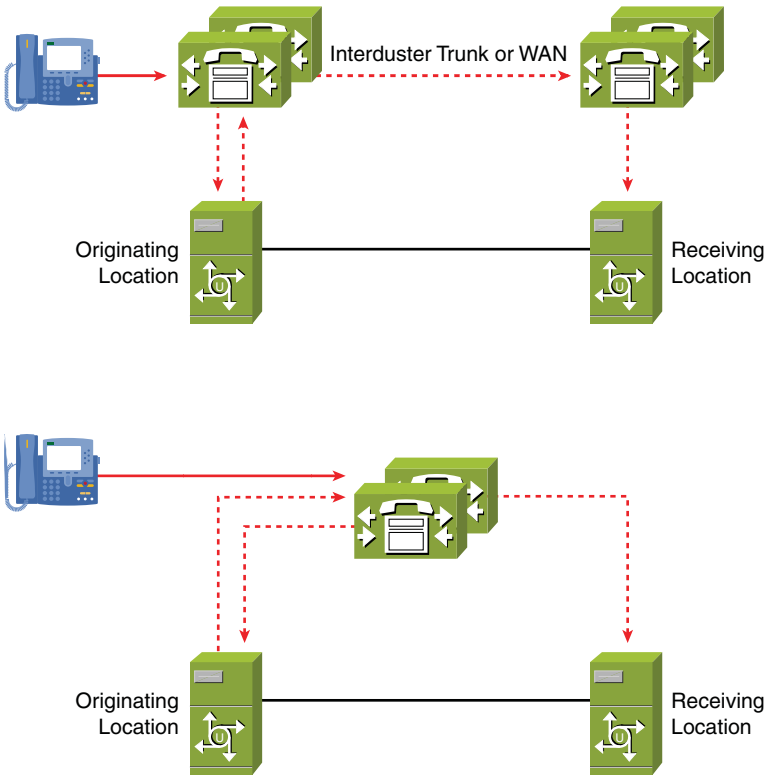

Figure 9-43 *Cross-Server Sign-In*

In both scenarios, a cross-server dial string must be programmed to provide the capability to access the receiving location. In the first scenario, this would consist of a dial string that matches a route pattern programmed in CUCM to enable access to the intercluster trunk or WAN. In the second scenario, this dial string would be configured to match the hunt pilot for the integration on the receiving location. In either case, the dial string must match the configuration programmed on the phone system to enable access to the receiving location.

When the receiving location is reached, the users must enter their PIN for authentication to the voicemail. From this point, the hand-off request is complete. From the users' perspective, the capabilities that they experiences when they reach their voicemail is the same as if they accessed voicemail directly from their home location.

If you plan to implement cross-server sign-in in your organization, your design consideration must take into account the port usage and additional traffic that will be incurred. In this case, two ports are used at the originating location, and one port is used at the receiving location. If you use this feature between CUCM clusters, or different phone systems, additional traffic will be encountered across the intercluster trunk or WAN links.

www.it-ebooks.info

Cross-Server Transfer

Cross-server transfer provides for the transfer of calls from a user, directory handler, or another object to be sent to a different location. This option also requires additional ports, like the cross-server sing-in feature. Figure 9-44 illustrates the cross-server transfer.

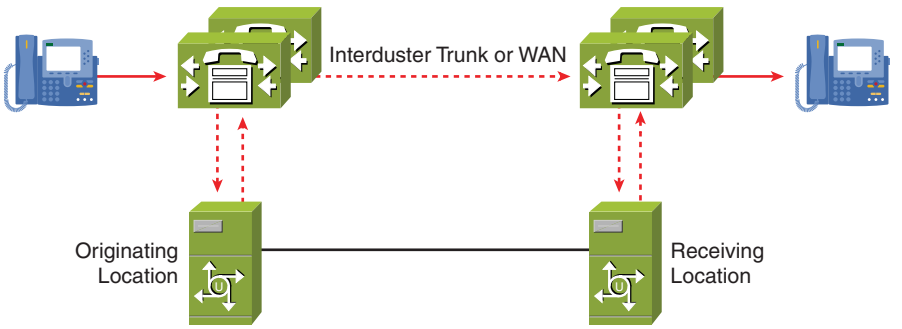

Figure 9-44 *Cross-Server Transfer*

In this scenario, a caller attempts to transfer to a user located on a remote location. The original call is directed to the originating location, where the caller enters the extension of a user. The originating location finds the user in its database and determines that this is a remote user. Again, this information was learned through the directory synchronization process.

When the user is located, the originating server attempts a cross-server handoff to the receiving location, which is the home location of the target user or object. During this time, the caller hears the response "one moment please" from the originating location. As in the cross-server sign-in, two ports are required at the originating location, which are the incoming port that the user accesses the server, and an outgoing port that the originating location uses for the cross-server handoff.

The cross-server dial string must be programmed to provide the capability to access the receiving location, as discussed for cross-server sign-in. The dial string must match the configuration programmed on the phone system to enable access to the receiving location, whether the scenario uses a single or multiple phone systems.

After the receiving location is reached, the transfer is accepted and forwarded to the selected user. All call screening and transfer capabilities configured for this specific user that are configured at the home location can be observed.

Cross-Server Live Reply

Live reply enables users to be transferred directly to a user, while listening to a message from that specific user. The cross-server live reply accomplishes this same task between locations. The users' class of server determines their access to the live reply feature. If a

www.it-ebooks.info

cross-server transfer is enabled, a cross-server live reply is available to users that have the proper Class of Service (CoS). Therefore, the call flow can follow the same path as the cross-server transfer feature.

For the cross-server transfer and live reply features, the target user's call transfer and call screening options are used accordingly. The cross-server transfer option uses the release-to-switch option, along with the cross-server transfer extension. This feature is available on the users' User Basic page. If cross-server is not configured, callers hear the greeting when they attempt to transfer to this user from another location.

To use the interlocation features, the Cisco Unity Connection server must be configured to respond to cross-server handoff requests. Each server in the site must be configured to respond to these requests to use the various interlocation features.

Cross-Server Feature Configuration

To begin the configuration of the various cross-server features, log in to Cisco Unity Connection Administration on the originating location that will be used to initiate the various cross-server features. From the navigation pane on the left, Select **Networking > Locations**. On the Search Locations page, select the remote location from the Display Name column that will be used as the receiving location. This is the home location of the user attempting to sign in, for cross-server sign-in. Also, this is the home location of the user that a caller can attempt to transfer to, or perform a live reply to. The Edit Location page displays, as shown in Figure 9-45.

On the Edit Location page, the Interlocation Call Routing Configuration provides the options to enable the cross-server features. Because this remote location is the receiving location for the cross-server requests, you need to select the following options:

- **Allow Cross-Server Sign-In to this Remote Location:** Provides cross-server login to the designated remote location.
- **Allow Cross-Server Transfer to this Remote Location:** Provides cross-server transfer and live reply to this remote location.

These features are disabled by default and must be configured from the originating location for each receiving location that will accept the cross-server feature specified. For example, if you want to receive all incoming calls at the headquarters location, this configuration must be performed from that location, configuring all remote locations to allow cross-server sign-in and transfer from this location.

In the Cross-Server Dial String field, enter the hunt list or route pattern that the originating location will use to contact the receiving location. Only one dial string can be entered here for each remote location. If you need to configure redundant or backup paths, this should be accomplished in the call processing system. For CUCM, this is configured using the route list and route group constructs. However, the discussion of route list and route groups is beyond the scope of this text.

www.it-ebooks.info

Figure 9-45 *Edit Location Page for Configuration of Cross-Server Features*

Note Cross-server sign-in, transfer, and live reply requires a complete integration for these features to be successfully implemented. Cross-server handoff requests are made through the defined integration.

For cross-server features, you might need to adjust the delay and timeout when using a WAN connection. This is necessary to allow the call to be set up, in the case of PSTN and call switching delays. Otherwise, the cross-server feature selected will timeout before the connection to the receiving location has been set up. The following three options are available to configure the delays and timeouts:

- **Cross-Server Max Rings:** Sets the maximum number of rings that the originating location waits for the receiving end to answer the call when doing the cross-server transfer or live reply. If this number is exceeded, the call is directed to the user's voice mailbox. The default for this option is four rings.
- **Cross-Server Send Delay:** Sets the delay between the cross-server dial string and the time that the cross-server hand-off request is sent to the receiving location. If you configure a receiving location across the WAN, this option needs to be increased appropriately to allow the call to properly set up across the WAN or PSTN. The default for this option is 200 milliseconds.

www.it-ebooks.info

- **Cross-Server Response Timeout:** Sets the maximum timeout for the cross-server handoff when performing cross-server features. For cross-server transfer and live replay, if this timeout is exceeded, the call is directed to the user's voice mailbox. Or if the user is configured with a Cross-Server Transfer Extension on the User Basics page, the call is directed to the selected extension. For cross-server sign-in, if this timeout is exceeded, the call is disconnected and the caller receives a response that the server is unavailable. The default for this option is 5 seconds.

If you configure the Cisco Unity Connection Site with a single CUCM cluster, the default options should function properly for most implementations but can adjusted as necessary to enable the proper transfer.

You need to complete these steps for all receiving locations in the site that will be responding to the cross-server handoff requests from this originating location.

Case Study: Configuring Cross-Server Features

Tiferam Corporation wants all calls to be received at its administration department, where the opening greeting will be used as the main company greeting for all callers. When these callers need to reach a user in the engineering department, it wants the call to transfer this user via Cisco Unity Connection. Also, remote users need to access their voicemail to retrieve messages. This capability must be available for both administrative and engineering personnel. Both departments' Cisco Unity Connection servers use a single common CUCM integrated using two different hunt pilot numbers. Therefore, when employees in administration contact voicemail from their office, they select the Messages button on their phone or dial 2990. And when people in the engineering department contact voicemail from their office, they select the Messages button on their phone or dial 3990.

Figure 9-45 illustrates the configuration that must be performed on the Admin _Bldg5 (originating) location for the Eng_Bldg5 (receiving) location. The **Allow Cross-Server Sign-In to This Remote Location** and **Allow Cross-Server Transfer to This Remote Location** options are selected. Finally, the **Cross-Server Dial String** is configured with the hunt pilot required to reach the receiving location. In this case, this option is configured with **3990**. The **Save** button is then clicked to commit the changes to the database.

This configuration enables the originating location to perform the cross-server handoff to the receiving location. However, the receiving location must be properly configured to accept the cross-server handoff request and forward it to the respective user or system object. Therefore, the following configurations must be performed on all receiving locations that will be accepting cross-server handoff requests.

To complete the configuration of the receiving location, you must log in to Cisco Unity Connection Administration at the receiving location. Then, from the navigation pane on the left portion of the page, select **System Settings > Advanced > Conversations**. The Conversation Configuration page displays.

www.it-ebooks.info

Select the check box for the **Respond to Cross-Server Handoff Requests** option. Finally, complete this task by clicking **Save.** This procedure must be completed on all receiving locations that will be receiving cross-server handoffs. By default, this option is not selected, meaning that all locations will not respond to any cross-server handoff requests.

In Figure 9-46, the Eng_Bldg5 (receiving) location is configured to respond to cross-server handoff requests under the Conversation Configuration page because this was configured as the receiving location in the previous task.

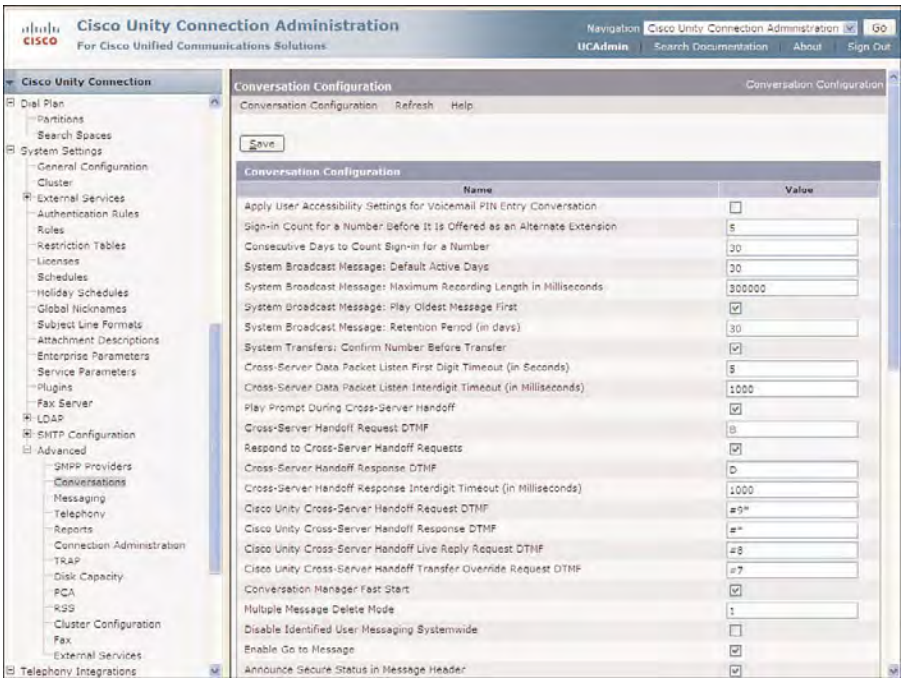

Figure 9-46 *Conversation Configuration Page for the Receiving Location*

The cross-server handoff requests and responses are sent between the originating and the receiving location using dual tone multi-frequency (DTMF) tones. This information can be viewed in the Conversation Configuration page, as shown in Figure 9-46. The various cross-server handoff requests and responses are configured by default to begin with **#**. Therefore, if you use the default direct routing rules that send calls to the Opening Greeting from an unidentified caller, you need to edit the Caller Input for the **#** option and uncheck the **Ignore Additional Input (Locked)** selection. Otherwise, the remaining characters sent after the **#** for the respective cross-server request will be ignored and the cross-server handoff will fail. Additionally, you can create a new system call handler to receive calls from this location and create a new direct rule and conditions using the procedures that were detailed in the section two of this text.

www.it-ebooks.info

The cross-server handoff options on the Conversation Configuration page do not need to be edited or modified when using Cisco Unity Connection servers and will function properly using the defaults. However, they must agree between the originating and receiving locations in your network.

Configuring Users for Live Reply

Live Reply enables the users to respond directly to callers after listening to their message. By default, all users can record a reply to the callers, as long as the partition of the callers who left the message is in the user's search space. However, Live Reply enables this user to transfer directly to the caller by dialing 4-4 after listening to the message.

The previous configuration described for cross-server transfer must be completed for users to use Live Reply. By configuring the **Allow Cross-Server Transfer to This Remote Location** option under the Edit Location for the receiving location, the Live Reply feature is automatically enabled. However, only users that have this feature enabled in their CoS can access this feature.

To enable the user to use the Live Reply feature, from the navigation pane for the originating location, select **Class of Service > Class of Service**. In this case, this would be the home location for the user using Live Reply. These options are as follows:

- **Users Can Reply to Messages from Other Users by Calling Them:** Enables the user to use the Live Reply feature to contact other users that are identified callers or users in the network. The default selection for this option is disabled.
- **Users Can Reply to Messages from Unidentified Callers by Calling Them:** Enables the user to use the Live Reply feature to contact callers not on the system and identified by the callerID or ANI. In this case, the Conversation Configuration page (refer to Figure 9-45) enables the administrator to configure a dial prefix when placing an outgoing call for Live Reply. The specific option called **Dial Prefix for Reply to Unidentified Callers** must be configured for the Live Reply feature to function properly. The dial prefix must match the route pattern configuration with the integration call processing system. The default selection for this option is disabled.

In Figure 9-47, the CoS for voicemail users displays the Live Reply configuration, enabling users assigned to this CoS to use Live Reply when contacting other users identified on the system and outside callers. In this case, the system prefixes the called number as per the configuration for Dial Prefix for Live Reply to Unidentified Callers, under **System Settings > Advanced > Conversations**. If an organization uses 9 as an access code, this would add this prefix to the number before placing a call for a live reply. In this case, CUCM has a route pattern that matches this dialed number and strips the **9** before sending it to the PSTN.

A caller is recognized as a user by the originating number or alternative extension. This means that a message from an identified caller was placed from that user's voicemail using his phone or a valid alternative extension. In either case, if a user in the system makes a

www.it-ebooks.info

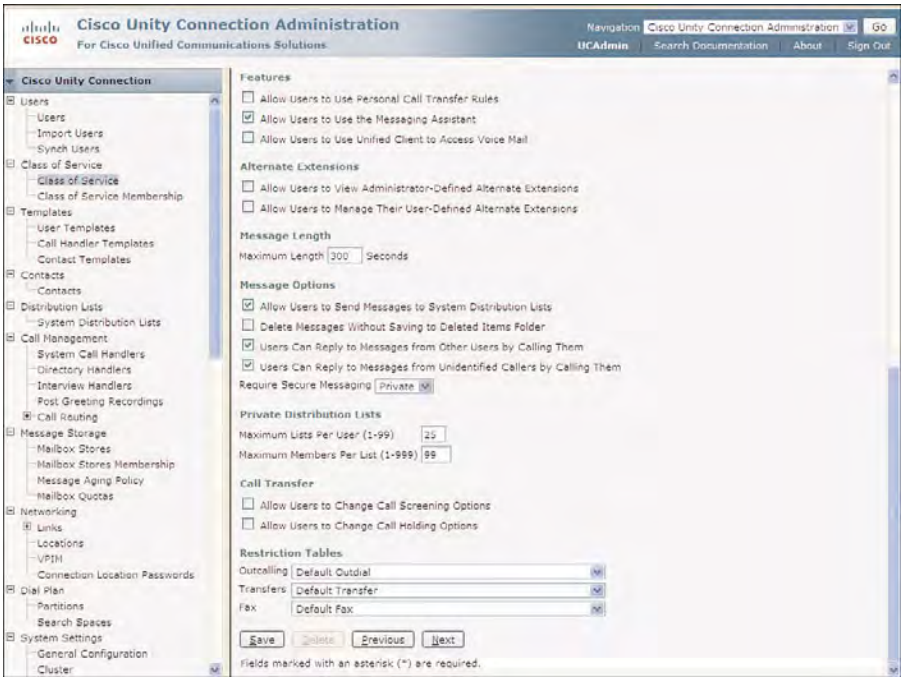

Figure 9-47 *CoS Configured for Live Reply*

direct call from an outside extension that is unknown to the system, this call and its corresponding message are classified as originating from an unidentified caller.

Transfer Using Phone System Trunks

There might be a need to allow a transfer out of Cisco Unity Connection for users located on a completely different system that is not in the Cisco Unity Connection network. The phone system trunk provides this feature.

In some cases, you might have a voicemail system that does not enable networking. For example, an older legacy or a different manufacturer's system might not provide a network option—or quite possibly where the servers are located where networking is impossible. However, callers might still need to reach these users from Cisco Unity Connection by being transferred to these remote voice-messaging systems.

In this case, the configuration of phone system trunks in Cisco Unity Connection provides this feature by enabling the transfer of calls between multiple systems, and associating users with a remote voice-messaging system.

The phone system trunk enables calls on one phone system to be transferred to extensions or outside numbers on another system without using extra ports on the Cisco Unity Connection server. The configuration of phone system trunks does not require port groups and ports configuration for the integration.

www.it-ebooks.info

To configure phone system trunks, the first task that needs to be performed is to create a new phone system that will be associated with the remote system. Therefore, select **Telephony Integration > Phone System** and add a new phone system that is to be associated with the remote system. The Status section at the top of the page informs the administrator that a port group must be configured. This warning can be ignored because port group and port configurations are not required when using phone system trunks.

Then, you need to create the phone system trunk by selecting **Telephony Integrations > Trunk** and then selecting **Add New** on the Search Phone System Trunks page. The New Phone System page displays, as shown in Figure 9-48.

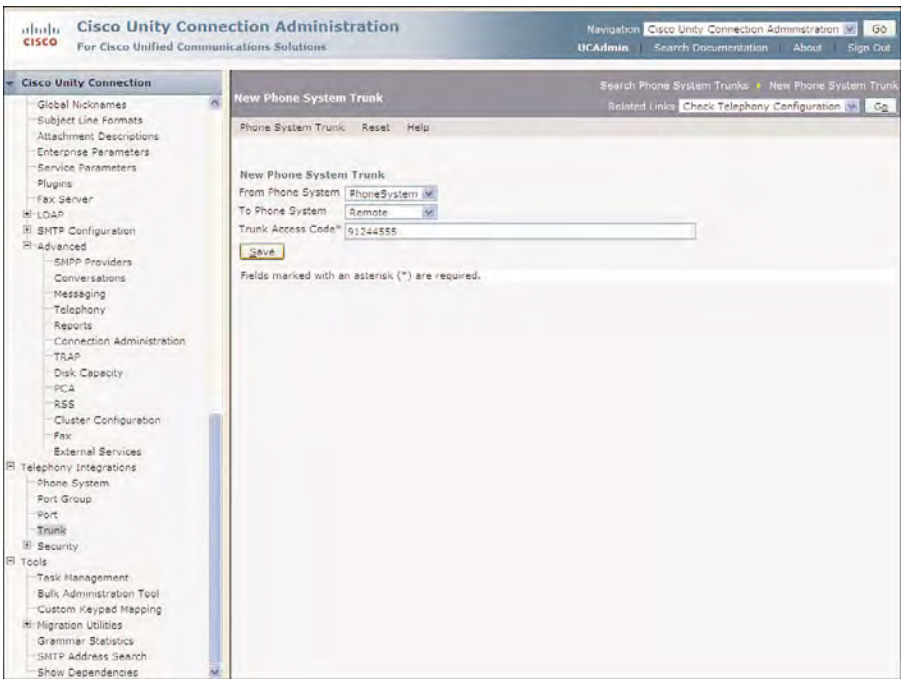

Figure 9-48 *New Phone System Trunk Configuration in Cisco Unity Connection*

On the New Phone System page, select the **From Phone System** and **To Phone System** options from their respective drop-downs. In this case, the phone system integrated with this Cisco Unity Connection server is selected for the **From Phone System** drop-down. The new phone system associated with the remote system, **Remote**, is selected from the **To Phone System** drop-down.

The phone system integration requires a prefix of **9** to place an outgoing call. An organization might require that users be contacted using their 4-digit extension. Therefore, the Trunk Access Code is configured as **91244555** as the main number of the remote location is **12445557000**.

www.it-ebooks.info

Finally, the remote user needs to be configured and associated with this phone system. To perform this task, select **Users > Users**; then select **Add New** to create a new user. Configure the user as normal, but select the **Remote** phone system from Phone System drop-down. The extension needs to be entered that associated with user.

In Figure 9-49, Mike Stanley is configured with extension **7442** and associated with the phone system **Remote**. When a user, attempt to call this user, she can locate the user in directory or dial **7442**. This user is recognized as being associated with the Remote phone system, which prefixes the Trunk Access Code followed by the extension. In this case, the number, **912445557442** will be dialed from the attached phone system, which must be configured to route the call to the proper gateway. When the call is completed, the port used by the caller to access Cisco Unity Connection will be released (idle).

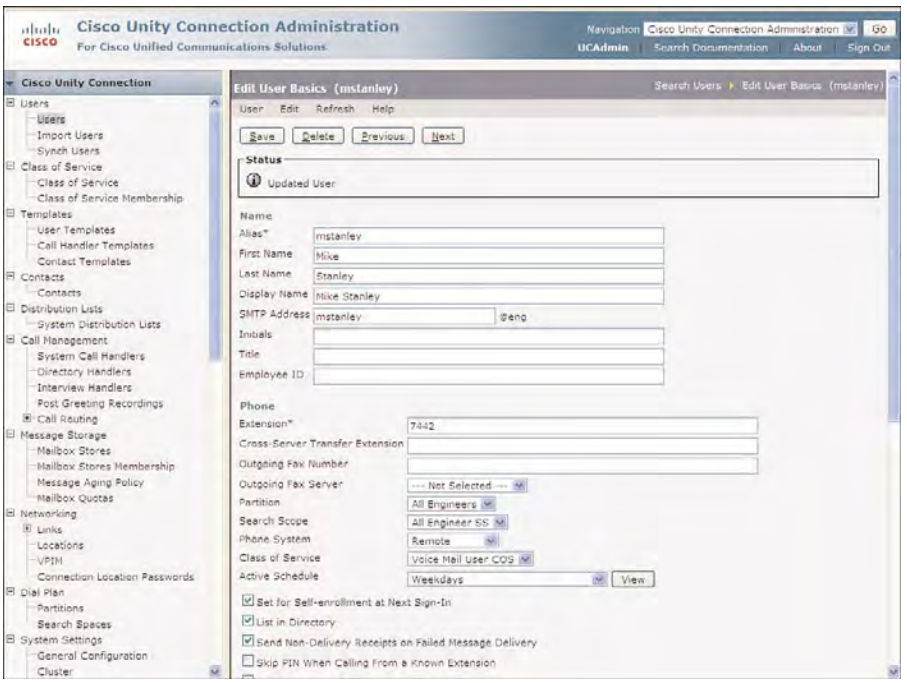

Figure 9-49 *User Basics Configuration for User Associated with a Remote System*

To review the users associated with a specific phone system, in Cisco Unity Connection Administration, select **Telephony Integration > Phone System**. The Search Phone Systems page displays. Then, select the desired phone system to display the Phone System Basics page. Finally, from the toolbar, select **Edit > Phone System Associations**. The Phone System Associations page displays showing the users associated with the system. In Figure 9-50, two users are associated with the phone system **Remote**. Users must be associated with the phone system that is configured for a phone system trunk to use the transfer feature.

www.it-ebooks.info

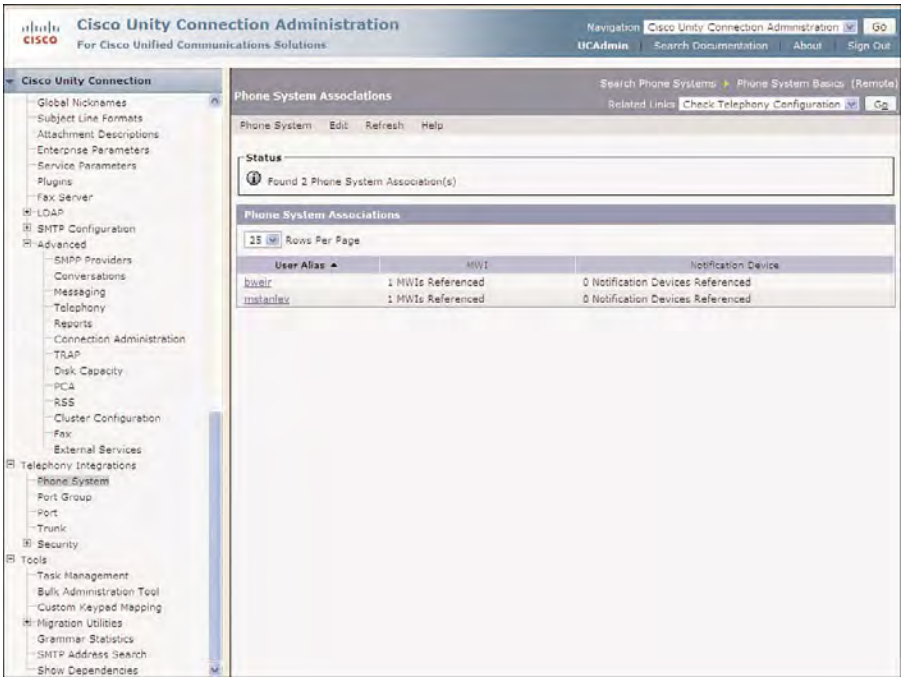

Figure 9-50 *Phone System Associations Page in Cisco Unity Connection Administration*

You can access the User Basics page for a user by selecting the name from the User Alias column on the Phone System Associations page. In this way, the administrator can change the association for any user from this location.

Other Post-Networking Considerations

You need to consider a number of post-networking considerations:

- When using an SMTP Smart Host, user credentials are not transmitted between locations. However, it is necessary to ensure that the SMTP Smart Host is configured to properly route messages because SMTP address information can be extracted from these messages.
- Users can add remote users to private lists; however, private lists are not replicated to other locations. If a location is removed from the site, the remote users are removed from any private list that exists on that server.
- Broadcast messages are sent only to users on a single-homed location and cannot be sent to multiple locations in a site.

www.it-ebooks.info

- When using Cisco Personal Communications Assistant and IMAP clients, users must access their home location. Cross-server sign-in is not available for web applications because this capability is supported only for the phone interface.
- Directory replication pauses while bulk edit and bulk administration is operating; however, it resumes as soon as these operations are complete.
- When the location is a cluster pair, directory updates configured on a subscriber server are replicated using the publisher server; therefore, ensure that the publisher has the Primary status to keep the directory current.
- When a user sends a message to a remote user, Cisco Unity Connection can identify the message as being from this user on the remote location. In this case, the phone system integration is not used for the message transfer but transferred to the remote location via SMTP.
- When a user places a call or leaves a message for another user, Cisco Unity Connection uses identified user messaging. This means that the local and remote users are configured as users within a specific site.

Summary

This chapter provided an understanding of networking Cisco Unity Connection voice-messaging system. You should now have a solid grasp of the following:

- The Simple Mail Transfer Protocol and how it provides the mechanism for message transfer and directory synchronization between Cisco Unity Connection version 8.x servers.
- The various elements used for networking voice-messaging servers, including locations, sites, intrasite links, and intersite links to create a Cisco Voicemail Organization.
- The preparations required before networking Cisco Unity Connection servers, such as configuring display names, SMTP domains, search spaces, partitions, and distribution lists.
- The configuration and verification of the networking Cisco Unity Connection servers and cluster pairs.
- The function, features, and configuration of the various interlocation cross-server features.
- The function of phone system trunks to provide transfer capabilities to remote systems.
- The various post-networking considerations for the various networking elements, users, and system objects.

www.it-ebooks.info

This page intentionally left blank

www.it-ebooks.info

Chapter 10

Implementing Voice Profile for Internet Mail (VPIM)

This chapter covers the following subjects:

- **Voice Profile for Internet Mail:** This section covers the functions, features, and purpose of VPIM.
- **Preparation for a VPIM Implementation:** This section describes the considerations and required action before implementing VPIM between voice-messaging systems.
- **Configuration of VPIM:** This section describes the configuration of VPIM in Cisco Unity Connection Administration.
- **VPIM Licensing:** This section reviews the VPIM license requirements in Cisco Unity Connection.
- **Configuring VPIM Locations:** This section describes the configuration of VPIM locations in Cisco Unity Connection.
- **VPIM Contacts:** This section covers the purpose and function of contacts; their creation, modification, and management.
- **VPIM Features:** This section describes the features of VPIM and the configuration of alternative names for VPIM locations and contacts, and SMTP proxy addresses.

Voice Profile for Internet Mail (VPIM) is a standard-based protocol for defining the transfer and exchange of electronic messages (voice, text, or fax) between different or disparate messaging systems. The VPIM standard is defined in RFC 3801 and details a subset of multimedia message protocols called Multipurpose Internet Mail Extensions (MIME). However, the actual message transfer is accomplished by using Simple Message Transfer Protocol (SMTP). The VPIM standard has become widely accepted among manufacturers of voice-messaging systems. Therefore, it has grown in popularity as a means for viable message transfer between various voice-messaging systems.

www.it-ebooks.info

The addressing used for VPIM is defined as using the message format familiar to email users (address@domain.com). However, the main purpose of this addressing format is to provide a standard format for message transfer between dissimilar systems.

Cisco Unity Connection supports the VPIM protocol enabling message transfer to other manufacturers' voice-messaging systems that support the VPIM standards implementation. Using VPIM, Cisco Unity Connection can also be networked with other Cisco voice-messaging products that support VPIM, such as Cisco Unity Connection 2.x, Cisco Unity, or Cisco Unity Express.

In this chapter, you gain a working grasp of the following:

- The purpose of Voice Profile for Internet Mail (VPIM)
- The capabilities and features of VPIM implementation in Cisco Unity Connection
- The configuration of VPIM in Cisco Unity Connection Administration
- The various methods of VPIM contact creation in Cisco Unity Connection Administration

Voice Profile for Internet Mail

If someone in an organization needs to send a voice message to a person in another company, she might have to call that individual at his location and leave a message by accessing his voicemail directly; however, the recipient's contact information might not be accessible. Also, without VPIM, it is not possible to forward messages to someone in a different organization that uses a completely different model or type of voice messaging.

VPIM provides this mechanism, enabling a user to address, forward, and send messages to users on different voice-messaging systems. The standard accomplishes this transfer by encoding the message using MIME and transporting the MIME contents using SMTP. These contents might include the actual voice message, spoken name, fax attachments, or vCard information. VPIM accomplishes the transfer of messages between servers, not the presentation of those messages to users. However, the VPIM standard includes the capability to perform automatic updates of directories based on received information or directory synchronization based on message transfer.

Before message transfer can occur, the actual message is encoded according to the MIME standard. The VPIM standard describes the use of G.726 for voice coding. This codec provides toll quality voice at 32 kbps, enabling a reasonable bandwidth usage and an acceptable level of voice quality. Cisco Unity Connection enables the administrator to select between G.726 or the codec in which the message was sent or recorded. This decision must take the remote VPIM location into consideration and whether it supports a codec other than G.726, and the amount of bandwidth used when selecting a different codec.

If you network between Cisco Unity Connection version 7.x and version 8.x servers, using digital networking and the concepts of *sites* provides the most functionality.

www.it-ebooks.info

Message transfer is not possible between Cisco Unity Connection and other Cisco voice-messaging systems without the use of VPIM, however. VPIM enables Cisco Unity Connection version 8.x servers and cluster pairs to use VPIM for message transfer to these other Cisco voice-message products, including Cisco Unity Connection version 2.x or Cisco Unity 4.x and later systems, and Cisco Unity Express. You can also use an Intersite link to interconnect Cisco Unity Connection version 8.x and Cisco Unity 8.x server. However, when using this approach, all servers must be version 8.x.

Preparing for Configuring VPIM Networking

A number of design considerations must be understood before beginning the configuration of VPIM in Cisco Unity Connection. These considerations must be discussed and determined in relation to the entire networking and dial plan within the organization. These considerations are discussed in this section; however, other considerations and variations might exist in your corporation.

License Considerations

VPIM is a licensed feature in Cisco Unity Connection and must be purchase and installed before beginning the VPIM configuration. You will also most likely need to purchase a license for any third-party voicemail products.

Determine the Number Scheme for Dial IDs

If the remote VPIM location that is going to accept messages from the local VM system includes the same or overlapping extensions, you need to include a Dial ID to prefix these addresses. These Dial IDs must be unique within Cisco Unity Connection and between VPIM locations. Also, ensure that these Dial IDs use a different number range than all Cisco Unity Connection users to avoid conflict. Also, you need to keep the Dial IDs at a fixed length to avoid conflict with the existing dial plan and other VPIM locations. When configuring any element that affects the dial plan, consistency and uniformity should be maintained at all cost.

Determine the Dial Plan

On all remote locations, you need to determine the partitions and calling search spaces to be used for VPIM locations. If you want specific users to have accessibility while restricting others, you must consider the configuration of partitions for each VPIM location. It is strongly suggested that you gain a thorough understanding of these concepts in the chapters in Part II.

www.it-ebooks.info

VPIM Contact Creation

A contact (as discussed in the chapters in Part II) is a user that has a voicemail on another messaging system, or a user that does not have voicemail and is strictly configured for transfer capabilities. In the case of VPIM, contacts are users that have their voicemail on another system or VPIM location. Meaning, VPIM is the mechanism used to encode and forward these messages from one system to the other. To transfer messages between systems, specific directory information must be created in Cisco Unity Connection for these remote VPIM contacts. This information might include specific information and addressing about the user and a recorded name for these users. This contact information enables the local Cisco Unity Connection user to address, forward, and send messages to these remote VPIM contacts and have their messages sent and delivered successfully.

Cisco Unity Connection provides a number of means to create these contacts. They can be created individually through the Bulk Administration Tool or automatically using various VPIM contact creation parameter configurations in Cisco Unity Connection Administration. The automatic creation, modification, and deletion provide the mechanism to enable contacts to be managed automatically. The administrator can select to manage these contacts based on incoming VPIM messages or when the remote user has been changed or deleted entirely.

Blind Addressing

Blind addressing enables users to address messages to VPIM locations without a known VPIM contact existing in the database. In this case, the user sending a message to a VPIM contact will have the message delivered to that user, as long as the target user exists on the remote system. This is an available feature for each VPIM location that must be enabled on a per location basis. This method of addressing is dependent on directory synchronization between voice-messaging systems and can be used to minimize the database size of existing contacts. For example, it might be advantageous to allow blind addressing and not perform directory synchronization in cases in which there is a select group of users needing to send messages to VPIM contacts. Blind addressing is based entirely on the digits dialed by the caller.

Distribution List Considerations

Distribution lists have two features that need to be considered as part of the preparations for VPIM. The first consideration has to do with allowing VPIM contacts to be included in specific distribution lists. The default is to not include contacts. Also, you can allow distribution lists to accept messages from foreign systems, which include VPIM locations. This means that users at other VPIM locations can address messages to these lists. If you allow this feature, VPIM contacts cannot be included in these distribution lists. The reason for this restriction is to disallow messages from one VPIM location to be sent to another, especially where these VPIM locations might be completely different companies.

www.it-ebooks.info

For example, a message sent to a distribution list creates a dispatch message to its members. Therefore, the configuration of distribution lists would normally restrict the sending of dispatch messages to an outside company. In most cases, dispatch messages are usually directed to internal users. This characteristic should be considered because dispatch messages can be configured to be sent from a distribution list to users outside the company.

Domain Name Considerations

The domain name considerations discussed in Chapter 9, "Understanding Cisco Unity Connection Networking," should also be observed for VPIM networking. Because all messages are sent using SMTP, the message formation is defined as address@domain.com. Therefore, this domain name should be unique between the local system and all VPIM locations to avoid message delivery failure. The administrator needs to review the domain name configured under the SMTP Server Configuration page in Cisco Unity Connection Administration.

SMTP Smart Host and DNS Considerations

Chapter 9 introduced the SMTP Smart Host, which provides message delivery between VPIM locations where direct delivery using SMTP is not possible. SMTP access list configuration is also required for message delivery to the remote subscriber because it doesn't participate in the directory synchronization.

Domain Name System (DNS) provides the name resolution of network names to IP addresses in the network. In the case of SMTP, the name of the actual VPIM location needs to be resolved for message delivery. The DNS server should include an address (A) record and mail exchange (MX) record to ensure proper message transfer and delivery.

In some cases, the SMTP Smart Host implementation can perform the DNS function as well; however, you need to consult the documentation for your specific SMTP Smart Host device.

Networking and Connectivity Considerations

VPIM locations deliver messages using SMTP. As stated earlier, this protocol uses TCP port 25. Therefore, you need to verify that this port is not blocked by firewalls or access lists between servers. Also, verify connectivity by performing a ping test to each prospective VPIM location.

Configuring VPIM in Cisco Unity Connection

Before beginning the configuration of VPIM in Cisco Unity Connection, you must consider the aforementioned preparatory steps and verify connectivity between voice-messaging systems and between locations that use VPIM networking.

www.it-ebooks.info

For multiple locations, best practices would dictate developing a phased approach by starting with a single VPIM location. If possible, select a low-priority, low-volume location to minimize the impact of testing. When the configuration and contact creation is complete and verified according the expected results, you can proceed with the configuration of the remaining VPIM locations.

Case Study: Controlling Directory Synchronization

MAGS Inc. has partnered closely with Re-FIT Services for its internal server support. To assist IT support with communication between the organizations, MAGS and Re-FIT have decided to implement a VPIM network between their voice-messaging systems. Both organizations use Cisco Unity Connection version 8.5 server for voice messaging. However, VPIM will be used between these system to control the directory synchronization and accessibility between systems. With VPIM, each organization can control the information shared about users and contacts created, based on the contents of the SMTP messages.

In this case study, the two organizations have decided that messages can be addressed to remote users in either organization using blind addressing. In this case, blind addressing enables users to address messages to recipients at the remote VPIM location, even though these recipients are not defined in the directory. To minimize the number of contacts, MAGS Inc. has also decided to have Cisco Unity Connection manage the creation and deletion of VPIM contacts as messages are received from the remote VPIM location.

All preparation steps have been taken to verify connectivity and ensure a successful VPIM network between organizations. Finally, a high-level design for the VPIM deployment and configuration for Cisco Unity Connection servers was developed. This scenario depicts how two organizations can control the directory synchronization and addressing between their systems when using Cisco Unity Connection servers.

VPIM could also be used if one of the organizations did not have Cisco Unity Connection but was using a different voicemail system that supported VPIM. Figure 10-1 illustrates the VPIM network that will be deployed if this way considering Re-FIT Services had an installed third-party voicemail system.

Configuring the SMTP Domain Name

In most cases, the SMTP domain name will be unique between different organizations. However, this must be verified as being unique because the messages are addressed in the format of *mailbox_number@domain_name*.

www.it-ebooks.info

Chapter 9 covered the SMTP domain name configuration in detail; however, to complete this step, select **System Settings > SMTP Configuration > SMTP Server Configuration** in Cisco Unity Connection Administration, as shown in Figure 10-2. The SMTP domain for MAGS Inc. is currently configured to be **mags.net**.

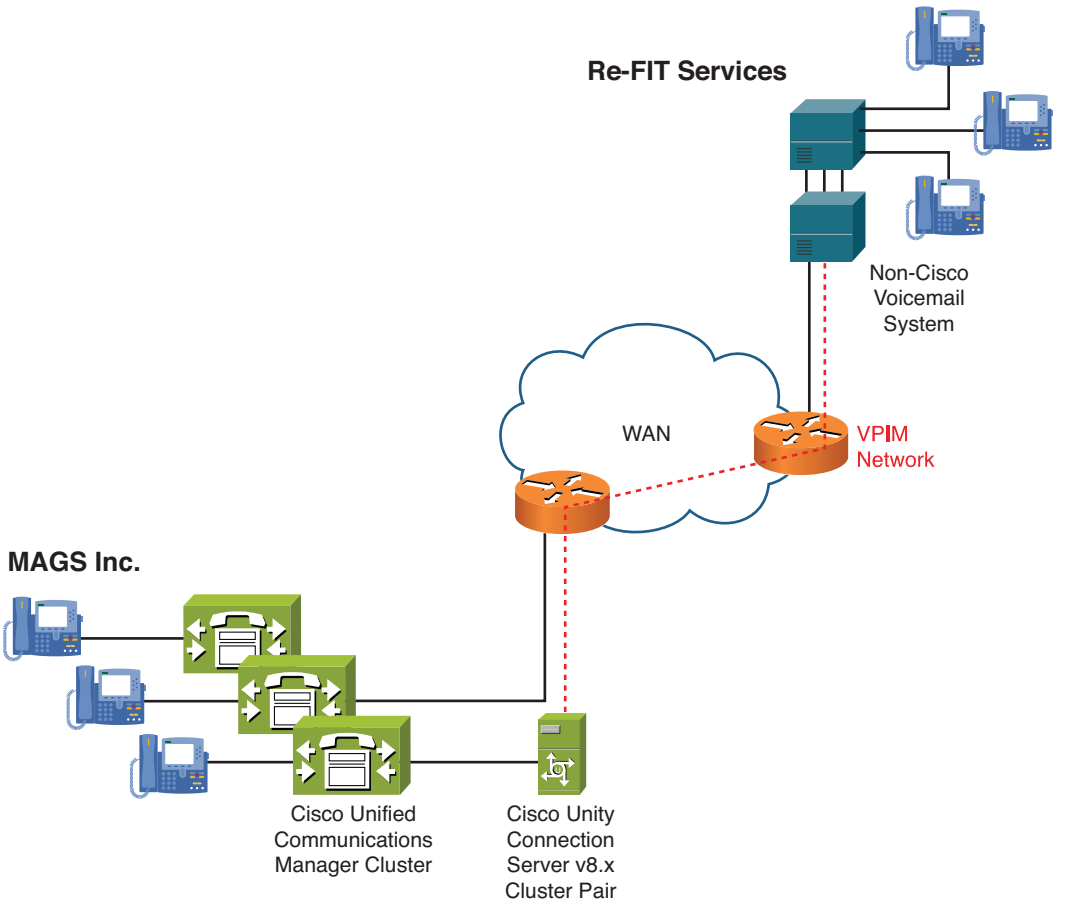

Figure 10-1 *Deployment for VPIM Networking Between MAGS Inc. and Re-FIT Services*

www.it-ebooks.info

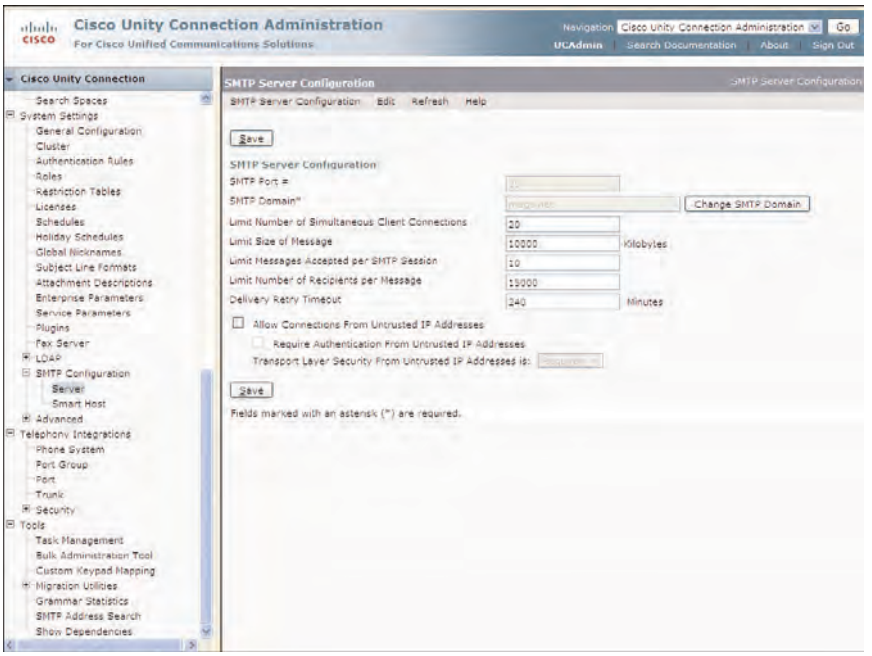

Figure 10-2 *SMTP Server Configuration for MAGS Inc.*

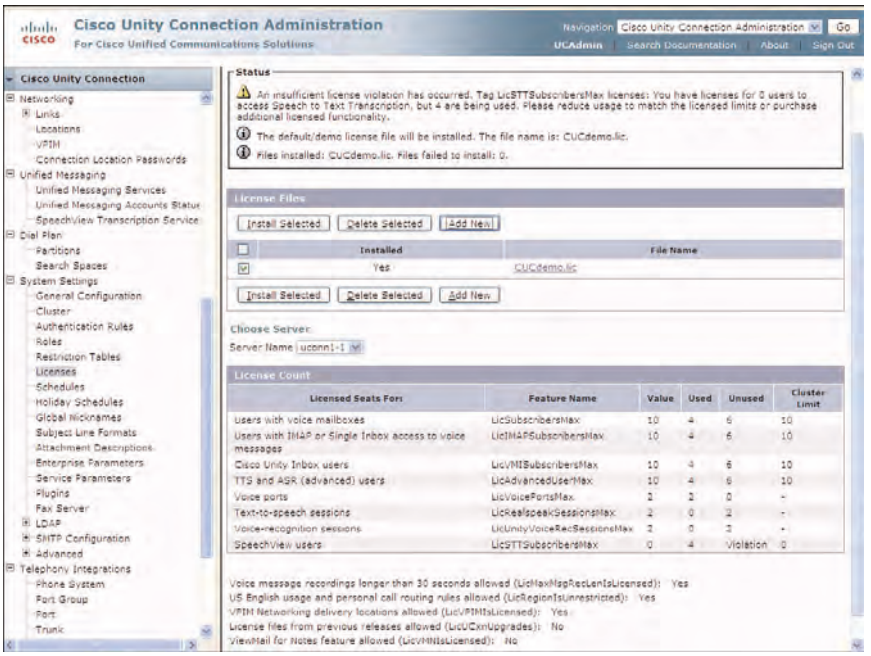

Figure 10-3 *Licenses in Cisco Unity Connection Administration*

www.it-ebooks.info

Verify VPIM Licenses

VPIM is a licensed feature in Cisco Unity Connection. Therefore, you need to verify that this license is available; from the navigation pane on the left in Cisco Unity Connection Administration, select **System Settings > Licenses**. Figure 10-3 shows the resulting Licenses page. Verify that the **VPIM Networking Delivery Locations Allowed (LicVPIMIsLicensed)** option is set to **Yes**.

Configuring VPIM Locations

When the SMTP Domain and VPIM licensing have been verified, you can configure the VPIM locations. To complete this step, from the navigation pane in Cisco Unity Connection Administration, select **Networking > VPIM**. The Search VPIM Location page displays. There are no VPIM locations currently configured, so click **Add New** to create a new VPIM location. The New VPIM Location page displays, as shown in Figure 10-4.

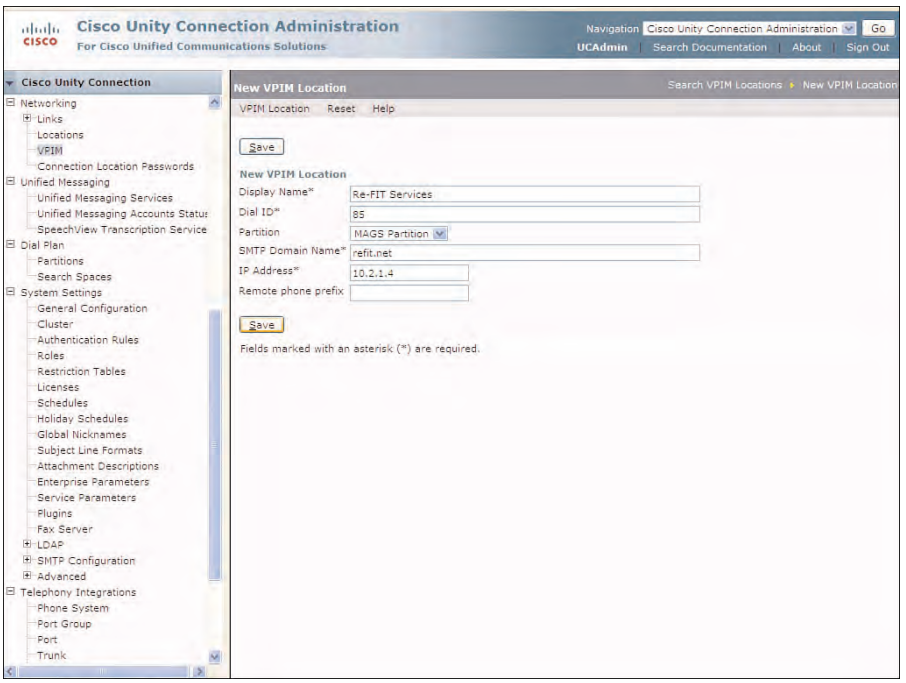

Figure 10-4 *New VPIM Location Page in Cisco Unity Connection Administration*

In the New VPIM Location page, configure the VPIM configuration options for each remote VPIM location. In this case, the configuration was completed for the MAGS Inc. system and the remote VPIM location, Re-FIT Services. Following are the configuration options on this page:

- **Display Name:** A descriptive name to identify the remote VPIM location. In this case, the Display Name of Re-FIT Services was selected to define the remote VPIM location.

www.it-ebooks.info

- **Dial ID:** The DTMF Access ID that prefixes all VPIM messages to identify this location. In this case, the Dial ID of **85** was chosen because it is unique within the current numbering plan. Re-FIT Service has chosen a Dial ID of **75** for its implementation.
- **Partition:** The partition to which this VPIM location belongs, which defines reachability. Users must have the defined partition in their search scope to address messages. All users at MAGS Inc. are currently defined in a single partition called MAGS Partition. This partition is made available in a single search scope called MAGS Search Scope.
- **SMTP Domain Name:** The SMTP domain name of the remote VPIM location. In this case, the remote SMTP domain name called **refit.net** is defined. This SMTP domain name is used when formatting messages to users at the remote VPIM location. Therefore, a message Andy Parsons (aparsons) at 3001 will be sent as 85_3001@refit.net, where **85** is the Dial ID prefix for the remote VPIM location.
- **IP Address:** The IP address of the remote VPIM location. This server can connect to this remote VPIM location to deliver outgoing VPIM messages and accept incoming messages.
- **Remote phone prefix:** Accommodates for the local dial plan. This feature is optional but can be used to ensure uniqueness of remote VPIM domain names (for example, if you have two VPIM domains that have a similar configuration).

After you complete the configurations for the VPIM location, click **Save** on the New VPIM Location page. The Edit VPIM Location page appears, as shown in Figure 10-5.

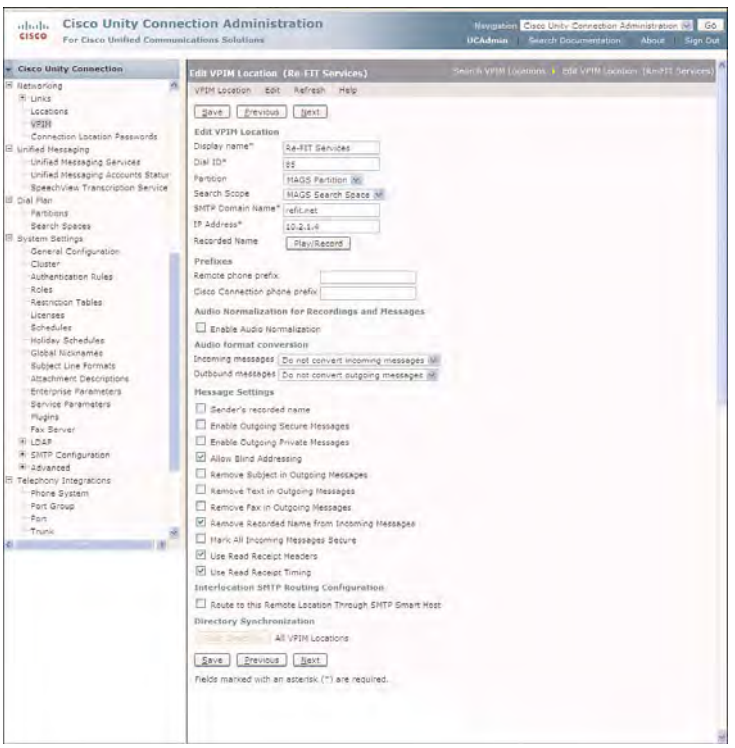

Figure 10-5 *Edit VPIM Location Page*

www.it-ebooks.info

This Edit VPIM Location page defines a number of options that you can customize for each location:

- **Prefixes:**
  - **Remote phone prefix:** (Optional) Additional prefix added to the extension for outgoing messages and removed for incoming messages. This prefix makes each VPIM location unique according to the defined numbering plan.
  - **Cisco Connection phone prefix:** (Optional) Similar to the Remote Phone Prefix but applies to the Cisco Unity Connection users. It is prefixed to Cisco Unity Connection users' extension for outgoing messages and removed for incoming messages.
- **Audio Normalization for Recordings and Messages:**
- **Enable Audio Normalization:** Enables Cisco Unity Connection to adjust the volume of the VPIM message to match the configured recording level. The actual decibel level is configured in the General Configuration parameters. To view this configurable option, in Cisco Unity Connection Administration, select **System Settings > General Configuration**. Audio normalization is unselected by default.
- **Audio format conversion:**
  - **Incoming messages:** Select the audio format of incoming messages. The two options here are to not convert the message or convert the message according to the recording codec. The Recording Format option is selected on the General Configuration page and can be viewed and modified by selecting **System Settings > General Configuration** in Cisco Unity Connection Administration.
  - **Outgoing messages:** Select the audio format of the outgoing messages. The two options here are to not convert the message or transcode the message to G.726 format before forwarding. If the remote VPIM location is Cisco Unity Connection or Cisco Unity, it is advisable not to transcode the message because the two systems already use a compatible format. If the remote VPIM location is a non-Cisco voice-messaging system, use the G.726 format because this is compatible with the standard requirement for VPIM.
- **Message Settings:**
  - **Sender's Recorded Name:** Includes the sender's recorded name in the outgoing message. The default setting is unselected.
  - **Enable Outgoing Secure Messages:** Enables secure messages to be sent to the remote location. The default setting is unselected. In this case, the sender receives a non-deliverable receipt (NDR).
  - **Enable Outgoing Private Messages:** Enables private messages to be sent to the remote location. The default setting is unselected. In this case, the sender receives an NDR.

www.it-ebooks.info

- **Allow Blind Addressing:** Enables users to send messages to the remote VPIM location by entering the remote VPIM location and voicemail extension. In this case, users can send message to the remote VPIM location, even if the recipients of the message are not defined as contacts. The default setting is unselected. In this case, the sender can send messages only to remote VPIM contacts defined in Cisco Unity Connection.
- **Remove Subject in Outgoing Messages:** Removes the subject line from messages sent to this VPIM location. The default setting is unselected. In this case, the subject line is not removed.
- **Remove Text in Outgoing Messages:** Removes any attachments or message body text from messages sent to this VPIM location. The default setting is unselected. In this case, attachments or message body text are not removed from messages.
- **Remove Fax in Outgoing Messages:** Removes any fax attachments from messages sent to this VPIM location. The default setting is unselected. In this case, fax attachments are not removed from messages.
- **Remove Recorded Name from Incoming Messages:** Removes the sender's recorded name from incoming messages. The default setting is selected. In this case, the recorded name is removed from the message. However, the recorded name that is part of the message header is still played. Unselecting this option might cause the recorded name to be heard twice: once with the message header followed by a second time from the message itself. This option does not affect the contact creation and update feature.
- **Mark All Incoming Messages Secure:** When selected, all incoming messages are marked as secure. Cisco Unity Connection version 7.x does not support secure VPIM messaging. The default setting is unselected.
- **Use Read Receipt Headers:** When selected, read receipt notifications are sent to this location in response to read receipt requests. When unselected, delivery receipt notifications are sent to this location in response to read receipt requests. The default setting is selected.
- **Use Read Receipt Timing:** When selected, responses to return receipt requests are sent when the message is opened. When unselected, responses to return receipt requests are sent when the message is delivered to the recipient. The Use Read Receipt Headers option determines the type of response sent. The default setting is selected.

- **Interlocation SMTP Routing Configuration:**
- **Route to This Remote Location Through SMTP Smart Host:** Enables the use of an SMTP Smart Host to route messages to this VPIM location. This option is unselected by default. When selected, the SMTP Smart Host must be defined. The configuration of the SMTP Smart Host in Cisco Unity Connection has been discussed in Chapter 9.

www.it-ebooks.info

- **Directory Synchronization:**
- **Push Directory - All VPIM Locations:** Updates all VPIM locations with users and recorded names from the local server/location. This option affects all VPIM locations.

In Figure 10-5, the configuration for MAGS Inc. includes sending the recorded name with each message sent to the remote VPIM location. Also, users are allowed to send messages to Re-FIT Services contacts using blind addressing. This allows users to address messages to the remote users, even when these users are not defined contacts in Cisco Unity Connection Administration. The Push Directory option is not selected to minimize the number of contacts at remote VPIM location. Therefore, the VPIM contacts are created and managed based on the received SMTP messages between VPIM locations.

Creating VPIM Contacts

After the VPIM locations are created, each organization needs to determine the method to create contacts. Unless blind addressing is allowed, contacts must be created to allow users to send messages to the remote VPIM location.

You can use a number of methods to create these contacts. You can create them individually in Cisco Unity Connection Administration or by using the Bulk Administration Tool, which enables you to create multiple contacts. If you want to have all users accessible by the remote VPIM location, on the VPIM Locations page, click **Push Directory - All VPIM Locations** so that all local user information is sent and updated to all remote VPIM locations. The amount of information sent to the remote VPIM location and contact information created must be considered. As discussed in the chapters in Part I, Cisco Unity Connection v.8x has a design limitation of 10 VPIM locations and 100,000 users and contacts per location or standalone server. The contacts defined here are the combined local and VPIM contacts.

For example, the Search User page in Figure 10-6 displays the current users for MAGS Inc.

The **Push Directory - All VPIM Locations** button is selected on the VPIM Location page enabling all voicemail user information to be sent automatically to all remote VPIM locations. Depending on the configuration of the remote location, these users can be added to the remote database, or if the remote VPIM location is another Cisco Unity Connection server or cluster pair, the users can automatically be created as VPIM contacts.

In this case, the remote VPIM location is a Cisco Unity Connection with the VPIM location configuration, as shown in Figure 10-7. The Dial ID is configured as **75**, as configured at the Re-FIT Services for the MAGS VPIM location.

In some cases, only a few remote VPIM contacts might need to be available to send messages. In these cases, it you might want to manually create the desired contacts manually or by using the Bulk Administration Tool. You can also simplify the administration of contacts by allowing Cisco Unity Connection to create and remove contacts based on the received VPIM message information. The default options for VPIM locations are to not automatically create or modify contact information.

www.it-ebooks.info

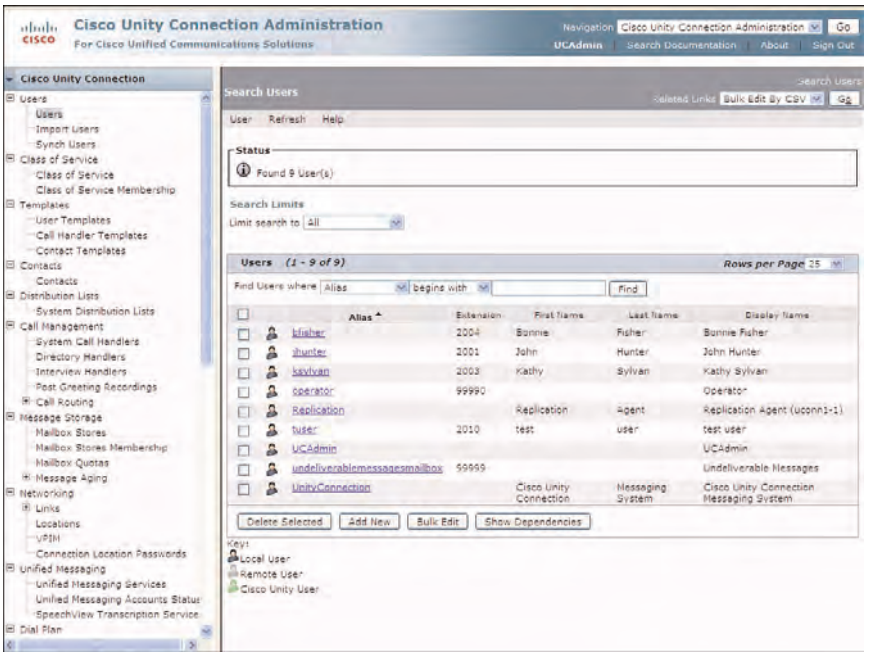

Figure 10-6 *Current Search Users Page*

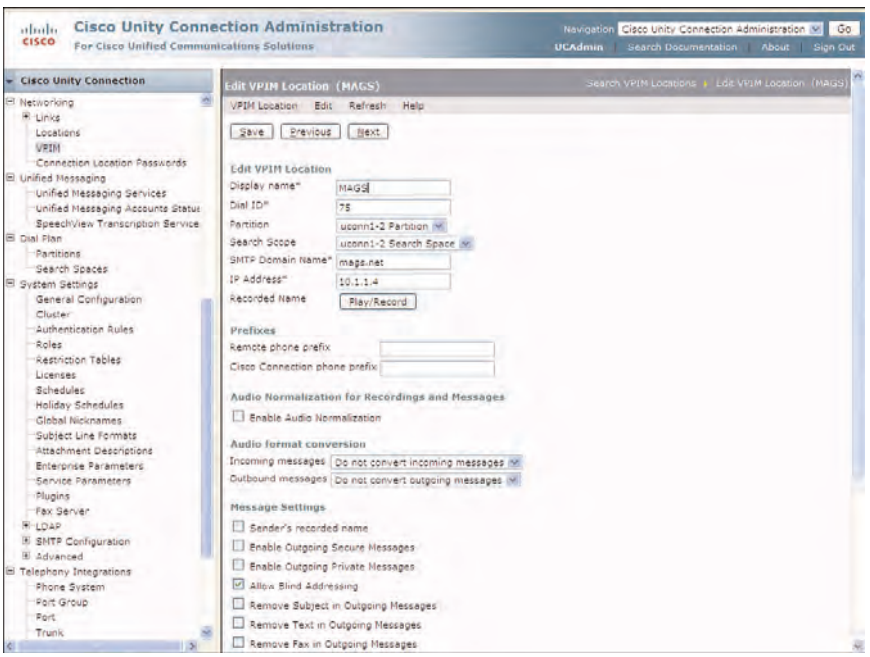

Figure 10-7 *VPIM Location Configuration at the Re-FIT Services Using Push Directory*

www.it-ebooks.info

To configure the VPIM contact creation parameters, from the toolbar on the Edit Location page, click **Edit > Contact Creation.** The Contact Creation page displays, as in Figure 10-8. On this page, the options to automatically create and update VPIM contacts are enabled. Also, the **Location Dial ID and Phone Number** option is selected from the **Map VPIM Contact Extensions To** drop-down.

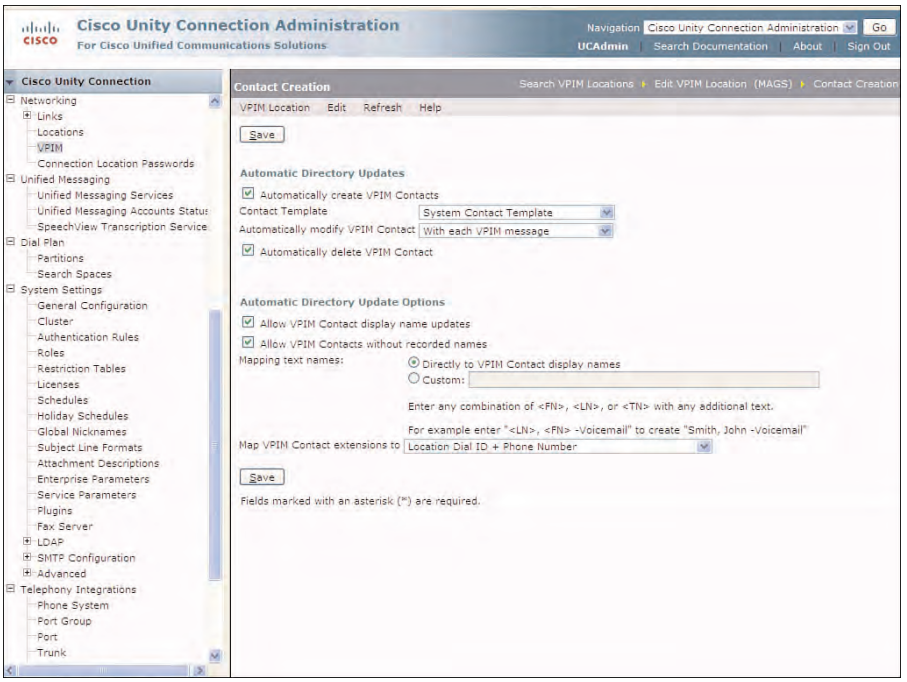

Figure 10-8 *Contact Creation Page at the Re-FIT Services Remote Site*

Figure 10-9 shows the result of configuration options selected on the Search Contacts page. Based on these VPIM location configuration selections, each user with voicemail is created as a VPIM contact with the remote extension, preceded by the Dial ID configured for the VPIM location based on the System Contact Template.

On the Contact Creation page (refer to Figure 10-8), you can configure how Cisco Unity Connection handles contact creation when enabling automatic updates of contacts. The following are the available options.

Automatic Directory Updates

- **Automatically Create VPIM Contacts:** Enables the automatic creation of contacts when a new message arrives and the contact does not currently exist in Cisco Unity Connection Administration. The default is unselected.

www.it-ebooks.info

- **Contact Template:** Creates the contacts, when you select the Automatically Create VPIM Contacts check box.
- **Automatically Modify VPIM Contact:** Provides for the automatic modification of contacts based on the incoming VPIM messages. These options are as follows:
  - **No Automatic Update of Contacts:** Contacts are not changed with any updates or changes of sender's information for VPIM messages.
  - **Only When the Text Name Changes:** Updates current contact information only when the senders' name has changed.
  - **With Each VPIM message:** Updates contact information with every VPIM message received from the remote VPIM location.
- **Automatically Delete VPIM Contact:** Automatically deletes existing VPIM contacts from Cisco Unity Connection when a message is returned back as undeliverable (NDR). This would be the case if the remote user was removed at the remote location and the mailbox no longer exists. The SMTP 5.1.1 message will be returned as a NDR. The default is unselected.

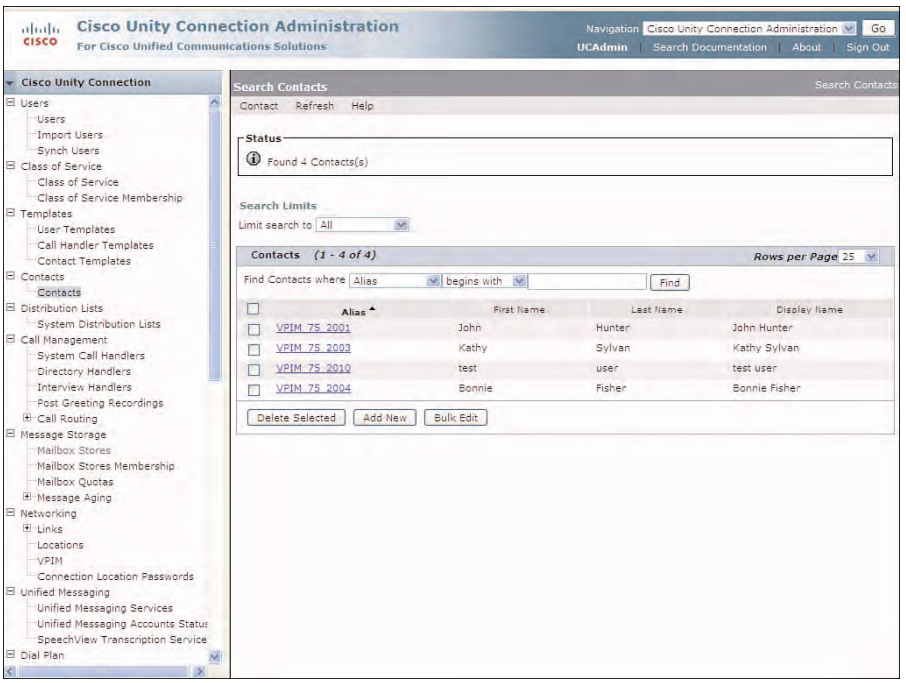

Figure 10-9 *Search Contacts Page for the Re-FIT Service Remote Site*

www.it-ebooks.info

Automatic Directory Update Options

- **Allow VPIM Contact Display Name Updates:** Enables updates to the display name of contacts when the sender's name has changed. The default is unselected.
- **Allow VPIM Contacts Without Recorded Names:** Enables automatic updates of contacts without the sender's recorded name; otherwise only updates are applied to contacts that have a recorded name. The default is unselected.
- **Mapping Text Names:** These options provide for the selection of how the text names are mapped. These options provide mapping text names.
  - **Directly to VPIM Contact Display Names:** Text names will be mapped to the display name of the VPIM contact.
  - **Custom:** Customize the mapping of the text names based on first name, last name, and text name. These descriptors or tokens can be entered as follows (when using multiple descriptors, enter a space, comma, or semicolon between each descriptor):
    - **First Name:** <FN>
    - **Last Name:** <LN>
    - **Text Name:** <TN>
- **Map VPIM Contact Extensions To:** Provides the option to map the extensions of the incoming VPIM messages. This option provides the following selections:
  - **Phone Number:** Extensions are mapped directly to the received phone number of the remote VPIM contact.
  - **Phone Number - Remote Phone Prefix:** Extensions are mapped to the phone number after the remote phone prefix is removed.
  - **Location Dial ID + Phone Number:** Extensions are mapped to the phone and prefixed with the Location Dial ID of the VPIM location.
  - **Location Dial ID + Phone Number - Remote Phone Prefix:** Extensions are mapped to the phone after the remote phone prefix is removed and prefixed with the Location Dial ID of the VPIM location

Case Study: Directory Updates and Blind Addressing

MAGS Inc. and Re-FIT Service tested the Push Directory option and decided against pushing directories between organizations because of the amount of user information that would be generated. Therefore, to minimize the amount of information, they decided to implement automatic contact creation. Both organizations have decided to create contacts based on the received VPIM messages and delete contacts when NDRs are received. Additionally, blind addressing is enabled to permit the sending of messages to VPIM locations in which the VPIM contacts are not currently defined.

www.it-ebooks.info

The administrators at MAGS require that the display names appear with the following format: **last name, first name; text name** (the display name of the remote users).

The Contacts Creation page for the Re-FIT VPIM location is configured for automatic contact creation, as shown in Figure 10-10. You will notice the custom configuration for the Mapping text names option to enable the configuration of the display name of the VPIM contacts. Also, the VPIM contact extension will be mapped to the Location Dial ID along with the remote phone number of the users' extension at the VPIM location.

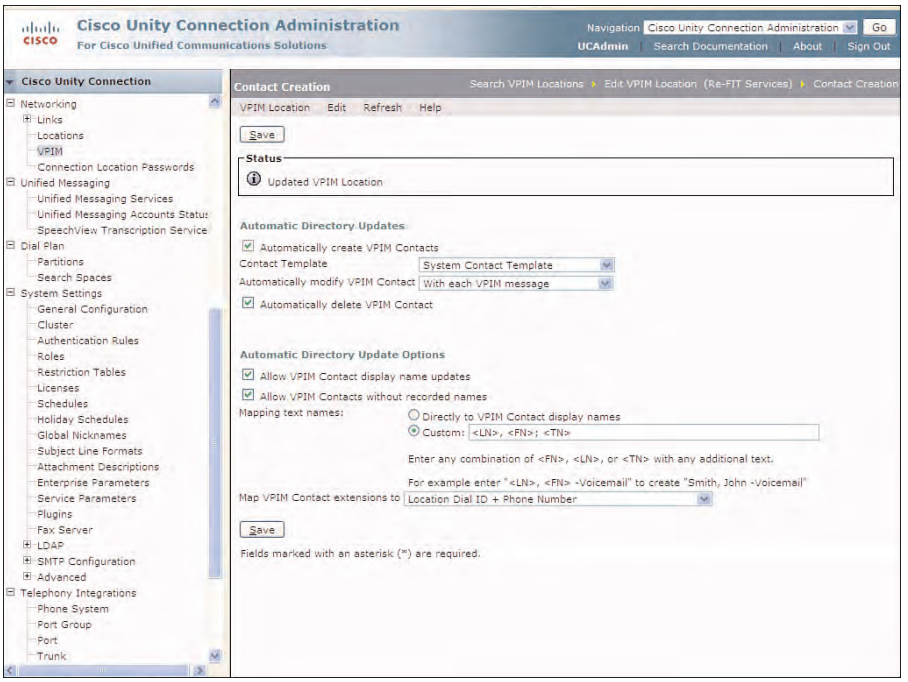

Figure 10-10 *Contact Creation Page for Re-FIT VPIM Location*

Because the administrators will not be pushing the directories using the **Push Directory** option on the Edit VPIM Location page, no contacts are created until a message is successfully received and delivered to the local user from the remote VPIM location.

Blind Addressing Using Cisco Unity Connection Inbox

A user at the remote location needs to send a message to the local user to create the VPIM contact. Because contacts do not exist at either location, blind addressing must be enabled to enable users to send messages to the remote location without the configuration of the VPIM contact in the local database.

www.it-ebooks.info

Blind addressing can be done by phone, IMAP client, or Cisco Unity Connection Inbox. To send a message by Cisco Unity Connection Inbox, the user needs to address the message to the specific VPIM contact to the proper extension, preceded by the correct Dial ID.

In Figure 10-11, the remote user, Ron Smith at extension 3261 is addressing a message to the VPIM contact at MAGS Inc. The remote extension **2004** is preceded by the Dial ID of **75** for the remote VPIM location. The complete address is 75_2004@mags.net. The user can record the message using Media Master with the PC speakers or the IP phone. After the message is addressed, the user can select the **Send** button to send the message to the remote VPIM contact.

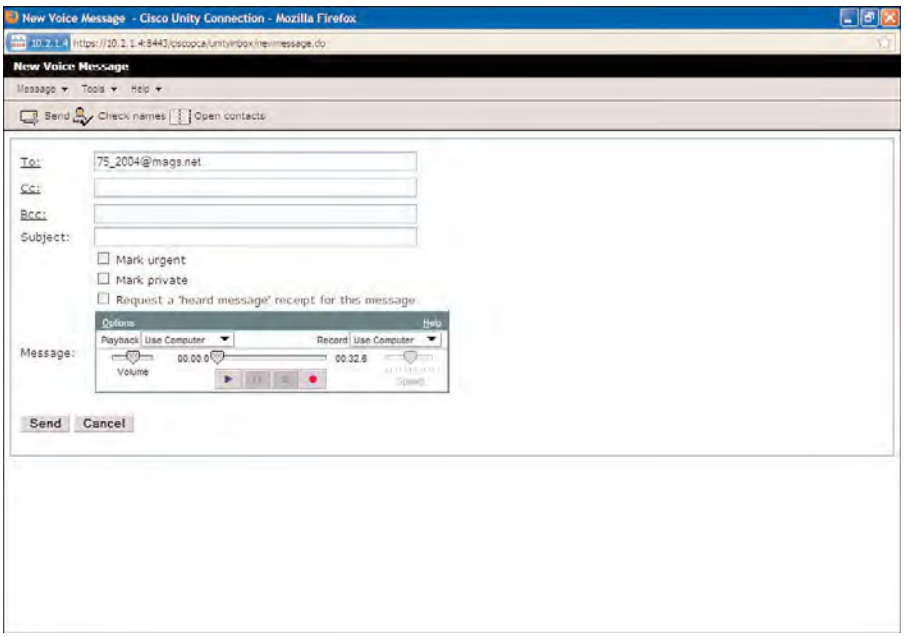

Figure 10-11 *New Message Using Blind Addressing with the Messaging Inbox*

When the message is sent to the remote VPIM location, the Dial ID is removed from being forwarded. After the message is received at the target location, the message is delivered to the proper user based on the phone number extension. If the extension at the target VPIM location does not exist, an NDR is returned to the sender's mailbox representing a delivery failure.

Automatically Create Contacts

At the remote VPIM location, when the message is received and delivered correctly to the local user, and the **Automatically Create VPIM Contacts** option is selected along with the option to create these contacts with each VPIM message on the Contacts

www.it-ebooks.info

Creation page, the new VPIM contact is created for each sender as the message is successfully received and delivered to the local users.

After the message is sent to the remote VPIM contact, from Cisco Unity Connection Administration, click **Contacts > Contacts**. The contact for Ron Smith is created for the remote user automatically as the message from Re-FIT Services was received at MAGS Inc., as shown in Figure 10-12. In this case, contacts are created with the Location Dial ID and remote phone number as configured under the Edit VPIM location page. Also, the display name is created according to the customized display name requirement of **last name, first name; text name**.

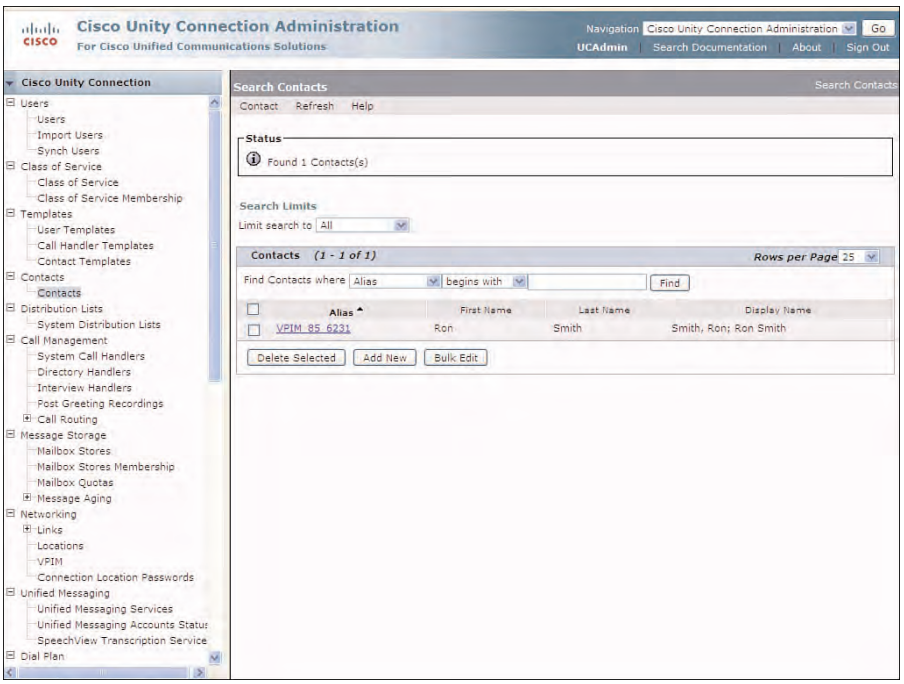

Figure 10-12 *VPIM Contact Automatically Created in Cisco Unity Connection*

By selecting the VPIM contact, the Edit VPIM Contact page for this user displays, as shown in Figure 10-13. The VPIM Settings, for the Delivery Location, VPIM Remote Mailbox Number, and Local Extension determine how the VPIM contact is defined at the local and remote locations and how the messages are to be addressed for proper delivery between locations.

You can manually change any of the configurations on the Edit Contacts Basics page if required, even though the contact creation is configured for automatic creation, modification, and deletion.

www.it-ebooks.info

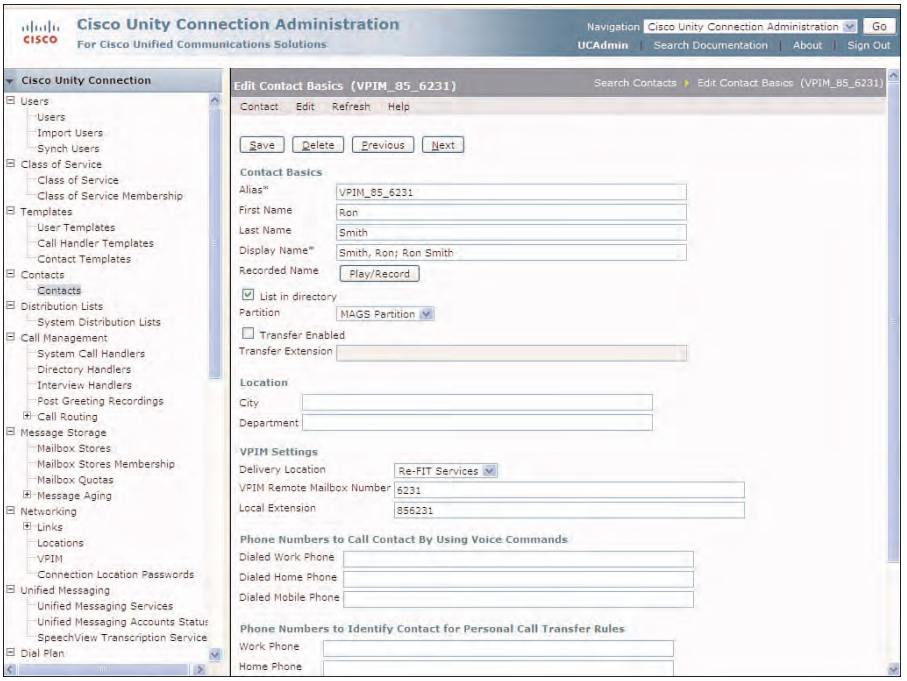

Figure 10-13 *Edit Contact Basics Page for the VPIM Contact*

Users at MAGS Inc. can now send messages directly to Ron Smith provided that the MAGS Partition is included in their Search Scope. In this case, blind addressing is not required because Ron Smith is a defined contact in the database. The contact can also be selected from the directory because the List in Directory option is selected, as shown in Figure 10-13. If the organization permits blind addressing, the contact must be created locally or synchronized from the remote VPIM location.

Automatically Delete Contacts

If Ron Smith is removed from Cisco Unity Connection at the Re-FIT Services location, this information is not forwarded to MAGS Inc. Therefore, users can still send messages and selected them in the directory, even though these VPIM contact may no longer exist. The option selected on the Contact Creation page for MAGS Inc. enables the contacts to automatically be removed when an NDR is received in response to an undeliverable message. Figure 10-10 shows the **Automatically delete VPIM Contact** option.

To demonstrate this behavior, the user Ron Smith was removed from the Cisco Unity Connection server at Re-FIT Services. Then, a user, John Hunter at MAGS Inc. sends a message to Ron Smith at 85_6231@refit.net, as shown in Figure 10-14.

www.it-ebooks.info

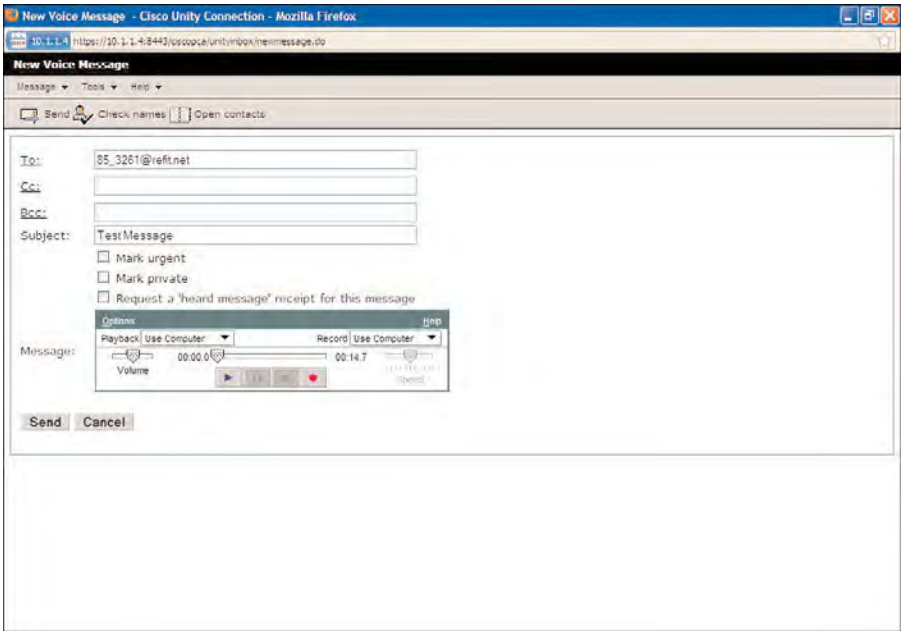

Figure 10-14 *New Voice Message Sent to Ron Smith at 85_6231@refit.net*

Because Ron Smith's voicemail no longer exists at Re-FIT Service, an NDR message will be received at John Hunter's mailbox.

When the returned NDR message is opened to review the details, the message shows a reason code of 5-1-1, which indicates that the mailbox for the message recipient does not exist as displayed in Figure 10-15. In this case, if this contact exists in the database, and the **Automatically Delete VPIM Contacts** option is selected on the Contacts Creation page for this VPIM location; then, the contact is removed from the database at the time the 5-1-1 reason code is returned.

After reselecting the **Contacts > Contact** page in Cisco Unity Connection Administration, the VPIM contact for Ron Smith was automatically removed from the database. This action was taken based on the NDR response. The Search Contacts page after the NDR was received is shown in Figure 10-16.

However, even though there were no messages delivered at Re-FIT, and an NDR was sent, the user John Hunter was learned and automatically created as a VPIM contact, as shown on the Search Contacts page at Re-FIT Services in Figure 10-17.

www.it-ebooks.info

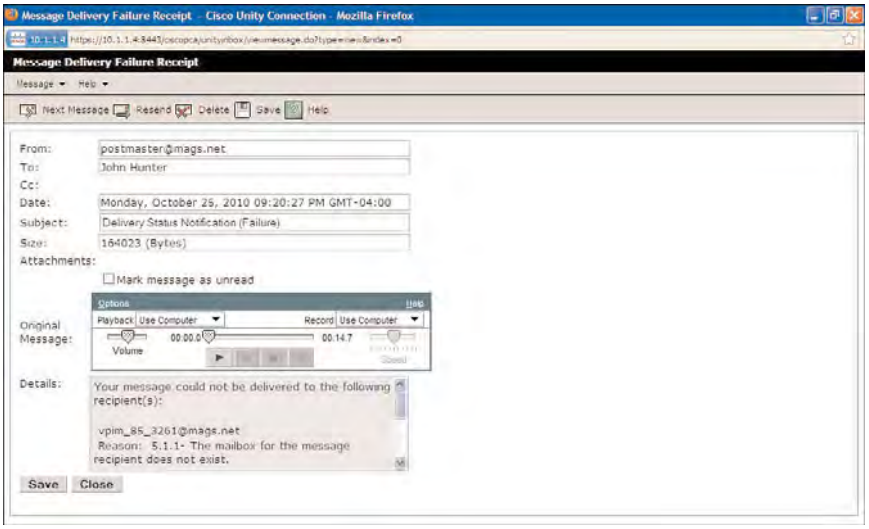

Figure 10-15 *NDR with Reason Code 5-1-1*

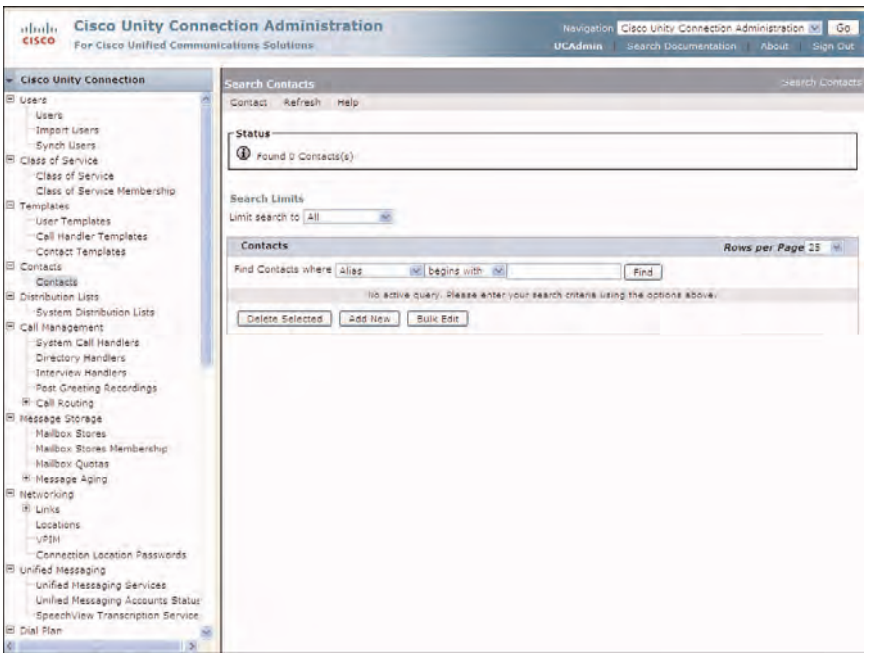

Figure 10-16 *Search Contacts Page After NDR Was Received*

www.it-ebooks.info

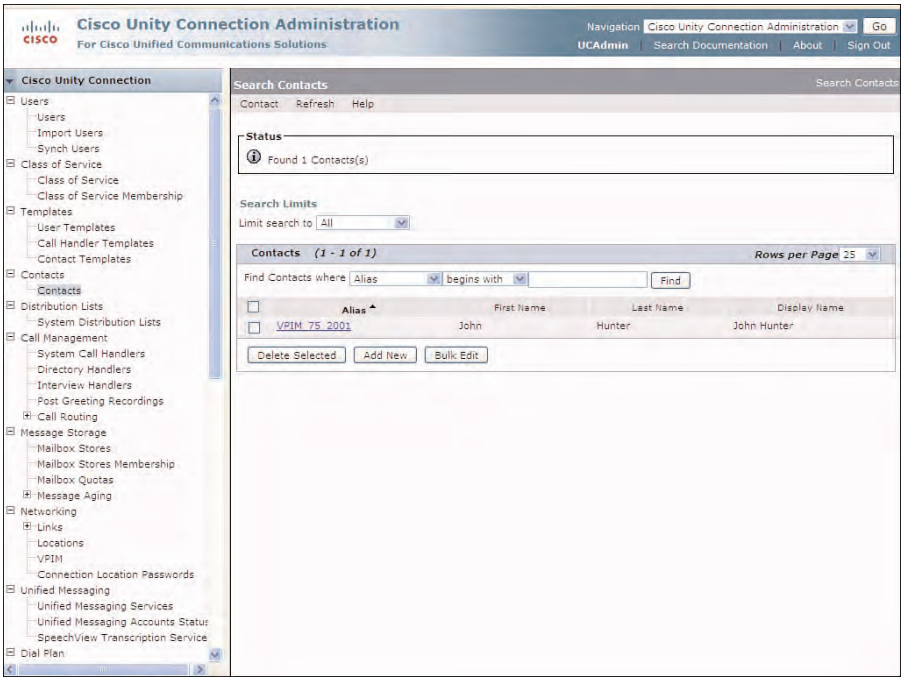

Figure 10-17 *Search Contacts Page at Re-FIT Services*

VPIM Features

In some cases, it might be advantageous to use an alternative name for a remote VPIM user, rather than using the Dial ID. If users use voice recognition, they can simply say John Hunter in Cleveland. Also, multiple alternative names can be added and configured to match a specific name phonetically.

Case Study: VPIM Features

Chuck Watts, the Re-FIT services director, has been using Personal Communications Assistant to address messages to VPIM contacts at MAGS Inc. However, he would like to use the voice-recognition feature to address messages to these individuals.

The VPIM configuration for the MAGS VPIM location at Re-FIT Services will be configured with an alternative name of Cleveland and MAGS. After Chuck is assigned to a Class of Service that enables the use of the voice-recognition feature, he can address messages directly to these remote contacts by saying the extension followed by the alternative name. For example, “2002 in Cleveland” addresses this message to this VPIM contact.

To complete the configuration of alternative name, in Cisco Unity Connection Administration, select **Networking > VPIM**. The Search VPIM Location page displays. You then need to select the MAGS location from the Display Name column. On the Edit

www.it-ebooks.info

VPIM Location page, select **Edit > Alternate Names** from the toolbar. The Alternate Names page displays, as shown in Figure 10-18. In this example, two alternative names are configured for this location. Enter the desired alternative name in the Display Name field, and click **Add New**. The alternative name displays in the Edit Alternate Names field, where it can be changed or deleted as required. You can add multiple alternative names as required for each VPIM location. This might be necessary to facilitate how people work, or refer to the various VPIM locations. In some cases, users can refer to the location by the name, city, or purpose.

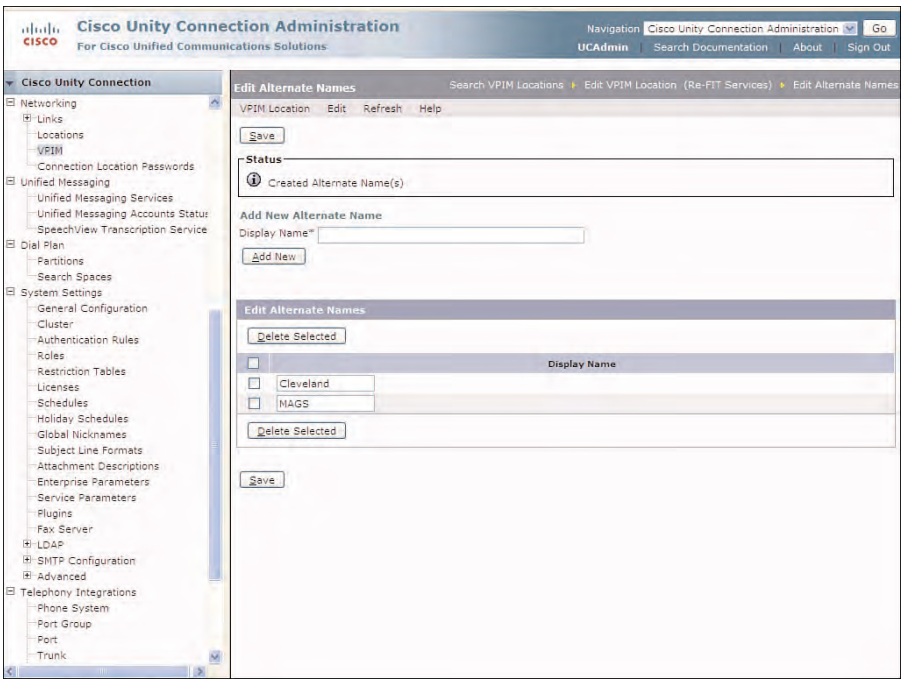

Figure 10-18 *Configuring Alternative Names for VPIM Locations*

Figure 10-18 addresses the VPIM location. However, the VPIM contacts might not be addressed by the phone number extension because this information might not always be known to the local users. In this case, it might be more expedient to add alternative names for VPIM contacts, so Chuck Watts can use the voice-recognition feature to address his message to John Hunter by simply saying, "John Hunter in Cleveland."

To complete the configuration of alternative names for VPIM contacts, from the navigation pane in Cisco Unity Connection Administration, select **Contacts > Contacts**. Then, from the toolbar, select **Edit > Alternate Names.** Figure 10-19 shows the Edit Alternate Names page, which is configured similar to alternative names for the VPIM location.

SMTP proxy addresses can also be configured for each VPIM contact. SMTP proxy addresses map the recipient of the incoming message to the proper VPIM contact when

www.it-ebooks.info

using an IMAP client. To configure the SMTP proxy addresses for a VPIM contact, from the toolbar on the Edit Contacts Basics page, select **Edit > SMTP Proxy Addresses**. The SMTP Proxy Addresses page displays. Click **Add New** and enter the desired SMTP address in the field, as shown in Figure 10-20. In this case, John Hunter is configured with the SMTP address of jhunter@mags.net. Multiple SMTP proxy addresses can be configured as needed.

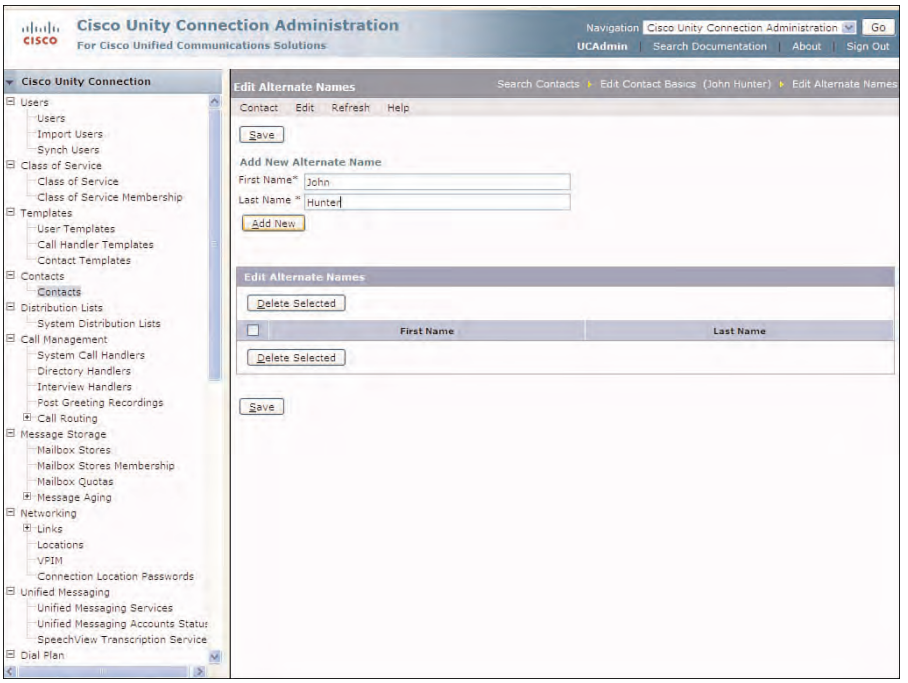

Figure 10-19 *Alternative Names Configuration for VPIM Contacts*

After this configuration is complete, the users at Re-FIT Services can now address messages to John Hunter using the configured SMTP proxy address using IMAP. Figure 10-21 illustrates a voice message addressed to John Hunter at MAGS Inc. concerning its billing. This message is sent using the Messaging Inbox in Personal Communications Assistant.

www.it-ebooks.info

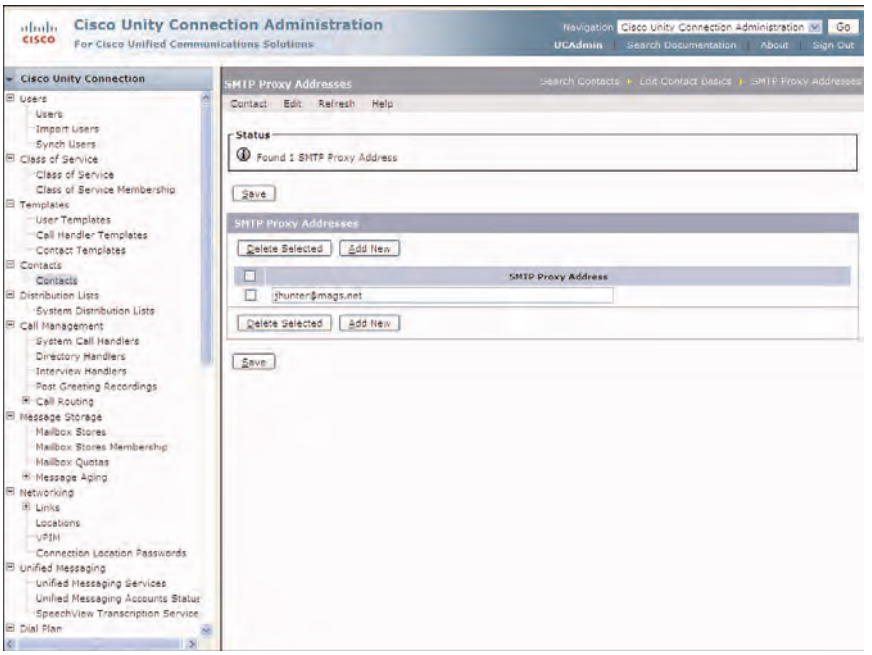

Figure 10-20 *SMTP Proxy Address Configuration for VPIM Contacts*

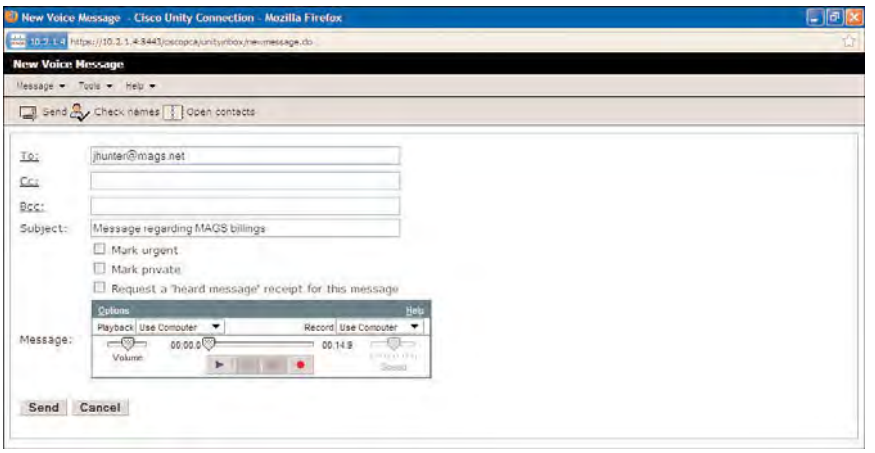

Figure 10-21 *Voice Message Addressed to VPIM Contact Using the SMTP Proxy Address*

www.it-ebooks.info

Summary

This chapter provided an understanding of VPIM networking in Cisco Unity Connection. You learned how to do the following:

- Understand the features, function, and purpose of VPIM networking between Cisco Unity Connection and various voice-messaging systems.
- Explore the preparatory steps required before configuring VPIM networking between Cisco Unity Connection servers and other voice-messaging systems.
- Describe the configuration of VPIM networking in Cisco Unity Connection.
- Understand the various manual and automatic methods of creating, modifying, and deleting contacting in Cisco Unity Connection.
- Describe the configuration of VPIM features, addressing, and alternative names in Cisco Unity Connection.
- Configure SMTP proxy addresses to allow the addressing to VPIM contacts using IMAP clients.

www.it-ebooks.info

Chapter 11

Using Cisco Unity Connection Tools and Reports

This chapter covers the following subjects:

- **Real-Time Monitoring Tool (RTMT):** Covers the feature, purpose, and configuration of RTMT to provide performance monitoring, trace, and troubleshooting.
- **Cisco Object Backup and Restore Application Suite (COBRAS):** Describes the functions and setup of the COBRAS application to export and import users and messages from earlier versions of Cisco Unity Connection and Cisco Unity.
- **Migrate Utilities:** Reviews the function of the migrate utilities in Cisco Unity Connection Administration to migrate users and messages using SSH from previous versions of Cisco Unity.
- **Task Management:** Describes the system-level tasks and schedules in Cisco Unity Connection Administration.
- **Reports:** Covers the various reports available in Cisco Unity Connection and illustrate the procedure, configuration, and format.

Your Cisco Unity Connection voice-messaging system is now configured and operating according to the proposed design and configuration; however, administrators need to monitor the performance of the system, troubleshoot issues, and create reports to take a proactive approach to system administration and management. Cisco Unity Connection incorporates a number of tools to assist engineers and administrators with this task. Also, system and user reports assist administrators with troubleshooting issues and assist in the task of keeping documentation current.

This chapter discusses the Real-Time Monitoring Tool. Engineers and technicians familiar with this tool in Cisco Unified Communications Manager (CUCM) can appreciate the similarities, as the same tool is used with Cisco Unity Connection.

www.it-ebooks.info

In some cases, tools assist with a specific administration task, such as migrating users and messages from one system to another. Cisco Unity Connection includes a migration utility, the Cisco Object Backup and Restore Application Suite (COBRAS), that enables an organization to migrate users and messages. COBRAS is an external tool that runs as a client-side application that enables organizations to migrate users from earlier versions of Cisco Unity Connection and Cisco Unity voice-messaging system.

In this chapter, you gain a full understanding of the following:

- The purpose, function, and features of the Real-Time Monitoring Tool (RTMT) to monitor system performance, view syslog messages, and collect/view system traces.
- How Cisco Object Backup and Restore Application Suite (COBRAS) is used to migrate users and messages from earlier versions of Cisco Unity Connection and Cisco Unity voice-messaging systems.
- The Migrate Utilities client that resides in Cisco Unity Connection Administration and note the differences between using the Migrate Utilities and COBRAS.
- The Task Management features in Cisco Unity Connection Administration and the scheduling of system maintenance and troubleshooting tasks.
- The various reports that can be run in Cisco Unity Connection.

Cisco Unity Connection Tools

Engineers and administrators use Cisco Unity Connection Tools to assist in the building and repair of an implementation. You can use a number of tools for different purposes. Just as a good carpenter knows his tools and purpose of each, the skillful engineer understands when to use the right tool.

A few months ago, I visited a friend who had an extensive workshop in his garage with all the latest woodworking tools, saws, drills, and the like. As I asked a few questions about what each one did, he eloquently explained the purpose, features, and functions of each one. This skill didn't happen overnight or by reading a book. His skills were honed through years of hands-on experience working with these tools. Sure, knowledge and understanding is gained through reading, learning, and watching others; however, there is no substitute for experiential knowledge gained by working with each tool.

In the same way, Cisco Unity Connection engineers and administrators should do due diligence by taking the time to read, learn, study, and work with the tools to get a working knowledge of each. The time to understand the Cisco Unity Connection tools is not when you have a problem that you need to troubleshoot, but when everything works properly. How else can you understand what the results should look like when everything operates properly? Therefore, you need to take the time and become familiar with each of tools included in this section. These tools can help you in troubleshooting, testing, and monitoring system performance, but only if you take the time to thoroughly understand their features, function, and configuration.

www.it-ebooks.info

Using the Real-Time Monitoring Tool

Chapter 4, "Integrating Cisco Unity Connection," discusses the Real-Time Monitoring Tool (RTMT) in dealing with voicemail integration, where you use the RTMT to access the Port Monitor. If you remember from this discussion, the Port Monitor feature enabled you to view the traffic on each port between Cisco Unity Connection and the phone system integration in real-time. In this section, you learn some of the other functions and features of the RTMT. Just like the skillful carpenter, you need to take the information included in this chapter and put it to practice by using this tool.

Accessing RTMT

As discussed in Chapter 4, the Cisco Unified RTMT is downloaded from Cisco Unity Connection Administration, by selecting **System Setting > Plugins** and selecting to download the RTMT application. The tool is available in a Windows or Linux version. You should download the tool from Cisco Unity Connection Administration rather than using an older version to ensure that you maintain all functionality and features applicable to your software version.

At press time, Cisco Unity Connection 8.5 software uses the Cisco Unified Real-Time Monitoring Tool version 8.7 (004). A number of features and functionality have been improved with this version to make it easy for monitoring performance and system status. However, the RTMT versions are usually backward compatible enabling the administrator to use the new tool to connect to an older version.

The RTMT application is an executable file that requires specific Java components; therefore, ensure that your Java is up-to-date on your workstation before beginning the installation. After you download the application from Cisco Unity Connection Administration, select the application to open and install it on your workstation. You need to log in using the proper credentials, as discussed previously in Chapter 4. When logged in, the main interface displays with the navigation pane on the left portion of the page. The navigation includes links for System and Unity Connection or Server monitoring utilities, as shown in Figure 11-1. The Unity Connection option displays the Port Monitor, which was discussed in Chapter 4. This chapter focuses on the System tools in the RTMT tool.

The navigation pane enables the user to select the various options to view either of the following features:

- **System Summary:** Displays information about the Virtual Memory, CPU, common partition usage, and the Alert History
- **Server:**
  - **CPU and Memory:** Provides detailed information about the server virtual memory and CPU usage on a server-by-server basis
  - **Process:** Provides real-time list and status of all processes

www.it-ebooks.info

- **Disk Usage:** Provides detailed information of the Common, Swap, and Spare Partition usage of the server disk
- **Critical Services:** Displays a real-time status of all critical services

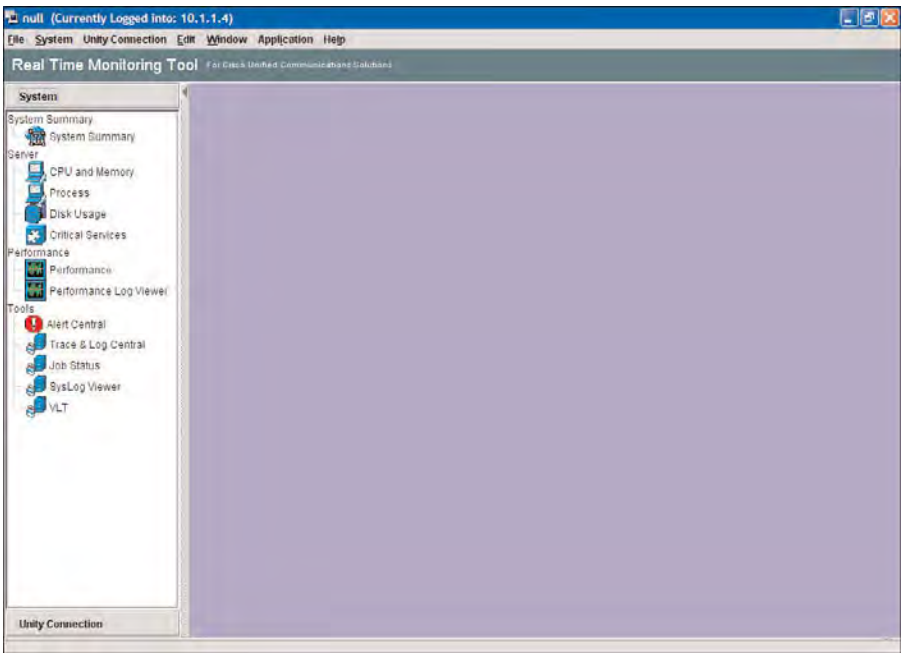

Figure 11-1 *Cisco Unified Real-Time Monitoring Tool for Cisco Unity Connection Version 8.5*

- **Performance:**
  - **Performance Monitoring:** Customizable performance monitoring of selectable performance monitoring counters within the Cisco Unity Connection server
  - **Performance Log Viewer:** Log viewer providing the ability to view a previous performance log file with selectable counters
- **Tools:**
  - **Alert Central:** Provides for the configuration and editing of alerts and viewing the alert history
  - **Trace & Log Central:** Provides the ability to configuration on-demand trace collection based on specific criteria
  - **Job Status:** Provides the status of current jobs for trace and log file collection
  - **SysLog Viewer:** Provides a view of current and past SysLog files, with detailed descriptions

www.it-ebooks.info

- **VLT:** Provides troubleshooting of complex System Diagnostic Interface (SDI) trace-log message files, making them easier to read to assist in troubleshooting basics

System Summary

The System Summary is a good place to start to get a benchmark on the current performance of Cisco Unity Connection. You can easily view the System Summary by selecting the System Summary option from the navigation pane on the left portion of the Cisco Unified RTMT.

Think of this as your 10,000-foot overview, enabling you to view the current CPU and virtual memory usage and the alert history. By selecting System Summary, the page body displays with the three graphs for system usage, along with the Alert History displayed below these graphs, as shown in Figure 11-2.

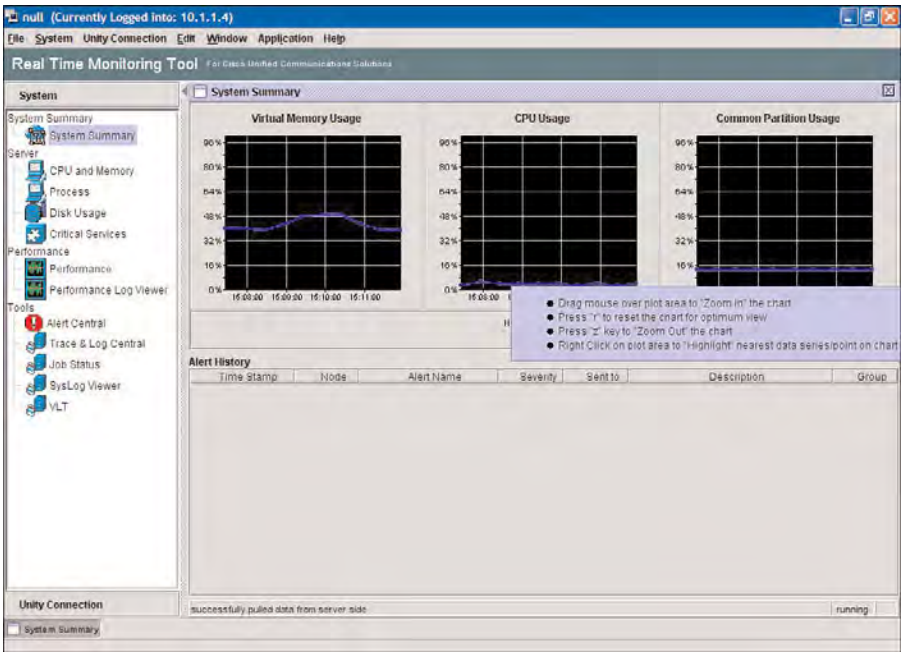

Figure 11-2 *System Status Displayed Using the RTMT*

You can modify the view of each of the graphs. If you move the mouse over the graph portion of the chart, a pop-up reveals the controls. These controls enable the user to do the following:

- Drag the mouse over plot area to "Zoom In" the chart.
- Press "r" to reset the chart for optimum view.

www.it-ebooks.info

- Press the “z” key to “Zoom Out” the chart.
- Right-click on plot area to “Highlight” nearest data series/point on chart.

Note To ensure that the data you view is current, verify that the display states: Successfully Pulled Data from Server Side near the lower-left portion of the page and the word “running” near the lower right.

In Figure 11-3, the Virtual Memory graph is zoomed in by clicking the portion close to the section where you want to zoom.

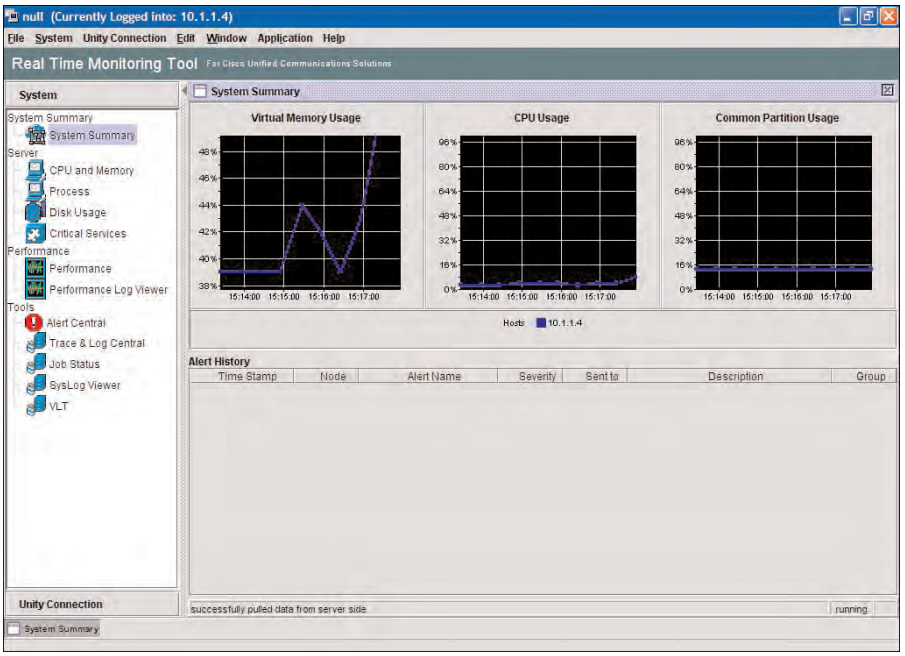

Figure 11-3 *Zoom in Function on the RTMT*

In Figure 11-4, each of the graphs is selected for the optimum view by selecting the “r” key. This view provides the greatest readability between the minimum and maximum values and provides the data in a easily viewable format. In this case, the CPU usage currently runs between 3 percent and 8 percent, whereas the virtual memory is currently running steady at approximately 40 percent with a peak up to 54 percent. There are no current alerts or any alerts in the history.

www.it-ebooks.info

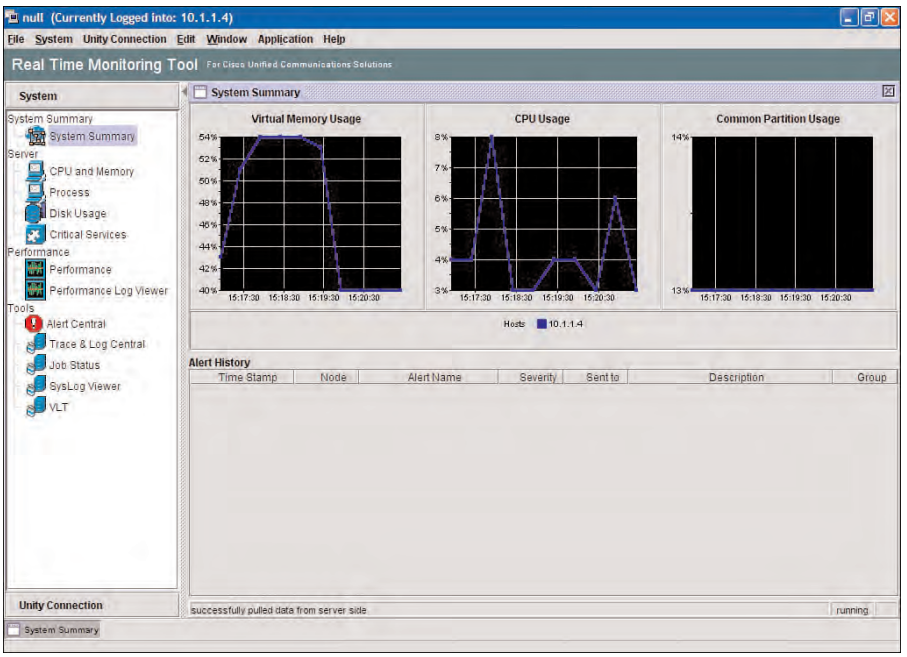

Figure 11-4 *Optimized View of the System Summary for the RTMT*

Server-CPU and Memory

As mentioned previously, this is a high-level view based on the CPU and virtual memory performance. To get a more detailed view of the server, on the navigation pane, select the **CPU and Memory** option. The CPU and Memory page displays, as shown in Figure 11-5. This page provides the necessary graphs but also a detailed breakdown of the current numbers and percentages.

Server-Process

By selecting the **Process** option from the navigation pane, the RTMT displays the current processes with their status and CPU usage, as shown in Figure 11-6.

If you see unusually high CPU utilization, this view would be a good place to locate which process might be causing the issue.

Server-Disk Usage

Disk usage is an important area to monitor as the additional users are configured and added to a specific server. However, you need to observe the design considerations discussed in Part I about the server sizing. From the navigation pane, select the Disk Usage option. The Disk Usage page displays, as shown in Figure 11-7.

www.it-ebooks.info

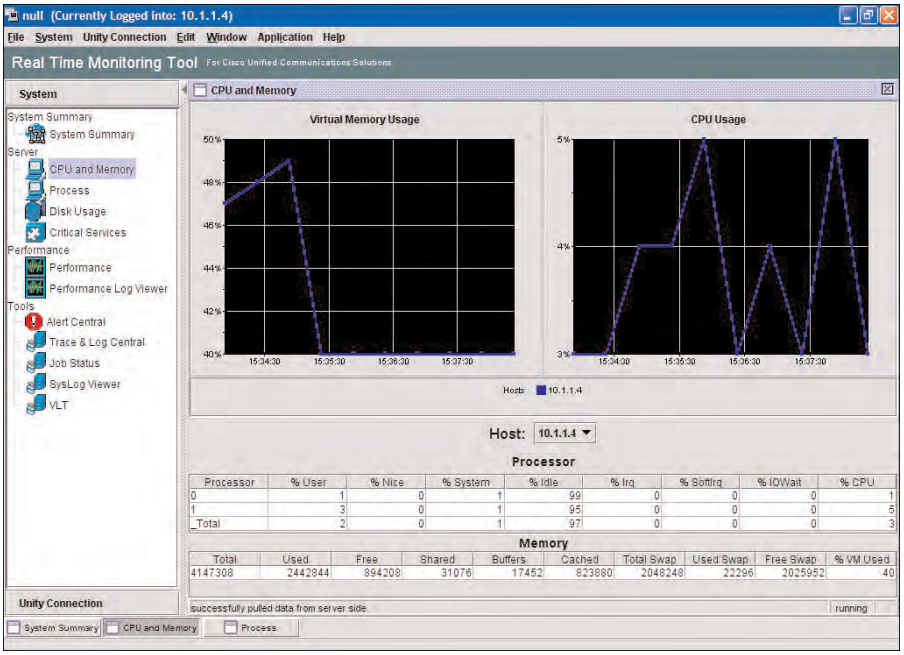

Figure 11-5 *CPU and Memory Usage in RTMT*

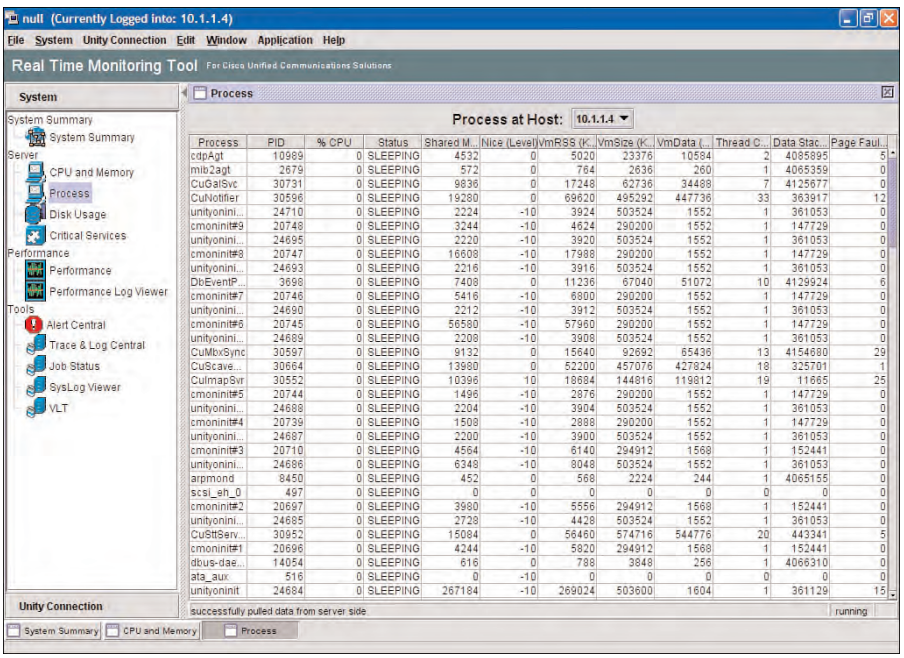

Figure 11-6 *Process in RTMT*

www.it-ebooks.info

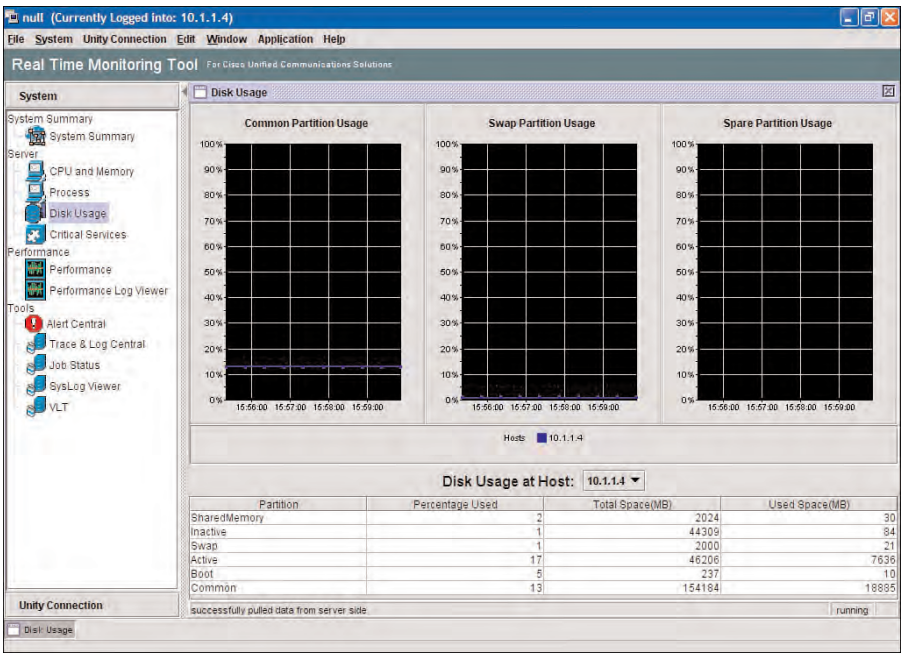

Figure 11-7 *Viewing the Disk Usage in RTMT*

The details of the server's Disk Usage displays the disk space used out of the total hard drive disk space and displays the usage based the type, which is either active, inactive, swap, boot, common, or shared memory. Software upgrades are performed by uploading software to the inactive partition and then initiating a switch version operation in the Cisco Unified OS Administration or command-line interface (CLI). The swap, boot, common, and shared memory are used by Cisco Unity Connection software for the server, software, and configuration database operations.

Critical Services

The Critical Services selection provides information about all services crucial to the proper operation of Cisco Unity Connection. All services will be indicated with the current status of whether the service is up, down, starting, stopping, not active, or stopped on purpose by the administrator.

Two tabs display the various services. The System Services tab displays in Figure 11-8. System Services are divided into six categories:

- Performance and Monitoring
- System Services
- Platform Services
- DB Services

www.it-ebooks.info

- SOAP Services
- Backup and Restore Services

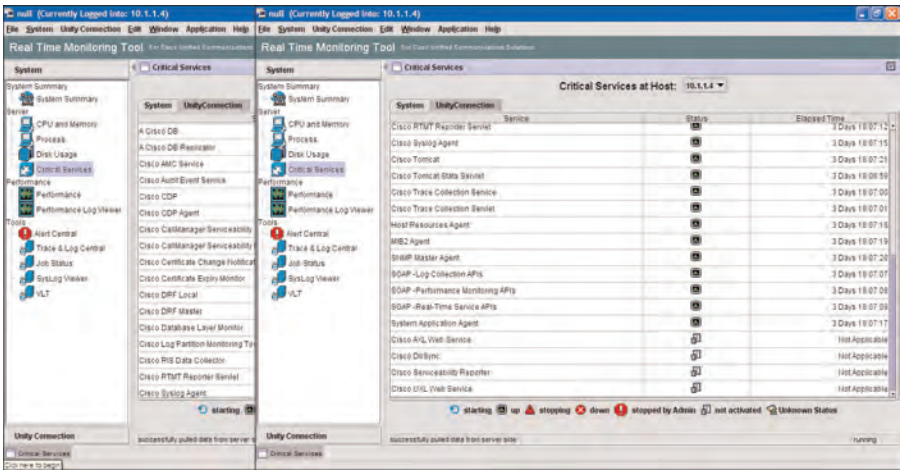

Figure 11-8 *Critical Services (System) Using RTMT*

The System Services are listed as follows:

- **Cisco DB:** Platform Service that supports the database engine for Cisco Unity Connection.
- **Cisco DB Replicator:** Platform Service that supports the database configuration, replication, and synchronization between publishers and subscribers (only used with Cisco Unified CM).
- **Cisco AMC Service:** Alert Manager and Collector Service - Performance and Monitoring Service that enables the RTMT to retrieve real-time information from Cisco Unity Connection servers.
- **Cisco Audit Event Service:** Performance and Monitoring Service that monitors and logs configuration changes by the administrator.
- **Cisco CDP:** System Service that advertises to network management applications. This service is used for SNMP and CiscoWorks.
- **Cisco CDP Agent:** Platform Service that provides SNMP access to other network management workstation based on the CISCO-CDP-MIB.
- **Cisco CallManager Serviceability:** System Service that supports the Cisco Unified Serviceability web application interface.
- **Cisco CallManager Serviceability RTMT:** Performance and Monitoring Service that provides support to the RTMT to collect and view traces, performance objects, alerts, devices, and applications.

www.it-ebooks.info

- **Cisco Certificate Change Notification:** Platform Service that monitors and report change to certificates.
- **Cisco Certificate Expiry Monitor:** Platform Service that monitors expiration of certificates. This service works directly with the Cisco Certificate Change Notification service.
- **Cisco DRF Local:** Backup and Restore Service that executes all local commands from the Cisco DRF Master Agent. This service is responsible to send status, logs, and responses to the master agent.
- **Cisco DRF Master:** Backup and Restore Service works with the CLI and Disaster Recovery Service web interface to execute all backup and restore functions and provide the storage for backup and restore processes.
- **Cisco Database Layer Monitor:** DB Service that performs monitoring and change notification for the database.
- **Cisco Log Partition Monitoring Tool:** Performance and Monitoring Service that monitors the disk usage of the logs stored on the server according to the configured thresholds/polling interval.
- **Cisco RIS Data Collector:** Real-Time Information Service - Performance and Monitoring Service that monitors all real-time information such as device registration, perform, alarms, and the like to be used by other interfaces and applications.
- **Cisco RTMT Reporter Servlet:** Performance and Monitoring Service that provides the report interface for the RTMT.
- **Cisco Syslog Agent:** Platform Service provides the collection of syslog messages from the various components in Cisco Unity Connection. This service used the CISCO-SYSLOG-MIB.
- **Cisco Tomcat:** Platform Service that provides the web service for the various interfaces in Cisco Unity Connection.
- **Cisco Tomcat Stats Servlet:** Performance and Monitoring Service that provides the monitoring using the CLI and RTMT.
- **Cisco Trace Collection Service:** System Service that provide trace collection and viewing of traces for the RTMT. Works with the Cisco Trace Collection Servlet.
- **Cisco Trace Collection Servlet:** System Service that provide trace collection and viewing of traces for the RTMT. Works with the Cisco Trace Collection Service.
- **Host Resources Agent:** Platform Service that provides SNMP access to host information for Cisco Unity Connection, using HOST-RESOURCES-MIB.
- **MIB2 Agent:** Platform Service that provides the SNMP service (RFC 1213).
- **SNMP Master Agent:** Platform Service is the SNMP protocol engine that provides authentication, authorization, and access control for SNMP requests.

www.it-ebooks.info

- **SOAP - Log Collection APIs:** SOAP Service responsible for the collection of log files and scheduling of the collection process.
- **SOAP -Performance Monitoring APIs:** SOAP Service responsible for the performance monitoring of SOAP process.
- **SOAP -Real-Time Service APIs:** SOAP Service provides the collection of real-time information, as well as, stopping, starting, and activation of the SOAP process.
- **System Application Agent:** Platform Service that provides SNMP access to applications, using the SYSAPPL-MIB.
- **Cisco AXL Web Service:** Database and Admin Service that provides the modification of database entries using AXL.
- **Cisco DirSync:** Directory Service that provides LDAP services and support for database access and synchronization.
- **Cisco Serviceability Reporter:** Performance and Monitoring Service that provides and generates reports accessed via the Cisco Unified Serviceability Tools menu.
- **Cisco UXL Web Service:** Database and Admin Service that provides authentication and authorization when using the Cisco IP Phone Address Book Synchronizer.

These services can be stopped or restarted in Cisco Unified Serviceability. Because the same RTMT is used for Cisco Unified Communications Manager, some of the services do not directly apply to Cisco Unity Connection implementations. However, it will be necessary to take a moment to review these services and the Cisco Unified Serviceability web pages. You will also notice in Figure 11-8 that the Cisco DirSync, Cisco Serviceability Reporter, and Cisco UXL Web Service are showing as Not Applicable. These services are deactivated by default.

Cisco Unified Serviceability

Services in Cisco Unified Serviceability include both the Feature and Network Services automatically started and apply to the various aspects of the Cisco Unity Connection. As stated previously, some of these services apply to Cisco Unified Communications Manager, even though they are included in the display.

To view these services, from the Cisco Unified Serviceability toolbar, select **Tools > Control Center - Network Services**, and select the desired server from the Server drop-down. The Control Center - Network Services page displays, as shown in Figure 11-9.

These services are network services that control the various aspects of the Cisco Unity Connection software and operation. These services are activated and started when the server is started. Additional services are deactivated by default and can be activated as needed. These are available in the Service Activation page in Cisco Unified Serviceability. These Services include the Cisco AXL Web Service, Cisco UXL Web Service, Cisco Serviceability Reporter, and the Cisco DirSync service. Many of the

www.it-ebooks.info

services, such as the platform service (for example, the Cisco Tomcat service) can be restarted only from the CLI.

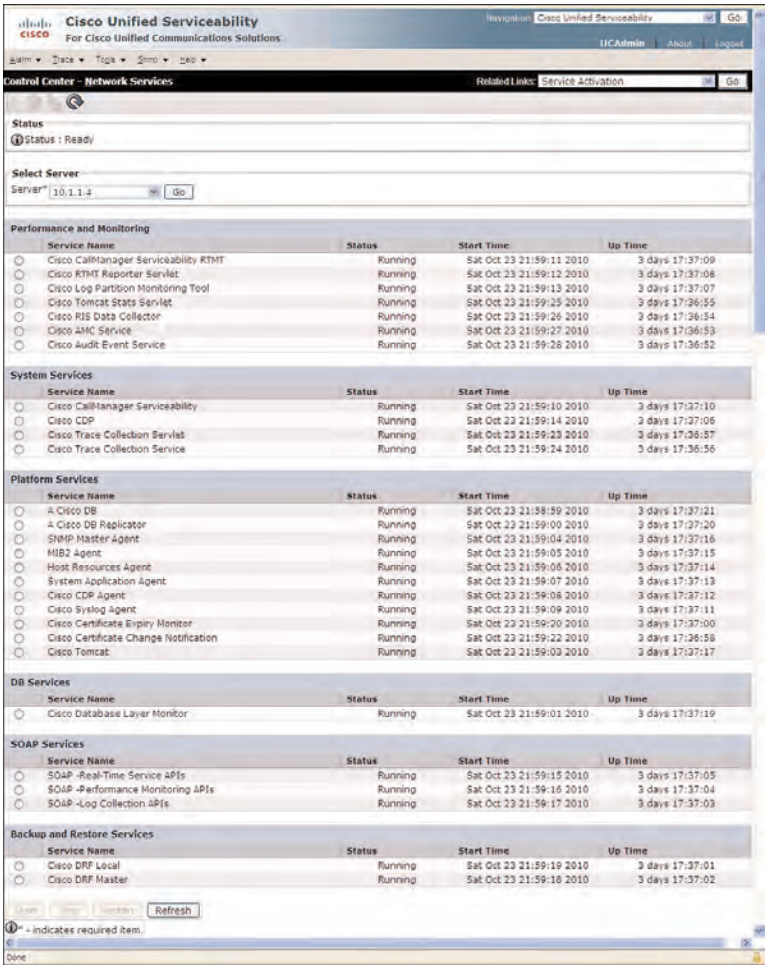

Figure 11-9 *Cisco Unified Serviceability - Control Center - Network Services*

To view these services, from the Cisco Unified Serviceability toolbar, select **Tools > Control Center - Feature Services**; then, select the desired server from the Server drop-down. The Control Center - Feature Services page displays, as shown in Figure 11-10.

Cisco Unity Connection Services—RTMT—Critical Services

You can view the services that relate directly to Cisco Unity Connection by selecting the **UnityConnection** tab at the top of the Critical Services page, as shown in Figure 11-11.

www.it-ebooks.info

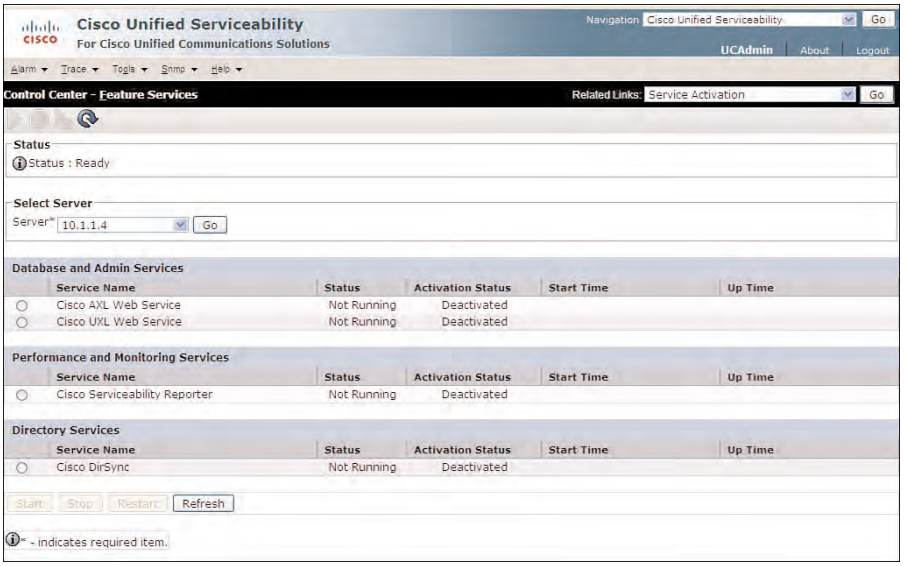

Figure 11-10 *Cisco Unified Serviceability—Control Center—Feature Services*

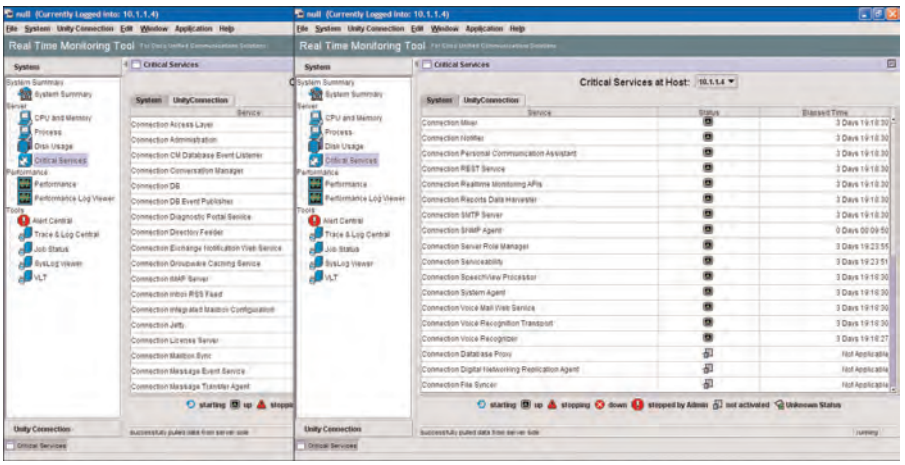

Figure 11-11 *Critical Services (UnityConnection) in RTMT*

Some of these services are critical and base services required for specific functions and applications. However, many other services are optional and required only when using specific services. The Connection Database Proxy, Connection Digital Networking Replication Agent, and Connection File Syncer show as Not Applicable. These services are deactivated by default.

www.it-ebooks.info

You can stop and restart these services using the Cisco Unity Connection Serviceability web pages. Therefore, take a moment to review these services in the Cisco Unity Connection Serviceability web pages.

Cisco Unity Connection Serviceability

Services in Cisco Unity Connection Serviceability are required to ensure the proper functionality to the various aspects of Cisco Unity Connection. To view these services, log in to the Cisco Unity Connection Serviceability website, and select the desired server from the Server drop-down. Then, from the toolbar, select **Tools > Service Management**. The **Control Center - Feature Service** page displays, as shown in Figure 11-12.

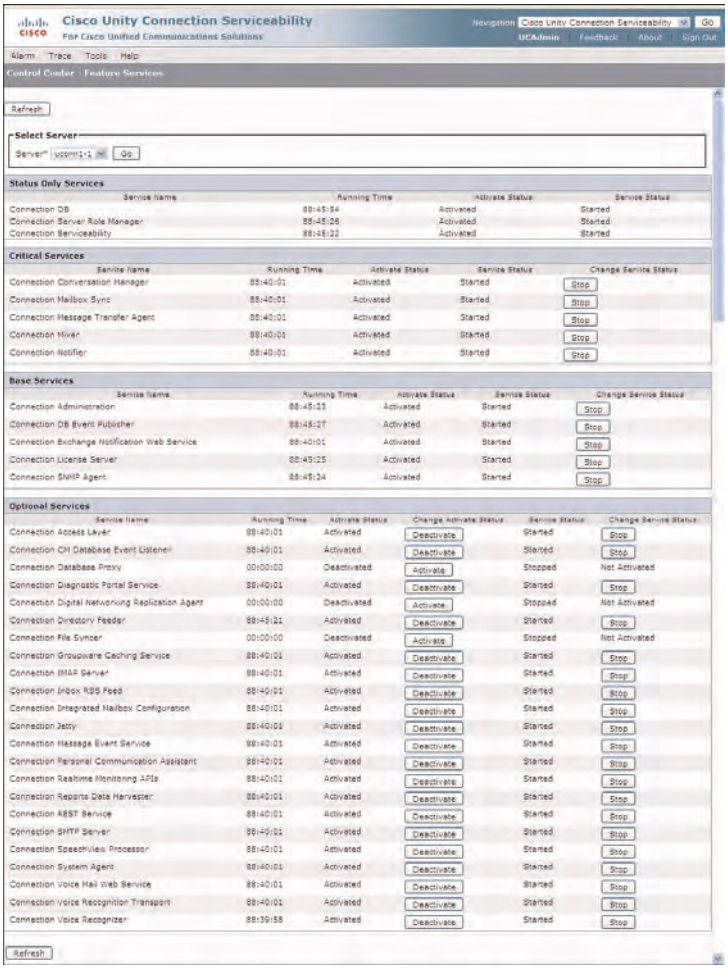

Figure 11-12 *Cisco Unity Connection Serviceability—Service Management*

www.it-ebooks.info

These various services are categorized as follows:

- **Status Only Services:** Connection DB, Connection Server Role Manager, Connection Serviceability services that displays the current status of these critical services.
- **Critical Services:** Connection Conversation Manager, Connection Mailbox Sync, Connection Message Transfer Agent, Connection Mixer, Connection Notifier.
- **Base Service:** Connection Administration, Connection DB Event Publisher, Connection Exchange Notification Web Service, Connection License Server Connection SNMP Agent. These various services provide support and performance monitoring to the various critical services.
- **Optional Services:** Noncritical service to provide the necessary support for various applications.

Case Study

For security purposes, Tiferam Corporation decided to deny access to the RSS Feed. The administrator must stop this service and verify the services using the RTMT.

Solution

Amy Price, the administrator for Tiferam Corporation has logged in to the Cisco Unity Connection Serviceability web page and accessed the Service Management page, as previously described. The Connection Inbox RSS Feed service is then stopped by selecting the **Stop** button on the Change Service Status under the Optional Services section. The Service Status changes to Stopped, and the **Stop** button changes to a **Start** button, enabling the administrator to restart the service as necessary. Figure 11-13 displays the current status of the Connection Inbox RSS Feed.

After the service is stopped, the RTMT is then used to display the current status of the service in real-time. Figure 11-14 displays the current status of the Cisco Unity Connection service. The Connection Inbox RSS Feed indicates as being **stopped by Admin**.

All services display in real-time status according to the current status of each service.

Performance

The Performance section of the RTMT tools provides access to the Performance Log Viewer enabling users to view previously collected log files, which becomes a valuable tool in troubleshooting efforts.

This section provides the ability to create customized views of the various performance monitoring counters. Performance monitoring counters monitor the various aspects of the Cisco Unity Connection services, database, message stores, and administration. The customizable views enable users to create up to six views naming each according to their needs.

www.it-ebooks.info

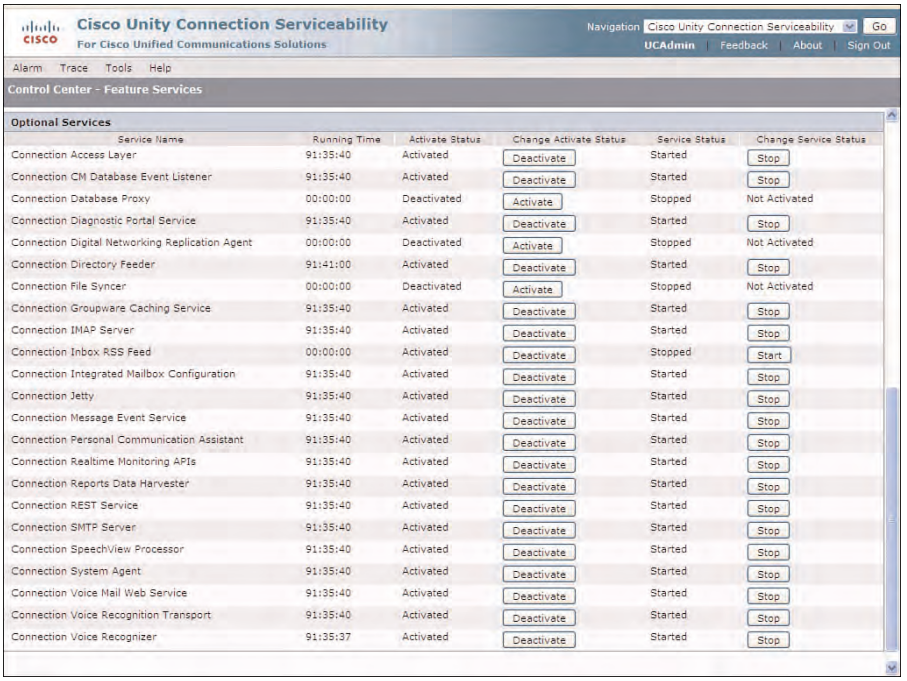

Figure 11-13 *Control Center—Feature Service—Connection Inbox RSS Service Stopped*

To create a specific view, in the System pane on the left portion of the RTMT, select **Performance** option. You can notice the current Cisco Unity Connection server or cluster indication. Select the icon next to IP address of the server to expand the listing of performance monitoring counter categories. Each category contains one or more performance monitoring counters that can be selected to be added to the display. In Figure 11-15, the CUC Message Store category was selected revealing the various performance monitoring counters that relate to the message store.

When you right-click a specific performance monitoring counter, a pop-up box enables you to either add the performance monitoring counter to the view on the right or display the description of the counter. You can also simply double-click a counter to have it automatically added to the view. When added to the view, the monitoring of the wanted aspect begins displaying real-time details of the each performance monitoring counter. In Figure 11-16, the Messages Delivered Total under the CUC Message Store was selected, and the counter description. From this display, you can see that there are a total of 11 messages delivered to various mailboxes in the current message store.

www.it-ebooks.info

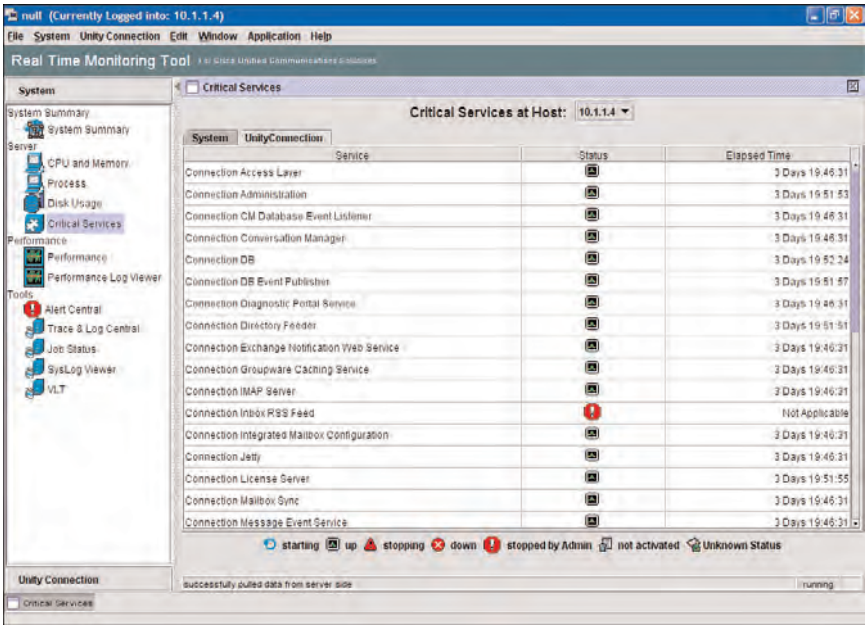

Figure 11-14 *RTMT Showing the Connection Inbox RSS Feed Being Stopped*

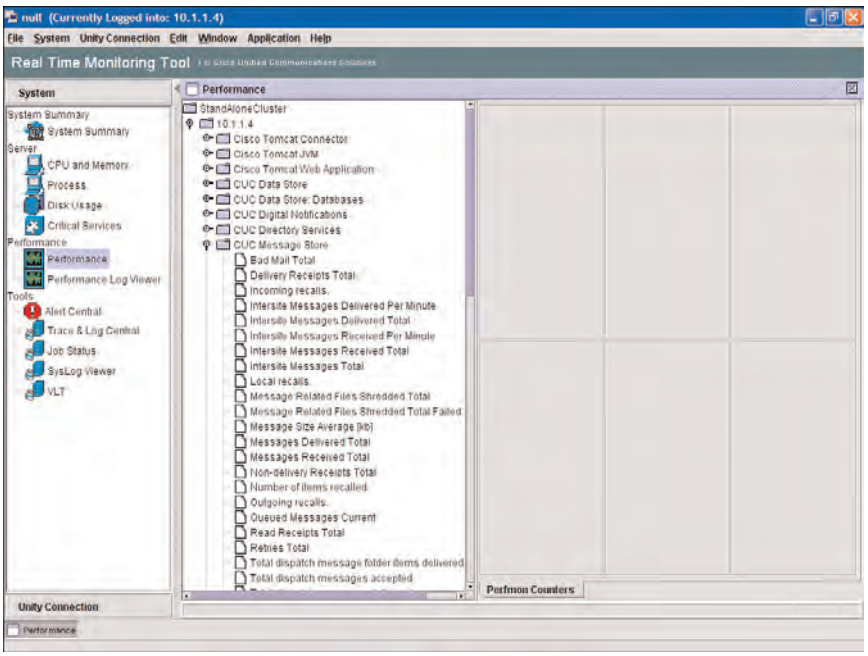

Figure 11-15 *Performance Monitoring Using the RTMT*

www.it-ebooks.info

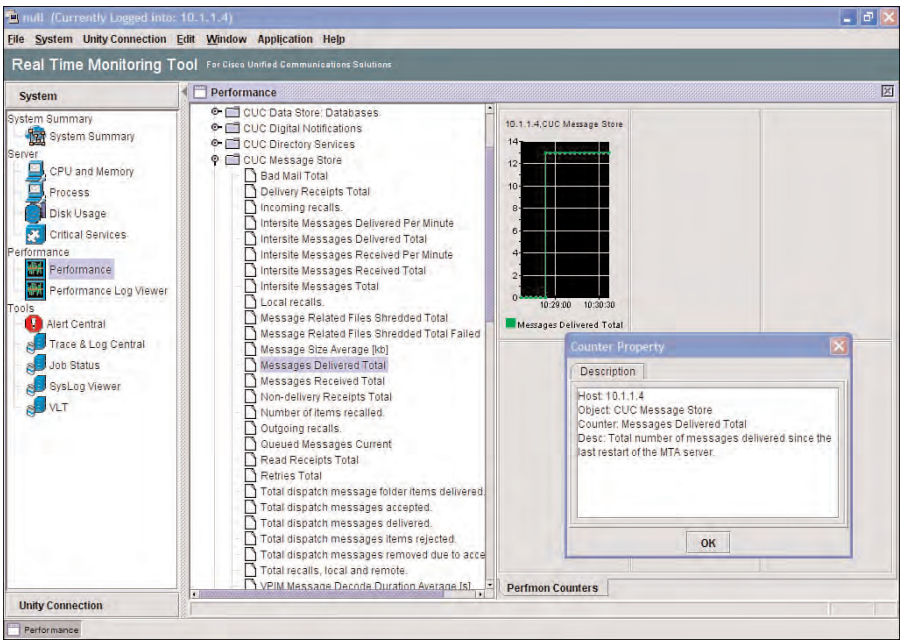

Figure 11-16 *Performance Monitoring Counter for Messages Delivered Total*

In Figure 11-17, three more performance monitoring counters for message received non-delivery receipts, and the average message size were selected. You can also retrieve more specific information by double-clicking on a specific graph. In this example, the Message Size Average was selected. A pop-up now displays specific information about the details of the performance monitoring counter selected.

Finally, each view can be renamed and other views created as needed, by right-clicking the tab for the specific view. In this example, the view has been renamed from Performance monitoring Counter to Message Store because this specific view contains information and counters that relate directly to the message store.

In this section, you learned how to make the various selections using the options and icons in the RTMT and right-clicking and selecting the desired feature. You can also use various options from the RTMT toolbar to complete much of the same operations.

After you complete creating the views, monitoring begins automatically as each counter is selected. However, exiting out of RTMT can cause the views to be lost unless you save your configuration options to a profile.

To save the current views to a profile, from the RTMT toolbar, select **File > Profile**. The Profile pop-up page displays. From this page, you can choose to save your selections as the default or a new profile, and add a description to the profile. Select the **Save** button and choose to save the view as a new name. After you save the view, you can use the

www.it-ebooks.info

Restore button at any time while using RTMT to revert to this saved view. Finally, you can remove a profile at any time by selecting the **Delete** button.

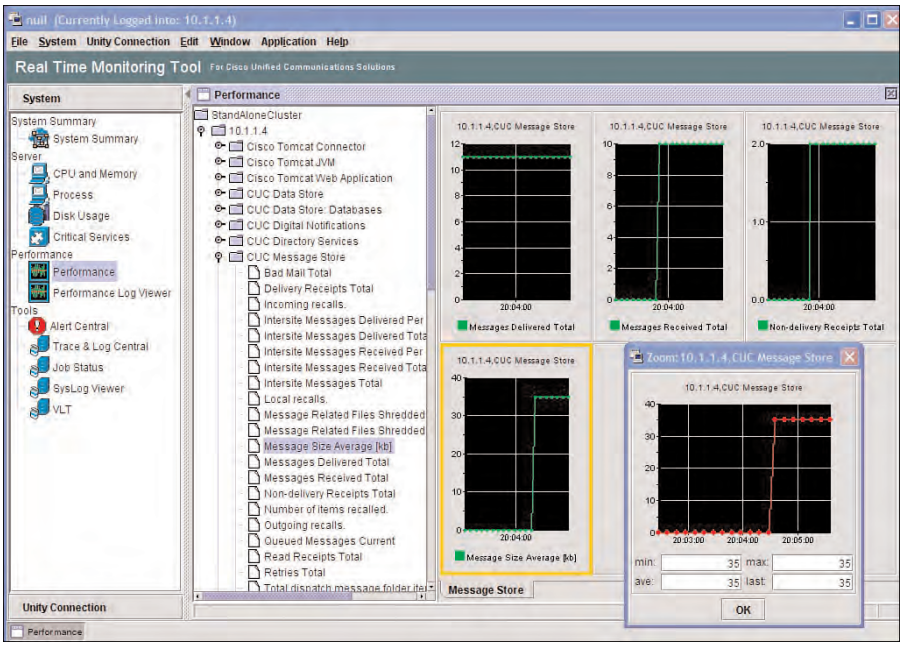

Figure 11-17 *Message Store Performance monitoring Counters View Created in RTMT*

The next time you start the RTMT, the **Select Configuration** pop-up displays the saved profiles. In Figure 11-18, the Message Store Monitoring profile is selected. The description of the profile displays. After you select the profile by double-clicking the profile or selecting it and clicking **OK**, the RTMT opens with the saved performance monitoring counters and views.

Performance Log Viewer

The Performance Log Viewer provides the ability to view collected log files. These can either be the local performance monitoring logs or the Realtime Information Server Data Collection (RisDC) logs. The local performance monitoring logs are created from information and data stored locally on the administrator workstation.

To view use the Performance Log Viewer, from the System pane on the left portion of the RTMT tool, select the **Performance Log Viewer** option. From the RTMT toolbar, you can also select **System > Performance > Open Performance Log Viewer**.

To view the RisDC Performance monitoring Logs, select the **RisDC Perfmon Logs** radio button and select the desired server from the drop-down box. After you select the **Open**

www.it-ebooks.info

button, a pop-up window displays the collected CSV log files. Select a file and select the **Open File** button, as shown in Figure 11-19.

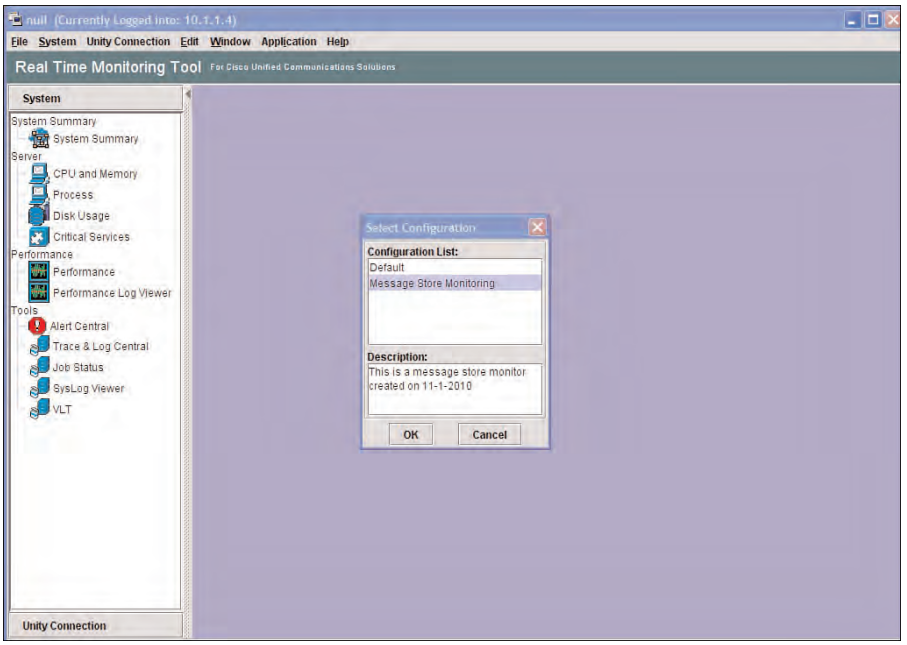

Figure 11-18 *Profile Selection Using the RTMT*

After selecting the wanted CSV file, the **Select Counters** pop-up window displays enabling the user to choose which performance monitoring counters should display. Multiple counters can be displayed and viewed. In Figure 11-20, the percentage of CPU Time is selected for the various selections by clicking the check box to the right of the desired performance monitoring counter. Complete the operation by selecting **OK**.

The selected performance monitoring counters from the chosen RisDC log files now displays the graph window in different colors. Users can right-click the color chart and change colors as needed and highlight the specific counter, as demonstrated in Figure 11-21. In the display, the performance monitoring counter for the percentage of CPU Time for the active partition is highlighted and changed to a violet color for easy reading.

The user can further edit the graph or minimize the display as needed. In Figure 11-22, all the performance monitoring counters were unselected in the chart displayed at the bottom of the page. Then, the mouse was dragged over a portion of the graph. In this case, the selection was made from 14:00 through 14:30 and from Y-values of zero to 3 percent.

This feature enables the engineer to troubleshoot issues that occur in previous time intervals.

www.it-ebooks.info

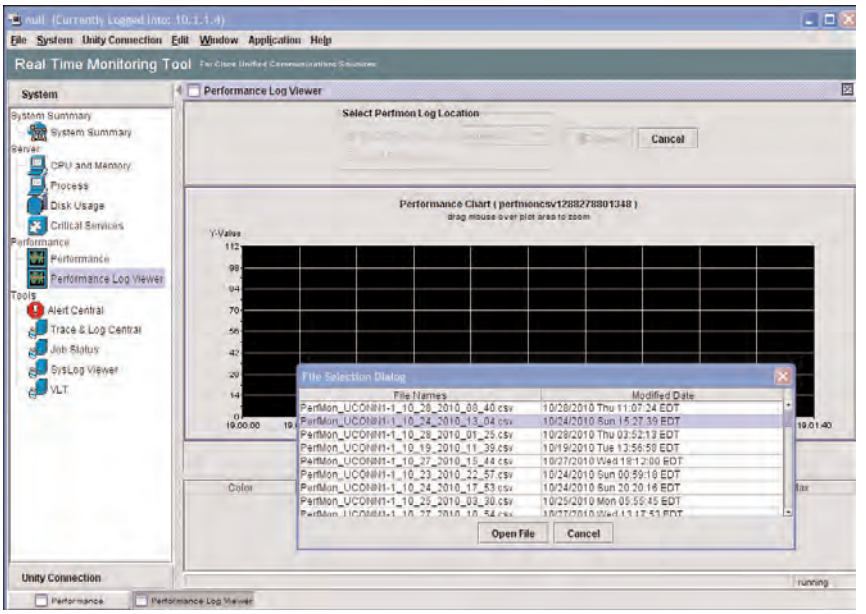

Figure 11-19 *Performance Log Viewer Setup in RTMT*

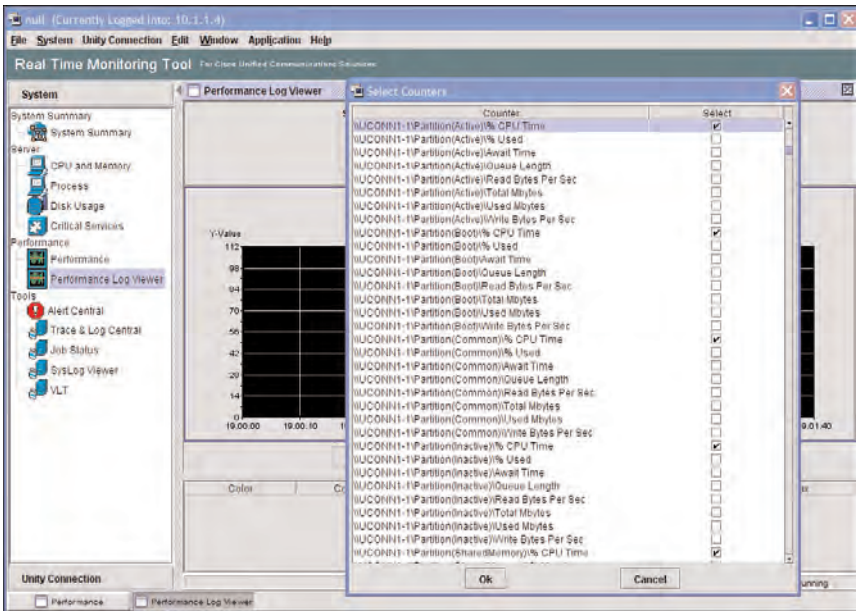

Figure 11-20 *Performance Monitoring Counter Selection in the Performance Log Viewer of RTMT*

www.it-ebooks.info

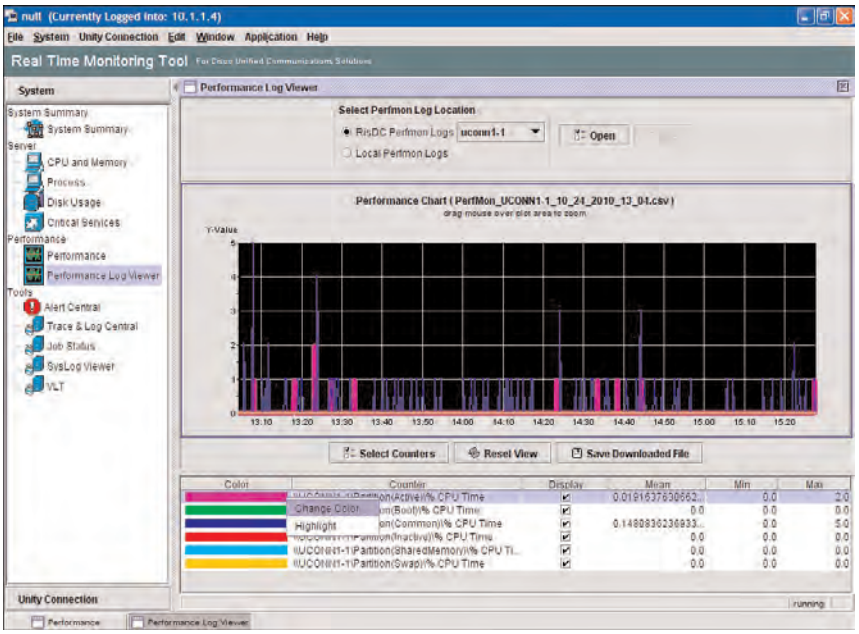

Figure 11-21 *Changing Colors in the Performance Log Viewer*

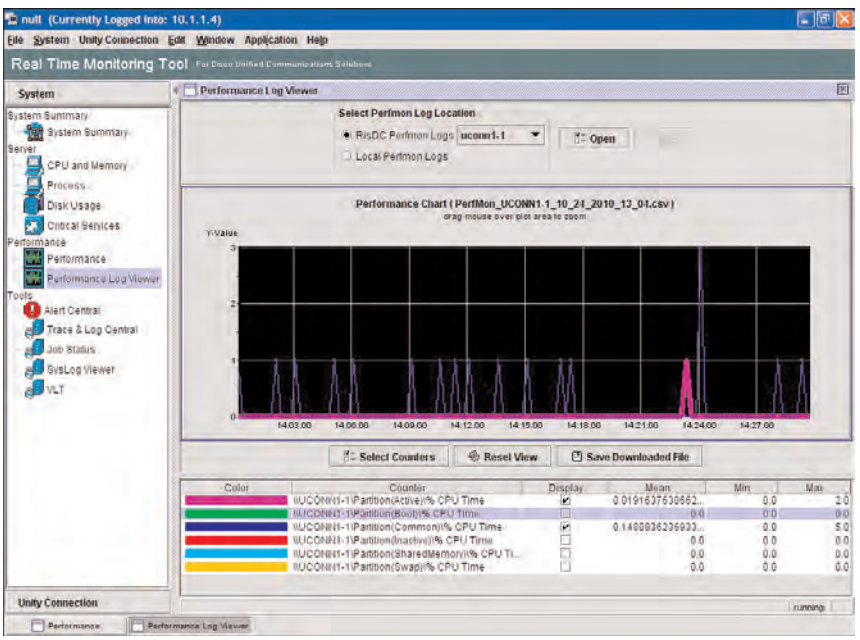

Figure 11-22 *Zoom Feature Using the Performance Log Viewer*

www.it-ebooks.info

Tools

The Tools section includes the Alert Central, Trace & Log Central, Job Status, and SysLog Viewer as they relate directly to Cisco Unity Connection.

Alert Central

The Alert Central displays a listing of current alerts and a history of past alerts. Alerts are defined to notify engineers and administrators of impending conditions that exist. These alerts can either be predefined or user-defined based on specific alert properties. RTMT can also be configured to send email notifications based on an active alert.

Alerts are configured for specific performance monitoring counters using value thresholds and set alert properties. Depending on the type of counter used, the thresholds and properties can be based on a specific threshold, duration, frequency, or the like. There are alerts configured for both System and UnityConnection. The UnityConnection alerts are preconfigured and cannot be edited. However, the System alerts can be changed by highlighting the desired alert, right-clicking and selecting the **Set Alert/Properties** option. Optionally, you could highlight the alert and select **System > Tools > Alerts > Set Alert/Properties** from the RTMT toolbar. The Alert Properties pop-up window displays, enabling the user to view and change the various thresholds, frequency, and details of the alert. In Figure 11-23, the **LowActivePartitionAvailableDiskSpace** alert is selected. The description of the alert provides the user with the details about the alert, which are as follows:

```
This alert occurs when the percentage of available disk space of the Active
 Partition is lower than the configured value.
```

In Figure 11-23, the **SyslogSeverityMatchFound** alert displays in red indicating that an alert was active in the past history. The history displays the date that the alert was raised.

The RTMT application can also be set up to send an email or page to the administrator for a specifically configured alert notification.

Trace & Log Central

The Trace & Log Central portion of the RTMT is a powerful feature for troubleshooting that enables the user to not only view the various log files, but also to view real-time traces in much the same way that the tool is used with Cisco Unified Communication Manager.

To view the trace files in real-time, you need to configure the trace options in Cisco Unified Serviceability. To complete this operation, log in to Cisco Unified Serviceability and select **Trace > Configuration** to display the Trace Configuration page. Select the Server, Service Group, and Service from their respective drop-downs. The level tracing can be changed from Info to either **Debug**, **Warn**, **Error**, or **Fatal** depending on the level of information desired that should be included in the trace. By selecting **Info** or **Debug**, more information is included in the display. This might not be desirable for viewing a trace. Therefore, to view specific issues or problems, select **Warn**, **Error**, or **Fatal**. If you work directly with the Cisco TAC, it informs the administrator what level of tracing to use.

www.it-ebooks.info

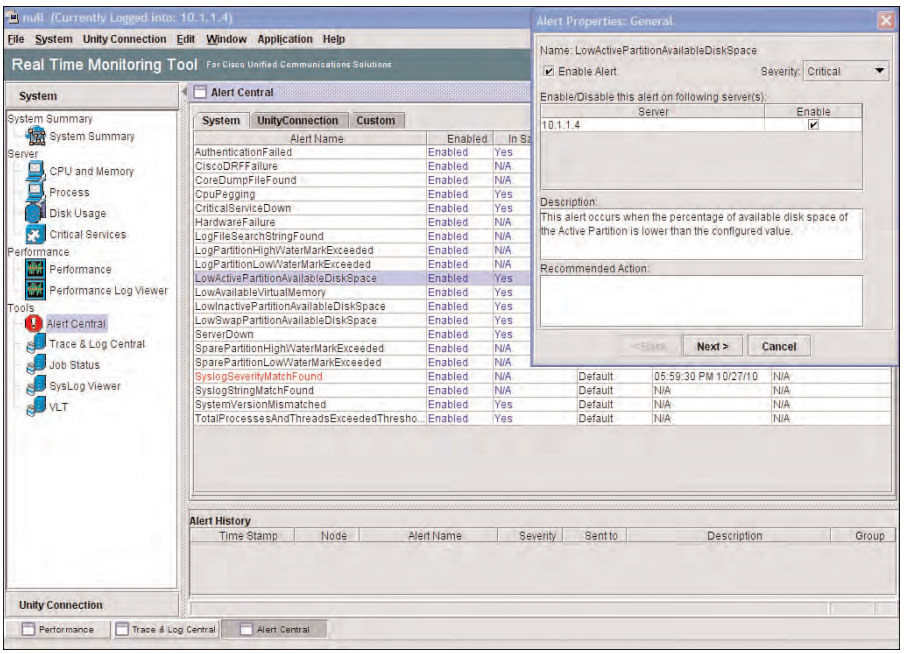

Figure 11-23 *Set Alert Properties in the Alert Central Tool in RTMT*

When the trace configuration is completed, select the **Save** option. In Figure 11-24, the Performance and Monitoring Service was selected for the Cisco AMC Service on 10.1.1.4.

After the trace configuration is complete, return to the Trace & Log Central page and select the **Real Time Trace > View Real Time Data** option in RTMT by double-clicking this option. Then, from the pop-up menu, you need to select the Node, Product, Services, and Trace File Type. In this example, the specific server was selected with System, Cisco AMC Service, and the log4j file type, as shown in Figure 11-25.

When the selections are complete, you need to click **Finish** . At this point, the log viewer displays the real-time trace information. You can change the auto-scrolling option, clear the display, and perform a search by selecting the respective option on the page. The search feature is a powerful option enabling the user to quickly find specific information. A search was performed on Perfmon Object, as displayed in Figure 11-26. The search matches are highlighted in color.

The Trace & Log Central tool also enables the user to browse remote or local log files and schedule the collection of information for log files. The schedule collection option enables the user to schedule as many as six concurrent activities for collecting trace files and download these files to an SFTP or FTP server.

www.it-ebooks.info

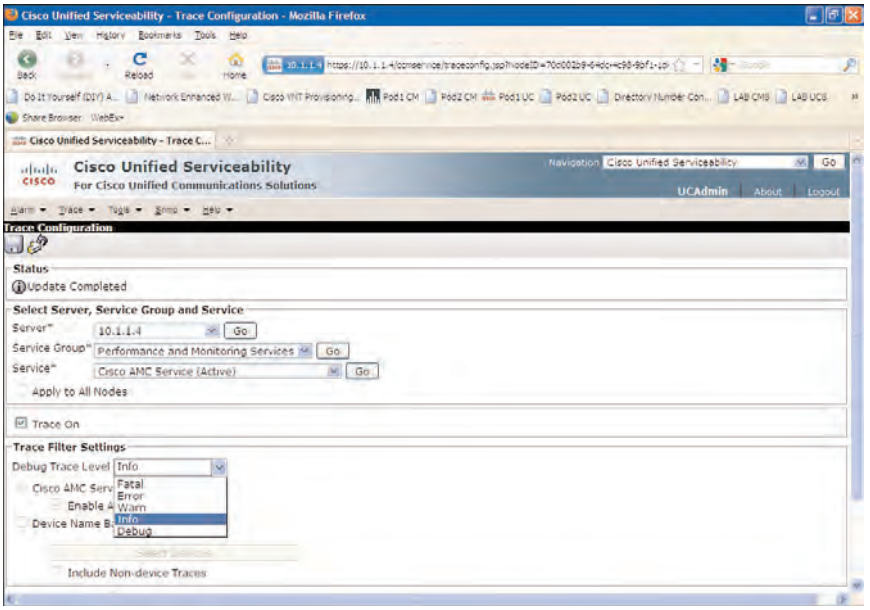

Figure 11-24 *Trace Configuration in Cisco Unified Serviceability*

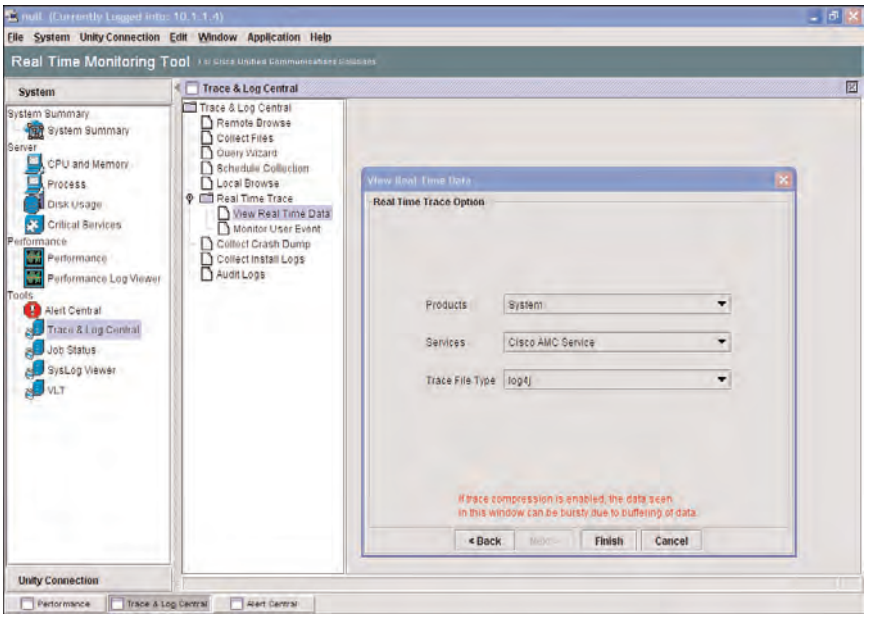

Figure 11-25 *Trace and Log Central Setup for Viewing Real Time Data*

www.it-ebooks.info

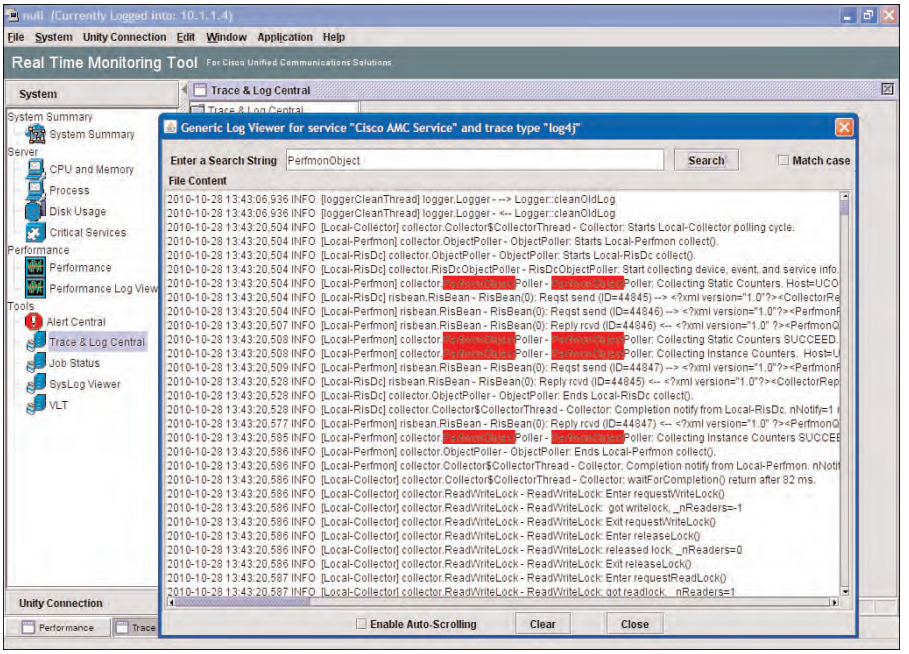

Figure 11-26 *Real-Time Log Viewer in the Trace & Log Central Tool*

Job Status

The Job Status section of the RTMT tool enables the user to view the status of current operations. To use the Job Status feature, from the System pane, select the **Job Status** option, or from the RTMT toolbar, select **System > Trace > Job Status**.

In Figure 11-27, the Job Status section displays three canceled operations and two currently running operations. By double-clicking an entry, a pop-up displays the specifics as shown in the display. In this case, the Job Status indicates two instances of the log viewer are currently open.

SysLog Viewer

The SysLog Viewer is an easy way to view the various system, application, and security log files using RTMT without having to resort to using an external SysLog server. To use the SysLog Viewer, from the System pane in RTMT, select the SysLog Viewer, or from the RTMT toolbar, select **System > Tools > SysLog Viewer > Open SysLog Viewer**. In Figure 11-28, the **CiscoSyslog** application log is selected for the uconn1-1 server. The lower portion screen provides a time-stamped listing of the various collected logs.

www.it-ebooks.info

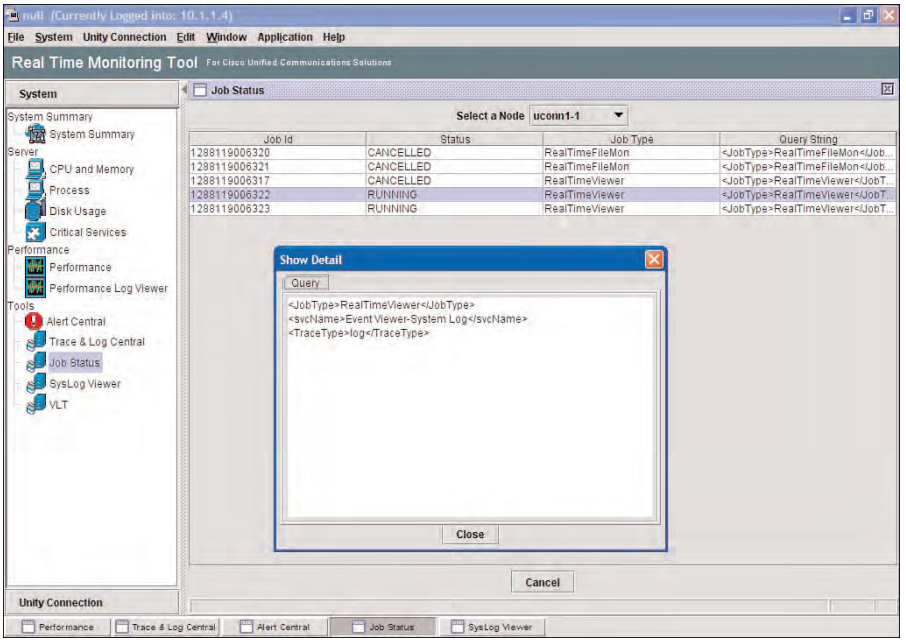

Figure 11-27 *Job Status Tool in RTMT*

From this page, you can double-click any of the specific entries to view the details and provide a more detailed description of the log entry. In Figure 11-29, a selected entry was selected, where the Show Detail pop-up description now displays. Also, the user can scroll through the various entries by selecting the Up and Down arrows.

The RTMT is a powerful, multifaceted tool that enables engineers to view and troubleshoot the operations of Cisco Unity Connection servers and cluster pairs. Users need to become familiar with this tool during normal operation to understand the current operations and acceptable benchmarks for your system.

Cisco Object Backup and Restore Application Suite (COBRAS)

Cisco Object Backup and Restore Application Suite (COBRAS) provides an external application that runs on the administrator's workstation and provides a tool to migrate user data and messages from earlier version of specific voice-messaging systems to the current Cisco Unity Connection server. You can use COBRAS to migrate users from the following systems:

- Cisco Unity 4.0(5) or later
- Cisco Unity Connection 1.2

www.it-ebooks.info

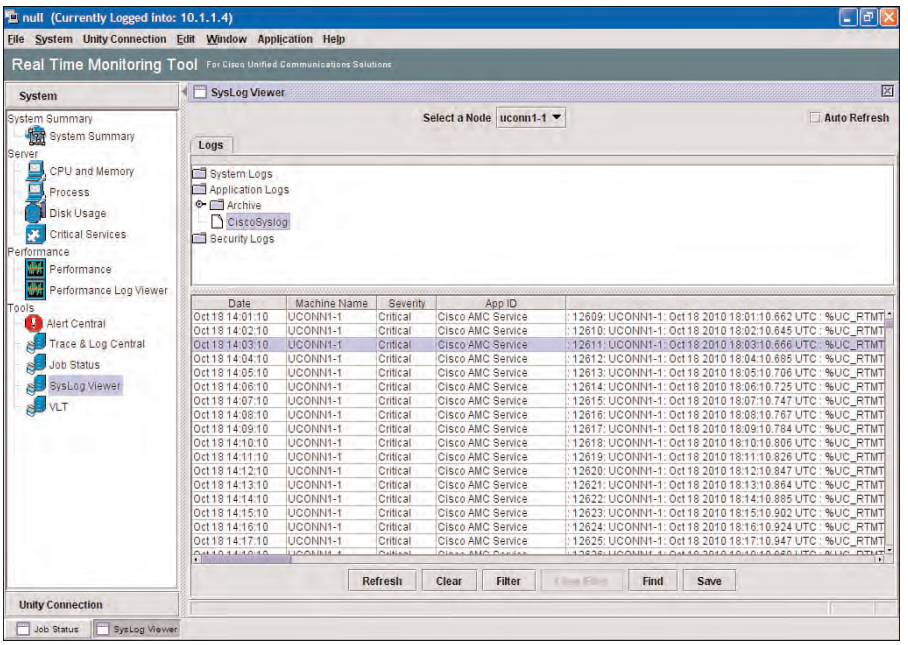

Figure 11-28 *SysLog Viewer Used to Display the CiscoSyslog Application Log File*

There is no option for backup from Cisco Unity Connection 2.x versions using COBRAS, however. Also, for Cisco Unity 4.0(4) and earlier, the Migrate Utility in Cisco Unity Connection provides the necessary resources for these operations.

COBRAS provides a complete set of tools to migrate users and perform a partial backup and restore to different versions of Cisco Unity Connection as required. The backup operation in COBRAS is different than the backup performed using the DRS tools because COBRAS is not designed to perform a full backup and restore. The purpose of COBRAS is to provide a partial restore operation by performing a merge of data to an existing Cisco Unity Connection server. COBRAS uses a Microsoft Access database operation to perform the backup storage medium to the administrator's workstation for the merge operations. Figure 11-30 provides an overview of the merge operation using COBRAS.

COBRAS includes a backup of call handlers, subscribers, interview handlers, public distribution lists, and schedules. It does not include class of service (CoS), restriction tables, directory handlers, locations, contacts, holidays, policies, and subscriber templates. Therefore, these options need to be configured manually or through the Bulk Administration/Bulk Edit utilities after the COBRAS operation has been completed.

www.it-ebooks.info

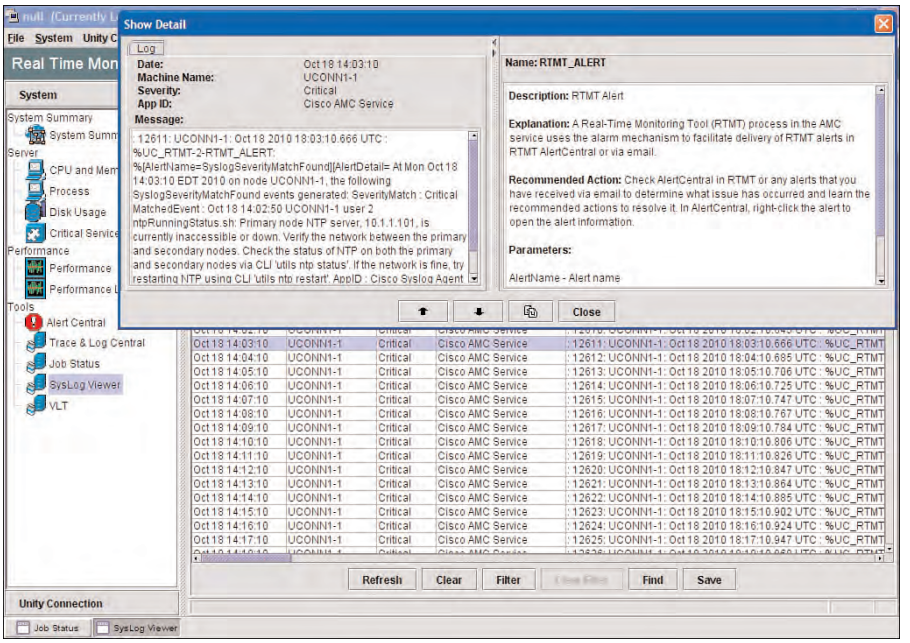

Figure 11-29 *Show Details for the SysLog Viewer in RTMT*

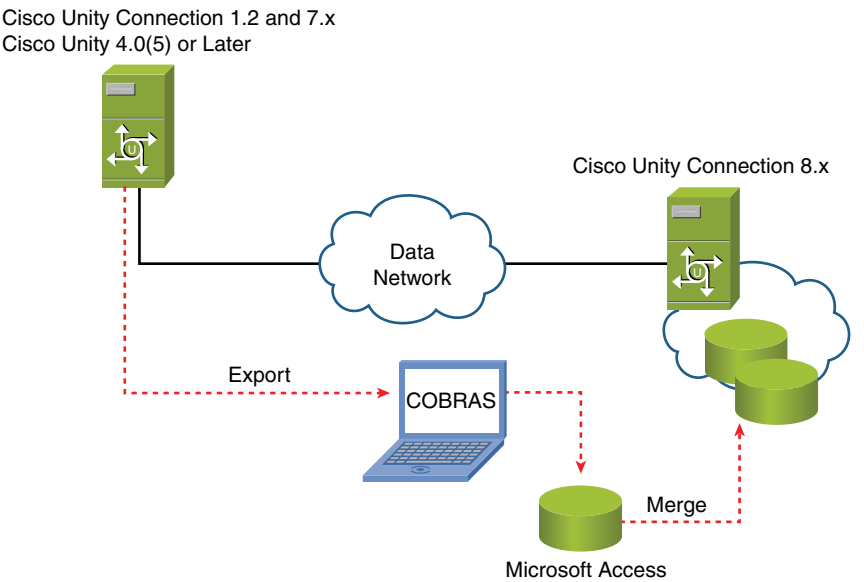

Figure 11-30 *Merge Operation Using COBRAS to Migrate Users and Messages*

www.it-ebooks.info

Use COBRAS in two different modes:

- **Hot mode:** Used when migrating users from Cisco Unity to Cisco Unity Connection, when Cisco Unity runs in Exchange. In Hot mode, both servers (backup and restore targets) must be accessible for proper Hot mode operation. In Hot mode, the users are actually moved from the backup to the target server; therefore, changes are made directly to the Cisco Unity server during the Hot mode operation with COBRAS.
- **Briefcase mode:** Provides the ability to perform a backup from an earlier version and partially restored to multiple targets or as many times as needed. In Briefcase mode, the backup can be performed as a completely separate operation. In this case, the backup server does not need to be available during the restore or merge operation.

To begin to use the COBRAS, you need to download the COBRAS Export utility from www.ciscounitytools.com, as shown in Figure 11-31. COBRAS has a specific version for each different server. Therefore, you need to ensure that you download the proper version of COBRAS for your specific server installation.

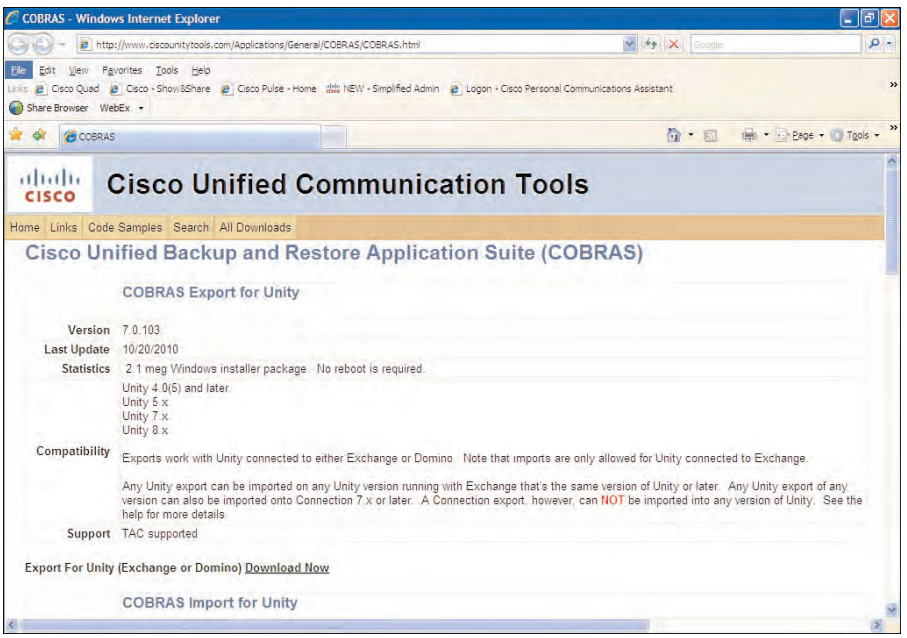

Figure 11-31 *COBRAS Export Utility Download*

Not many options are available to complete for the backup because COBRAS captures the entire directory structure when performing a backup. After you export the necessary information using the COBRAS Export Utility, you need to access the COBRAS Import

www.it-ebooks.info

Utility from www.ciscounitytools.com and import the wanted data to Cisco Unity Connection. Figure 11-32 shows the download operation.

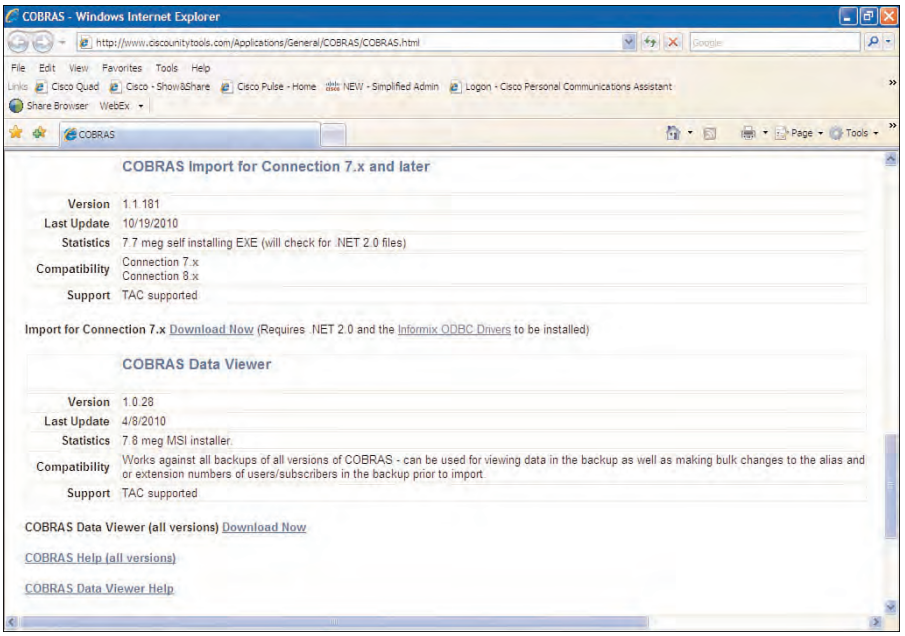

Figure 11-32 *Download COBRAS Import Utility*

After you download the COBRAS Import utility, you also need to download and install the ODBC drivers to the administrator workstation. Before starting the installation, you need to allow access to Cisco Unity Connection from COBRAS to import the wanted data.

The user chosen for authentication must have remote administrator right (assigned to the remote administrator role). To assign the user to remote administrator role, select the user from the Search Users page in Cisco Unity Connection Administration. The chosen user can be an existing or new user with a mailbox or an administrative user without a mailbox.

On the Edit User Basics page, select **Edit > Roles** from the toolbar. The Edit Roles page displays. From the Available Roles pane, Select the **Remote Administrator** role, and click the Up arrow to move this role to the Assigned Roles pane, as shown in Figure 11-33. In this case, the **UCAdmin** user was selected to be the Remote Administrator from which COBRAS uses to authenticate.

COBRAS is actually functioning as a proxy to the database to perform the merge operation; therefore, the Database Proxy option must be allowed in Cisco Unity Connection Administration. This is completed by selecting **System Settings > Advanced > Connection Administration**. The **Database Proxy: Service Shutdown Timer (in days)**

www.it-ebooks.info

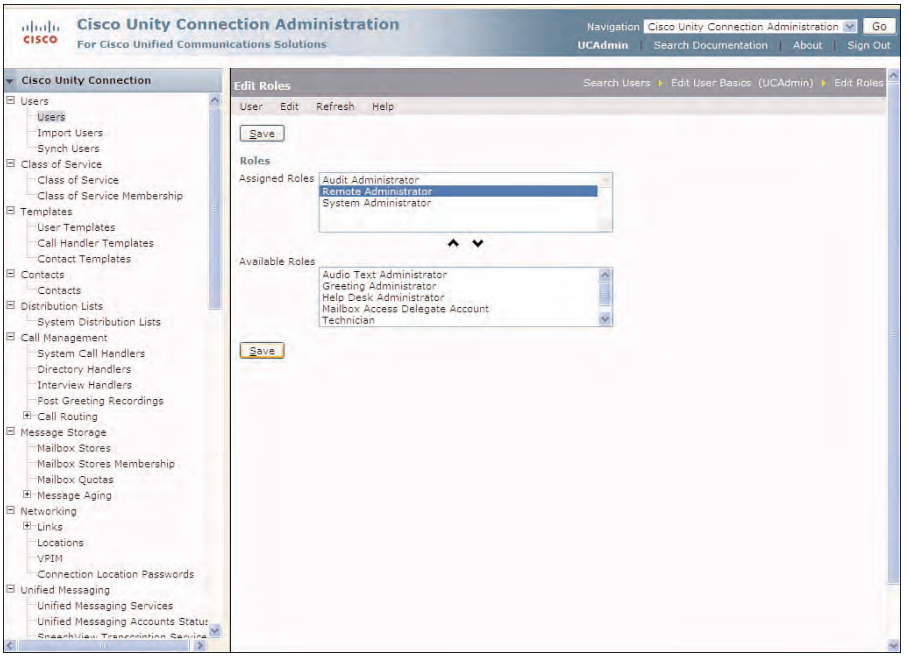

Figure 11-33 *Edit Roles Page for the Remote Administrator Role*

must be enabled to access to the COBRAS utility. This option provides security to automatically disable the database proxy after a set amount of days.

Finally, the Connection Database Proxy service must be activated under the Optional Services in the **Tools > Service Management** section of the Cisco Unity Connection Serviceability web page.

After these steps have been completed, open the COBRAS Import utility to begin the import operation. The COBRAS Import utility displays, as shown in Figure 11-34. Select the database file that was exported by browsing to the desired file. The Cisco Unity Connection information displays in the upper section (the target server), followed by information of the server from where the file was exported.

You need to select the **Next** button. The wizard begins by presenting a series of 32 pages of options, where the user can select which subscribers and objects are to be imported to Cisco Unity Connection. After the import operation has been completed, the COBRAS utility can be closed.

Cisco Unity Connection Migrate Utilities

Use the migrate message utility to migrate users and messages to Cisco Unity Connection 8.x servers. However, it is recommended to use COBRAS because COBRAS migrates more data than the Migrate Utilities in Cisco Unity Connection Administration.

www.it-ebooks.info

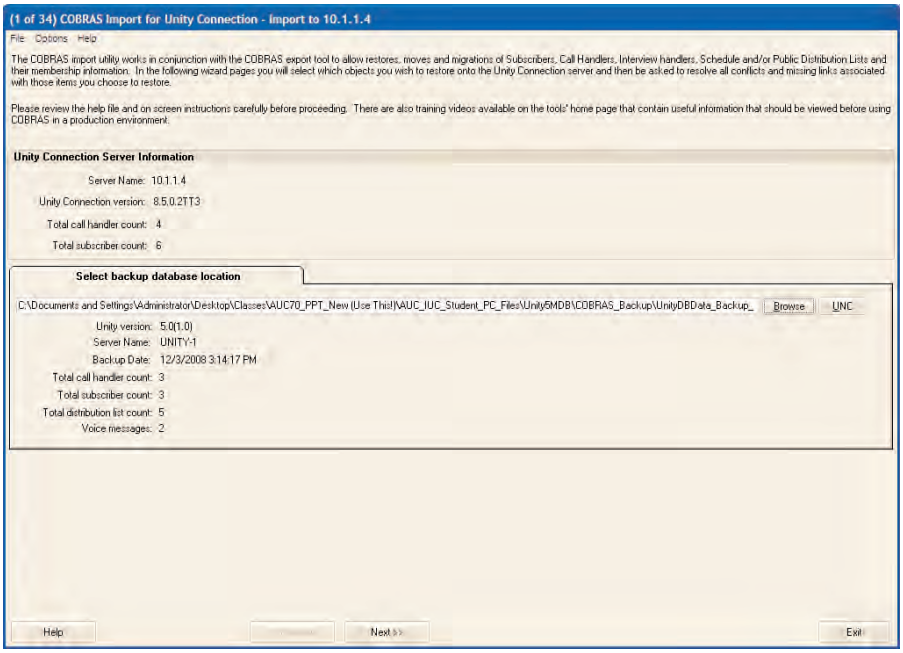

Figure 11-34 *COBRAS Import Utility*

Also, COBRAS does not require that an SSH server be configured. If you decide to migrate messages, you must first migrate users before performing this operation.

To use the migrate utilities, from the navigation pane in Cisco Unity Connection Administration, select **Migrate Utilities > Migrate Users**. The Migrate Users page displays, as shown in Figure 11-35.

You need to import the specific information using SSH. Complete the Migrate Messages operation in much the same way by selecting **Migrate Utility > Migrate Messages**.

Cisco Unity Connection Task Management Tool

Task Management in Cisco Unity Connection Administration displays the various system maintenance and troubleshooting tasks. These tasks are optimized to automatically run on a specific schedule. Because these tasks are already optimized for functionality and performance, you should not change these options. A number of these tasks are critical to the operation of Cisco Unity Connection.

To view the Task Management pages, in Cisco Unity Connection Administration, select **Tools > Task Management**. Figure 11-36 shows the Task Definitions page.

www.it-ebooks.info

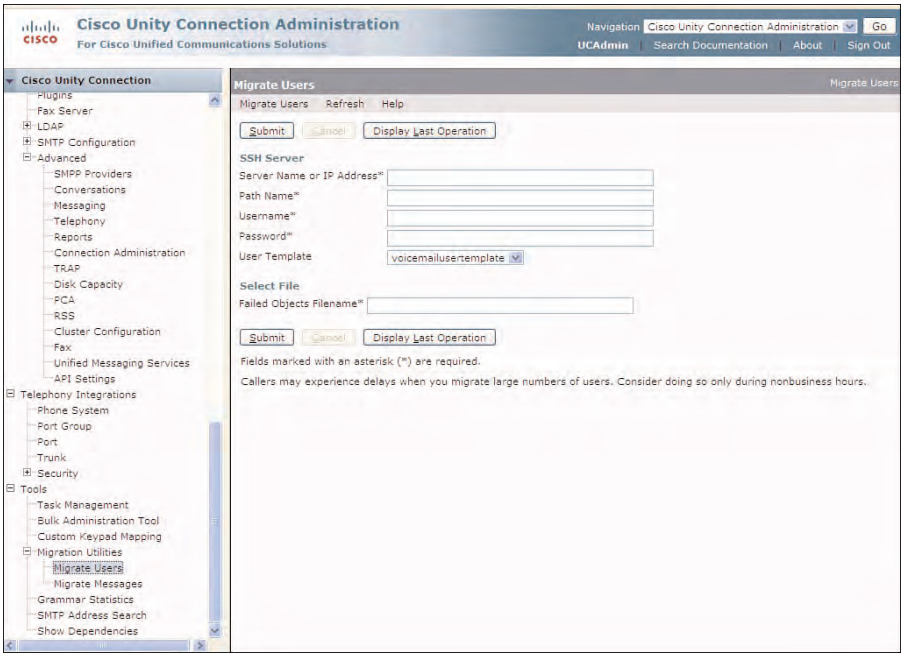

Figure 11-35 *Migrate Users Operation in Cisco Unity Connection Administration*

By selecting a specific task, you can to view the system task results and the predefined schedule for each task. In Figure 11-37, the task definition for checking the telephone configuration page is selected. Notice by the Summary that this task is responsible to check for potential problems or conflicts. Any issues located are indicated in the Alert Central of the RTMT and through configurable SNMP alerts.

To review the task schedule for a task definition, from the toolbar, select **Edit > Task Schedule**. Figure 11-38 shows the Task Schedule for the Check Telephony Configuration. This task is scheduled automatically to run by default at 2:15 a.m. every day. As noted previously, all system tasks are optimized to maintain the best possible performance. Therefore, it is not necessary, nor advisable, to modify these schedules.

Understanding Reports

You can select a number of reports to run directly from Cisco Unity Connection. These reports can assist engineers and administrator with troubleshooting and administration and can display in a number of different formats including HTML, PDF, or CSV formats.

www.it-ebooks.info

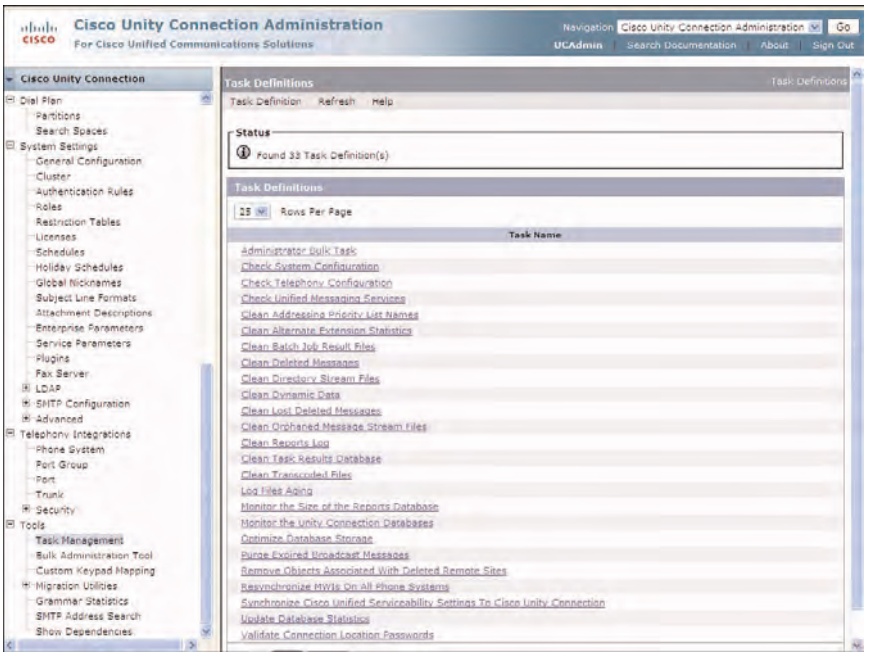

Figure 11-36 *Task Definitions Page in Cisco Unity Connection Administration*

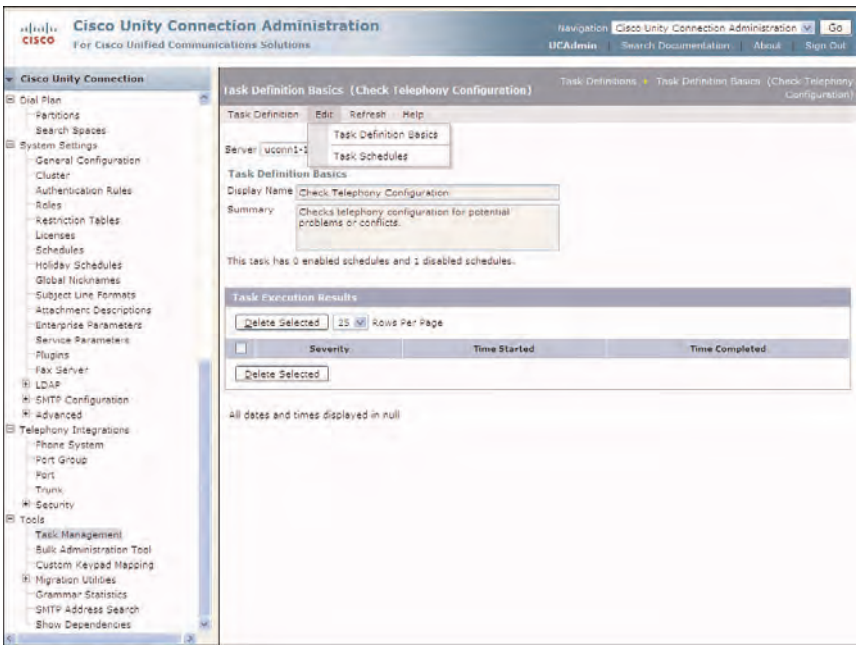

Figure 11-37 *Task Definition Basics Page for the Check Telephony Integration Task*

www.it-ebooks.info

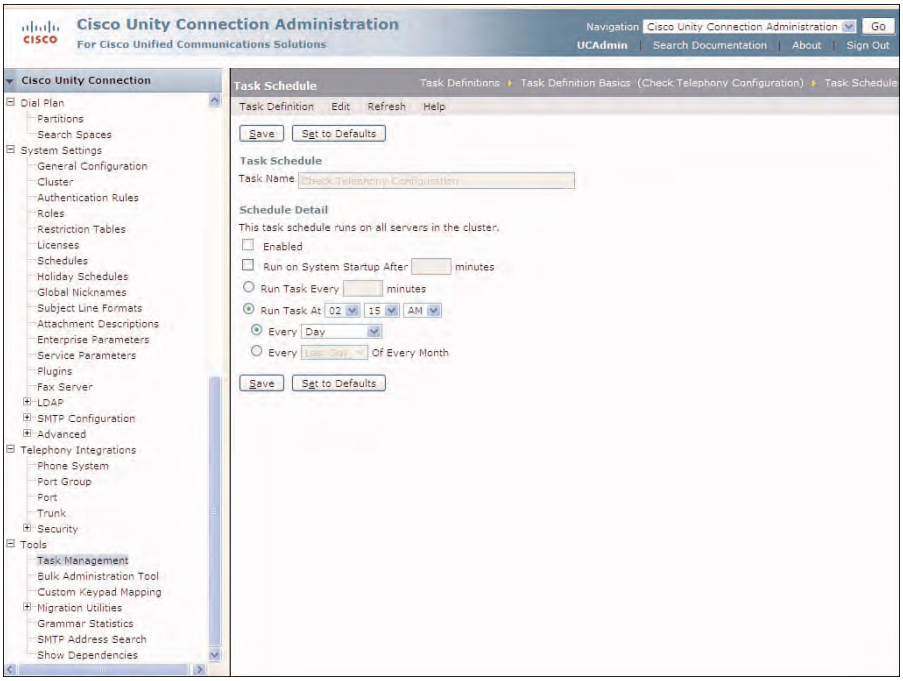

Figure 11-38 *Task Schedule for the Check Telephony Configuration Task*

To view the available reports, from the Cisco Unity Connection Serviceability toolbar, select **Tools > Reports.** Figure 11-39 shows the Serviceability Reports page.

The available reports in Cisco Unity Connection Serviceability are as follows:

- Phone Interface Failed Logon Report
- Users Report
- Message Traffic Report
- Mailbox Store Report
- Dial Plan Report
- Dial Search Scope Report
- User Phone Login and MWI Report
- User Message Activity Report
- Distribution List Report
- User Lockout Report

www.it-ebooks.info

- Unused Voicemail Accounts Report
- Transfer Call Billing Report
- Outcall Billing Details Report
- Outcall Billing Summary Report
- Call Handler Traffic Report
- System Configuration Report
- SpeechView Activity Report By User
- SpeechView Activity Summary Report

Figure 11-39 *Serviceability Reports Page*

To view the Users Report, from the Serviceability Reports page, select the report. The Users Reports page displays, enabling the user to decide the format type for the report. In this case, the HTML format is selected for all users, as shown in Figure 11-40.

Finally, select the **Generate Reports** button to display the report. Figure 11-41 shows the final product for the User Report formatted in HTML format.

www.it-ebooks.info

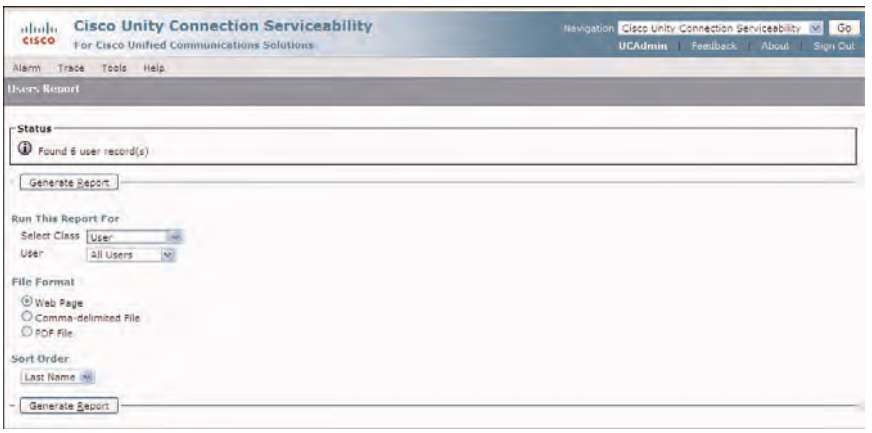

Figure 11-40 *Users Report Page in Cisco Unity Connection*

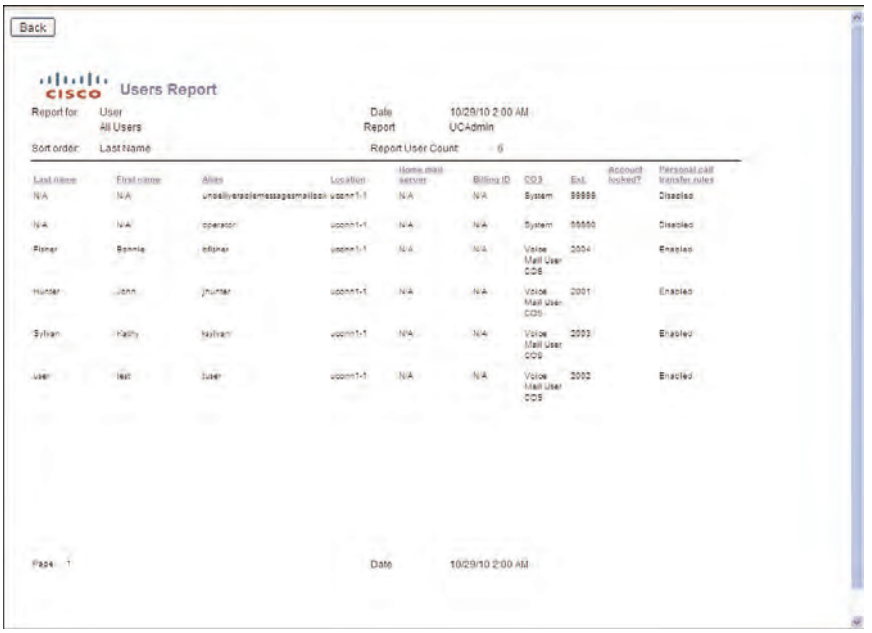

Figure 11-41 *HTML-Formatted User Report*

www.it-ebooks.info

When using external tools to view data, or when reports include a large amount of data, use the comma separated values (CSV) format and choose to run these reports during nonbusiness hours or a maintenance window to avoid any negative impact on server performance.

It might be advantageous to limit the number of records in reports and the length of time that report data should be kept. You can view and modify these parameters by selecting **System Settings > Advanced > Reports** in Cisco Unity Connection Administration, as shown in Figure 11-42.

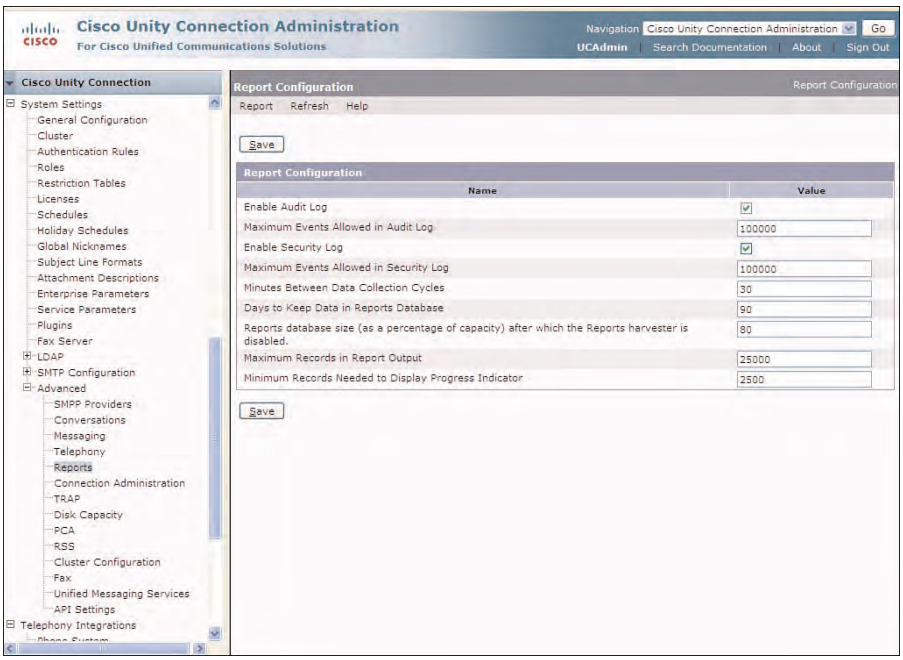

Figure 11-42 *Report Configuration*

Summary

This chapter provided an understanding of the various tools in Cisco Unity Connection, including RTMT, COBRAS, Migrate Utilities, and Reports. You learned how to

- Understand the features, function, and purpose of RTMT tool in Cisco Unity Connection.
- Describe the purpose and feature of the COBRAS to migrate users, objects, and messages from earlier versions of Cisco Unity Connection and Cisco Unity to Cisco Unity Connection version 8.x.

www.it-ebooks.info

- Describe the Migrate Utilities in Cisco Unity Connection and understand the differences between using this utility and COBRAS.
- Review the task definitions and schedules in the Task Management for the various system-level tasks in Cisco Unity Connection.
- Review the various reports available in Cisco Unity Connection and understand their configuration and format.

www.it-ebooks.info

This page intentionally left blank

www.it-ebooks.info

Chapter 12

Maintaining Cisco Unity Connection

This chapter covers the following subjects:

- **Disaster Recovery System (DRS):** Covers the configuration and best practices for performing backup and running the Restore Wizard to restore Cisco Unity Connection.
- **Certificate Management:** Provides an overview of certificate management in Cisco Unified OS Administration.
- **Licensing and Warm Standby Server:** Describes the warm standby operation and licensing for performing backup and restore.
- **Cluster Management:** Provides an understanding of the cluster management in Cisco Unity Connection Serviceability.
- **Survivable Remote Site Voicemail (SRSV):** Provides an overview of SRSV to backup voice-messaging services for remote users.
- **Cisco Voice Technology Group Subscription Tool:** Describes the subscription tool to provide updates.
- **Cisco Unity Connection Tools:** Covers the various tools, videos, and updates available to engineers and administrator on the Cisco Unity Tools website.
- **Simple Network Management Protocol:** Explores the Simple Network Management Protocol (SNMP) and how it is used to provide server status and information to SNMP workstations to assist in monitoring performance and troubleshooting.

At this point, you have Cisco Unity Connection version 8.5 configured and optimized to provide the best possible voice-messaging support to users with the required features. Going forward, the administrative tasks are now focused on keeping the software functioning at the proper level, maintaining redundancy, configuring backups, and configuring the system for ongoing upgrades and growth. Cisco Unity Connection provides the

www.it-ebooks.info

necessary tools, both internal and external, to fulfill these needs. This chapter explores these tools and features and consists of the following:

- **Disaster Recovery System:** Web-based application built into Cisco Unity Connection that provides backup and restore capabilities
- **Warm Standby:** Allows the configuration of a backup server for Cisco Unity Connection server or cluster pair in the event of a server outage
- **Cluster Administration:** Administration of Cisco Unity Connection servers within the cluster pair
- **Subscription Tool:** Provides updates and notifications about changes, updates, and information related to new releases of software
- **Cisco Unity Connection Tools:** Provides online access to updated tools, training information, and videos for Cisco Unity Connection

Elements in this chapter might be considered as optional because the system is operational, and everything is functioning according to design. Still, you should exercise due diligence to ensure that these items are not ignored. For example, a properly performed backup and configured schedule can ensure that there is minimal effect on the organization after a server outage or in the event of a disaster. A good understanding of the available tools can ensure that changes and growth in the business organization do not prevent the Cisco Unity Connection voice-messaging system from operating at optimal performance. You must also stay informed about the latest developments, software updates, and improvements using the Subscription Tool. Finally, through the cluster administration and Cisco Unity Connection Tools website, you can use various tools to further manage the Cisco Unity Connection voice messaging to ensure optimal performance.

This chapter provides coverage of the following:

- Features, configuration, and functions of the Disaster Recovery System (DRS) in Cisco Unity Connection.
- The various aspects of server administration including warm standby and cluster administration.
- The Cisco Voice Technology Group Subscription Tool, which provides notification for the latest updates and product software releases available.
- The Cisco Unity Tools website to understand the various tools, training, and videos available for download.

Disaster Recovery System

The Disaster Recovery System (DRS) application provides all the necessary features for organizations to initiate backups to remote file shares or tape drives (depending on the platform) and restore a server if a failure occurs. If you are already familiar with the DRS

www.it-ebooks.info

application used for Cisco Unified Communications Manager, this information will be quite familiar because Cisco Unity Connection uses the same application. However, the various backup components are obviously different.

The DRS application provides full backup and restore capabilities, either manually initiated or through the built-in scheduler. Using the DRS scheduler, the administrator can initiate backups to multiple locations to provide redundancy. It is advisable to develop a backup schedule and policy consistent with your current backup policies; however, it is strongly suggested to use multiple backups and preferably, at different locations. In most cases, you want to set a schedule that performs a nightly backup during a defined maintenance window. When using multiple backup locations, each location is configured to use a different schedule. In any case, you want to schedule backups during a time when there is the least amount of server and network traffic. Also, you can perform any OS administration tasks, such as network or platform changes or modifications while a backup is in progress.

The DRS application uses a master and local agent to perform the backup functions. The master agent runs on the publisher server of the cluster pair and is responsible for storing all system information and maintaining schedules and tasks. The local agents run on all servers and are responsible for running selected manual backups and receiving schedule tasks from the master agent for execution. All configuration settings in the Disaster Recovery System are updated by the master agent.

Certificate Management Overview

The communication between the master agent on the publisher server and the local agent on the subscriber server is performed using Secure Sockets Layer (SSL) communication using IPsec certification for key exchange. No administrator configurations are required because this communication is completed internally by Cisco Unity Connection during the software installation. The certificate information is stored in the following files:

- **ipsec:** Certificate information included in the ipsec.pem file
- **ipsec-trust:** Certificate information included in the hostname.pem file

This information is accessed through the Certificate Management pages in Cisco Unified OS Administration. To view these files, from the toolbar in Cisco Unified OS Administration, select **Security > Certificate Management**, as shown in Figure 12-1. The certificate list is displayed showing the two certificate files and the two tomcat files used for the various web pages in Cisco Unity Connection:

- **tomcat:** Certificate information included in the tomcat.pem file
- **tomcat-trust:** Certificate information included in the hostname.pem file

From the Certificate List page, as shown in Figure 12-1, you can also upload or generate a new certification and download or generate a new Certificate Signing Request (CSR).

www.it-ebooks.info

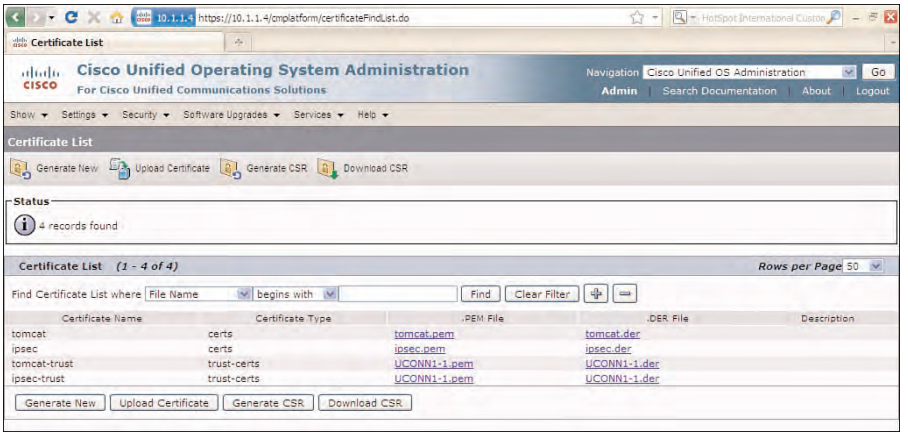

Figure 12-1 *Certificate List in Cisco Unified OS Administration*

To view the contents of the **pem** file, select it from the .PEM File column on the Certificate List page. In Figure 12-2, the **UCONN1-1.pem** file is selected displaying the contents of the file. The certificate information consists of the hostname, location, serial number, and configuration information from the Cisco Unity Connection server. If you delete this file, you must upload the **ipsec** file to **ipsec-trust**; otherwise, the DRS master and local agents cannot function properly.

From the Certificate Configuration page, the user can also download the certificate directly to the workstation.

Performing a Backup

When using the DRS application, the backup is written to a tar file using either local tape drives (depending on the server model) or network file shares using Secure File Transfer Protocol (SFTP) or FTP. The backup information consists of a full backup of the selected components, which includes all configurations along with the associated backup information, devices, and schedules included in the DRS facility. If a restore is required, the replacement server must be installed with the same software level and release. The restore operation cannot be used to perform an upgrade of the system software. Therefore, when you upgrade your server or cluster, ensure that a backup is performed with the current level of software and exact patch level.

You can access the DRS application directly from the Navigation drop-down option using the web browser in Cisco Unity Connection Administration. However, the administrator needs to supply the proper authentication credentials, which are the platform

www.it-ebooks.info

administration username and password to access the DRS application. The steps to configuring a backup include the following:

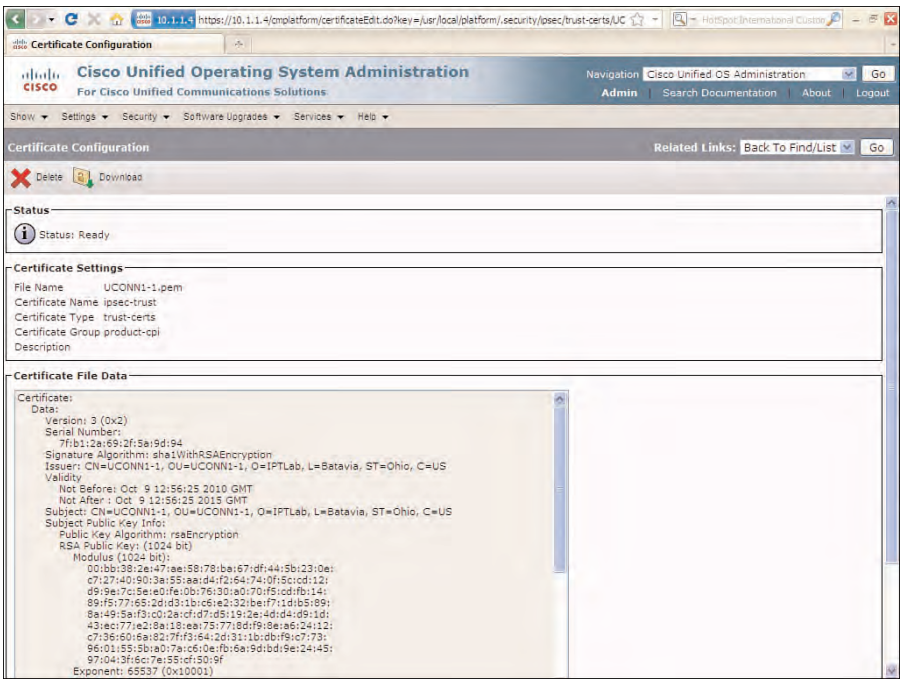

Figure 12-2 *Certificate Configuration Page for the UCONN1-1.pem file*

Step 1. **Configure the backup target location:** Ensure the backup location is configured and accessible before beginning the backup configuration in the DRS application. This step consists of configuring the server backup tape drive (for specific models), or network file shares. When using the network for backups, Secure File Transfer Protocol (SFTP) is used for communications between Cisco Unity Connection and the backup target location. The configuration of the backup target location must be completed before DRS can be configured.

This configuration consists of the shared directory configuration, authentication credentials, and location for Cisco Unity Connection to access the shared files or directory. It is also necessary to ensure that sufficient drive space is located in this target location. You must consider the number of stored backups configured and size of the database as the organization grows.

Step 2. **Configure the backup devices:** After the target tape drive or network drive is configured, this backup device must be configured in Cisco Unity Connection using the Disaster Recovery System pages. This includes the

www.it-ebooks.info

backup location, authentication credentials, and number of backups to store. Depending on the backup policy and organization, it is advisable to create multiple backup locations for redundancy. If the organization consists of multiple locations, these backups should be distributed between the locations.

Step 3. **Start a manual backup:** Run a manual backup after configuring or changing a backup device. This ensures that a backup is current and successful at the backup target. Also, you need to run a backup before upgrading or making any hardware changes to the server or cluster to provide the most current backup file if a server issue occurs. This step should be done to ensure that the backup location and communication between Cisco Unity Connection and the backup target is properly operating. In this way, the scheduled backup can operate properly when an administrator is not available to verify its success.

Step 4. **Review the backup history:** Review the backup history after starting a manual backup to ensure the successful backup configuration and operation.

Step 5. **Create a backup schedule:** A backup schedule for each backup device should be configured, each running a different time during a defined maintenance window, or when network traffic is at the lowest level. In most cases, you need to create different daily backup schedules for different target backup locations and configure them to run at different times.

Backup Device Configuration

Before configuring the backup device in Disaster Recovery System (DRS), you need to ensure that the backup target location is configured and accessible by Cisco Unity Connection. If you use the tape drive, the hardware must be installed and accessible before the configuration in DRS can be completed. If you use the network file share, ensure that the backup directory and authentication credentials are properly configured. Also, SFTP must be available and operational on the network server designated to be the target backup server. A number of SFTP applications are available on the market that work perfectly for this purpose.

Note FreeFTPd and Core FTP mini SFTP server is a readily available and a suggested SFTP client for backup.

Note The configuration of the various SFTP applications is beyond the scope of this book. The illustrations used throughout this section come from an available SFTP application configured on a Windows desktop workstation.

After the backup target location is configured and ready to accept backup files using SFTP, you can begin the configuration of the DRS in Cisco Unity Connection.

www.it-ebooks.info

To begin the backup device configuration, you must first access the DRS. This is completed by selecting the DRS from the Navigation drop-down in Cisco Unity Connection Administration, or selecting the following web page:

https://ip_address_publisher_server/drf

On the login page, you need to enter the platform administrator credentials. As discussed previously, these credentials are created at the time of installation but can be modified or other credentials can be added through the command-line interface (CLI).

After logging in to the DRS, the main DRS page displays. Two separate drop-downs are provided for backup and restore configuration. To begin the backup device configuration, select **Backup > Backup Device** from the toolbar. The Backup Device configuration page displays. Click **Add New** to create a backup device. Figure 12-3 shows the resulting New Backup Device page.

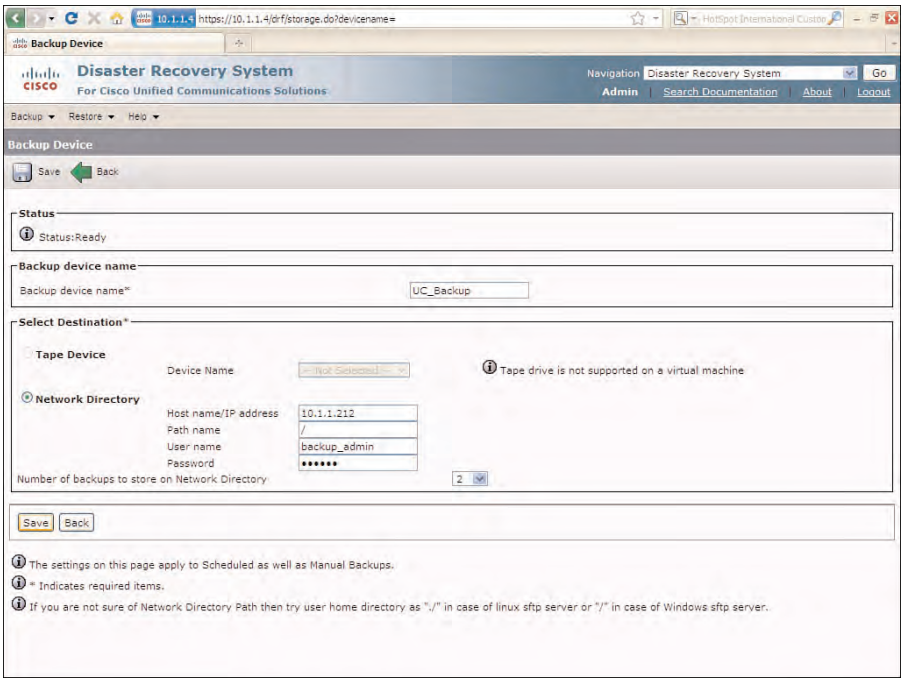

Figure 12-3 *Backup Device Configuration in Disaster Recovery System*

From this page, you can select either a tape or network drive; although, a network file share would be the most common and suggested. If the tape drive is going to be used, it must be configured on the server and available at the time the backup device is created. The tape drive has a limitation of only a single backup being written to a single tape. Therefore, administration requires that the tape must be changed between backups;

www.it-ebooks.info

otherwise, the existing data will be overwritten. Conversely, when using the network directory option, a single network directory location can store multiple backups to a directory.

In this example, a backup device name is created for a network directory backup. The name is configured as **UC_Backup** and is configured for SFTP to the target location with IP address 10.1.1.212. The path and authentication credentials must also be configured. Finally, select the number of backups that will be stored on the backup server. Each backup is saved as one or more .tar files, depending on the backup components configured. The number of files created depends on the specific options selected for backup. These options are selected under the manual and scheduled backup configuration pages. Two backups is the default, meaning that there will always be two backups stored on the backup server. When a third backup is run, the oldest backup file on the server is overwritten. Each backup is time stamped enabling the administrator to easily select which .tar file is to be used for the restore operation. After the information is entered on the Backup Device page, click **Save** to complete the operation. At this point, Cisco Unity Connection verifies the credentials and directory location at the target location. However, the actually storage size is not calculated for the number of backups and projected growth of the database; therefore, ensure that the target network drives for all backup devices have more than sufficient drive space to handle current and future growth of the voice-messaging system. The save operation can actually verify the target location, credentials, and backup directory to ensure that all future backups are successful. If a failure occurs during this step, you are required to troubleshoot your target backup server; therefore, make sure that you review any messages in the Status section for a successful save operation. The backup device configuration will not be saved to the database until this verification procedure has successfully completed.

Backup Components

Before covering how to perform a manual backup and configure a backup schedule, you first need to understand the various files and components backed up. From both an engineering and administrative perspective, this can help you properly configure backup locations and schedules, especially multiple Cisco Unity Connection servers and cluster pairs, and other Cisco Unified servers involved, such as Cisco Unified Communications Manager.

A single backup operation in Cisco Unity Connection consists of a number of components that the administrator can select:

- **CONNECTION_DATABASE:** Cisco Unity Connection configuration database.
- **CONNECTION_MESSAGES_UNITYMBXDB1:** Contains all messages in the defined mailbox store.
- **CONNECTION_GREETINGS_VOICENAMES:** Contains all user greetings and recorded names. This component also requires that the Connection database be included in the backup.
- **CUC:** Various Cisco Unity Connection server and platform components.

www.it-ebooks.info

These four components enable the administrator to create separate backups based on the various components. If you create additional mailbox stores, these are included in the selection for CONNECTION_MESSAGES with the mailbox name. To ensure a complete backup is performed, select all components when performing manual and scheduled backups. You do have the option to perform partial backups, consisting of the various components that can be created and scheduled as needed. If you perform a partial backup and select the CONNECTION_GREETINGS_VOICENAMES component, however, the CONNECTION_DATABASE component is also required to be included in the backup operation because the database includes the specific user configurations required for backing up greetings and recorded names.

Figure 12-4 illustrates the backup directory where two full backups of all components in the Cisco Unity Connection database were performed. In this example, there are two mailbox stores configured on the server, UnityMbxDb1 and UnityMbxDb2. If your configuration has only one mailbox store, or more than one mailbox store, the number of files varies accordingly.

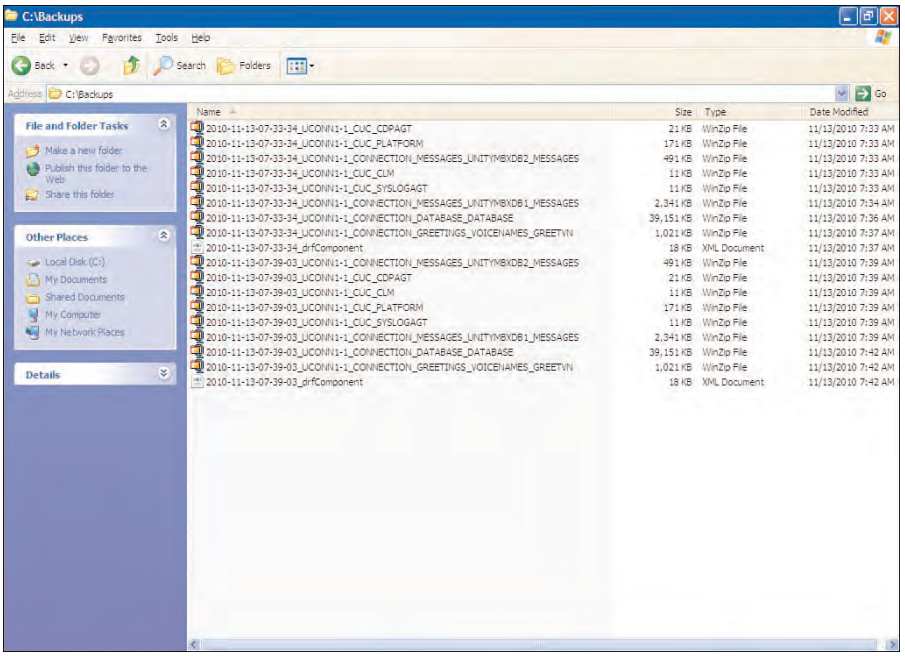

Figure 12-4 *Backup Directory Reflecting Two Complete Backups*

Within each backup operation, there are one or more files included with each component backed up. The CONNECTION_DATABASE, CONNECTION_GREETINGS_VOICENAMES, and each mailbox store components are included in specific individual files, whereas the CUC components are included in multiple files. Finally, an XML file called

www.it-ebooks.info

drfComponent is written to the directory as a catalog of all related components of the backup. When a backup is written to a specific directory, the backup operation monitors this file as the new backup is completed by removing older backups based on the number of backups selected on the Backup Device configuration page. In this example with two mailbox stores and a complete backup of all components, each backup operation included nine files.

The backup files are in a .tar format and encrypted using the security password that was configured at the time of installation. If you decide to change this password, perform a full backup immediately as the older files will not be available to the server or cluster pair without restoring the security password to its available settings. This same security password must be configured on the replacement server as well, when performing a restore operation.

If you use the same network drive for different servers, create a separate directory for each server or cluster pair because the number of backups selected uses the **drfCompnent** xml files within the target directory, not the actually components or the .tar files. Therefore, if you have a number of Cisco Unity Connection servers or cluster pairs, and other servers such as Cisco Unified Presence Server (CUPS), Cisco Unified Communications Server, or other devices, ensure that the backup device target location is configured for different target directory locations, or preferably completely different backup servers, if possible. This is an important concept to remember when configuring your backup strategy, as illustrated in the following case study.

Case Study: Backing Up Mailbox Stores

A new administrator has joined the organization at Tiferam Corporation. This administrator was tasked with the responsibility to create a backup of the two configured mailbox stores. The administrator was unaware of the previous backup target location and configured the same backup network device and directory that was used for performing the full backups that run nightly during the organization's maintenance window.

The backup was created for the two mailbox stores to the same backup location where the backups were previously run, as shown in Figure 12-4. After two backups were run to the same target network directory, the final result of these backup operations is displayed in Figure 12-5.

The full backups created previously were completely removed and replaced with the two backup operations consisting of three files, each with only these selected mailbox stores. Only two backups are written to the network directory, regardless of the components selected because the Backup Device configuration page was configured for two backups to store at this directory location, (refer to Figure 12-3). Therefore, each backup device configuration must be configured with its own target directory to ensure the proper backup configuration is performed and not overwriting existing data from other backups.

www.it-ebooks.info

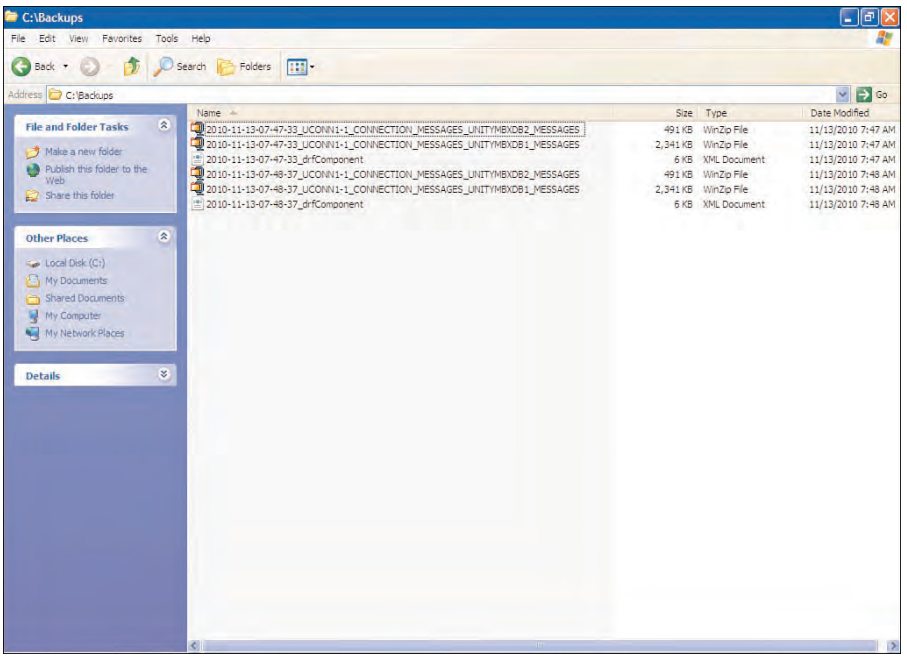

Figure 12-5 *Backup Directory After Performing a Mailbox Store Backup*

Manual Backup

After the backup device is configured, to run a manual backup to ensure that the target backup drive space is sufficient and the backup location is operating properly. Also, this ensures that a backup is available if a restore is required before an actual scheduled backup is performed. In most cases, an administrator might not be available or aware of a completed backup for a scheduled event because this would normally be completed during off-hours or a maintenance window.

To perform a manual backup, from the toolbar on the Disaster Recovery System page, select **Backup > Manual Backup**. The Manual Backup page then displays enabling the administrator to select the configured backup device from the Backup Device selection. Finally, the Select Features section enables the administrator to select the various components to be backed up. These components were described in the previous section. However, when performing a manual backup for the first time after the backup device is configured, make sure that you select all listed components for backup.

When performing a partial backup, you need to backup the database and greetings with recorded names, minimally. The mailbox store's backup is optional but should be considered to be included with all backups. When completed with the various configurations for the manual backup, click **Start Backup** to begin the backup operation. Figure 12-6 illustrates the configuration of a manual backup created to perform a full backup of all components.

www.it-ebooks.info

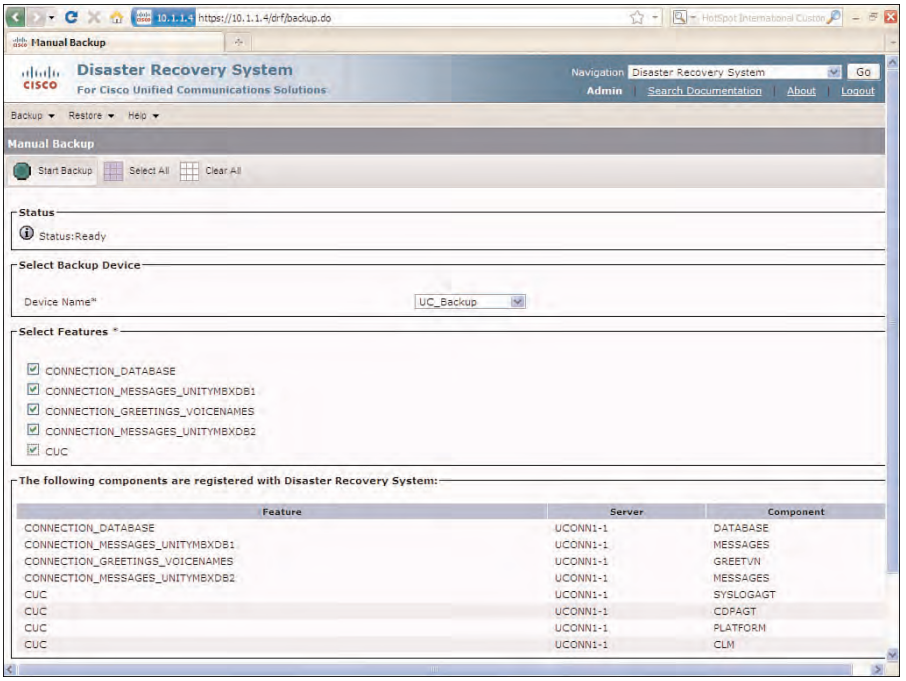

Figure 12-6 *Manual Backup Configuration in Disaster Recovery System*

After clicking **Start Backup** on the Manual Backup configuration page, the backup status is immediately displayed providing the administrator with the current status of the backup operation, as shown in Figure 12-7.

The Backup Status page provides real-time feedback on the current components being backed up and the current status. From this page, the .tar filename is described in the Backup details section, which also provides information about the backup device, operation, and the percentage completed. At this point, the backup is 50 percent complete and is currently backing up the Connection Database. Each component includes a specific log file after the specific backup component completes. If an error occurs with any single component, the administrator can open this file to identify the specific error. From this page, the administrator can also cancel the backup by clicking **Cancel**. Then, the backup ends only after the current component being backed up completes.

If you leave the Backup Status page, you can redisplay the state of the current or last performed backup by selecting **Backup > Current Status** from the toolbar in Disaster Recovery System. You can also view the status of all backups by selecting **Backup > History** from the toolbar.

The amount of time required to complete the backup depends on the size of the database and the number of components backed up; however, the backup must complete in 20 hours before timing out, as described in the notes of the current status page. This is more

www.it-ebooks.info

than sufficient to complete the backup for a large enterprise organization because the backup should complete in a number of hours during a maintenance window.

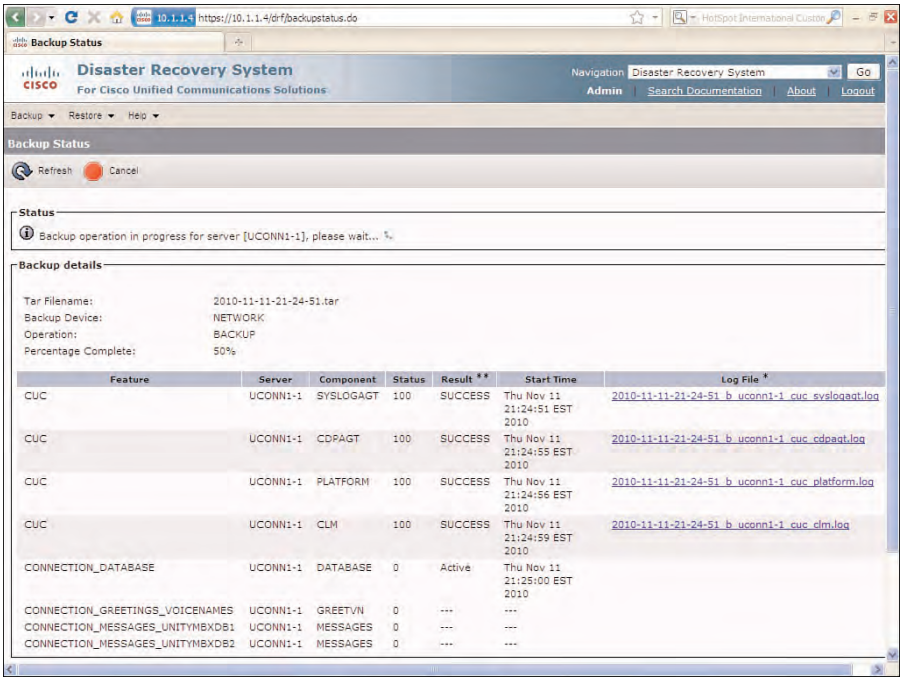

Figure 12-7 *Backup Status of the Manual Backup Performing a Full Backup*

Backup Scheduler

As mentioned previously, the backup operation should be configured to be run during a maintenance window or when network traffic is at the lowest level (off-peak hours), which can vary between organizations. Also, you should avoid running a backup during the Update Database Statistics task, which runs at 4:00 a.m. daily and is the task that optimizes the database based on the current operational statistics. If necessary, this task schedule can be edited as needed under Task Management in Cisco Unity Connection Administration.

Up to ten backup schedules can be configured, each having its own backup device, features, and components. You can configure backup schedules through DRS or the CLI; however, DRS is the most preferable method to perform any of the various backup configuration functions.

To create a backup schedule in DRS, from the toolbar on the Disaster Recovery System page, select **Backup > Scheduler**. The Schedule List page displays, where the administrator can view the current schedule and create new schedules. Click **Add New** to create a new schedule. On the Scheduler page, enter the schedule name and select the backup

www.it-ebooks.info

device, followed by the specific components to be backed up, as illustrated in Figure 12-8. Further down the page, below the components section, are the schedule options. You need to create a backup schedule according to the backup policy defined for the organization, which must include the start time and frequency of backups.

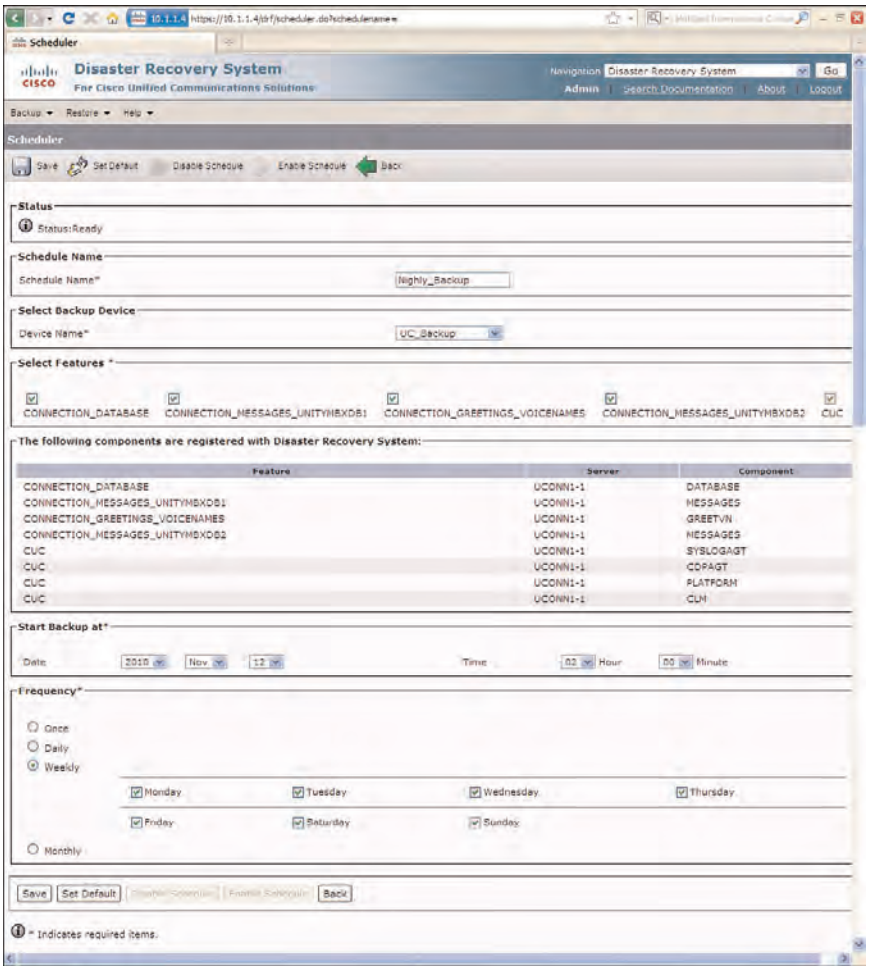

Figure 12-8 *Backup Schedule Configuration in Disaster Recovery System*

The **Set Default** button enables the administrator to configure the backup schedule to perform Weekly backups on Tuesday through Saturday. After all the option are configured, you must select **Save** and click **Enable Schedule** to have the schedule begin to run the backup operation according to the configured options. The schedule will not run until you click **Enable Schedule**. Options on this page enable the administrator to also disable the schedule if needed, without having to delete the schedule entirely.

www.it-ebooks.info

Performing a Restore

If a restore is required, you must install a new server with the exact same software and patches as the server being removed from service and whose backup files will be used for the restore operation. Also, the hostname, IP address, and deployment type (single server or cluster pair) must match the configuration of the former server. If you restore a cluster pair, the restore operation is performed on the publisher server. As mentioned earlier, you cannot use the restore operation as a vehicle to perform an upgrade to different software or patch level.

Using the Restore Wizard

After you install the replacement server with the exact Cisco Unity Connection software and patch level, you need to log in to the Disaster Recovery System and create the backup device by selecting **Backup > Backup Device**. This is the exact configuration that was completed for the backup device when running a backup as defined in the previous section. The location is same network drive or tape device defined during the backup configuration for the former server or cluster pair.

To begin the restore, from the toolbar in Disaster Recovery System, select **Restore > Restore Wizard**. The Restore Wizard assists the administrator to complete the restore by providing a four-step process to complete the operation. This is especially helpful when attempting to complete this operation during an outage, which could tend to be a stressful situation for the organization.

As the Restore Wizard begins, Step 1 displays, allowing the administrator to select the backup device from the drop-down, as shown in Figure 12-9. In this case, the **UC_Backup** device is selected. Click **Next** to move to the next step of the Restore Wizard.

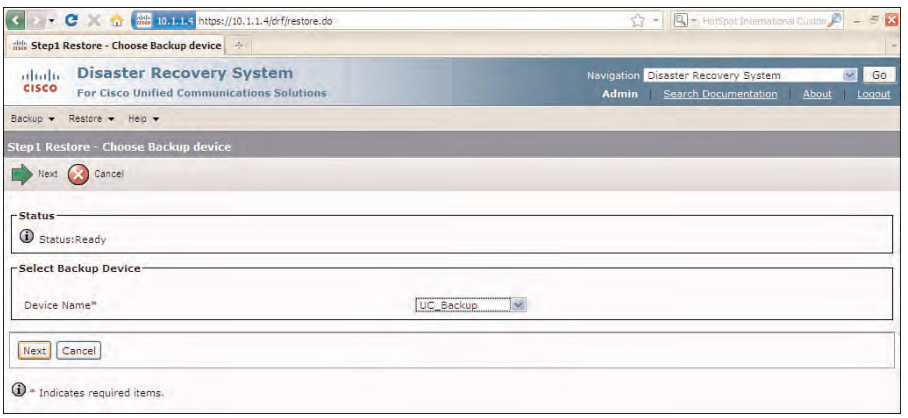

Figure 12-9 *Step 1 Restore - Choose Backup Device*

www.it-ebooks.info

After you click **Next**, Step 2 of the restore operation displays. On this page, you need to select the backup file to be used for the restore operation. Use The selected backup device to view the various backups, which were date stamped during the backup operation. There will be multiple backups depending on the number of backups selected to be stored at this location during the Backup Device configuration. The backup information displayed here is read from the **drfComponent** xml files within the target directory.

Figure 12-10 illustrates the backup file selection, where two backups are currently stored at the specific target backup directory. Choose the desired backup from the drop-down, and click **Next**.

Figure 12-10 *Step 2 Restore - Choose the Backup Tar File*

After you click **Next** on the Step 2 page, the next option in the Restore Wizard is to select the desired components to be restored. You can restore only the selected components that were previously backed up. As shown in Figure 12-11, for Step 3 of the Restore Wizard, all components were selected to complete a full restore. After you select the desired components, click **Next** to move to the final step of the restore operation.

Finally, after you click **Next** on the Step 3 page, the final page of the restore operation displays. On the Step 4 page of the Restore Wizard, you select the specific server to restore each component. Additionally, you have the option to have Cisco Unity Connection perform a file integrity check as part of the restore operation. This is advisable to ensure that the files are valid and have not been corrupted during the backup or restore operations. Click **Restore** to begin the restore of the selected .tar files to the server, as shown in Figure 12-12. This page is your final warning, where making this final selection can overwrite all existing data on the destination server. All existing data for the selected features will be lost as described in the Warning section.

www.it-ebooks.info

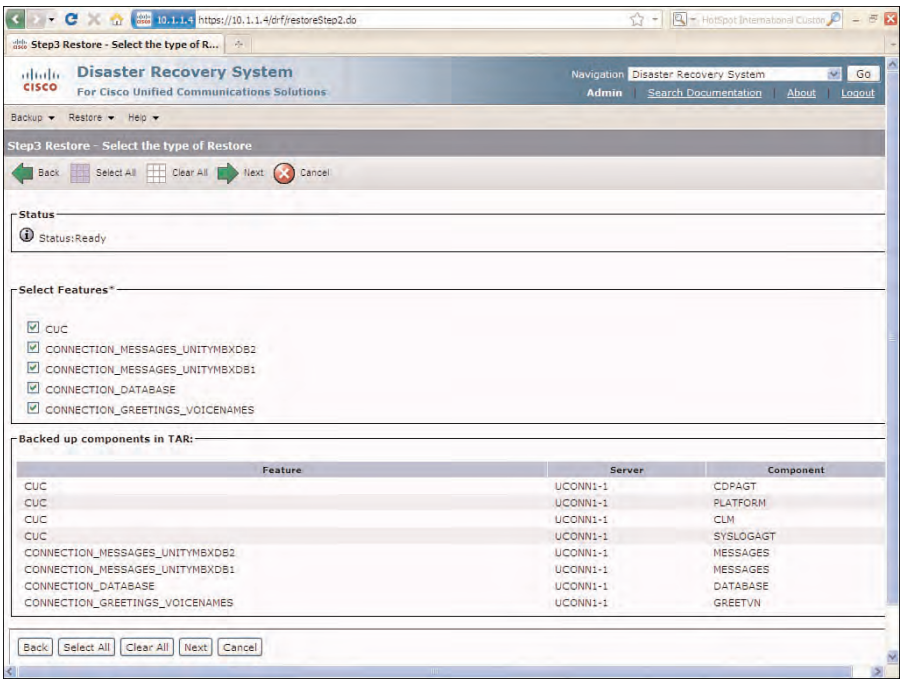

Figure 12-11 *Step 3 Restore - Select the Type of Restore*

After you click **Restore** on the Step 4 Restore page, the Restore Status page then displays showing the various components being backed up. In Figure 12-13, a restore is run on a server showing that it is currently backing up the database for which it is 55 percent complete. The backup should continue and refresh as the backup continues to completion.

When the restore is complete, the Restore Status page indicates that the server must be restarted for the changes to take effect, as shown in Figure 12-14. After the restart, the server can be tested, verified, and moved to production. Again, the time to restore depends on the size of the database and the components restored.

Warm Standby Server

In a network that requires a higher level of availability for voice messaging, the cluster pair serves the organization providing a redundant solution as needed. Another available option for backup and restore is to provide a Cisco Unity Connecter server in warm standby at each specified location. The warm standby server is installed with the exact software and patch level as the production server, but the database is left unconfigured. Backups are still performed as normal according to the defined backup schedule using the DRS application.

www.it-ebooks.info

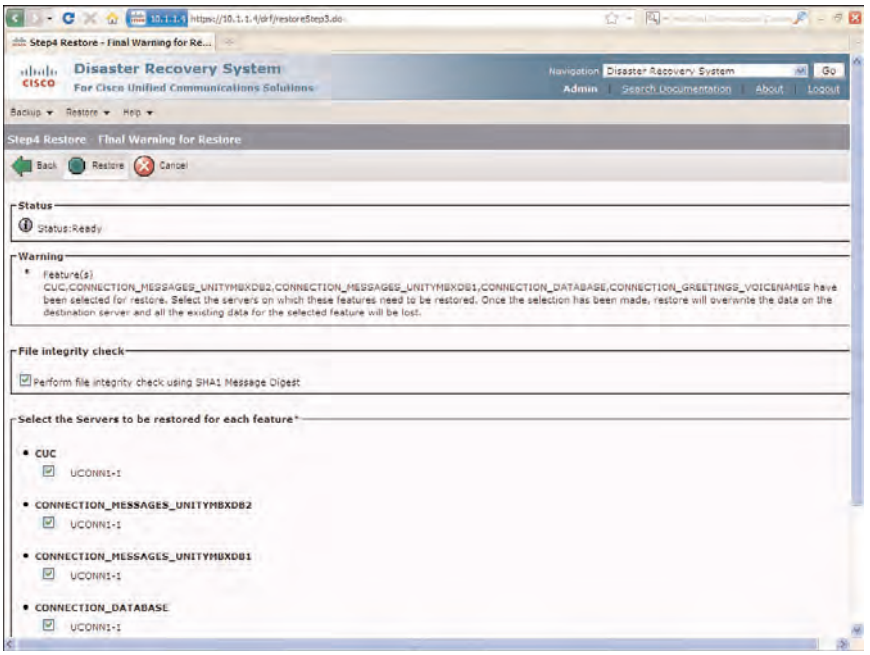

Figure 12-12 *Step 4 Restore - Final Warning for Restore*

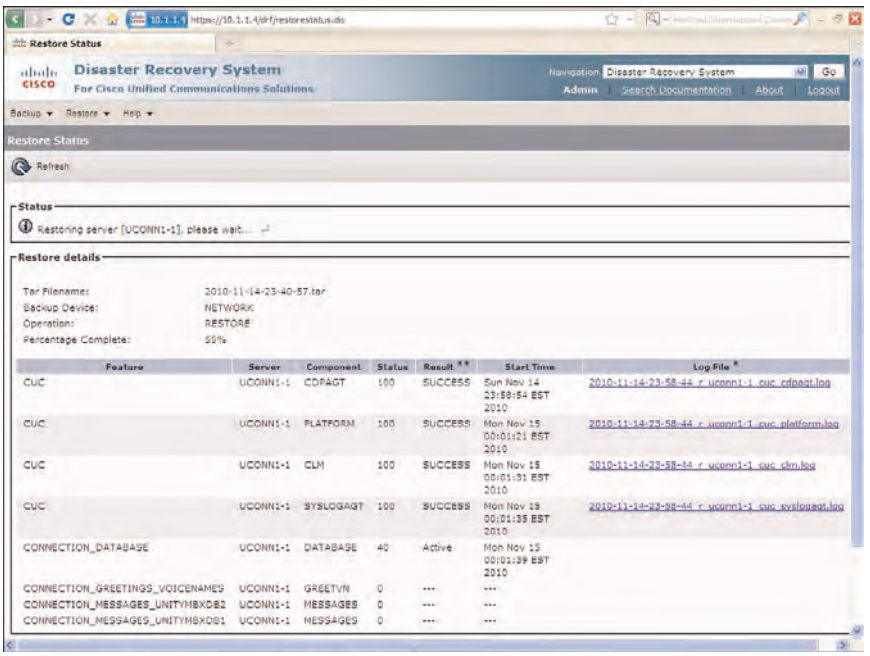

Figure 12-13 *Real-Time Restore Status in Disaster Recovery System*

www.it-ebooks.info

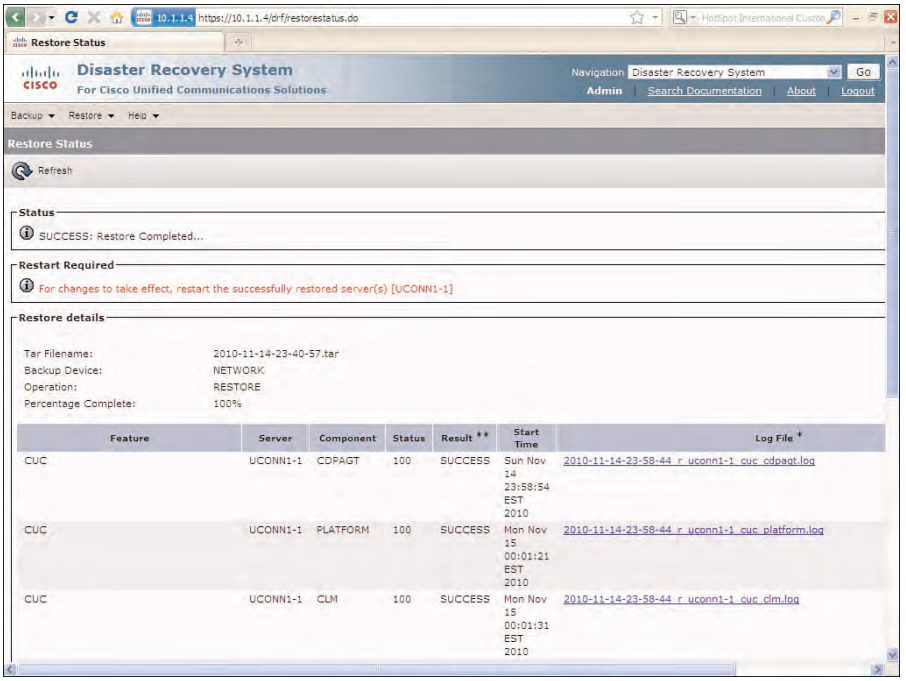

Figure 12-14 *Restore Status Complete*

When a server outage occurs, the backups are restored to this warm standby server. A single warm standby server can be a replacement for single server or an entire cluster pair but cannot be a replacement server in a cluster pair with an existing server. In other words, it cannot replace the publisher of a cluster pair operating with the existing subscriber server.

To use the warm standby option, the proper licenses need to be installed for the warm standby server. Of course, you always have the option to purchase identical licenses with the same features as the production server. However, this might not be practical or cost-effective. This latter option enables this server to be used as a warm standby for any server in the network.

Another option might be to use the warm standby with the backup files and licenses from the backed up server. This obviously causes a license violation because the MAC address for the license file does not match the server but enables the administrator to use the server in this state for up to 24 hours before having to perform a reboot. In this case, the warm standby server can provide a stop-gap resolution until the replacement server is installed and operational. The final option requires interaction with Cisco, by requesting a replacement license with the MAC address of the warm standby. This would be the best solution if you are likely to keep the warm standby in operation for an extended period. The server and license file MAC address must match when replacing any server. There

www.it-ebooks.info

also might be a delay to obtain the required license file from Cisco because this process is not immediate.

The DRS or Cisco Object Backup and Restore Application Suite (COBRAS) tools can be used for backup and restore to the warm standby server. The COBRAS application was discussed previously in Chapter 11, "Using Cisco Unity Connection Tools and Reports." This application enables the administrator to perform partial backups of selected users, messages, and system objects. However, the DRS application provides the necessary facility to create a full backup and perform restore functions using the Restore Wizard within DRS.

Cluster Management

Chapter 9, "Understanding Cisco Unity Connection Networking," provides an overview of the cluster management concepts; however, it would be remiss if this important subject were not addressed in this chapter dealing with maintenance tasks and issues. In a normal operating mode of a Cisco Unity Connection cluster pair, the publisher server should operate as the Primary, whereas the subscriber server should operate as the Secondary. The function of the Primary and Secondary server were discussed in Part I.

To review the current cluster status, from the Navigation drop-down, select **Cisco Unity Connection Serviceability** and click **Go**. After logging in with the application administration credentials, from the toolbar on the Cisco Unity Connection Serviceability page, select **Tools > Cluster Management**. Figure 12-15 shows the resulting Cluster Management page.

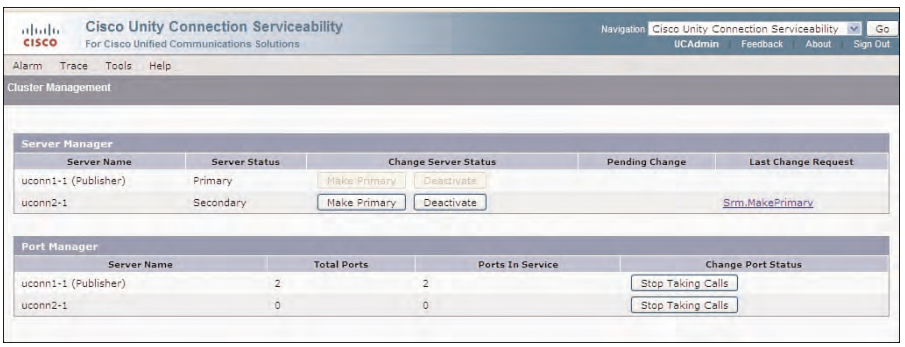

Figure 12-15 *Cluster Management in Cisco Unity Connection Serviceability*

In this case, the publisher server has the Primary status, whereas the subscriber server has the Secondary status. This should be the normal operating condition. If a server must be taken offline for any reason, it can be deactivated only after it has been relegated to Secondary status. The procedure is completed by changing the subscriber server (currently operating in Secondary status) to Primary status. To complete this step, in the

www.it-ebooks.info

Change Server Status column for the subscriber server within the Server Manager section, click **Make Primary.**

After this server's status has changed to Primary, you need to ensure that the Secondary server (the server to be deactivated) is no longer accepting calls. To complete this operation, from the Change Port Status column within the Port Manager section, click **Stop Taking Calls**. If you fail to complete this step before deactivating the server, current calls terminate automatically during the deactivation procedure.

The deactivate process does not wait for calls to complete and automatically terminates all calls in progress. Therefore, to ensure that users and callers do not get disconnected abruptly, use the Port Monitor in the Real-Time Monitoring Tool (RTMT) to ensure all ports are in the idle state. This might take a few minutes to ensure that all current calls are cleared. Figure 12-16 shows the Port Monitor showing calls currently active on the server. Chapter 4, "Integrating Cisco Unity Connection," covers the configuration and details of the Port Monitor.

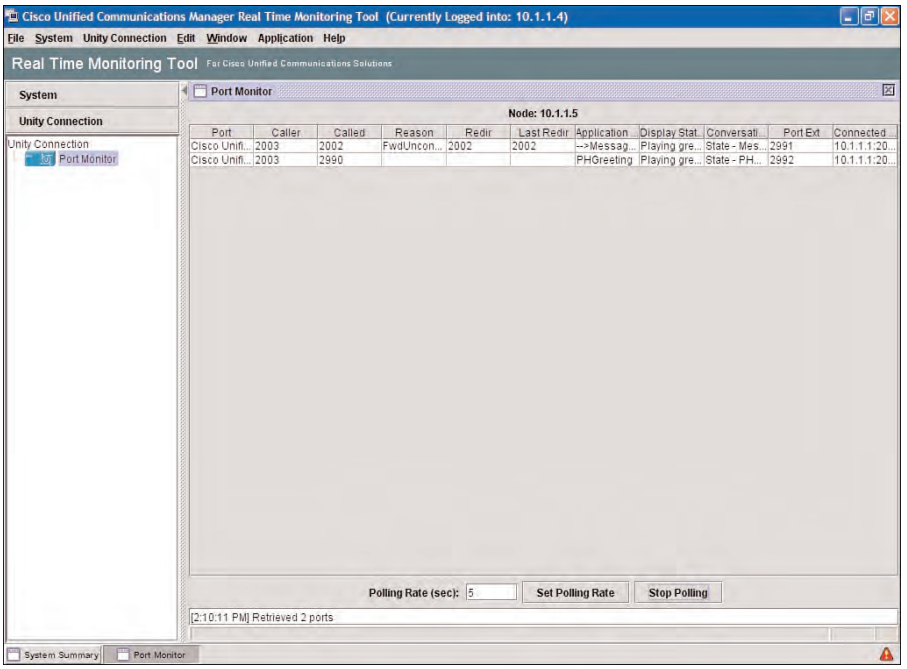

Figure 12-16 *Port Status Monitor in Real-Time Monitoring Tool*

After you complete these two procedures and all ports are idle, under the Change Server Status column within the Server Manager section, you can safely click **Deactivate.** After the deactivation of the server is complete, the server can be powered off and removed from the network.

www.it-ebooks.info

Overview of Survivable Remote Site Voicemail

Another backup option in a centralized voice-messaging system is Survivable Remote Site Voicemail (SRSV), where Cisco Unity Connection supports voice messaging for the central location and all remote locations. In this case, Cisco Unity Express is used at the branch locations as a backup solution for users at those specified locations when Cisco Unity Connection is unavailable because of a network or WAN outage.

At the central location, Cisco Unified Messaging Gateway provides the mechanism to coordinate SRSV messaging with Cisco Unity Express, Cisco Unified Communications Manager, and Cisco Unity Connection. When an outage occurs and users lose communication to the central location, the remote phones register to the remote gateway using SRST. Each remote gateway provides phone registration and feature services at each remote site, whereas Cisco Unity Express provides voice messaging for the users at that location. When the network is restored, Cisco Unity Express uploads all stored messages that were saved and deleted during the outage to Cisco Unity Connection.

Figure 12-17 shows this design of SRSV. The discussion of Cisco Unity Express and Cisco Unified Messaging Gateway is beyond the scope of this text.

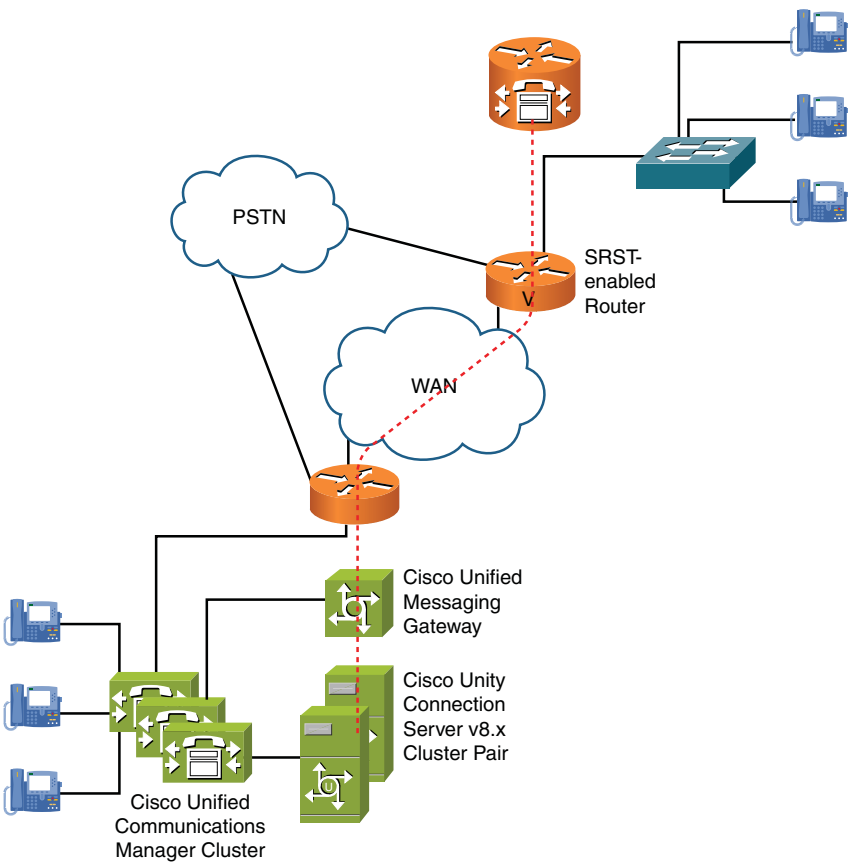

Figure 12-17 *Survivable Remote Site Voicemail*

www.it-ebooks.info

Cisco Voice Technology Group Subscription Tool

Cisco provides a method to notify by email for software updates. This is the Cisco Voice Technology Group Subscription tool. For information on this tool, go to Cisco.com.

Cisco Unity Connection Tools Online

The Cisco Unity Connection Tools online information was discussed throughout this text for updates and specific tools. However, many more resources are located at this site. Many of the updates for the tools and additional "use at your own risk" tools can be found here. To access this site from any browser, select the following URL:

www.ciscounitytools.com

Some of the tools located at this site are labeled "use at your own risk" because the Cisco Technical Assistance Center (TAC) does not support these applications. This location can be valuable to not only acquire the latest and newest tools, but to also access training videos and documentation about Cisco Unity Connection and other Cisco Unified voice-messaging products.

Configuring Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application-level management protocol that provides management information between various network devices of all types and manufactures. With SNMP information, the administrator can monitor the performance of the various services, receive advanced notification on the critical errors, and use the collected information to facilitate troubleshooting and quickly resolve problems. One the most powerful features of SNMP is to provide preventive maintenance by noting trends in growth and server performance.

SNMP is an industry-standard implementation available in three versions, where v3 provides authentication if needed. To configure SNMP, you need to obtain the community strings, users, and notification destinations. The notification destination is the organization's Network Management workstation configured to collect SNMP information from all the various network servers and devices. In most cases, the Network Management workstation can be configured to send alerts to cell phones and pages on defined critical errors.

You need to configure the SNMP by logging in to Cisco Unified Serviceability and selecting **SNMP > V1/V2 > Community String**. The SNMP Community String Configuration page displays, enabling the administrator to configure the various parameters. Select the **Add New** button to create a new community string.

www.it-ebooks.info

In Figure 12-18, a new community string, public, is created with read only privileges from three defined network management workstations. This configuration applies only to the local node, unless you select the **Apply to All Nodes** check box.

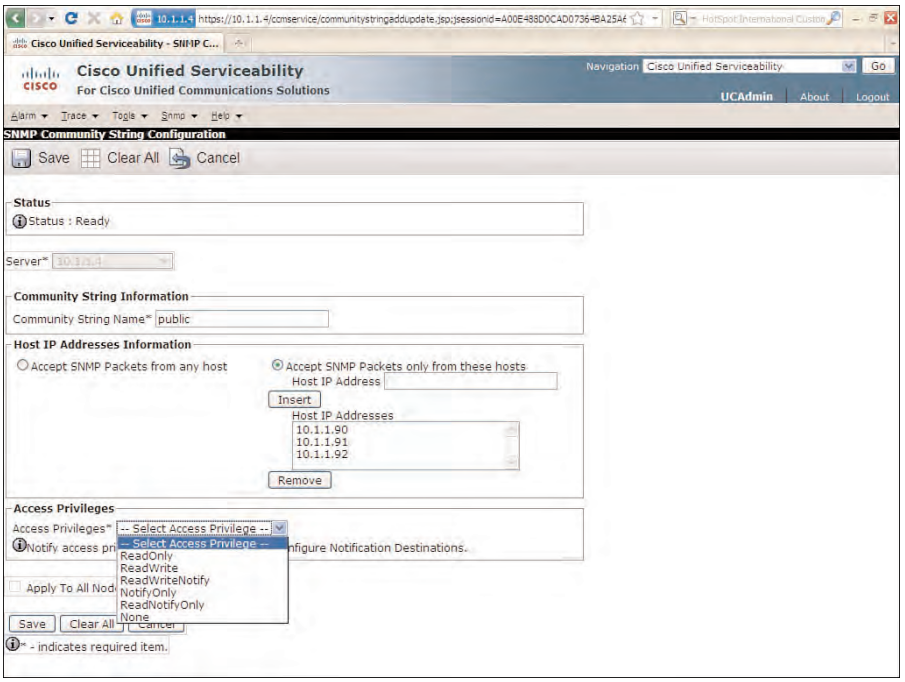

Figure 12-18 *SNMP Community String Configuration*

As shown in Figure 12-19, a pop-up message informs the administrator that any changes cannot take effect until the SNMP master agent restarts. This is completed by accessing Service Management in Cisco Unity Connection Serviceability. Click **OK** on the pop-up to automatically restart the SNMP master agent without having to access the Cisco Unity Connection Serviceability pages. Wait to complete the configuration of all community strings before performing the restart.

Finally, you need to configure the notification devices. To complete this step, select **SNMP > V1/V2c > Notification Destination** to display the resulting SNMP Notification Destination Configuration page, as shown in Figure 12-20. You need to configure the notification destination to the specific notifications for traps or informs. Click **Save** to complete the configuration.

SNMP notifications are sent to an SNMP workstation such as HP OpenView, Solarwinds, and the like to enable the administrator to get a visual status of the operating condition of the various network devices. These network management tools provide early notification on the problems or network conditions that might need attention. In many cases, the SNMP provides enough notification to engineers and support, where they can quickly troubleshoot and resolve the issue before users detect a problem.

www.it-ebooks.info

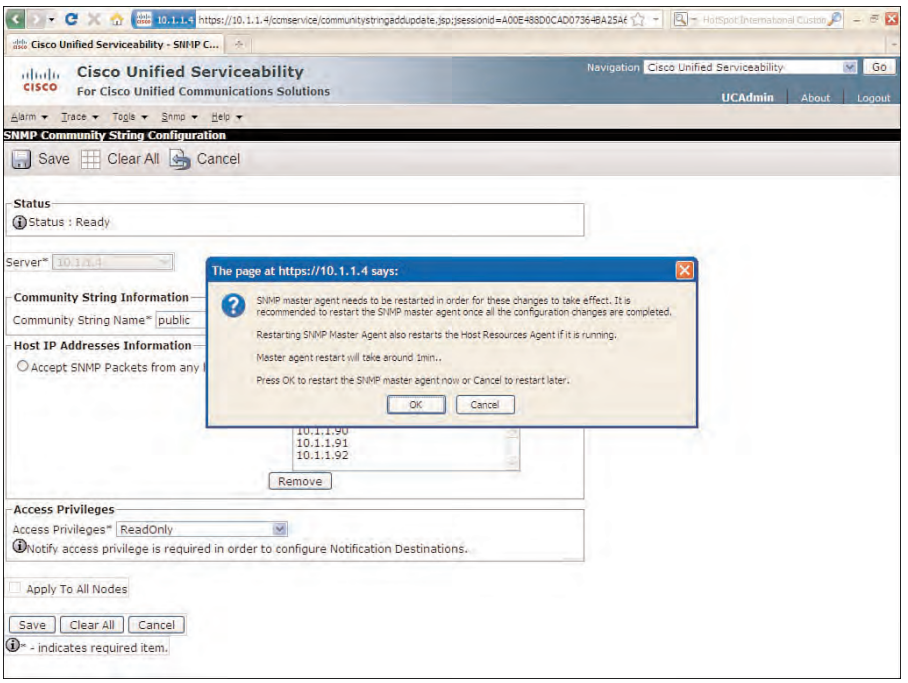

Figure 12-19 *Pop-Up Warning Regarding the SNMP Master Agent Restart*

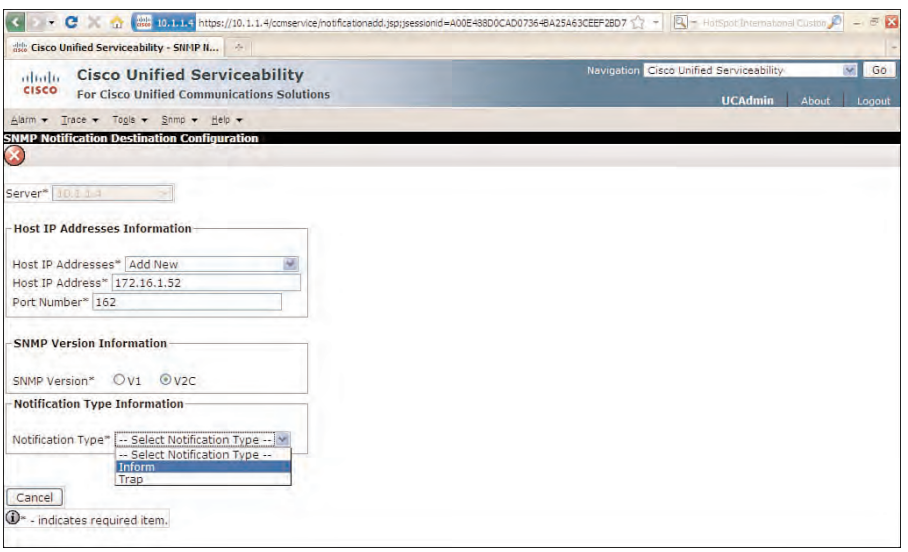

Figure 12-20 *SNMP Notification Destination Configuration*

www.it-ebooks.info

Summary

This chapter provided an understanding of some of the Cisco Unity Connection maintenance procedures and concepts. Specifically, you should be familiar with the following:

- The design, features, and configuration of performing backup and restore operations using the Disaster Recovery System (DRS) application.
- The concepts of the certification management in Cisco Unified OS Administration.
- The licensing and concepts required with Cisco Unity Connection and use of the warm standby server to provide a backup solution.
- The Cluster Management in Cisco Unity Connection Serviceability, the normal operation of the cluster pair, and the procedure to deactivate an existing server.
- How Survivable Remote Site Voicemail can be used for voice-messaging backup solutions to remote locations.
- The Cisco Voice Technology Group Subscription Tool to provide email notification for software updates.
- The Unity Connection Tools On-line site for software, tools, updates, and training videos and information.
- The SNMP configuration required for the Cisco Unity Connection to provide notification and server status information.

www.it-ebooks.info

Chapter 13

Advanced Features in Cisco Unity Connection

This chapter covers the following subjects:

- **Implementing Fax Integration:** Understand the concepts and configuration of fax integration in Cisco Unity Connection, allowing users to receive, forward, and print fax documents.
- **Understanding SpeechView:** Provide an overview of the SpeechView feature, providing users with the ability to receive transcriptions of voice messages.
- **Explore SMS Notification:** Explore the configuration of SMS notification devices in Cisco Unity Connection, and provide users access to the various configurable options through the Messaging Assistant in the Personal Communications Assistant.

In this chapter, you explore two advanced features that you can deploy in Cisco Unity Connection: fax integration and SpeechView. These features provide advanced capabilities beyond simple voice messaging, which include access to fax integration, SpeechView, and Short Message Service (SMS) notification.

The fax integration feature enables users to receive faxes in their mailbox and manage faxes using the phone, Messaging Inbox, or the Internet Message Access Protocol (IMAP) client. Users can also forward faxes to other users and send to a printer as required.

SpeechView enables users to have voice messages sent to a transcription service, where messages are then converted from voice to text. These features expand the users' capabilities beyond the sending, forwarding, and retrieving of voice messages within Cisco Unity Connection. In addition to these features, SMS notification devices can be configured to provide notification on specific message types.

In this chapter, you explore the following:

- The features, configuration, and functions of fax integration, which enable users to retrieve, forward, and print fax directly from messages in their voice mailbox.

www.it-ebooks.info

- A basic understanding of the SpeechView feature that enables users to forward voice messages to transcription service for conversion to text format.
- How to configure SMS notification within SpeechView and provide users access to notification device configuration using the Messaging Assistant.

Fax Integration

Fax Integration in Cisco Unity Connection enables users to receive faxes in their mailbox and forward a received fax to other users or fax machines for printing. Users can manage faxes using their phone, Messaging Inbox, or IMAP client. Cisco Unity Connection does create the fax itself but integrates with Cisco Fax Server.

Cisco Fax Server is an electronic delivery system for documents, voice, fax, and data that provides the delivery mechanism for many Cisco unified messaging solutions. This document delivery system provided with Cisco Fax Server is fast, secure, and provides the necessary confirmation required by most business organizations. Figure 13-1 illustrates the fax integration with Cisco Unity Connection.

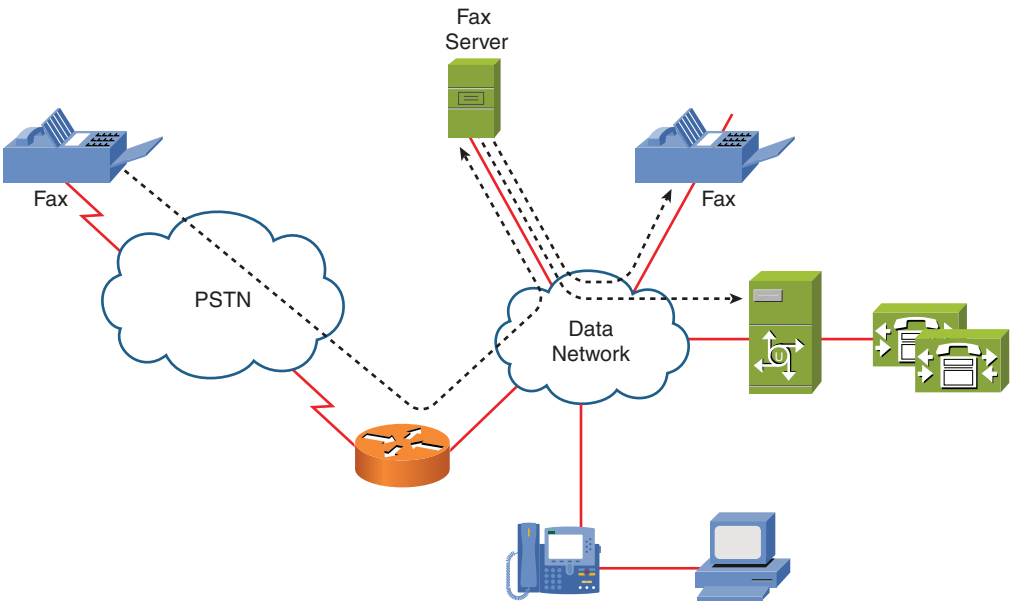

Figure 13-1 *Fax Integration with Cisco Unity Connection*

Cisco Fax Server version 9.0 or later is supported with Cisco Unity Connection v8.x software. Integrations with other manufacturers' products might function properly, though they might not be defined as being supported. The communication between Cisco Unity Connection and Cisco Fax Server is provided via the Simple Message Transfer Protocol (SMTP), whether faxes are inbound, destined for Cisco Unity Connection from Cisco Fax Server, or outbound sent from users to the Cisco Fax Server. The functionality with other

www.it-ebooks.info

fax server products depends on manufacturers' implementation of SMTP and document delivery mechanisms.

Preparation for Fax Integration

The Cisco Fax Server must be installed and configured before beginning the configuration of Cisco Unity Connection. All features and configurations of the Cisco Fax Server must be managed directly in Cisco Fax Server. Two of these configuration tasks are to configure the POP3 Service and Custom Messages for integration with the Cisco Unity Connection server.

When the fax server is configured and operational, it is responsible for managing all routing of inbound and outbound faxes, and providing cover pages, logs, alerts, and generating reports.

Faxable Document Types and Fax Reports

Cisco Fax Server supports the .txt, .docx, doc, and .tif file types, though other types can be added as needed, such as bmp types. If users send messages that include fax attachments, Cisco Unity Connection forwards only the attachment to the fax server, not the entire message. The faxable file types must also be configured in Cisco Unity Connection. By default, Cisco Unity Connection recognizes the .tif, .txt, .bmp, .doc, and .docx file types. This list of file types encompasses most faxable file types that will be encountered. Other files types can be configured as needed. However, if Cisco Unity Connection cannot recognize a specific attachment as a faxable file type, the message is forwarded along with the attachment appearing near the bottom of the message. The purpose of the fax integration is for users to receive, print, and share fax documents with other users on the system by forwarding them within Cisco Unity Connection.

To view the current file types, select **System Settings > Advanced > Fax** in Cisco Unity Connection Administration. The Fax Configuration is shown as in Figure 13-2. This page displays the faxable file types and the subject prefixes for successful and failed faxes. The defaults are indicated here but can be changed as needed. These prefixes are used by the Cisco Fax Server and Cisco Unity Connection for fax reporting and nondeliverable receipts (NDR). The Cisco Fax Server adds this prefix to the subject field for fax reporting to Cisco Unity Connection. Cisco Unity Connection then uses this report to generate receipts to a user's mailbox. In both cases, the Subject Prefixes configured in Cisco Unity Connection and Cisco Fax Server must agree. The configuration for the Cisco Fax Server configuration is performed in the Custom Messages section of the SMTP configuration on the fax server.

The fax report is sent from Cisco Fax Server to Cisco Unity Connection to indicate the status of any specific fax operation. When a fax is successfully delivered, the fax server returns a fax report with the Subject Prefix for Notification of a Successful Fax. Cisco Unity Connection compares the prefix of the report with the entry on this field. If it matches, a delivery receipt is generated and sent to the user's mailbox. Conversely, if the prefix of the report matches the Subject Prefix for Notification of a Failed Fax, Cisco

www.it-ebooks.info

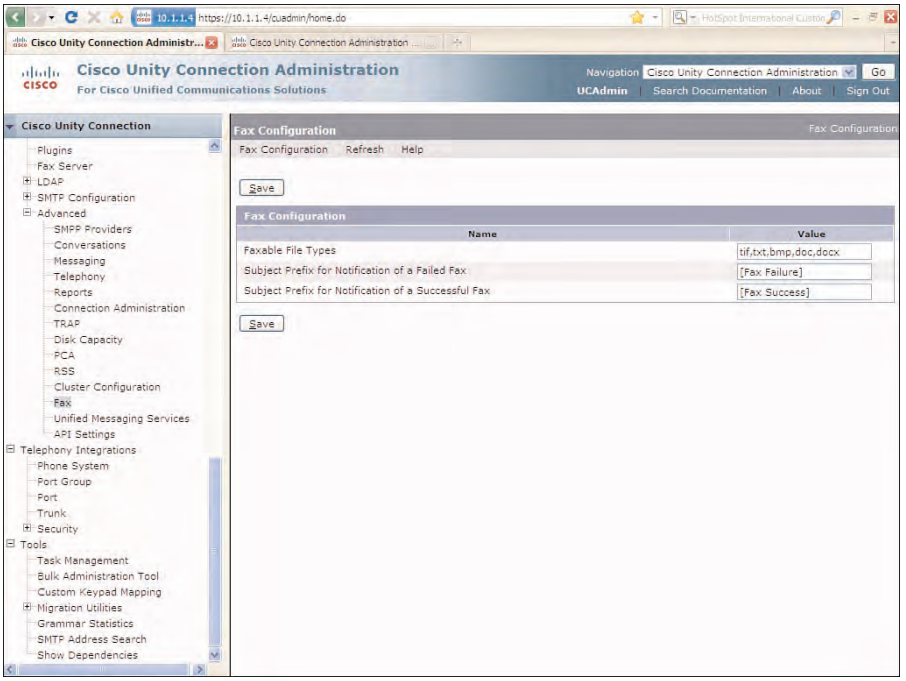

Figure 13-2 *Fax Configuration Page in Cisco Unity Connection Administration*

Unity Connection generates a nondeliverable receipt (NDR) and sends it to the user's mailbox to indicate the status of the fax. Therefore, the prefixes must be configured identically to ensure the proper fax reporting. If any modifications are made to any of these options, you select **Save** to commit any changes to the database.

Configuring Cisco Unity Connection Fax Integration

When the Cisco Fax Server configuration has been completed, you can then proceed with the fax integration configuration in Cisco Unity Connection. To begin, you must first allow access from the Cisco Fax Server because it sends and receives messages from Cisco Unity Connection. Therefore, the Cisco Fax Server *must* be configured as a trusted entity by adding the server's IP address to the access list. To complete this operation, select **System Settings > SMTP Configuration > Server** to display the SMTP Configuration page. Then, select **Edit > Search IP Address Access List** from the toolbar to display for Search IP Address Access List page, as illustrated in Figure 13-3.

The Search IP Address Access List page enables the administrator to create additional entries. Select **Add New** and enter the IP address of the Cisco Fax Server on the New Access IP Address page; select **Save**. The Access IP Address page redisplays with the configured address for the Cisco Fax Server. You need to ensure that the **Allow Connection** check box is selected. In this example, the IP address, 10.1.1.109 is configured as the IP

www.it-ebooks.info

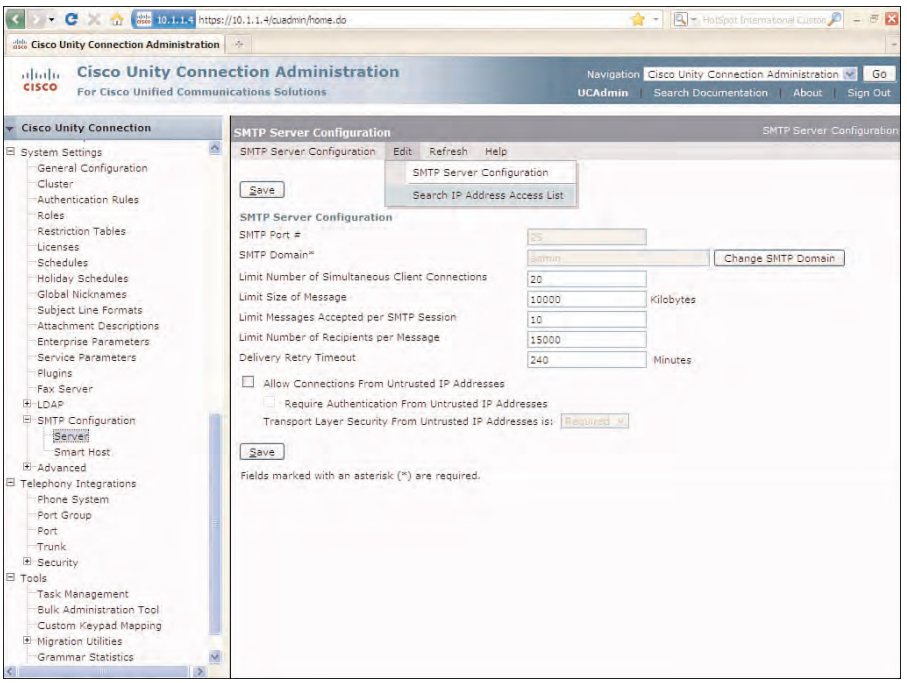

Figure 13-3 *Configuring the IP Address Access List*

address of the Cisco Fax Server. After all configurations are complete, select **Save** to commit all changes to the database.

Finally, you need to enable the Fax Server integration by selecting **System Settings > Fax Server**. The Edit Fax Server Configuration page displays, as shown in Figure 13-4. In this example, the HQ Fax Server is configured with an SMTP address of HQfax@tiferam.com and an IP address of 10.1.1.109. You also need to ensure that the **Enabled** check box is selected. The SMTP address must match the configuration for this domain on the Cisco Fax Server's POP3 Service configuration pages.

Depending on the organization's security policy and network design, fax integration can be configured to route traffic through an SMTP Smart Host by selecting the **Use SMTP Smart Host** check box. If the Smart Host is selected, however, you need to configure the Smart Host under the Smart Host configuration page by selecting **System Settings > SMTP Configuration > Smart Host** and add the Smart Host's IP address to the IP Address Access List configuration. The configuration of the Smart Host was discussed previously in Chapter 9, "Understanding Cisco Unity Connection Networking." If you deploy a Smart Host, it would be advisable to review this chapter in depth.

www.it-ebooks.info

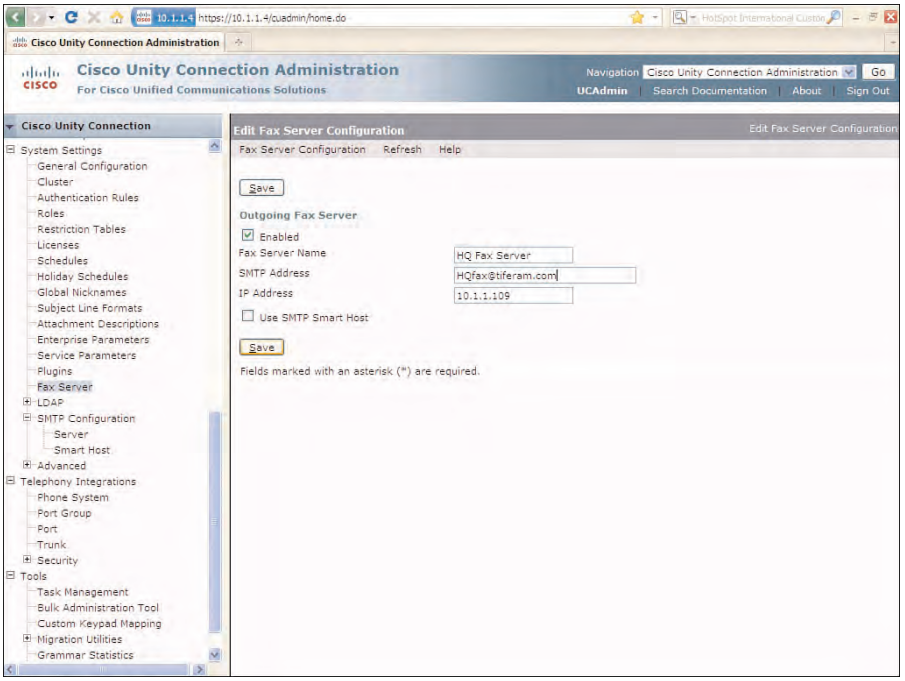

Figure 13-4 *Edit Fax Server Configuration*

Cisco Unity Connection User Account Fax Configuration

Depending on the options configured, users have the ability to perform the following functions related to sending and receiving faxes:

- **Receive faxes - available in the users' mailbox or IMAP client:** The use of the IMAP client to receive faxes depends on the configuration of the class of service for each user.
- **Forward faxes to a fax machine (printing):** Users also have the ability to change the configured fax machine through the phone interface.
- **Forward faxes to other users on the system:** Users can forward faxes from their mailbox using the phone interface, Messaging Inbox, and IMAP client. The use of the Messaging Inbox and IMAP client depends on the configuration of the class of service for each user. Inbound faxes from the Cisco Fax Server are directed to the fax extension configured on the Edit User Basics page for each user. An email gateway is used by the fax server to route faxes to the users' mailbox via SMTP.
- **Manage faxes via the phone interface, Messaging Inbox, and IMAP clients. The Text to Speech feature cannot be used for fax documents:** The user can use the Messaging Assistant to configure schedules and notifications for fax delivery

www.it-ebooks.info

Users configured in Cisco Unity Connection must exist in Cisco Fax Server to allow the sending and receiving of fax messages. Then, these users must be configured in Cisco Unity Connection with a corresponding Cisco Fax Server and fax machine configuration, which is used to allow printing of fax documents. To configure a user to send fax documents to a fax machine for printing, and receive faxes from other users, select **Users > Users** from the navigation pane in Cisco Unity Connection Administration. Then, select the specific users under the Alias column. The Edit User Basics page displays.

On the Edit User Basics page, you need to enter the phone number in the Outgoing Fax Number field and select the fax server from the Outgoing Fax Server drop-down. In Figure 13-5, the Outgoing Fax Number is configured for **8945**, whereas the **HQ Fax Server** is selected for the Outgoing Fax Server. Users can change the number for the Outgoing Fax Number from the phone interface menus. For users to send faxes, the Outgoing Fax Server option must be configured, and these users must be defined within the Fax Server configuration. These two options are for outgoing fax services. Therefore, even if these options are not configured, users can still receive from and forward fax messages to other users on the system as desired. On the Edit User Basics page, you need to select **Save** to complete the configuration.

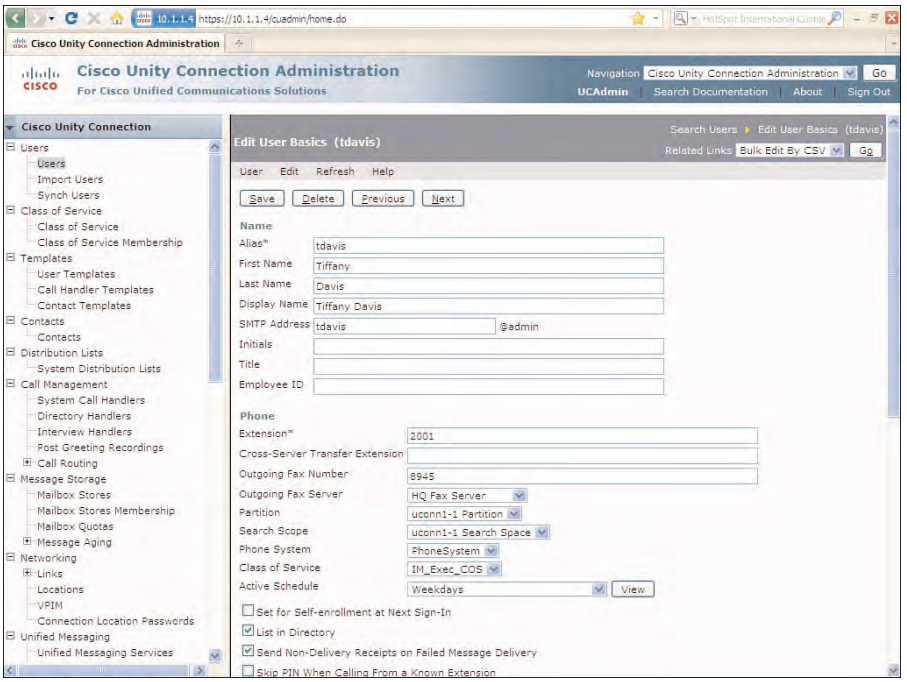

Figure 13-5 *User Configuration for Fax Integration*

www.it-ebooks.info

Fax Integration Testing and Verification

To test the fax integration for a specific user, send a fax directly to the fax extension configured for the user on the Cisco Fax Server. When the user accesses the mailbox and selects the option to play messages, Cisco Unity Connection informs the user that a fax was received, and where to send the document to the configured Outgoing Fax Number for printing or save it to the user's local workstation.

Gateway Configuration for Voice and Fax Integration

Users that have a configured Direct Inward Dial (DID) extension configured for their phone can also use this same number for voice and fax. This technology is typically referred to as *T.37 on-ramp faxing*. However, the gateway must be configured to detect the fax calling tone (CNG). The CNG tone is an 1100-Hz tone sent by a fax machine to another device to indicate a fax call. If no CNG is detected, the default configuration is that the call proceeds as a voice call.

If DID faxing is a requirement, you must download the application for fax detection from Cisco.com and configure the gateway for fax detection. The proper Cisco.com User ID (CCO) login credentials and necessary service agreement contract is required for download. From the software download page on CCO, select the Toolkit Command Language (Tcl) script file app_fax_detect.2.1.2.3.tcl or later, as illustrated in Figure 13-6. Tcl scripts require the gateway to be using H.323 or SIP because MGCP does not trigger a tcl application unless hair pinning to an H.323 or SIP gateway is configured.

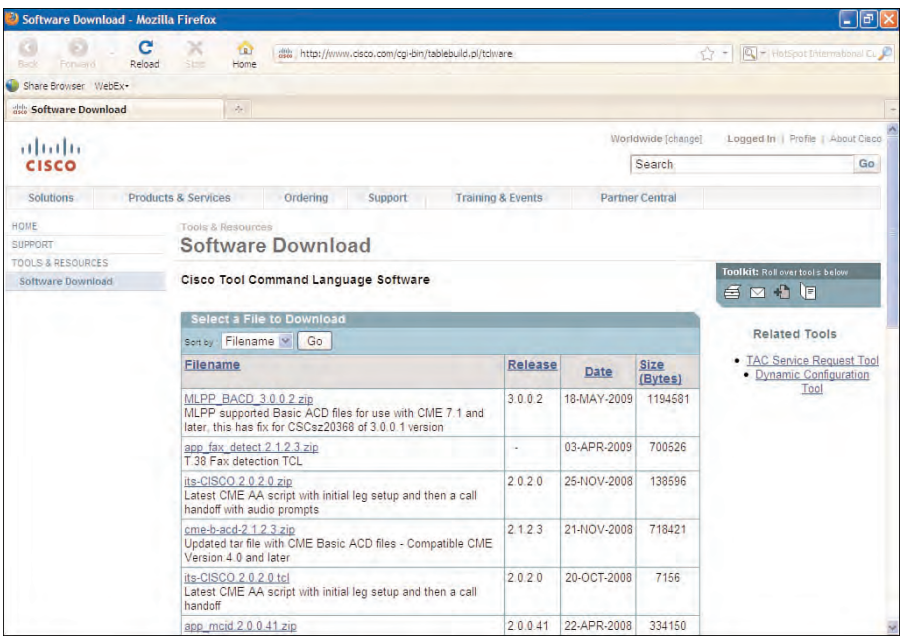

Figure 13-6 *Tcl Script for Download to Enable CNG Calling Tone Fax Detection*

www.it-ebooks.info

This Tcl application must be uploaded to the gateway and configured for fax detection. After the Tcl script is uploaded and the initial configuration is made, it requires a reload of the router to support all T.38 and T.37 IOS commands. By default, these do not display until after a reload. The Cisco Fax Server must then be configured with the DID for the applicable users. After the Tcl script is loaded on the router and defined in the configuration of the router, you need to configure this router as an on-ramp gateway for faxes. The purpose of the on-ramp gateway is to receive voice and fax calls. The gateway can be configured for either T.38 for fax-relay or T.37 store-and-forward using a mail transfer agent. The gateway configuration in Example 13-1 illustrates the partial configuration of the global and dial-peer configuration required for the T.38 fax-relay. This example is a partial configuration for demonstration purposes of the basic configuration for fax integration, and therefore further IOS configuration will be required.

Example 13-1 *T.38 fax-Relay Configuration*

```
voice service voip
 fax protocol t38
!
interface FastEthernet0/0
 ip address 10.1.1.101 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id ipaddr 10.1.1.101 1719
!
dial-peer voice 1 voip
 description Use T.38 fax-relay
 destination-pattern .
 session target ras
!
gateway
!
end
```

When testing and verifying the fax integration feature, and any feature in Cisco Unity Connection, it is advisable to select a single "test" user for this purpose. You need to test thoroughly all aspects of this feature with the test user before implementing these features to all remaining users on the production system.

www.it-ebooks.info

SpeechView

SpeechView is a new feature released with Cisco Unity Connection v8.x software whereby users can receive text copies of their voice messages. Users can review the text and print the messages as needed. This feature requires the use of a third-party transcription service to provide the actual mechanism to convert the voice message to text.

When SpeechView is enabled, all voice messages that arrive in a user's voicemail will have an attachment stating, "Transcription Pending" to inform the user that a copy of the voice message was sent to the configured transcription service. When the transcribed voice message is returned to the user's voicemail, the same attachment is updated with the actual text of the voice message. At all times, the user has access to the original voice message. SpeechView does have a limitation of allowing only the transcription of the first 500 characters for each voice message, however. If an error occurs during the transcription, this information would be updated in the attachment of the voice message.

To address the security concerns of sending voice messages to an external service, Cisco Unity Connection implemented the use of Secure/Multipurpose Mail Extensions (S/MIME) over SMTP for communication with the transcription service and the configuration of the SMTP Smart Host. The specific caller and user information is not sent to the transcription service. Also, a new key pair (for secure communication) is generated for each conversation between Cisco Unity Connection and the transcription service to ensure a secure connection.

Figure 13-7 illustrates the SpeechView communications between Cisco Unity Connection and the transcription service. In this example, the voice message is sent to the transcription service for users configured with the applicable Class of Service to allow the use of the transcription service. During this time, the user has access to the original voice message with an attachment. If the users access their messages through their IMAP client, they can access this attachment. At this point, the attachment simply has the message stating, "Transcription Pending" letting the users know that the transcription service is currently processing the message. The users still have access to the original voice message.

When the transcription service returns the transcribed voice message to the user, the attachment is updated with the transcribed message. The user then has access to the transcribed message using the IMAP client. The configuration of the SpeechView features requires the configuration of the SMTP Smart Host.

SpeechView Configuration

The configuration of the SpeechView feature begins with choosing the transcription service and obtaining the proper account information and network/authentication information. The discussion of specific third-party transcription services is beyond the scope of this text.

www.it-ebooks.info

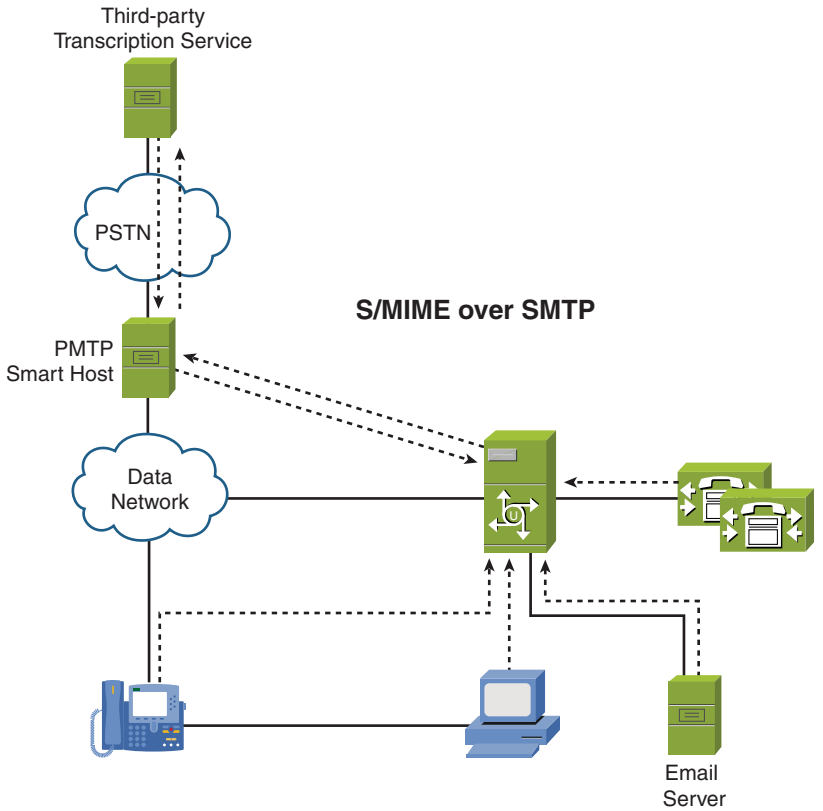

Figure 13-7 *SpeechView with Cisco Unity Connection and the Transcription Service*

After the transcription service is ready, the configuration of the SpeechView feature within Cisco Unity Connection can proceed. The steps to configure this service require that the proper licenses be installed in Cisco Unity Connection, the transcription service be defined in Cisco Unity Connection Administration, and users' Class of Service must be configured for access to the service.

SpeechView Licensing

Before any configuration of SpeechView, you must ensure that you have acquired the proper licensing from Cisco to use this feature. The default or demo licensing included with the software does not include the required licensing. To view and install the required licenses, select **System Settings > Licenses** from the navigation pane in Cisco Unity Connection Administration. Figure 13-8 shows the resulting Licenses page.

In this example, there are currently no SpeechView licenses installed as can be seen under the **Licensed Seats For** column for the SpeechView Users. This option indicates a Value of **0**. However, the User column indicates **8**, meaning that there are currently 8 users configured to use this feature by their Class of Service membership. A licensing violation has

www.it-ebooks.info

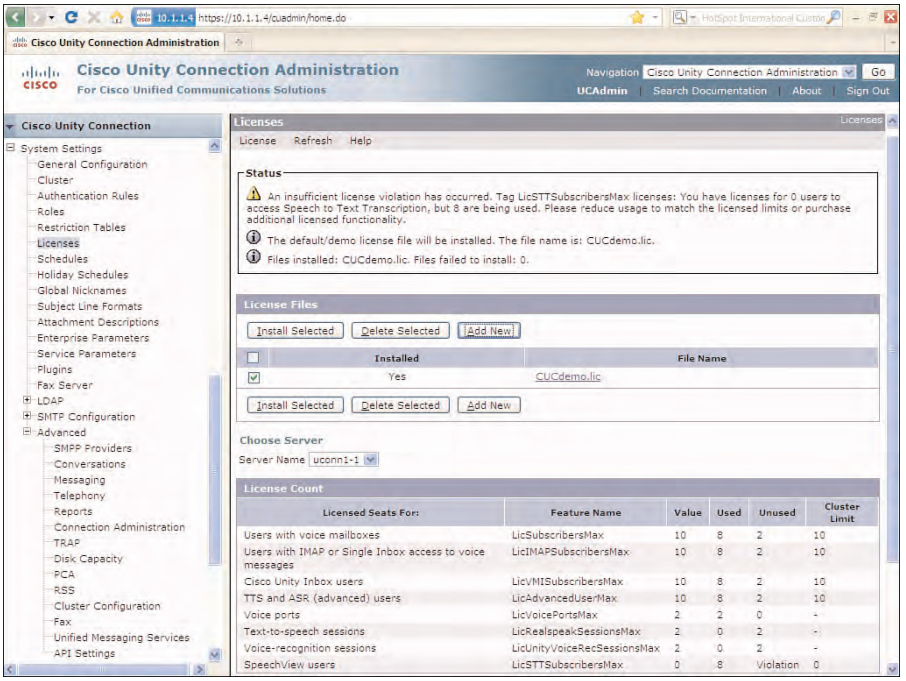

Figure 13-8 *SpeechView Licensing in Cisco Unity Connection Administration*

occurred, as shown in the Status section of this page. The licensing of SpeechView is acquired on a per user basis. This violation was caused intentionally to illustrate the licensing requirement. You must have the proper number of licenses for the desired number of users.

From the Licenses page, select **Add New** and browse to the proper license file on the Add New License page. After the license file has been added, return to the Licensing page to ensure that the correct number of SpeechView licenses is reflected under the Value option for the purchased license features. Also, you need to ensure that the violation has been removed from the Status section of this page.

Smart Host Configuration for SpeechView

To send messages from Cisco Unity Connection to a transcription service, you must configure an SMTP Smart Host to relay messages. An SMTP Smart Host is a separate server that functions as a mail relay server providing an intermediate point between two separate SMTP domains. The Smart Host also provides a level of security to filter inbound traffic from the internal servers. The Smart Host configuration must be completed by selecting **System Settings > SMTP Configuration > Smart Host** from the navigation pane in Cisco Unity Connection Administration. From the Smart Host page, you need to enter the IP address of the Smart Host in the Smart Host field and select **Save**. Refer back to Chapter 9 that covers the configuration and details of the SMTP Smart Host before beginning any configuration.

www.it-ebooks.info

Access List Configuration the Email Server for SpeechView

The email server needs to be a trusted entity because it routes incoming SpeechView traffic to Cisco Unity Connection. To complete this step, select **System Settings > SMTP Configuration > Server** and select **Edit > Search IP Address Access List** from the SMTP Server Configuration toolbar. The Search IP Address Access List page displays. You need to select the **Add New** button and enter the IP address of the email server. Finally, select **Save** to complete the configuration.

You need to ensure that the **Allow Connection** check box is selected to allow Cisco Unity Connection to enable connections from this server. The **Allow Connections From Untrusted IP Addresses** check box could be selected to allow connection for all servers, regardless of whether they are configured in the access list. However, this presents a security risk and should only be used for testing purposes or where other security features have been implemented. The configuration and details of Access Lists is discussed in Chapter 9. It would be advisable to review this section in its entirety before beginning any configuration.

Preparation for SpeechView Configuration

A number of steps must be configured beyond Cisco Unity Connection to allow the transcription service to communicate properly within the network:

Step 1. Configure the SMTP Smart Host with an external SMTP address that will be used by the transcription service to communicate to the network. All communications with the service will be initiated with this address from the Smart Host.

Step 2. Configure the external SMTP address to route messages to the SMTP address of the Incoming SMTP Address option that will be configured on Cisco Unity Connection. This address will be used by Cisco Unity Connection to route messages to the email server.

Step 3. Configure the email server to ensure that all incoming messages from Cisco Unity Connection are not filtered, and delivered properly.

SpeechView Configuration in Cisco Unity Connection Administration

After you install the proper licensing, you need to configure and register the new transcription service. To complete this step, select **Unified Messaging > SpeechView Transcription Service** from the navigation pane in Cisco Unity Connection Administration. The Transcription Service for SpeechView page displays. If you configured SpeechView for version 8.0, you an configure this option by selecting **System Settings > External Services > Transcription for SpeechView**. The menu change was implemented in version 8.5 with the introduction of the Unified Messaging feature. The Unified Messaging feature was discussed previously in Chapter 7, “Understanding User Features and Applications.”

www.it-ebooks.info

On the Transcription Service for SpeechView page, select the **Enabled** check box to enable the SpeechView service. You see the pop-up warning. Be aware of the implications of the SpeechView feature because messages are sent outside of the network to the transcription service. Figure 13-9 shows this warning message.

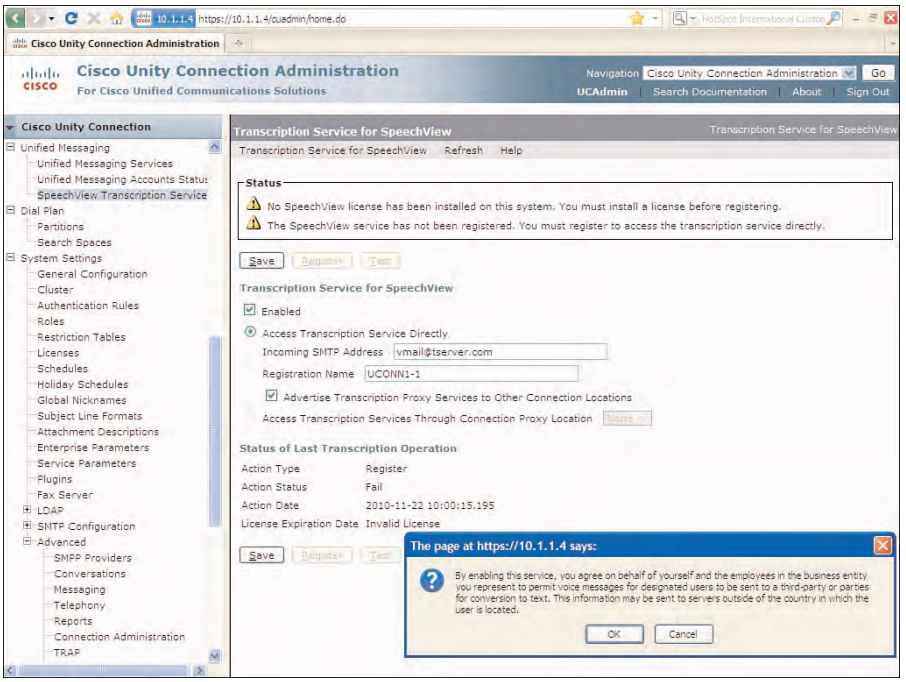

Figure 13-9 *Transcription Service for SpeechView Configuration*

In this example, the SpeechView service is enabled for communication to the transcription service at vmail@tserver.com, using the hostname of the Cisco Unity Connection server for the registration name. This communication is sent through the configured SMTP Smart Host. All communication with the transcription service is initiated from this server because you selected the **Advertise Transcription Proxy Services to Other Connection Locations** check box. In this way, all servers in the network do not need to be configured for communication to the transcription service. All communication is directed through the proxy server, enabling simpler configuration and troubleshooting.

All other networked Cisco Unity Connection servers have a configuration that has the **Enabled** option selected and the **Access Transcription Proxy Service to Other Connection Locations** radio button selected, and with this server selected from the drop-down. After all selections are completed, select **Save**. One server or cluster pair in the network should be designated as the proxy server. It is advisable to use the location with the lowest traffic volume as the proxy for connection to the transcription service.

www.it-ebooks.info

Finally, select **Test** to verify the connection to the transcription service. The network needs to be enabled with the proper SMTP information and Smart Host for access to this service. After the test has been performed successfully, select **Register** to register the transcription service. The registration should be completed within approximately 5 minutes and automatically timeouts after 30 minutes. After registration has completed successfully, the SpeechView feature is now ready for use; however, users need to be configured to use the service.

User Configuration for SpeechView

After the transcription service has been configured in Cisco Unity Connection Administration, users must have the proper access to this service based on their configured Class of Service. To complete this configuration, select **Class of Service > Class of Service** from the navigation pane in Cisco Unity Connection Administration. The Search Class of Service page displays, providing access to each currently configured Class of Service. Select the Class of Service that is to be configured to provide access to the SpeechView service or create a new Class of Service by selecting **Add New**. If you select an existing Class of Service, you must have the proper number of licenses installed to cover the current license count. Therefore, review the applicable Class of Service Membership for the Class of Service to be configured for access to the SpeechView feature.

In Figure 13-10, the **IM_Exec_COS** Class of Service is configured for SpeechView by selecting the **Provide Transcriptions of Voice Messages (SpeechView)** check box under the Licensed Features section. From this section, the administrator has the option to allow or disallow the transcription of secure messages, and to send secure messages to notification devices. In this example, the default was selected, which disallows the transcription of secure messages. All other messages can be viewed by members of this Class of Service by using their IMAP clients after the voice message has been transcribed and sent to the user's mailbox.

If users have messages relayed to an alternative SMTP address, these messages will not be available to the transcription service. If both the relay and transcription service is required for a specific user, you need to configure the user to accept and relay the message under the Message Action settings for the user.

To complete this configuration, select the specific user from the Search Users page. Then, select **Edit > Message Actions** from the Edit User Basics page to display the Edit Message Actions page, as shown in Figure 13-11. Select the **Accept and Relay the Message** option from the Voicemail drop-down, followed by the **Save** button.

In this case, the relay address was selected for the email server at HQemail@tiferam.com. Therefore, the user receives two copies of the message, one with the relayed copy of the message in .wav format, followed by a second message, which is the transcribed copy of the voice message, along with the notification. To avoid having two messages sent to the users' email, leave the default setting to Accept the Message option from the Voicemail drop-down. In this way, the users receive only the transcribed message in their email.

www.it-ebooks.info

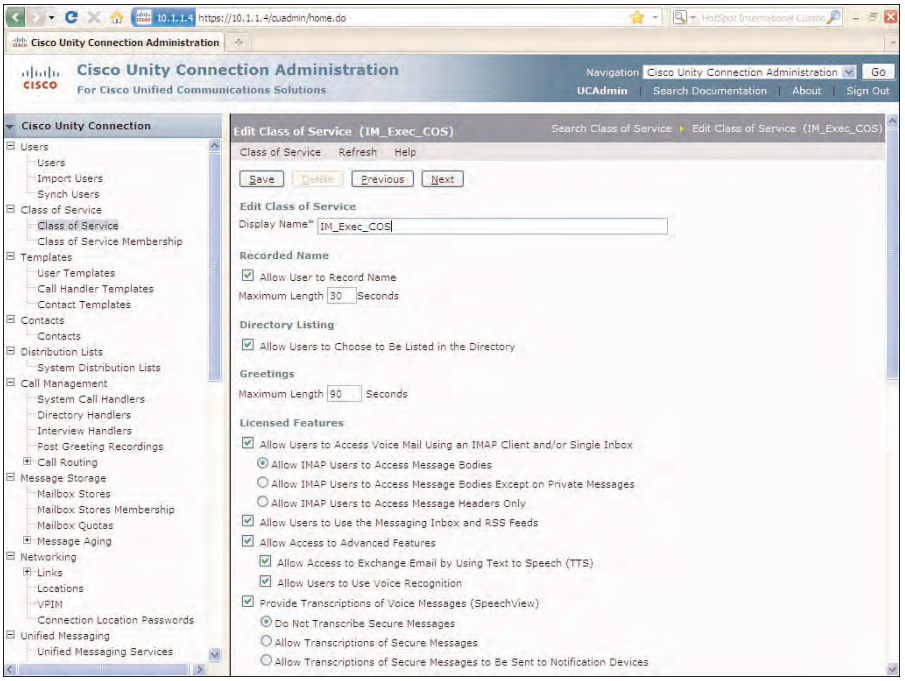

Figure 13-10 *Class of Service Configured for SpeechView*

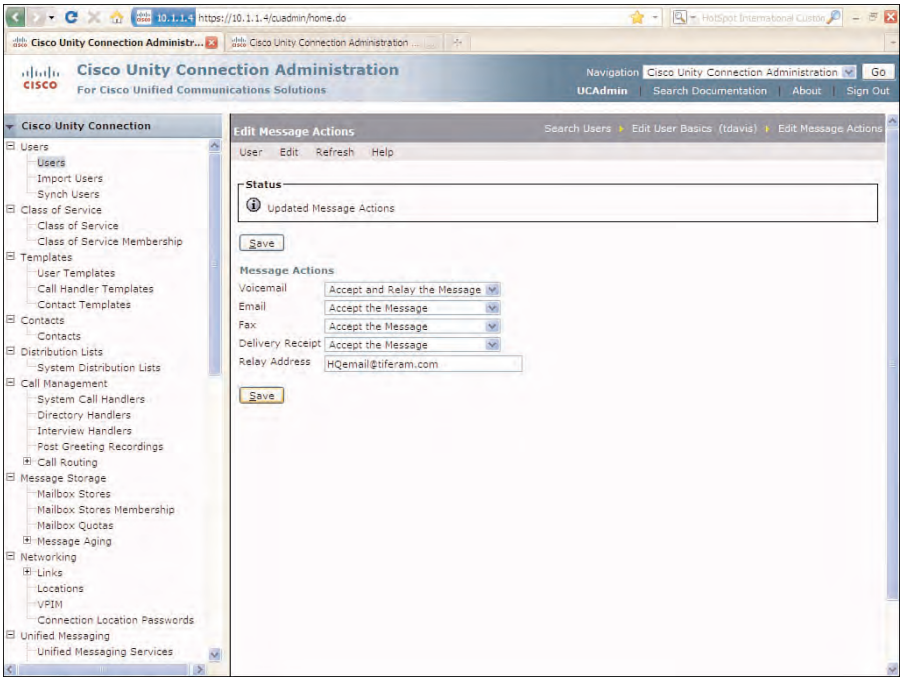

Figure 13-11 *Message Actions for SpeechView Users*

www.it-ebooks.info

However, the voice message are still available in the users' voice mailbox on Cisco Unity Connection.

Configuring Notification

Administrators can configure Short Message Service (SMS) or SMTP notifications to forward transcriptions as required. Additionally, users can configure the notification device through the Messaging Assistant within the Personal Communications Assistant (PCA) web pages.

When using this feature, only the transcribed message is included in the message, not the original voice message. However, you can configure the pilot number in the message to allow users to call Cisco Unity Connection to retrieve the message. Mobile users can forward their voice messages to Cisco Unity Connection, allowing these voice messages to be available to the transcription service. For best practices here, use a Direct Inward Dial (DID) number and configure an alternative extension for the mobile device in Cisco Unity Connection to avoid having the caller wait for multiple rings before answering.

Configuring SMTP and SMS Notification

SMTP notification can be configured by the user through the Messaging Assistant or by the Administrator using the Notification page in Cisco Unity Connection Administration. Also, for both SMTP and SMS Notification, you must ensure that ports are available and configured for notification.

To use SMS notifications, you need to configure your specific SMS provider in Cisco Unity Connection Administration. Complete this by selecting **System Settings > Advanced > SMPP Providers** and configuring Cisco Unity Connection for your specific SMS service provider. This information needs to be obtained by your SMS provider. After completing the configurations on the New SMPP Provider page, select **Save** to display the Edit SMPP Provider options.

Figure 13-12 illustrates the various configurable options for Short Message Peer-to-Peer Protocol (SMPP) on the Edit SMPP Provider page. If multiple notifications are sent to the device and depending on your specific SMS service, the final option allows the administration to replace a previous message that was delivered based on the same voice message. To configure this option, select the **Allow to Replace Message** check box. Select **Save** after all configuration options have been completed.

Cisco Unity Connection uses SMPP for communications to the configured service. The actual message is referred to as a Short Message Service (SMS) message and uses a store and forward transaction to deliver the message to the configured service, which forwards the message to the users' device. The advantage of the SMS store and forward feature enables the service to store the message until the device becomes available. When the device becomes available, all queued messages are forwarded to the device within seconds, making this option a much faster delivery option than SMTP notification.

www.it-ebooks.info

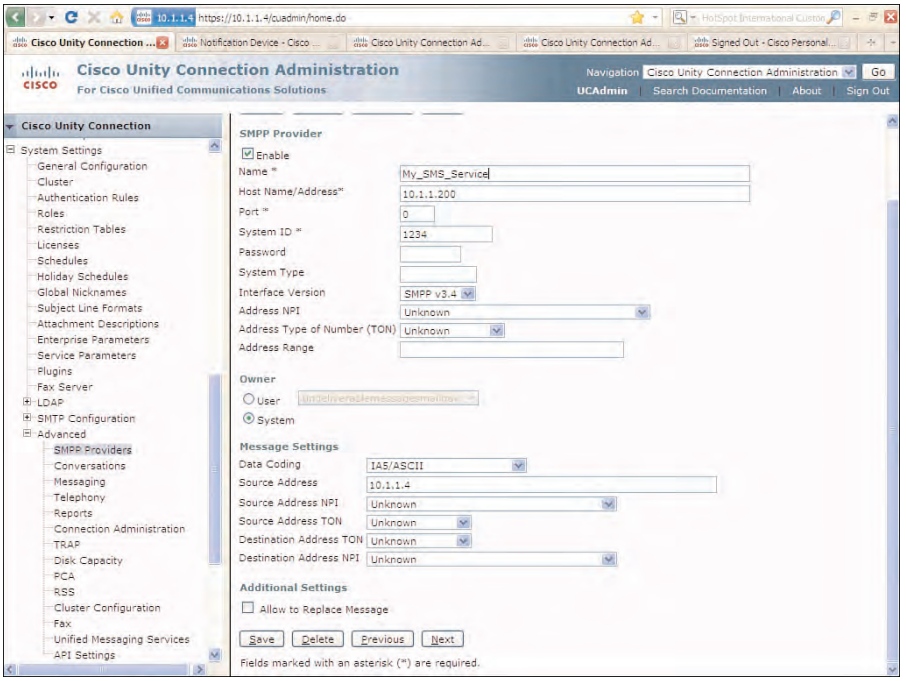

Figure 13-12 *SMPP Provider Configuration in Cisco Unity Connection Administration*

Finally, to configure the user to use this service, select the desired user from the Alias column on the Search Users page. Then, select **Edit > Notification Devices** from the toolbar on the Edit User Basics page. Select **Add New** on the Search Notification page to create a notification device for the SMS service. From the Notification Device Type drop-down, select the **SMS** option, and enter a Display Name for the applicable device. In the SMS Settings page, select the desired service provider from the SMPP Provider drop-down. Configure the **To** field with the phone number for the users' device to receive the SMS messages. In this case, the phone number is indicated using the E.164 format with "+" dialing. Of course, the actual format of the phone number depends on your specific SMPP provider. The **From** field indicates the number of the voicemail. Depending on the device, when users receive the message, they can select the Return Call button to call in to voice mail and retrieve the original voice message. Finally, the Message Text field provides information to the notification device of the specific notification. In this case, the message New Voice Message was configured. Also, this information and the message count are included in the message text, as illustrated in Figure 13-13. After you select the configuration options, click **Save** to commit your changes to the database.

www.it-ebooks.info

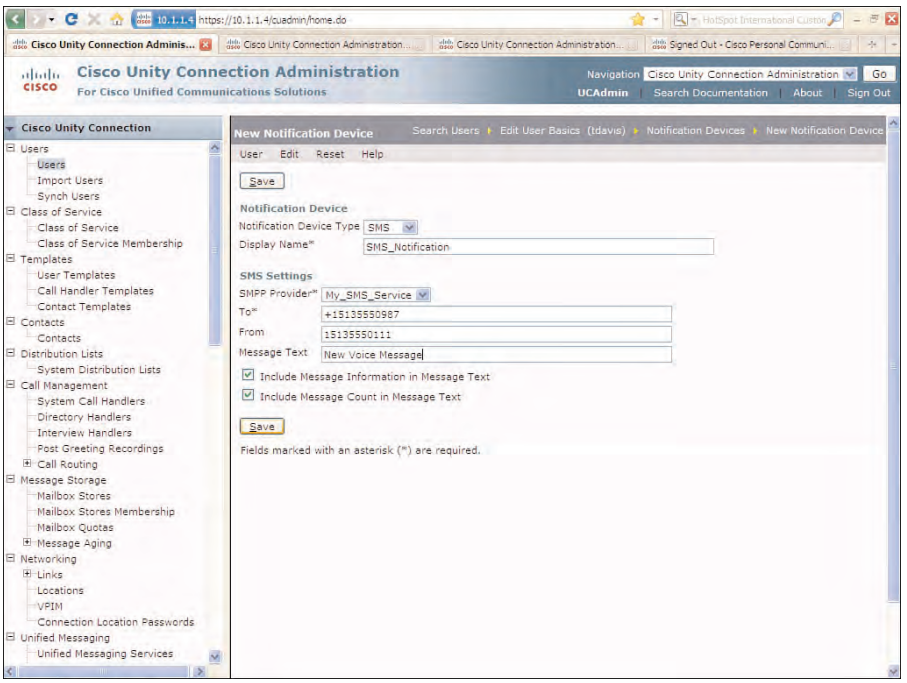

Figure 13-13 *New SMS Notification Device Configuration for SMS Notification*

After clicking **Save** on the New Notification Device page, the Edit Notification Device page displays enabling the administrator to select various options specific to this device. In Figure 13-14, this device is enabled to send notifications only for urgent voice messages.

After the configuration of the SMS device is complete in Cisco Unity Connection, users can be provided access to these configuration options in the Messaging Assistant in the Personal Communications Assistant. For users that have been provided access to the Messaging Assistant by their Class of Service, they can log in to the Personal Communications Assistant web pages and access the Messaging Assistant. From the Messaging Assistant pages, these users can select **Notification Devices > View Notification Devices** from the toolbar.

In Figure 13-15, the user configured in the previous steps selected the Notification Devices page in the Messaging Assistant. The Message Notification page displays showing the new SMS device that was previously configured.

From this page, the user can select the SMS device and configure the specifics regarding the notification device, options, and schedules, as shown in Figure 13-16.

When the configuration is complete, it is advisable that you test thoroughly with a “test user” before configuring other users on the production system.

www.it-ebooks.info

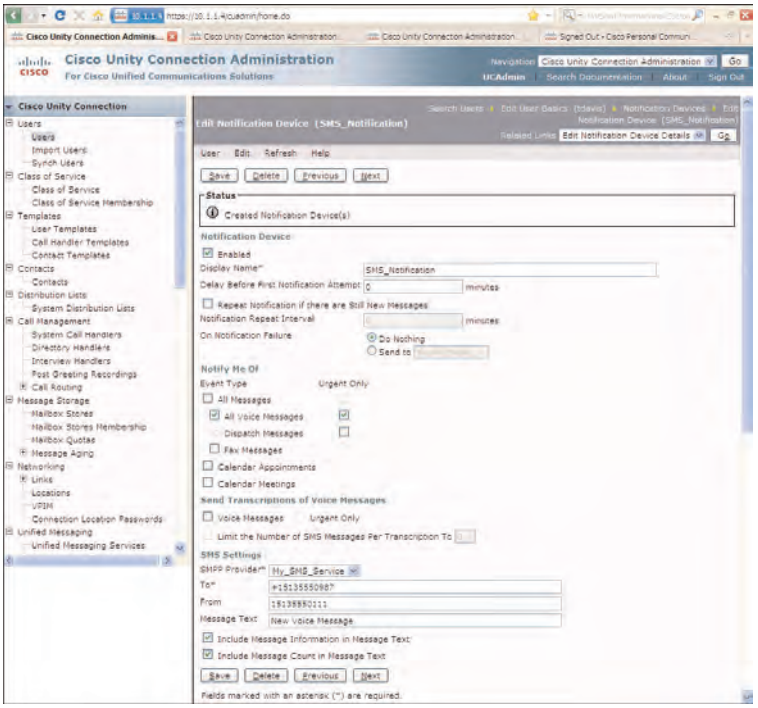

Figure 13-14 *Edit Notification Device Configuration for SMS Notification*

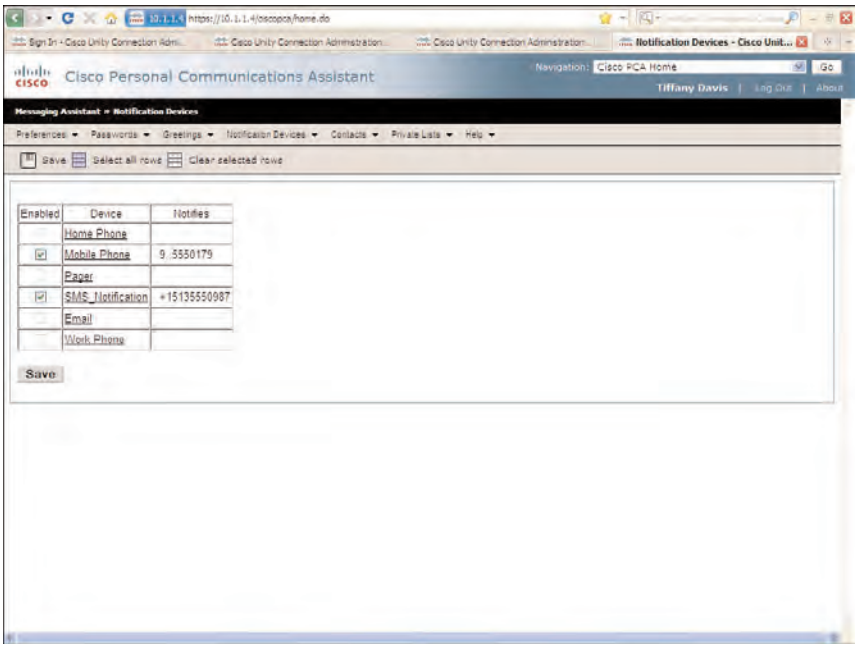

Figure 13-15 *Notification Device Page in the Messaging Assistant*

www.it-ebooks.info

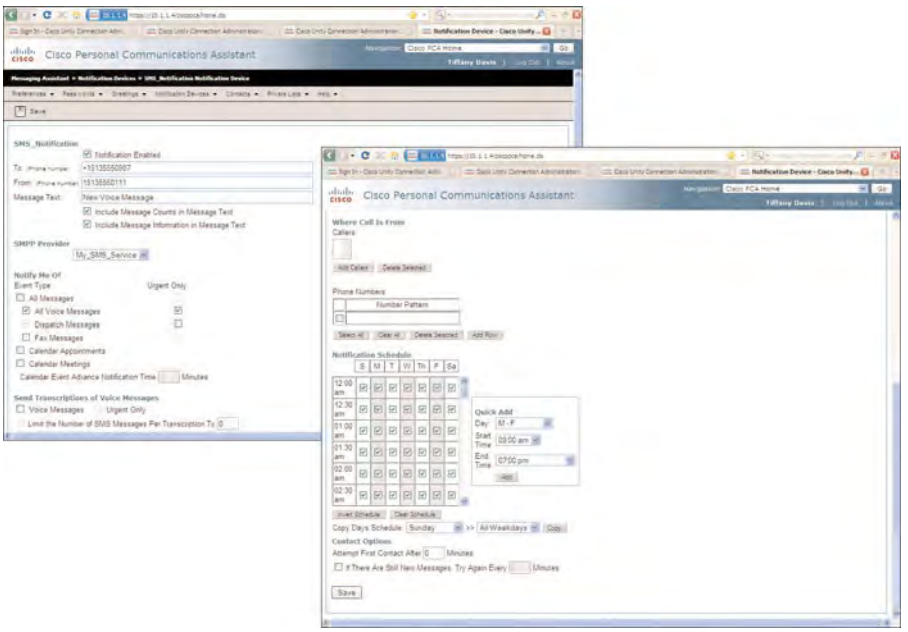

Figure 13-16 *SMS Notification configuration in Messaging Assistant*

Summary

This chapter provides an understanding of two of the advanced features that you can use in Cisco Unity Connection. You have learned how to do the following:

- Configure fax integration in Cisco Unity Connection to allow users to receive fax messages in their mailbox and forward to other users or send to another fax machine for printing.
- Investigate the SpeechView feature was released with Cisco Unity Connection version 8.x software to provide integration with a third-party transcription service allowing users to receive transcriptions of their voice messages.
- Configure SMTP notification and SMPP in Cisco Unity Connection to provide SMS notification and allow users the flexibility to configure notification using the Messaging Assistant.

www.it-ebooks.info

This page intentionally left blank

www.it-ebooks.info

Chapter 14

Troubleshooting Cisco Unity Connection: Case Studies

This chapter provides an understanding of the basic troubleshooting concepts and provides a technical review and case studies based on typical issues encountered in today's voice messaging system using Cisco Unity Connection. This overview consists of the following:

- **Troubleshooting Techniques:** Understand the concepts and procedures for effective troubleshooting to quickly resolve issues and problems.
- **Case Studies:** Provide a sample of typical case studies for issues reporting in a Cisco Unity Connection voice messaging system.

Your Cisco Unity Connection network has now been installed and configured according to the proposed and approved design; however, issues and problems can arise with even the best designed and planned implementations. Some of these issues are related to incorrect configurations, and some are related to changes in the network. Other issues are related to changes in user needs and concerns that were discovered during the implementation phase. A good design enables modification. There is no reason why adaptations should cause unnecessary turmoil in the organization, as long as the engineers and administrators have the necessary troubleshooting skills and understanding to address these issues. Engineers and administrators that work directly with the implementation phase or on an ongoing basis, including the optimization phase, need to understand some of the basic troubleshooting techniques. Also, these individuals must become familiar with the various tools in Cisco Unity Connection to quickly bring an effective resolution to any issues encountered. Many of these tools were discussed throughout the previous chapters.

This chapter attempts to provide a compilation of some of the more common issues that can be identified in Cisco Unity Connection. These issues are varied in scope, dealing with various aspects of features, integration, and networking. The information provided here is not intended to be an exhaustive list, but an overview of the more common issues to assist the engineers in their understanding.

www.it-ebooks.info

This chapter provides the following information:

- Basic troubleshooting techniques for resolving issues and problems with Cisco Unity Connection voice messaging systems
- An overview of common issues encountered with Cisco Unity Connection and their possible solutions

Basic Troubleshooting Techniques

Many engineers state that good troubleshooting techniques are skills learned over a number of years, are often based on past experience, and require a good understanding of the tools and technology. This is true in many ways, and you cannot trade good experience and knowledge. However, many experienced engineers who are excellent installers can explain the technologies quite elegantly, but often aren't the best troubleshooters.

Troubleshooting is an art, based on the individuals' craft and knowledge and their ability to quickly identify the problem and to implement a proper solution. An engineer that is good at troubleshooting and problem resolution will always be in high demand in most organizations. Unfortunately, there are many engineers that resolve to say they are just not good at it, and move on. However, most of there individuals can be better at troubleshooting by considering some basic troubleshooting techniques.

Throughout the last number of years, I have been traveling throughout the United States teaching Cisco technology courses. In nearly all these classes, I always discuss the basics of good troubleshooting because I believe it is important information that everyone working in the field should understand.

There are a lot of right ways to troubleshoot a problem; there are also many more wrong ways. Good troubleshooting is comparative to an expert marksmen shooting at a target. They identify the situation, focus on target, and hit the mark. This focus can involve assessing the situation and developing a plan and strategy before implementing any changes. Of course, the level of assessment and planning depends on the nature and size of the issue.

It is easy to take the wrong approach, especially when under pressure. This approach is the "shotgun approach" to troubleshooting. In other words, just aim in the general direction and fire away, trying anything that is in the general area or might relate to the issue, and hope you hit the target. If you miss, turn in the other direction and repeat. This approach is haphazard and should be avoided at all costs.

When the pressures come, it is easy to simply "try something," if that doesn't work, try something else. The problem with this trial-and-error approach is that little thought is given based on the problem, and what other issues might be caused by the changes being made. In most cases, any changes that had no effect on the situation were not removed and could possibly cause additional issues. Therefore, the marksmen approach is discussed, which provides a thorough assessment of the situation and a well-developed plan and strategy based on a complete understanding of the situation. Finally, the goal of this approach is to bring a proper, accurate solution to the issue.

www.it-ebooks.info

Stay the Course

In many cases, the problems with poor troubleshooting usually relates to an individual's approach to the problem and external distractions. I remember years ago, when I encountered a problem in the network while contracting at a large organization. I was the only person in the office at the time, and the network was down.... Hard down! I was attempting to resolve this issue on a complex network, while having the CIO and managers from various departments coming into my office asking me when the network would be up. At that time, I really wanted to tell them it would be up when they got out of my office, but decided that was not a good idea <wink>. Many of you reading this know exactly what I mean and have been in this situation. Anyway, I was able to get the issue resolved to the delight of these users, in spite of the undue stress these individuals added to the situation. Unfortunately, the constant inquiries from users don't help the troubleshooting process. However, issues and problems in the network directly affect the workflow and productivity of users; therefore, a little understanding and empathy is required during these situations.

A good troubleshooter continues on the path to resolve the issue, regardless of external forces, users, and managers that might not be necessarily adding to the solution. Continuing on this path means staying the course of using good troubleshooting techniques to resolve the problem. These techniques are varied from text to text, but include the basic following concepts:

Step 1. Assess the situation.

Step 2. Develop the plan and strategy.

Step 3. Use good troubleshooting procedures.

Step 4. Provide reporting, resolution, documentation, and lessons learned.

Assess the Situation

The first step in good troubleshooting techniques is to assess the situation by defining the scope of the problem. The tasks that need to be completed here include the following:

- Define the problem:
  - Are all users affected?
  - What systems are impacted?
  - Does the issue occur at a specific time of day?
  - Did it ever function properly?
- Gather the facts:
  - Interview users if necessary to get an understanding of the problem. Understand that this might require discussion with multiple individuals because some of this information or reported trouble might be vague.

www.it-ebooks.info

- Use the tools available to help identify the issue. The use of specific tools such as the Real-Time Monitoring Tool (RTMT) and the Remote Port Status Monitor might help to quickly locate specific issues.

Develop the Plan and Strategy

After you gather the necessary information and understand the scope of the problem, you will have a better understanding and be armed with the necessary information to develop a plan of attack in resolving the issue. Your plan should follow a defined path. Depending on the depth of the issue, this plan might include multiple options and directions. For example, if you work on an issue having to do with connectivity, always follow a plan that breaks the problem down into smaller parts, and test from source to destination.

Any plan should have a defined strategy, like a chess game in which the players look ahead by multiple moves. Any plan and strategy should include the following:

- **Develop a plan before beginning any configuration changes:** Any good plan has a developed strategy. Your plan must be explainable as to the reason for any changes that relate directly to the problem. The strategy should have a defined path of resolution from source to destination.
- **Understand your next move and keep notes on what was implemented or changed:** This can help you and your team to decide on the next moves and also to help develop a reporting mechanism to management on the situation. Finally, all changes must be documented and the current documentation updated. Good documentation or the troubleshooting procedures provides forensics to the current situation and resolution and also provides a reversion strategy, in the case where a specific change doesn't fix the issue. In this case, any changes can be easily reversed to avoid making unnecessary changes.

Use Good Troubleshooting Procedures

Observe the following points when employing good troubleshooting techniques:

- Use the marksman approach and stick to your plan; although, adjust the plan as changes to the issues are encountered.
- If changes are made to the network and no resolution has been identified, remove any configurations that were added that had no affect on the current situation. If the changes are left in place for any reason, document these changes.
- Break any problem down into smaller parts or sections.

www.it-ebooks.info

Provide Reporting, Resolution, Documentation, and Lessons Learned

Observe the following points when troubleshooting, to provide good reporting, resolution, documentation:

- Keep good notes throughout the process. This is necessary to report to management, and to update the current documentation.
- Review the entire situation from beginning to end. In some cases, your entire team might come together to review the problem. The reason for this review should be to understand the current situation in the aftermath of the resolution. Following are the items you need to address in this meeting:
  - Understand the issue and why it occurred.
  - Review the current status and understand the likelihood of a reoccurrence.
  - Define what modifications and upgrades need to be made based on the review.
  - Review and document the lessons learned for the team for any future occurrences of this or similar issues.
  - Update all documentation with any changes or modification made during the troubleshooting stage.

Troubleshooting MWI Issues

Trouble Ticket #1: Users in the finance department report that their MWI lights do not function.

Scenario

Wow! This is a good example of a bad trouble ticket that lacks information and definition. However, MWI issues are some of the most common and daunting issues encountered in voice messaging systems. This one is going to take some investigating, based on the level of information.

You need to discover the extent of the issue and who is affected by the problem. This discovery needs to include whether the problem is with a single user, the entire finance department, or other departments that didn't take the time to report an issue. However, at least you know that it originated in the finance department. So, you take a walk over to the finance department and decide to ask a few more questions. Because the finance department is on its own Cisco Unity Connection server, you suspect there might be an integration problem. On your way there, you start to think about its integration and MWI on and MWI off configuration between its server and the phone system. One of the junior engineers completed this configuration in the past week.

www.it-ebooks.info

When you arrive at the finance department, you ask the following questions:

- **Question:** What users have problems with their message waiting light?
  - **Answer:** Only Sally and Janis have the issue. (The remaining 20 users do not have any problems.)
- **Question:** What exactly is the MWI issue that these two users have?
  - **Answer:** The MWI light never turns on, even though new messages arrive at their mailbox.
- **Question:** Are these new users or existing users? Has their MWI ever functioned properly? And when did this problem start occurring with each user?
  - **Answer:** Sally is a new user, and her MWI has not worked since she started this past week. Other new users have not had this issue.
  - **Answer:** Janis is an existing user. Her MWI stopped working in the past week.

On your way back from the finance department, you decide to stop by at some of the other departments to verify there are no problems with the MWI lights. By asking a number of users, it appears that the extent of the problem is confined to the MWI lights for Sally and Janis.

Note It is important in the troubleshooting procedures to perform multiple tests to ensure that the issue is repeatable. Also, acquire all information pertinent to the situation, along with any logs available if you need to open a case with the Cisco TAC.

Resolution

After three questions, you now understand the scope of the problem. This appears to be a minor issue, and there is no need to review the options for the MWI configuration on the configuration because all other users are not experiencing problems. However, users can lose MWI synchronization, whereas other users might not be affected. Also, because one of these users is a new employee, you decide to review the configuration because this might directly relate to the issue.

From the investigation, you believe that the integration is operating correctly because other users on the system are not affected. You focus your troubleshooting efforts on two items; the user configuration for the new user and MWI synchronization.

Because Sally is a new user, from the Edit User Basics menu, you review the MWI configuration by selecting **Edit > Message Waiting Indicator**. On the Message Waiting Indicator page, you select the MWI-1 option to review the configuration. The Edit Message Waiting Indicator page displays. From this page, you notice that the **Enabled** checkbox is not checked, causing the MWI light to be disabled, as illustrated in Figure 14-1. You correct this issue by checking the **Enabled** checkbox and selecting **Save**. A call to the finance department confirms that the MWI light is now functioning properly on Sally's phone.

www.it-ebooks.info

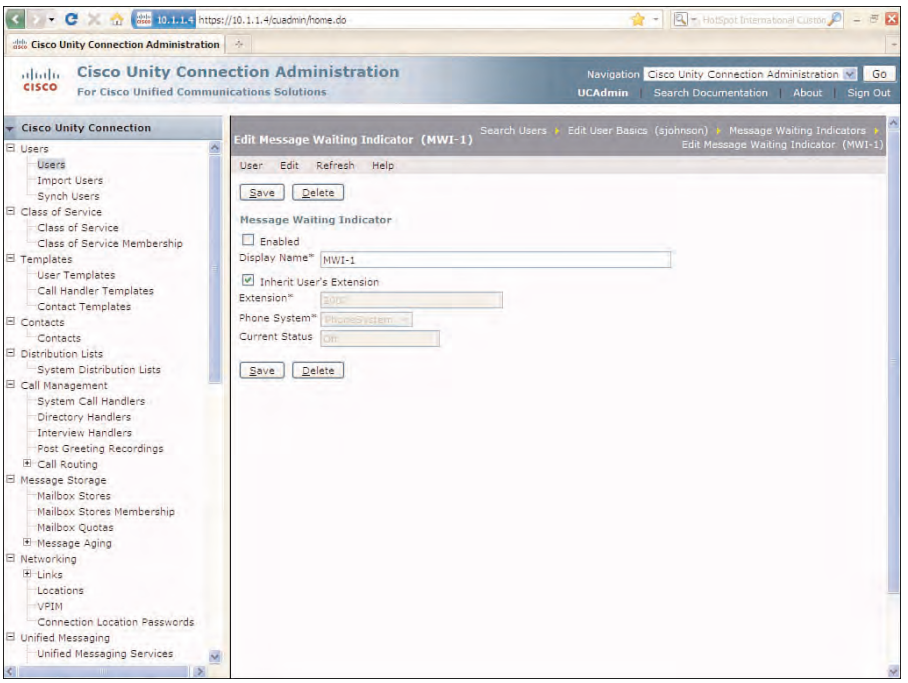

Figure 14-1 *Edit Message Waiting Indicator Configuration*

You check the same configuration options on Janis' configuration; however, it is configured properly. Because the configuration is correct and uses the same integration as all other users, you decide to synchronize the MWI. Therefore, from the navigation pane, you select **Telephony Integrations > Phone System** and select the phone system used for the finance department. Under the Message Waiting Indicators section, you select **Run** to Synchronize All MWIs on This Phone System, as shown in Figure 14-2.

You place a call to the finance department to check on the MWI status for Sally and Janis and learn that everything is function properly. You close the ticket, document the change, and instruct the administrators on the MWI configuration of new users.

This was a relatively easy problem to resolve. However, suppose that all users on a specific Cisco Unity Connection server were experiencing an issue. Then, the plan and strategy might begin with checking the configuration of the MWI on and MWI off on both Cisco Unity Connection port group configuration and Cisco Unified CM, if it were a new installation. If it were an existing implementation that worked previously, your plan might include this review, running the synchronization, checking port availability, and also using the Remote Port Status Monitor to monitor the sending of the MWI to Cisco Unified CM from Cisco Unity Connection port.

Figure 14-3 illustrates the use of the Remote Port Status Monitor to review the sending of MWI after the MWI synchronization was run under the Phone System configuration page.

www.it-ebooks.info

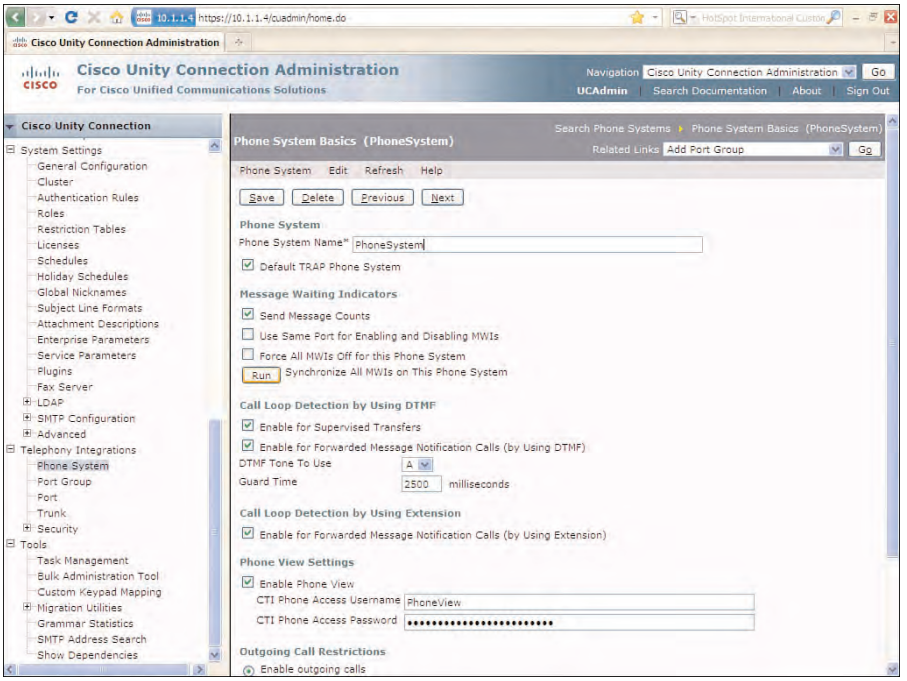

Figure 14-2 *MWI Synchronization on the Phone System Integrations Page*

Figure 14-3 *Remote Port Status Monitor to Monitor MWI*

www.it-ebooks.info

Troubleshooting Call Transfer Rules

Trouble Ticket #2: Incoming callers are no longer hearing the company opening greeting. Callers are hearing a recording informing them about implementation testing initiated on the new Cisco Unity Connection system.

Scenario

At first view of a ticket like this, you might easily get focused on the wrong issue. The problem is not the actual recording that the caller is hearing. The real questions to ask here are which users have this issue? And what are these users dialing? After asking these questions, you understand that all customers calling the headquarters' main phone number experience this problem. Further information informs you that these callers automatically ended up at this call handler, without making a menu selection.

Because the caller hears a different recording could mean that these callers are directed to the incorrect call handler. Therefore, the Direct Routing Rules need to be reviewed because these configuration options directly influence the caller experience for calls placed directly to Cisco Unity Connection. From here, you might need to review the specific call handlers identified within these routing rules. Also, you need to verify the specific greetings recorded for each call handler because someone might have changed the greeting on the wrong call handler using the greeting administrator.

Resolution

To begin your investigation, log in to Cisco Unity Connection Administration and review the direct routing rules by selecting **Call Management > Call Routing > Direct Routing Rules.** On the Direct Routing Rules page, you notice that a new rule exists as the first rule directing all calls to a call handler called TEST_CH, as shown in Figure 14-4.

After further investigation, you realize that a junior administrator was testing a new direct routing rule and meant to include a condition that would only direct the phone with extension 2034 to this new TEST_CH. The rule was added, but the condition was not included. Therefore, all calls were directed to the TEST_CH call handler. The junior administrator did not notice the Status warning at the top of the page that states that there are no conditions defined for this routing rule, and therefore all calls will be matched. However, this administrator still needed to run the test with the extension, so the condition was added to this new direct routing rule to resolve the issue. The condition stated that the rule would apply only to calls from extension 2034. All rules are acted on from a top-down basis. Figure 14-5 illustrates the resolution for the Direct Routing Rules.

www.it-ebooks.info

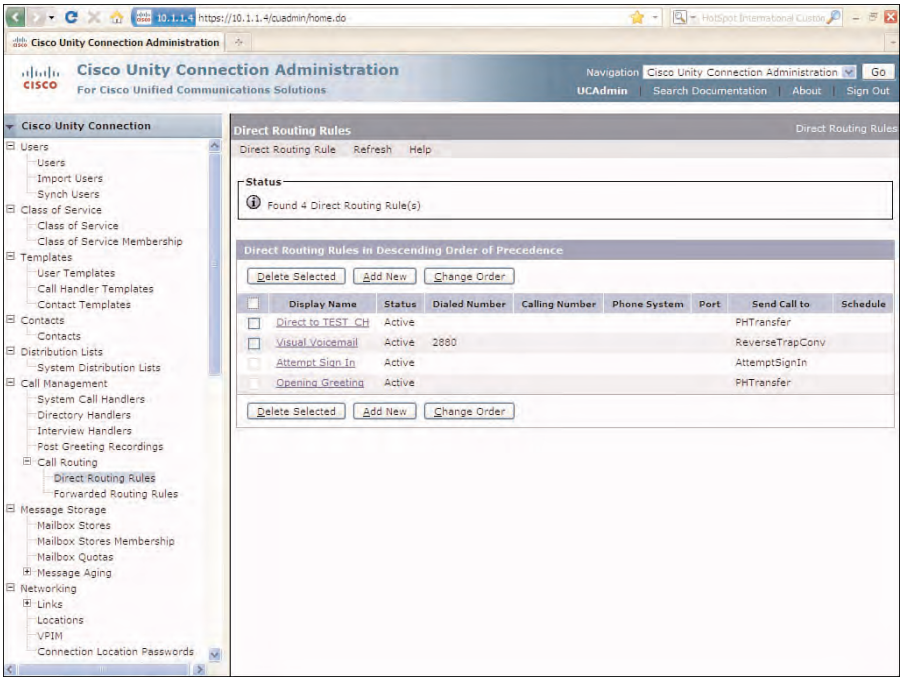

Figure 14-4 *Direct Routing Rules Review and Problem Identification*

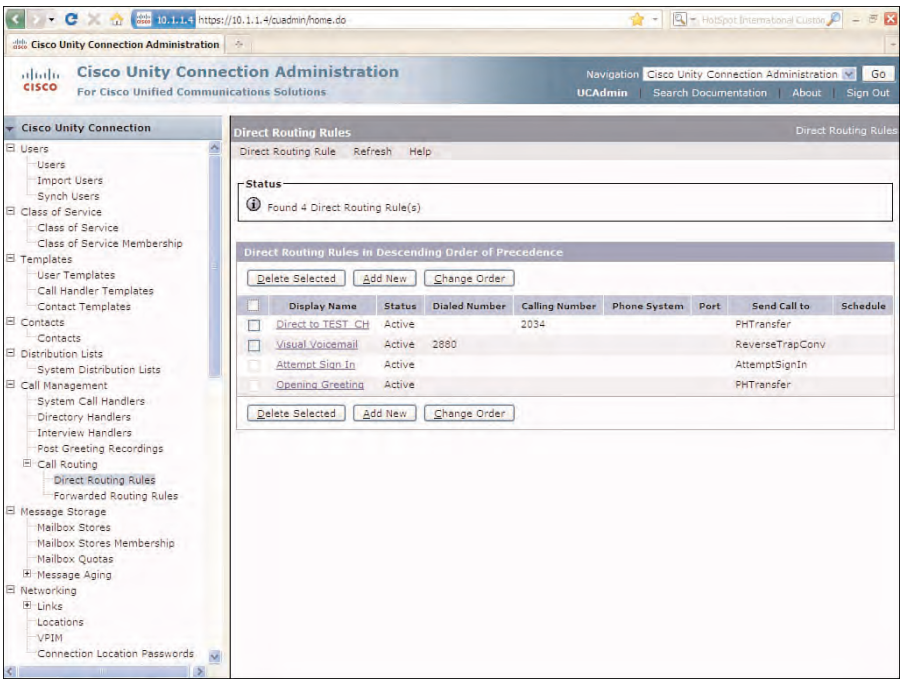

Figure 14-5 *Direct Routing Rules Resolution*

www.it-ebooks.info

After completing the configuration of the direct routing rules, testing and verification confirmed that all calls were directed to the Opening Greeting, with the exception of the junior administrator's extension (2034), which was directed to the TEST_CH call handler according to the first direct routing rule. The Remote Port Status Monitor could also be helpful in this situation to identify which call handler and routing rule is being matched.

Troubleshooting Partitions and Search Scopes

Trouble Ticket #3: Executive users cannot address messages to the Administrative users. Incoming callers dialing the corporate number do not hear the proper Opening Greeting.

Scenario

It was understood that this was a new implementation. You investigate this trouble ticket more thoroughly and find that this issue is specific to the Cisco Unity Connection server at the headquarters' locations. You interview a few executive users and find a common problem. That is, executive users cannot address messages to other users, and they cannot address messages to other executives or access the various directories or call handlers.

Resolution

Resolving issues of this type requires an understanding of what is actually happening when a user tries to address a message. Because you know that users can access their voice mailboxes, you can eliminate an issue with integration or routing rules. In this case, access to resources involves the configuration and assignment of the partitions and search scopes. Because this was a new implementation, you can begin your investigation of current configuration parameters, specifically the configuration for the dial plan.

To begin the troubleshooting procedure, you decide to use the marksman process by focusing on one specific user and tracking the problem down from source to destination. Jack Warner is and chief development officer at headquarters. You review his configurations on the Edit User Basics page and notice that the search scope is configured with the EXEC_SS, and the partition is configured with the Exec_PT. This is the correct configuration according to the design documentation.

Next, you review this search scope by selecting **Dial Plan > Search Spaces** from the navigation pane in Cisco Unity Connection Administration and selecting the **EXEC_SS** from the Names column. The Edit Search Space reveals the problem. All configured partitions are displayed under the Unassigned Partitions pane, as illustrated in Figure 14-6.

The **Admin_PT** and **Exec_PT** are added to the Assigned Partitions pane to resolve the issue, as shown in Figure 14-7. After retesting, you can verify that the executive users can

www.it-ebooks.info

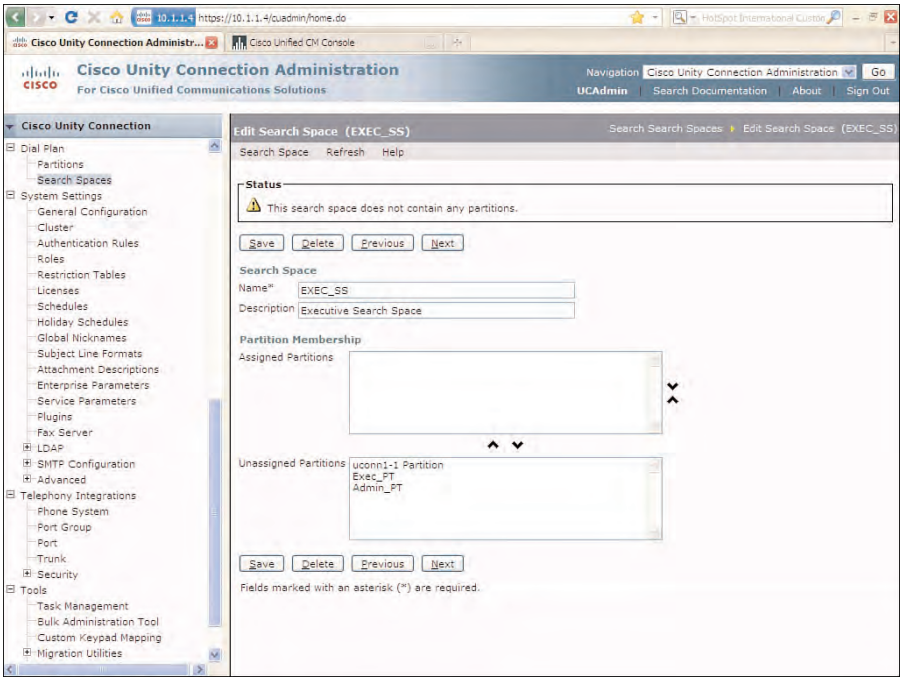

Figure 14-6 *Edit Search Space Review and Problem Identification*

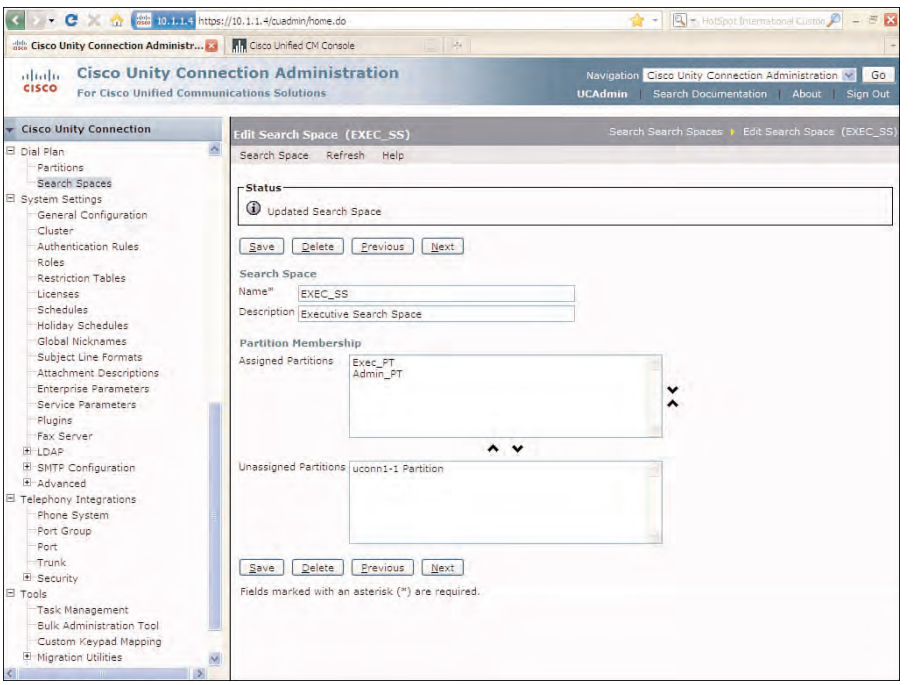

Figure 14-7 *Edit Search Space Resolution*

www.it-ebooks.info

now address messages and access all resources (distribution lists and call handlers) in the **Admin_PT** and **Exec_PT** partitions. You notice that even though the other users had the same search scope, they did not have the partition in their search scope and therefore could not address messages to these users.

Troubleshooting Dial Plan Issues in Digital Networks

Trouble Ticket #4: Admin users from the HQ location cannot address messages to the sales department. However, these users can call it directly.

Scenario

After further investigation, you realize that your partner just implemented a new Cisco Unity Connection cluster pair in the sales department and networked this location with the existing HQ location. Everything is operating properly at each location, but there is no access to resources and users between the two locations.

Resolution

By your understanding of the networking and the dial plan, you realize that the partitions from the remote location are not automatically added to the local search scope. The search space and partitions can be managed only at the location where the objects are created; however, the remote partitions can be added to the local search spaces to provide access to the remote users, distribution lists, and call handlers. Figure 14-8 illustrates the **EXEC_SS** at the HQ location. The only partitions included in the search space are the local partitions for HQ, which are the **Exec_PT** and **Admin_PT** partitions.

The two system partitions, **uconn1-1 Partition** and **uconn1-2 Partition**, are not used in the current implementation. Also, users in the EXEC_SS search scope have access only to resources in the **Admin_PT** and **Exec_PT** partitions. This is the default behavior after the networking was completed. Unfortunately, moving the remote partitions to the local search scopes was not completed to provide access to remote resources. To correct the issue, the **Sales_PT** partition is selected followed by the Up Arrow to move this partition from the Unassigned Partitions pane to the Assigned Partitions pane. Finally, select **Save** to commit the changes to the database. The Edit Search Space for the EXEC_SS search scope is shown in Figure 14-9.

www.it-ebooks.info

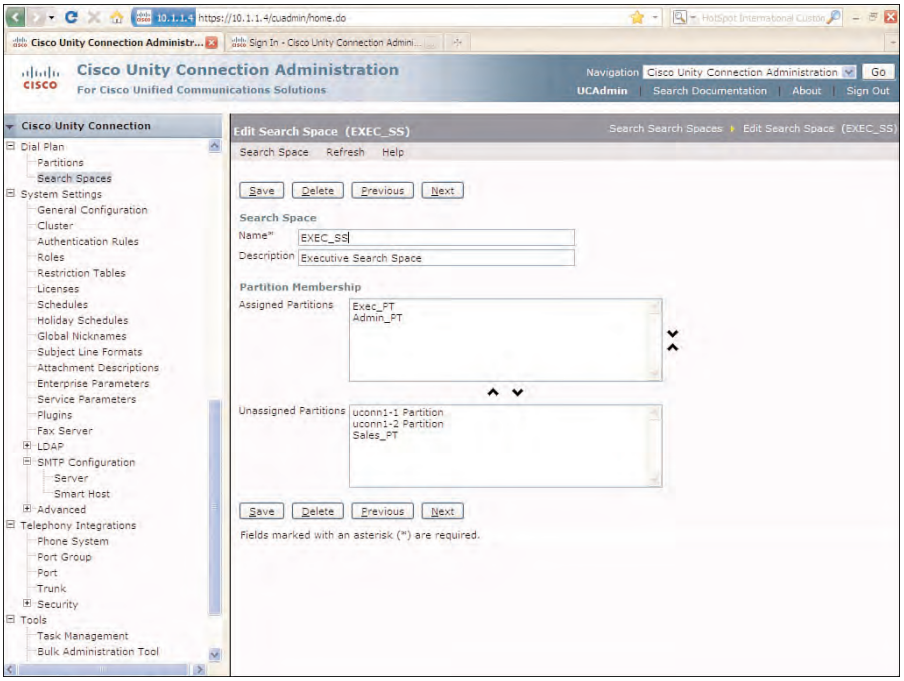

Figure 14-8 *Edit Search Space Review and Problem Identification*

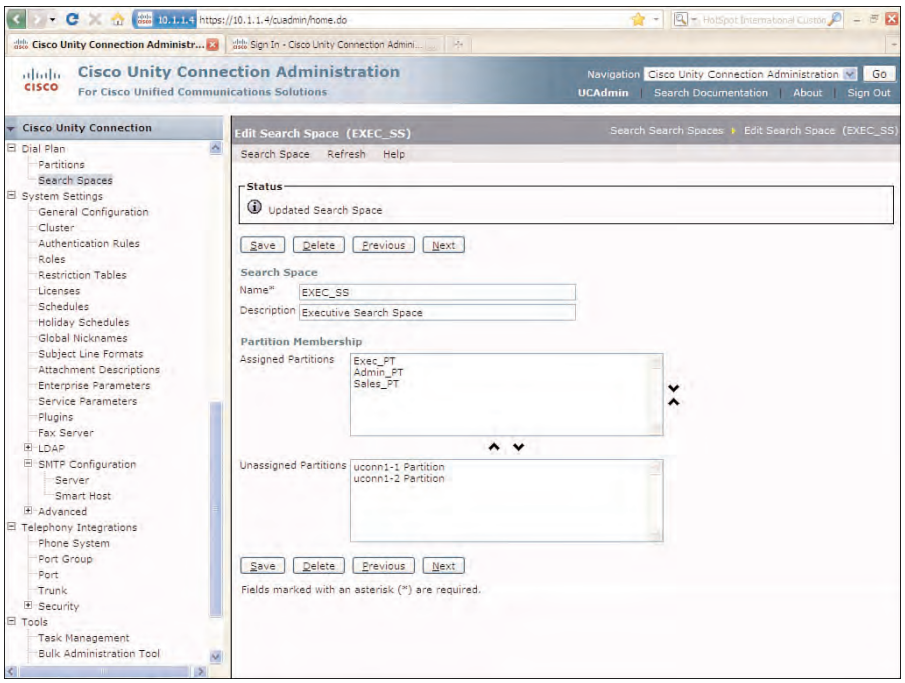

Figure 14-9 *Edit Search Space Resolution*

www.it-ebooks.info

After performing this configuration for the **EXEC_SS** at this location, these users can now address messages to users at the sales department. This same process must be completed for all other search scopes at both locations where access to the remote resources is required.

Troubleshooting Access to Features

Trouble Ticket #5: The new CEO does not have access to the Messaging Inbox and has repeatedly tried to access his account setting in Personal Communications Assistant but cannot log in.

Scenario

After understanding the situation, the troubleshooting efforts here are focused on identifying the issue and educating the user. As it turns out, the user attempted to log in to the Personal Communications Assistant using the incorrect password. He attempted this login procedure multiple times and ended up locking the account. The Authentication Rules was configured to lock the account after seven incorrect login attempts within a 5-minute period.

Resolution

After understanding the situation, the user's password was changed, and the account was unlocked by selecting the user in Cisco Unity Connection Administration and then selecting **Edit > Password Settings** from the Edit User Basics toolbar. The Edit Password Settings page displays. From the Choose Password drop-down, select the **Web Application** option. On the Edit Password Settings page, select **Unlock Password**, as illustrated in Figure 14-10. The Status section informs the administrator that the password policy has been updated.

The password is now unlocked for this user. Also, as an administrator, you might also want to reset the password by selecting **Edit > Change Password** option from the toolbar. Also, from the Edit User Basics page, you can select the Set for Self-Enrollment at Next Sign-In. However, the user needs to complete the entire voicemail setup again.

The user also was educated about changing his password using the Messaging Assistant. In reviewing this user's Class of Service, he did not have access to the Messaging Inbox to access his voice messages. As it turns out, the incorrect Class of Service was applied to this user. After the correct Class of Service was applied, the user can now successfully log in to the Personal Communications Assistant and has access to all necessary features.

www.it-ebooks.info

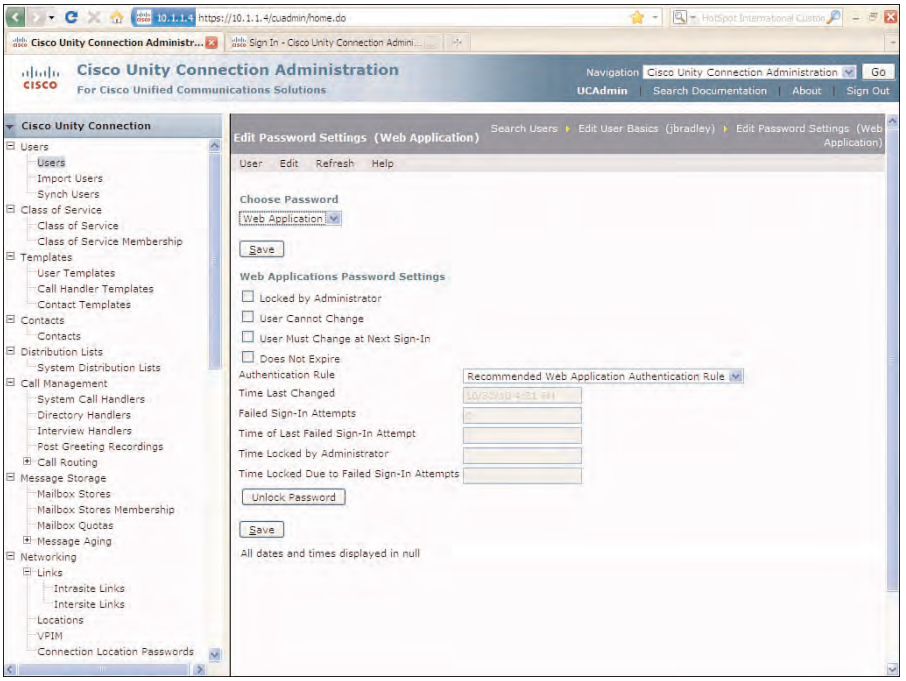

Figure 14-10 *Edit Password Settings Selection to Unlock a User's Password*

Troubleshooting Audiotext Applications

Trouble Ticket #6: After the new implementation, users are trying to access a directory by selecting option 5, as stated in the Opening Greeting. After selecting the 5 option, users hear the Opening Greeting again, instead of the directory.

Scenario

This issue relates directly to the configured Caller Input under the Opening Greeting. After further investigation, it appears that all callers are experiencing the same issue. Therefore, you decide to review the configuration options for Caller Input selection for the Opening Greeting.

Resolution

After reviewing the configuration parameters for Caller Input, option 5 was configured for the Call Action to Restart greeting, as shown in Figure 14-11.

To correct this issue, from the Caller Input page, the administrator clicked the 5 option and from the Directory Handler drop-down selected the System Directory Handler option. After clicking **Save**, the Caller Input page redisplays, as shown in Figure 14-12.

www.it-ebooks.info

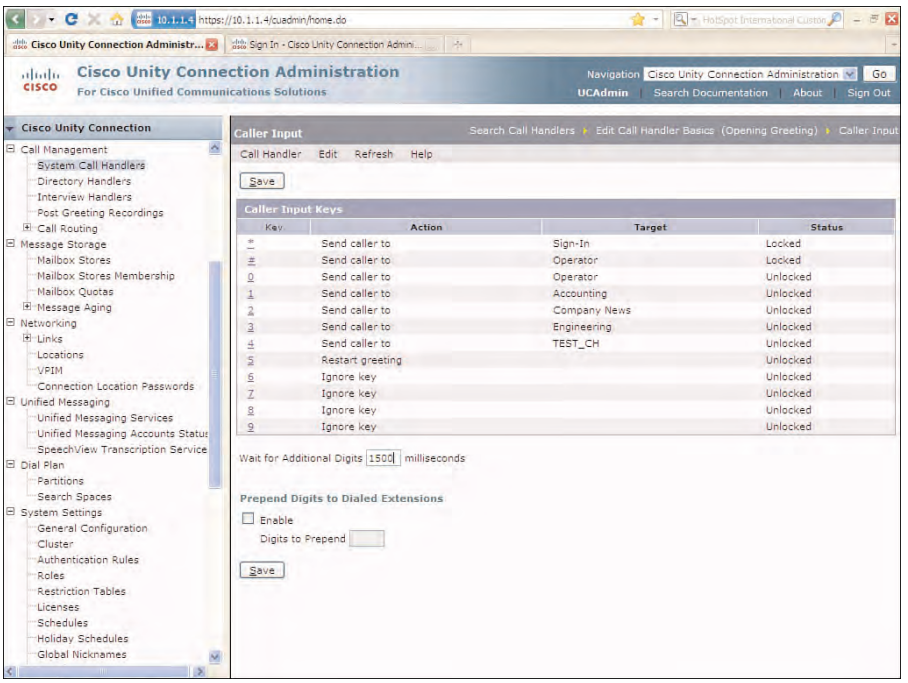

Figure 14-11 *Opening Greeting Caller Input Review and Problem Identification*

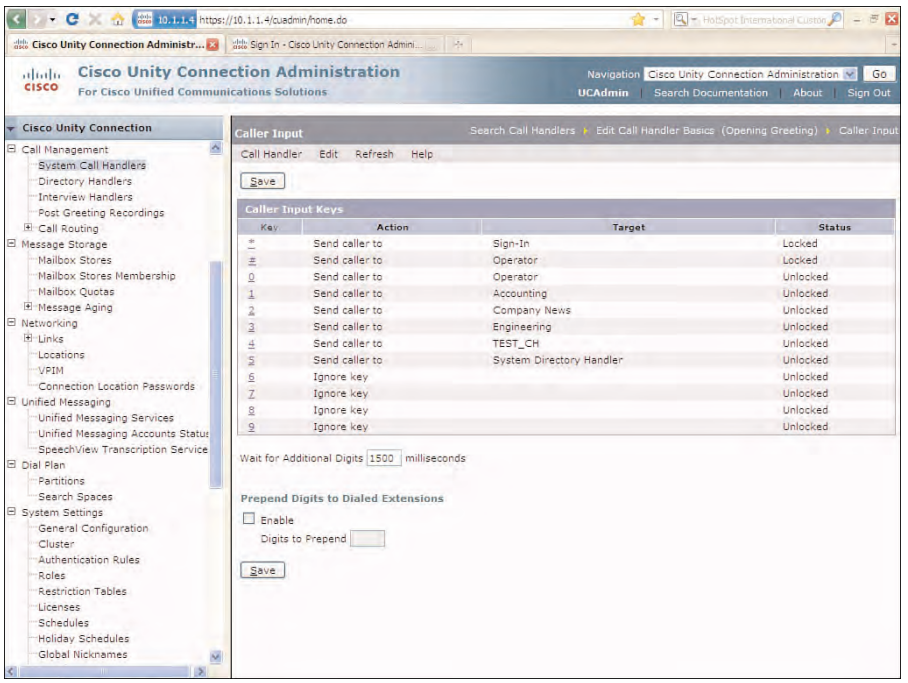

Figure 14-12 *Caller Input Resolution*

www.it-ebooks.info

After the configuration was completed, the Opening Greeting options were retested. The option 5 for Caller Input is now directing the caller to the System Directory Handler according to the original designs.

Troubleshooting Digital Networking Issues

Trouble Ticket #7: Network replication between the locations installed in the engineering department and the server installed in the research department is not operational. Users cannot log in to their voice mailbox from the remote server.

Scenario

The engineer implemented digital networking using the automatic method. The Connection Digital Networking Replication Agent service was started on the publisher server in the engineering department.

Resolution

After further investigation, at both the local and remote locations, it was discovered that the Connection Digital Networking Replication Agent service was started at the engineering department but not the research department, as shown in Figure 14-13.

It is advisable to always review the Status section at all locations. The Connection Digital Networking Replication Agent service must be started at both locations from the Cisco Unity Connection Serviceability web pages at each site. After this was completed, the replication automatically starts between the two locations.

To verify the replication, select **Networking > Locations** and review the USN messages, comparing the remote and local locations, as displayed in Figure 14-14.

In this case, the last USN Sent and Acknowledge is 48, whereas this location last received USN 22 from this remote location. The USN at the remote location for this location shows the reverse, as shown in Figure 14-15.

Additionally, you could select **Tools > Voice Network Map** in Cisco Unity Connection Serviceability and review the USN messages and network information.

Also, it was discovered that the cross-server login and transfer settings were not configured. The cross-server features were properly configured on the Edit Location page, as shown in Figure 14-16.

This configuration must also be completed at the remote location. Also, the **Respond to Cross-Server Handoff Requests** check box must be selected under the Conversation Configuration page to complete the cross-server configuration.

After the aforementioned configurations were completed, users could address messages to users at the remote location and had access to all cross-server features.

www.it-ebooks.info

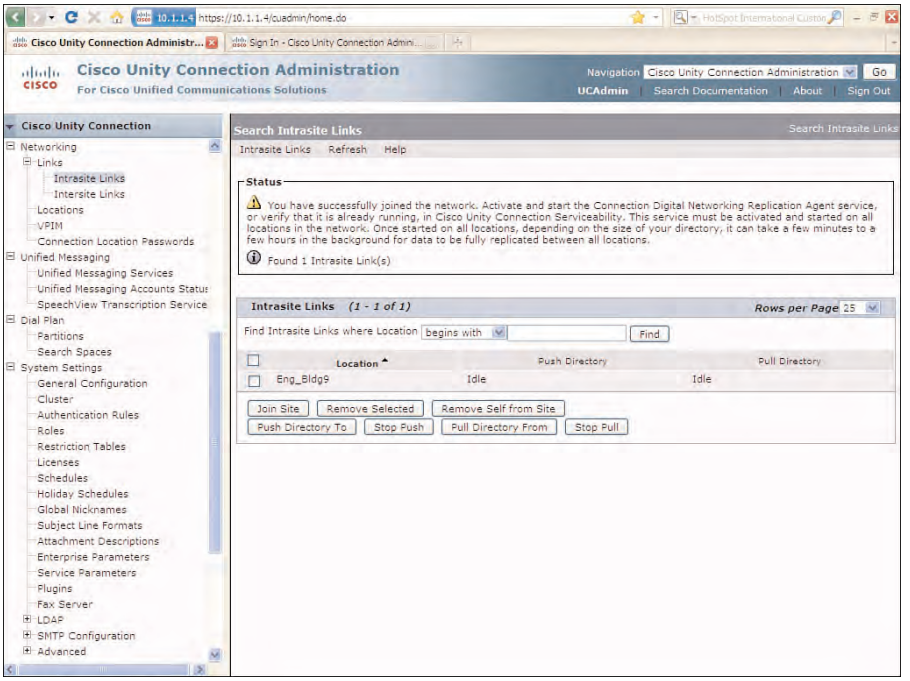

Figure 14-13 *Search Intrasite Links Review and Problem Identification*

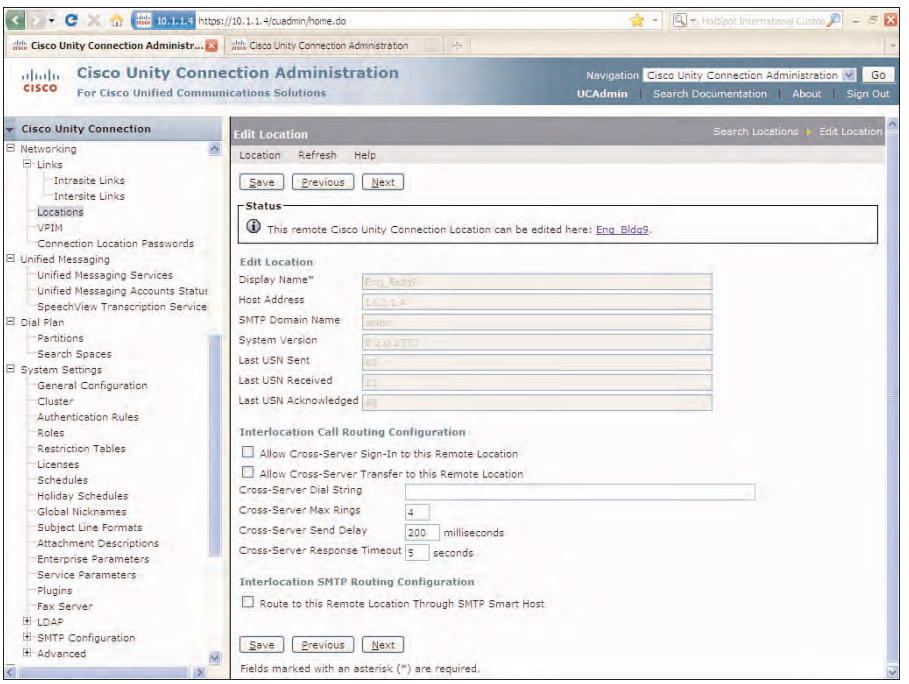

Figure 14-14 *Edit Location Page to Confirm Networking Between Locations*

www.it-ebooks.info

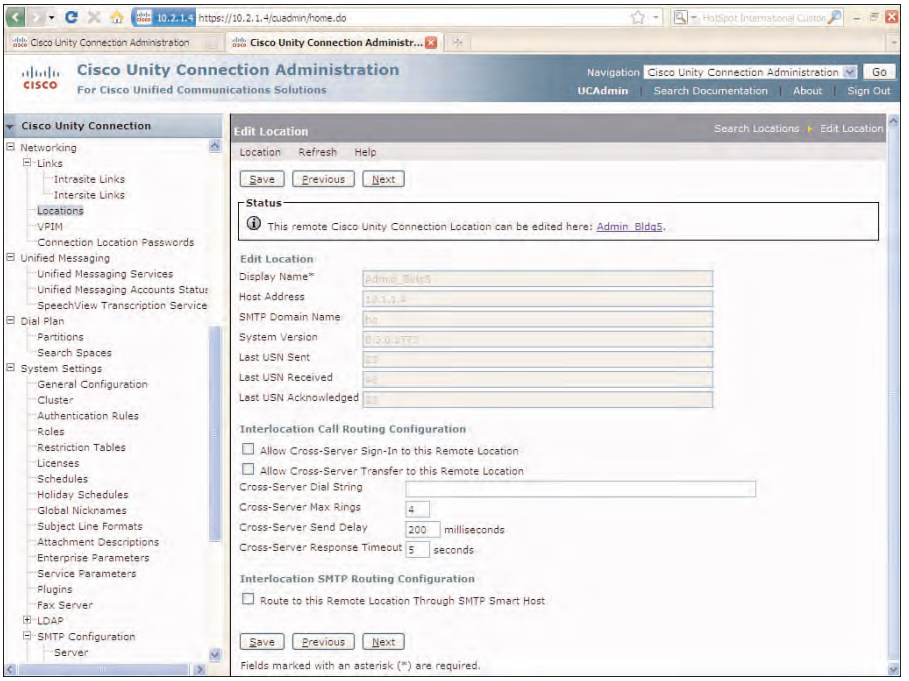

Figure 14-15 *Edit Location Page to Confirm Networking Between Locations*

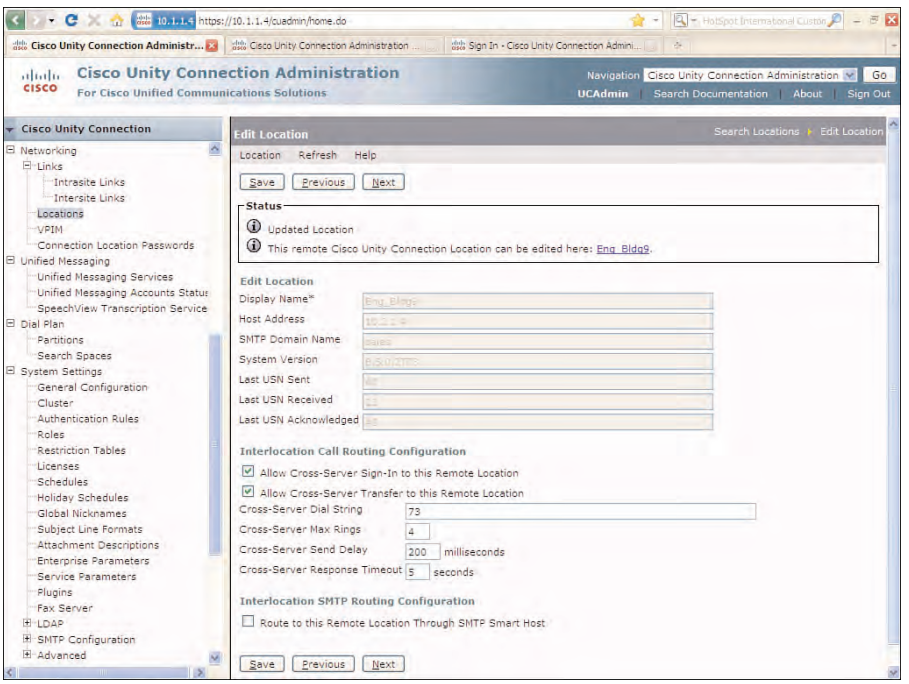

Figure 14-16 *Cross-Server Configuration on the Edit Location Page*

www.it-ebooks.info

Troubleshooting VPIM Networking Issues

Trouble Ticket #8: After VPIM networking was completed between the corporate headquarters and its service provider, users cannot send messages to users at the remote location.

Scenario

The review of the VPIM design indicates that all users should have access to address messages to the remote users at the VPIM location. The remote VPIM location cannot push the director information to the organization. Therefore, a different resolution must be identified and configured for addressing and for contact administration. A directory push must be manually initiated, and the configuration and authentication must be properly configured on both servers.

Resolution

The issue relates directly to addressing messages to the remote users. In the case of VPIM, remote users are configured as contacts. Contacts can be created in Cisco Unity Connection in a number of ways. The first way is to push directory information to the remote location, but this was stated earlier as not being an option.

Because contacts do not yet exist and users need to address messages, blind addressing was identified as the first part of this solution. Also, when remote users address messages to local users at the organization, the local VPIM configuration is configured with the following options that can make the contact management nearly self-administrating. These options are configured by selecting **Edit > Contact Creation** from the toolbar under the VPIM Location. Figure 14-17 illustrates the Contacts Creation page for this VPIM location.

Under the Automatic Directory Updates, select the **Automatically Create VPIM Contacts** check box to have Cisco Unity Connection create the contacts automatically. Then, from the Automatically modify VPIM Contact drop-down, select the **With Each VPIM Message** option. In this way, any changes to the remote contact will be automatically updated because each message is received from this remote location. Finally, select the **Automatically Delete VPIM Contact** check box. This option enables a contact to be deleted when a nondeliverable receipt is received because of a message sent to a user that was removed from the remote VPIM location. The **Allow VPIM Contact Display Name Updates** and the **Allow VPIM Contacts Without Recorded Names** check boxes are also selected for this VPIM location.

www.it-ebooks.info

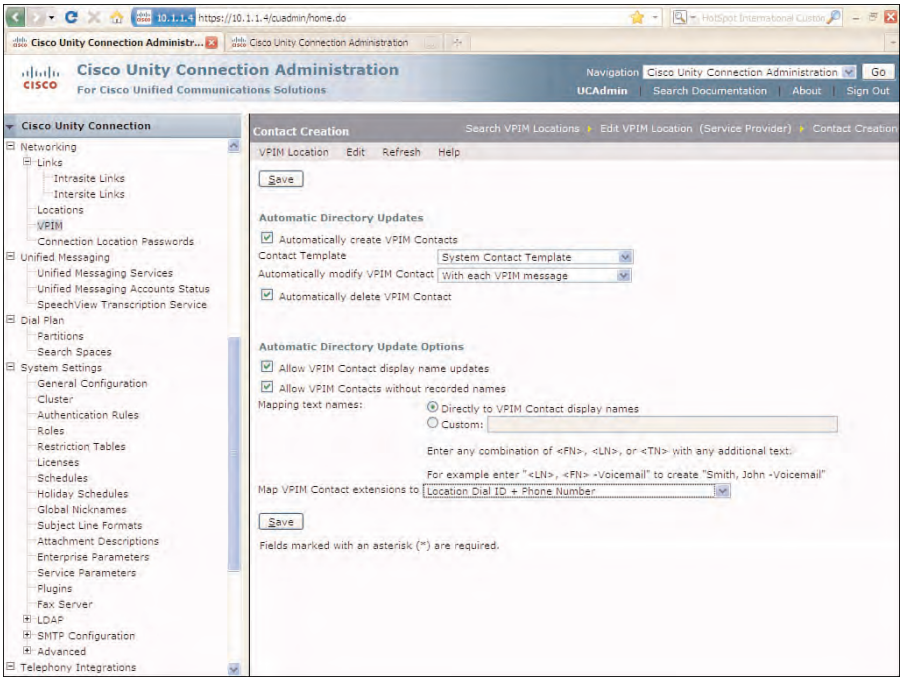

Figure 14-17 *Contacts Creation Page for the Remote VPIM Location*

Summary

This chapter provided an understanding of troubleshooting techniques and some of the more common issues encountered with voice messaging. In this chapter, you learned the following:

- How to approach most network and voice messaging issues and develop a plan for resolution.
- Good troubleshooting techniques including assessment, planning, and resolution.
- Some of the common trouble tickets encountered with implementations, networking, and various features in Cisco Unity Connection.

www.it-ebooks.info

Index

A

accessing voice messages
IP phones, 238-240
Phone View, 240-243
Visual Voicemail. See Visual Voicemail
phones, 213-214
alternate extensions, 219-220
message actions, 224
message settings, 223
MWIs, 216-219
Phone Menu options, 221-222
playback settings, 224
sending messages, 225
transfer rules, 214-216
web, 226
Connection Personal Call Transfer Rules, 231
Messaging Assistant, 230
Messaging Inbox, 229-230
Microsoft Outlook, 235-238
PCAs, 226-228
RSS feeds, 233-235
active-active cluster-pairs, 2
configuring, 76-77
first nodes, 78-80
publishers, 77
subscriber servers, 78
subscribers, 77
high availability/redundancy, 24-25
intrasite networking, 29
load-sharing, 77
redundancy, 77
verifying, 83-86
Adaptive Differential Pulse Code Modulation (ADPCM), 17
Administrative XML. *See* AXL
administrators
application, 158
backup, 176-178
greetings
configuration case study, 356-357
defined, 182

www.it-ebooks.info

help desk, 182
logins, 46
configuring, 60
Unified OS administration login, 73-76
verifying, 73
platform, 158
remote, 183, 476
security, 158-159
system, 183
administratortemplate, 173
ADPCM (Adaptive Differential Pulse Code Modulation), 17
AET Inc. phone number conversion case study, 199-200
After Greeting options, 327
aging policies, 268-272
alerts, 272-275
case study, 279-280
creating, 271
default, 269-271
optimizing, 271-272
users, 273
Alert Central (RTMT), 468
algorithms
ADPCM (Adaptive Differential Pulse Code Modulation), 17
PCM (pulse code modulation), 17
SB-ADPCM (Sub-Band Adaptive Differential Pulse Code Modulation), 17
aliases (users), 180
allvoicemailenabledcontacts distribution list, 301
allvoicemailusers distribution lists, 301
alternate extensions, 219-220, 296-299
automatically adding, 297
configuring, 297
restriction tables, 297-298
listing of, 297
pattern restrictions, 299
viewing, 297
alternate greetings, 281
Alternate transfer rules, 215
AMC service, 454
Answer File Generator, 86
answer files
downloading, 86
generating, 86
unattended installations, 86-88
applications
administrators, 158
audiotext, 339-341
configuring, 340
designs, 340
example, 340
greetings, 339
opening greeting example, 341
troubleshooting, 550-552
calendar integrations, 311
DRS
backup components, 494-496
backup schedules, creating, 499-500
backups, performing, 490-492
certificate management, 489-490
manual backups, 497-499
message stores, 496
overview, 488-489
restores, 501-503
warm standby servers, 503-506
installation, 67
Phone View, 240-243
CUCM integration, 240-241
Phone Menu options, 241
users, configuring, 240

www.it-ebooks.info

usernames/passwords, configuring, 64
web, authentication rules, 163
archiving messages, 272
attributes (integrations), 104
audio codecs, 15-20
audio quality, 19-20
decoding, 15
defined, 15
disk space, 267
G.711, 16
G.722, 16-17
G.726, 17
G.729, 16
iLBC, 17
implementing, 18
line side, 17-18
listing of, 20
PCM Linear, 17
recording, 18
sampling, 15-16
transcoding, 17-20
VPIM, 418
audiotext applications
configuring, 340
creating, 339-341
designs, 340
example, 340
greetings, 339
opening greeting example, 341
troubleshooting, 550-552
voicemail ports, 24
Audit Event service, 454
authentication
LDAP, 200201
rules, 162-163
default, 162
defining, 162
editing, 163
lockout policies, 162
trivial password checks, 162
user templates, 175
viewing, 163
voicemail, 163
web applications, 163
auto-negotiation configuration, 55-56
AXL (Administrative XML), 202-205
activating, 202
servers, configuring, 203
web services, 456

B

backing up
COBRAS
Connection Database Proxy service, 477
database proxy option, 477
downloading, 475
Export utility, 475
Import utility, 477
modes, 475
overview, 472-473
remote administrators, 476
user migration, 472-473
utility migration, 477-478
websites, 92
devices, selecting, 501
message stores, 258, 496
performing with DRS, 490-492
components, 494-496
devices, configuring, 492-494
history, 492
manual backups, 492
schedules, 492
target locations, 491

www.it-ebooks.info

scheduling, 499-500
SRSV (Survivable Remote Site Voicemail), 508
tar files, 502
backup administrators, 176-178
bandwidth, 109
BAT (Bulk Administration Tool), users, 183-184
configuring, 183-184
creating, 187
exporting, 184-185
updating, 188
verifying, 189
blind addressing
case study, 433-434
VPIM
contacts, 434-435
locations, 420, 428
Briefcase mode (COBRAS), 475
broadcast messages, 225
browsers supported, 73
Bulk Administration Tool. ***See*** **BAT**
Bulk Edit, 189-190
Business Edition, 2
busy extension transfer rule, 216
busy greetings, 281

C

calendar integrations, 311
call handlers, 320
directory, 334-335
full mailboxes, 278
greeting administrator configuration, 356-357
interview, 335-339
system, 321
caller inputs, 328-329
configuring, 322-324
default, 321-322
greetings, 325-328
message settings, 330-331
new, configuring, 332
owners, 331-332
post greeting recordings, 329-330
templates, 333-334
transfer rules, 325
troubleshooting, 543-545
call queuing, 216
call routing rules
default, 153
direct calls, 153
greeting administrator configuration, 356-357
Visual Voicemail, configuring, 244-245
forwarded calls, 154
call screening, 216
caller inputs
configuring, 287-289
greetings, 285
system call handlers, 324, 328-329
troubleshooting, 550-552
CallManager serviceability RTMT service, 454
CallManager serviceability service, 454
CDP Agent, 454
CDP service, 454
centralized messaging deployment, 111
certificates
change notification, 455
configuring, 60

www.it-ebooks.info

Expiry Monitor, 455
managing, 489-490
Check Telephony Integration task, 479
Cisco
DB service, 454
Objected Backup and Restore Application Suite. *See* COBRAS
Unified Communications Manager. *See* CUCM
Unified Messaging Gateway, 6
Unified Mobile Communicator (CUMC), 251-252
Unified Personal Communicator, 251
Unity, 5
Unity Connection. *See* CUC
Unity Express (CUE), 5
Voicemail Organization, configuring, 363-365
Class of Service. *See* CoS
clients
IMAP, 21-22
combining modes, 22
Idle-mode, 22
Non-Idle mode, 22-14
types supported, 21
clock synchronization, 46
closed greetings, 281
closed transfer rule, 215
cluster management, 371-373, 506-507
active-active cluster pairs, 2
configuring, 76-77
first node configuration, 78-80
high availability/redundancy, 24-25
intrasite networking, 29
load-sharing, 77
publishers, 77
redundancy, 77
subscriber servers, 78
subscribers, 77
verifying, 83-86
deactivation process, 507
manual failback events, 373
ports, 507
status, 373-372
current, viewing, 506-507
primary status, 372
CME (Communications Manager Express), 106, 145-151
dial-peer configuration, 146-147
ephone command, 147
port groups, 149-150
SIP, 150
telephony service, 146
verifying, 148-149
voicemail integration configuration, 147-148
CNG (fax calling tone), 520
COBRAS (Cisco Objected Backup and Restore Application Suite), 3
Connection Database Proxy service, 477
database proxy option, 477
downloading, 475
Export utility, 475
Import utility, 476, 477
modes, 475
overview, 472-473
remote administrators, 476
user migration, 472-473
utility migration, 477-478
website, 92

www.it-ebooks.info

Communications Manager Express. ***See*** **CME**
community strings, creating, 509-510
configuring
active-active cluster-pairs, 76-77
first node configuration, 78-80
publishers, 77
subscribers, 77
administrator logins, 60
alternate extensions, 297
application usernames/passwords, 64
audiotext applications, 340
auto-negotiation, 55-56
AXL servers, 203
backup devices, 492-494
caller inputs, 287-289
certificates, 60
Cisco Voicemail Organization, 363-365
CME telephony service, 146
cross-server features, 406-408
DHCP, 45, 5758
dial-peer, 146-147
DNS, 46
DNS clients, 59
fax integration, 516-517
IP addresses, 516
SMTP addresses, 517
SMTP Smart Hosts, 517
user accounts, 518-519
first nodes, 61
greeting administrators, 356-357
greetings, 282
hunt list, 122
hunt pilots, 124
intersite networking, 399-401
interview handlers, 335-339
intrasite links, 377
automatic versus manual, 377
automatically, 378-381
directory synchronization, verifying, 385-389
distribution lists, 391-392
manually, 381-384
system objects, 392
users, verifying, 389-391
verifying, 385
voice network maps, 393-396
LDAP filters, 196-197
live reply users, 410
MTU, 56-57
MWIs, 216-219
new system call handlers, 332
notification devices, 293-294
NTP, 46
NTP clients, 61
partitions, 344
phone system trunks, 411-414
phone systems, 115
Phone View application
CUCM integration, 240-241
Phone Menu options, 241
users, 240
PIMG/TIMG integrations, 151
platforms, 64
ports, 132-135
post greeting recordings, 290
post-installation, 67
rPSM, 137-138
RSS readers, 233
schedules, 167
search spaces, 346
security, 63

www.it-ebooks.info

server display names/SMTP domain names, 365-366
SIP trunk, 141-142
SMS notification devices, 530-531
SMTP
domain names, configuring, 422-423
hosts, 46, 63-64
Smart Hosts, 397-398
SNMP, 509-510
community strings, creating, 509-510
master agent restart warning, 510
notifications, 510
requirements, 509
SpeechView, 522-523
SpeechView transcription service, 525-527
subscriber servers, 78
system call handlers, 322-324
active schedules, 323
caller input, 324
creation times, 322
display names, 322
extensions, 323
greetings, 324
languages, 323
message settings, 324
owners, 324
partitions, 324
phone systems, 323
post greeting recordings, 324
recorded names, 324
searches, 324
time zones, 323
transfer rules,324
time zones, 45, 54
unified messaging service, 314
usernames/passwords, 47
users, 176
Administrative XML, 202-205
BAT, 183-184
Bulk Edit, 189-190
creating users, 187
DirSync service, activating, 192
exporting to CSV files, 184-185
importing from AXL, 203-205
importing from LDAP, 195-196
LDAP authentication, 200-201
LDAP directory configuration, 193-195
LDAP filters, configuring, 196-197
LDAP setup, 192-193
LDAP synchronization, 190-191
with mailboxes, 179-181
phone numbers, converting, 198
roles, 181-183
updates, 188
verification, 189
without mailboxes, 177-178
Visual Voicemail
Connection Administration, 243-244
CUCM, 247-249
direct routing rules, 244-245
hunt pilots, 243
IP phone subscriptions, 249-250
Java midlets, 245-246
voicemail pilots, 124-126
VPIM locations, 425-429
audio format conversions, 427
audio normalization, 427
Dial IDs, 426
directory synchronization, 429

www.it-ebooks.info

display names, 425
interlocation SMTP routing, 428
IP addresses, 426
message settings, 427-428
new locations, adding, 425
partitions, 426
prefixes, 427
remote phone prefixes, 426
SMTP domain names, 426
Connection Administration, Visual Voicemail configuration, 243-244
Connection Database Proxy service, 477
Connection Personal Call Transfer Rules, 216
connectivity
CUC, 68
locations, 365
VPIM, 421
contacts (VPIM), 420
alternative names, 441
automatic directory updates, 431-433
automatically creating, 435-437
blind addressing, 434-435
creating, 429
deleting, 437-438
remote, 429-431
SMTP proxy addresses, 442
troubleshooting, 555
CoS (Class of Service), 169-172
default, 169
membership, viewing, 172
new, adding, 170-171
private distribution lists, 308
RSS feeds, 233
SpeechView, 527
CPU performance, 451
critical services, 453-456
AMC service, 454
Audit Event service, 454
AXL web service, 456
CallManager serviceability, 454
CallManager serviceability RTMT, 454
categories, 453
CDP, 454
CDP Agent, 454
Certificate Change Notification, 455
Certificate Expiry Monitor, 455
Database Layer Monitor, 455
DB, 454
DB Replicator, 454
DirSync service, 456
DRF Local, 455
DRF Master, 455
Host Resources Agent, 455
Log Partition Monitoring tool, 455
MIB2 Agent, 455
RIS Data Collector, 455
RTMT Reporter Servlet, 455
Serviceability Reporter, 456
SNMP Master Agent, 455
SOAP, 456
Syslog Agent, 455
System Application Agent, 456
Tomcat, 455
Tomcat Stats servlet, 455
Trace Collection service, 455
Trace Collection servlet, 455
UXL web service, 456
cross-server features, 401-402
configuring, 406-408
live reply, 405-406
sign-ins, 403-404
transfers, 405

www.it-ebooks.info

troubleshooting, 552
cryptography, 6869
CSV format (reports), 484
CUC (Cisco Unity Connection)
1.2 updates, 92
Business Edition, 2
installing, 44-45
administrator logins, 60
application installation, 67
application usernames/passwords, 64
auto-negotiation configuration, 55-56
basic installation configuration options, 54
certificates, 60
completing, 70
DHCP, 57-58
DNS, 59
first node configuration, 61
hard drives, formatting, 66
licensing/cryptography, 68-69
MTU, 56-57
network connectivity checks, 68
network/host configurations, 68
NTP client, 61
operating system installation, 66
platform configuration, 64
platform installation wizard, 52-54
post-installation configuration, 67
pre-installation tasks, 45-47
processes, 47-48
product deployment selection, 50
security, 63
server restarts, 67
SMTP host configuration, 63-64
software, 47
software installation, 66
system installer/platform checks, 48-49
time zones, 54
login verification, 73-76
administrator logins, 73
Unified OS administration login, 73-76
online tools, 509
overview, 2, 5-6
server verification, 71-72
services, 457-460
CUCM (Cisco Unified Communications Manager), 251-252
confirmation, 120
device information, 117
directory numbers, 119, 126
hunt list configuration, 122
hunt pilots, 124
line groups, 120
message waiting indicators, 124
Phone View application, 240-241
ports, 117
profiles, 126
servers, 116-117
similarities, 2-3
Visual Voicemail configuration, 247-249
Voice Mail Port Wizard Results, 122
voicemail
configuration, 116-128
pilots, 124-126
CUE (Cisco Unity Express), 5
CUMC (Cisco Unified Mobile Communicator), 251-252
current network status/design, 7-8

www.it-ebooks.info

D

Database Layer Monitor service, 455
DB Replicator service, 454
DB service, 454
decoding, 15
default system message aging policy, 269-271
deleting
incoming messages, 428
outgoing messages
faxes, 428
subjects, 428
text, 428
partitions, 350-354
search spaces, 350-354
VPIM contacts, 437-438
demo licenses, 95
deployment (messaging), 110
centralized, 111
distributed, 112
Mag's Cycle Corporation case study, 113
single-site, 110
designs
audiotext applications, 339-341, 340
configuring, 340
example, 340
greetings, 339
opening greeting example, 341
high availability, 24-25
integrations, 28
networking, 28-29
intersite, 32-33
intrasite, 29-31
intrasite versus intersite, 34
VPIM, 36-38
platform overlays, 25-26
intrasite networking, 29-31
overview, 26
virtualization, 26-27
preliminary, 13-14
server sizing, 14-15
audio codecs. See audio codecs
clients supported, 21
IMAP support, 21-22
message storage, 20-21
voicemail ports, 22-24
Tamicka-Peg Corporation voicemail example, 27-28, 35
user locations, 27
devices
backup
configuring, 492-494
selecting, 501
notifications
configuring, 293-294
timing and delay options, 294
SMS, configuring, 530-531
DHCP (Dynamic Host Configuration Protocol), configuring, 45, 557-558
Dial IDs, 419, 426
dial plans
case study, 344
networking, troubleshooting, 547-549
partitions
assigning to search spaces, 346-348
configuring, 345
default, editing, 350
deleting, 350-354
overview, 341-342
reassigning, 351-353
users, assigning, 348

www.it-ebooks.info

search spaces
configuring, 346
default, editing,350
deleting, 350-354
overview, 342-343
partition assignments, 346-348
reassigning, 351-353
users, assigning, 348
troubleshooting, 354-356
VPIM locations, 419, 426
dial-peer configuration, 146-147
DID (Direct Inward Dial) faxing, 520-521
direct routing rules, 153
greeting administrator configuration, 356-357
Visual Voicemail, configuring, 244-245
directories
access, troubleshooting, 550-552
automatic updates, 431-433
handlers, 334-335
numbers
CUCM integrations, 126
line groups, adding, 119
synchronization
DirSync service, 192, 456
verifying, 385-389
VPIM, 422, 429
DirSync service, 192, 456
disabling
greetings, 283
notifications,294
Disaster Recovery System. *See* DRS
distributed messaging deployment, 112
distribution lists, 225
overview, 300
port activity,311
private, 308-310
addressing messages, 310
CoS configuration, 308
creating, 308-309
user configuration, 310
system, 300-306
access lists, 305
allvoicemailenabledcontacts, 301
allvoicemailusers, 301
case study, 306
default, 301
editing, 302
membership, 303-304
names, 305
new, creating, 302-303
undeliverablemessages, 301
viewing, 301
Tiferam Corporation case study, 375-377
verifying, 391-392
VPIM, 420-421
DNS (Domain Name System)
client, configuring, 59
configuring, 46
SMTP
configuring, 365-366, 422-423
VPIM locations, 426
VPIM networking, 421
DRF Local service, 455
DRF Master service, 455
DRS (Disaster Recovery System)
backups, performing, 490-492
components, 494-496
devices, configuring, 492-494
history, 492
manual backups, 492

www.it-ebooks.info

schedules, 492, 499-500
target locations, 491
certificate management, 489-490
manual backups, 497-499
message stores, 496
overview, 488-489
restores, 501-503
backup devices, selecting, 501
backup files, 502
components, restoring, 502
final warning, 502
status, 503
warm standby servers, 503-506
During Greeting options, 327
Dynamic Host Configuration Protocol (DHCP), configuring, 45, 57-58

E

Edit Interview Questions Page, 338
editing
authentication rules, 163
Bulk Edit, 189-190
mailbox quotas, 279
message actions,224
message stores, 259, 262
partitions, 350
schedules, 167
search spaces, 350
SMS notification devices, 531
system distribution lists, 302
transfer rules, 215
Elle-Mich Incorporated case study, 98-99
enabling
greetings, 283
notifications,294
ephone command, 147
error greetings, 281
expiration (messages), 275
Export utility, 475
exporting users to CSV files, 184-185
extensions
alternate, 219-220, 296-299
automatically adding, 297
configuring, 297
restriction tables, 297-298
busy, 216
system call handlers, 323
external service accounts, 311

F

fax calling tone (CNG), 520
faxes, 514-515
calling tone configuration, 520
configuring, 516-517
IP addresses, 516
SMTP addresses, 517
SMTP Smart Hosts, 517
file types supported, 515
outgoing messages, 428
preparations, 515
relay configuration, 521
reports, 516
testing, 520
user accounts, 518-519
verifying, 520
files
answer
downloading, 86
generating, 86
unattended installations, 86-88
backup, 496, 502
fax supported, 515

www.it-ebooks.info

log, installing, 76
pem, 490
performance log, 464-465
Tcl script, 520-521
Visual Voicemail midlets, 245-246
filters (LDAP), configuring, 196-197
finding user mailboxes, 263
first nodes
active-active cluster-pairs, configuring, 78-80
configuring, 61
subscribers/publishers
access, 83
configuring, 81
flash cut migration, 3
formatting hard drives, 66
forwarded routing rules, 154

G

G.711 codec, 16
G.722 codec, 16-17
G.726 codec, 17
G.729 codec, 16
Goodbye call handler, 321
greetings, 280-286
administrators
configuration case study, 356-357
defined, 182
alternate, 281
audiotext applications, 339
busy, 281
caller inputs, 285
case study, 290
closed, 281
configuring, 282
enabling/disabling, 283
errors, 281
During Greeting options, 327
After Greeting options, 327
holiday, 281
internal, 281
Messaging Assistant, 285
opening audiotext example, 341
post greeting recordings, 285, 324, 329-330
applying to users, 291
configuring, 290
playback settings, 292
recording, 291
transfers, 290
voicemail, 290
recording, 284, 326
standard
defined, 281
options, 327-328
overriding, 283
system call handlers, 324, 325-328
system default recording, 280-281
Times to Re-prompt Caller option, 327
transfer rules, 285
troubleshooting, 543-545

H

HA licenses, 96
hard drives, formatting, 66
headers, read receipts, 428
help desk administrators, 182
high availability, active-active cluster-pair designs, 24-25

www.it-ebooks.info

holidays, 165-169
default, 165-166
greetings, 281
new, adding, 166
Host Resources Agent, 455
Hot mode (COBRAS), 475
hunt list configuration, 122
hunt pilots
configuring, 124
verifying, 136
Visual Voicemail configuration, 243

I

iLBC (Internet Low Bitrate Codec), 17
IMAP (Internet Message Access Protocol), 21-22
combining modes, 22
Idle-mode, 22
Microsoft Outlook configuration, 237-238
Non-Idle mode, 22
implementing audio codecs, 18
Import utility, 476, 477
importing users
AXL, 203-205
case study, 205-207
LDAP, 195-196
incoming messages
marking secure, 428
recorded names, deleting, 428
installing
CUC, 44-45
administrator logins, 60
application installation, 67
application usernames/passwords, 64
auto-negotiation configuration, 55-56
basic installation configuration options, 54
certificates, 60
completing, 70
DHCP, 57-58
DNS, 59
first node configuration, 61
hard drives, formatting, 66
licensing/cryptography, 68-69
MTU, 56-57
network/host configurations, 68
NTP client, 61
operating system installation, 66
platform configuration, 64
platform installation wizard, 52-54
post-installation configuration, 67
pre-installation tasks, 45-47
processes, 47-48
product deployment selection, 50
security, 63
server restarts, 67
SMTP host configuration, 63-64
software, 47
software installation, 66
system installer/platform checks, 48-49
time zones, 54
license files, 97
log files, 76
software updates during, 89-90
subscribers/publishers, 81
first node access, 83
first node configuration, 81
installation dialogue, 81-82

www.it-ebooks.info

unattended installations, 86-88
Answer File Generator86
download instructions, 86
pre-existing configuration information, 88
virtual machines, 92-94
integrations
attributes, 104
calendar applications, 311
CME, 106, 145-151
dial-peer configuration, 146-147
ephone command, 147
port groups, 149-150
SIP, 150
telephony service, 146
verifying, 148-149
voicemail integration configuration, 147-148
CUCM, 104-105, 116-128
confirmation, 120
device information, 117
directory numbers, 119, 126
hunt list configuration, 122
hunt pilots, 124
line groups, 120
message waiting indicators, 124
ports, 117
profiles, 126
servers, 116-117
Voice Mail Port Wizard Results, 122
voicemail configuration, 116-128
voicemail pilots, 124-126
faxes, 514-515
calling tone configuration, 520
configuring, 516-517
file types supported, 515
preparations, 515
relay configuration, 521
reports, 516
testing, 520
user accounts, 518-519
verifying, 520
features supported, 103
flash cut, 3
hunt pilots, verifying, 136
legacy systems case study, 154-155
messaging deployment, 110
centralized, 111
distributed, 112
Mag's Cycle Corporation case study, 113
single-site, 110
multiple, 4, 109-110
overview, 28
phase-in, 3
phone system
basics, 128
configurations, 115
loop detection, 130
MWIs, 130
names, 128
outgoing call restrictions, 131
searching, 128
TRaP, 128
view settings, 131
PIMG/TIMG, 106-109
bandwidth, 109
configuring, 151
devices available, 108
PIMG ports, 107
serial connections, 107
TIMG digital connections, 107

www.it-ebooks.info

Port Monitor, 139
ports, 103
configuring, 132-135
groups, 115-116
verifying, 135-136
profiles, verifying, 136
real-time monitoring, 139
routing rules
default, 153
direct calls, 153
forwarded calls, 154
rPSM, 137-138
sending information
call-processing systems, 103
CUC, 103
SIP, 104, 144
port configurations, 144-145
port groups, 144
SIP trunk, 140-145
configuring, 141-142
route patterns, 142-143
troubleshooting, 136

interface speed, 45

interlocation cross-server features, 401-402
configuring, 406-408
live reply, 405-406
sign-ins, 403-404
SMTP routing, 428
transfers, 405

internal greetings, 281

Internet Low Bitrate Codec (iLBC), 17

Internet Message Access Protocol. ***See*** **IMAP**

intersite networking, 32-33
Cisco Voicemail Organization, 363-365
configuring, 399-401
versus intrasite networking, 34
sites, connecting, 363
Tamicka-Peg Corporation voicemail example, 35
VPIM connections, 37-38

interview handlers, 335-339

intrasite networking, 29-31
active-active cluster-pair designs, 29
configuring, 377
automatic versus manual, 377
automatically, 378-381
manually, 381-384
directory synchronization, verifying, 385-389
distribution lists, 391-392
versus intersite networking, 34
Live Reply, 32
locations, connecting, 362
MIME over SMTP, 30
single connection sites, 31
single/multiple call processing systems, 29
system objects, 392
users, verifying, 389-391
verifying, 385
voice network maps, 393-396

IP phones, voice message access, 238-240
Phone View, 240-243
Visual Voicemail. ***See*** Visual Voicemail

J

Java
RTMT components, 447
Visual Voicemail midlets, 245-246

www.it-ebooks.info

Jensen Industries case study, 36
Job Status section (RTMT), 471

L

languages, system call handlers, 323
LDAP (Lightweight Directory Access Protocol), 190-191
authentication, 200-201
directory configuration, 193-195
filters, configuring, 196-197
phone numbers, converting, 198
setting up, 192-193
synchronization, 190-191
users
importing, 195-196
verification, 198
legacy systems case study, 154-155
licensing, 68-69, 94-95
demo licenses, 95
HA, 96
license files, installing, 97
MAC addresses, 97
PAKs (Product Authorization Keys),97
registering, 97
servers, 96
Speech Connect, 96
SpeechView, 523-524
top-level, 95
users, 96
viewing, 94, 98
VPIM, 419, 425
warm standby servers, 505
Lightweight Directory Access Protocol. *See* LDAP
line groups
CUCM integrations, 120
directory numbers, adding, 119
line side codecs, 1718
live reply
configuring, 410
cross-server features, 405-406
intrasite networking, 32
LMN Corporation multisite design example, 38-39
load-sharing, active-active cluster-pairs, 77
locations, 362
connectivity, verifying, 365
cross-server features, 401-402
configuring, 406-408
live reply, 405-406
sign-ins, 403-404
transfers, 405
intrasite links, 362, 377
automatic versus manual, 377
automatically configuration, 378-381
directory synchronization, verifying, 385-389
distribution lists, 391-392
manually configuring, 381-384
system objects, 392
users verifying, 389-391
verifying, 385
voice network maps, 393-396
networking, troubleshooting, 547-549
SMTP Smart Hosts configuration, 398
users, 27
VPIM, configuring, 425-429
alternative names, 440-441
audio format conversions, 427
audio normalization, 427
Dial IDs, 426
directory synchronization, 429

www.it-ebooks.info

display names, 425
interlocation SMTP routing, 428
IP addresses, 426
message settings, 427-428
new locations, adding, 425
partitions, 426
prefixes, 427
remote phone prefixes, 426
SMTP domain names, 426
troubleshooting, 555
WANs,362
lockout policies, 162
log files, installing, 76
Log Partition Monitoring tool, 455
logins
administrator, 46
configuring, 60
Unified OS administration login, 73-76
verifying, 73
console login prompt, 70
troubleshooting, 549
verifying, 73-76
administrator logins, 73
Unified OS administration login, 73-76
loop detection, 130

M

MAC addresses, license files, 97
Mag's Cycle Corporation case study, 113
MAGS Inc case studies
blind addressing/directory updates, 433-434
directory synchronization, 422
Mail Transfer Agents (MTAs),361
mailboxes
access delegate account users, 182
aging policies, 268-272
alerts, 272, 273-275
case study, 279-280
creating, 271
default, 269-271
optimizing, 271-272
users, applying, 273
caller inputs, configuring, 287-289
greetings
alternate, 281
audiotext applications, 339
busy, 281
caller inputs, 285
case study, 290
closed, 281
configuring, 282
enabling/disabling,283
error, 281
holiday, 281
internal, 281
Messaging Assistant, 285
opening audiotext example, 341
post greeting recordings. See post greeting recordings
recording, 284
standard, 281, 283, 327
system call handlers, 324, 325-328
system default recording, 280-281
Times to Re-prompt Caller option, 327
transfer rules,285
troubleshooting, 543-545
message expiration, 275
quotas, 276-279

www.it-ebooks.info

controlling, 276-278
default, 276
editing, 279
full mailboxes, 278
stores, 257
aging policies, 268-272
backing up, 258, 496
delivered message example, 266
disk space, 266-267
editing, 259, 262
membership, 263-267
names, 262
new, creating, 261-262
options, viewing, 259-261
parameters, 258
searching, 259
sizes, 262
users, creating, 268
verifying, 266
voice message directory, 267
users, 159
maintenance
cluster management, 506-507
current cluster status, viewing, 506-507
deactivation process, 507
port status, 507
CUC tools online, 509
DRS
backup components, 494-496
backup schedules, creating, 499-500
backups, performing, 490-492
certificate management, 489-490
manual backups, 497-499
message stores, 496
overview, 488-489
restores, 501-503
warm standby servers, 503-506
SNMP configuration, 509-510
community strings, creating, 509-510
master agent restart warning, 510
notifications, 510
requirements, 509
SRSV, 508
Voice Technology Group Subscription tool, 509
Maximum Transmission Unit (MTU), 45
Media Master, recording greetings, 284, 326
membership
CoS, 172
message stores, 263-267, 263
system distribution lists, 303-304
memory, viewing, 451
message stores, 257
aging policies, 268-272
alerts, 272, 273-275
case study, 279-280
creating, 271
default, 269-271
optimizing, 271-272
users, applying, 273
backing up, 258, 496
delivered message example, 266
disk space, 266-267
editing, 259, 262
membership, 263-267
moving users, 263-264
user mailboxes, finding, 263
names, 262
new, creating, 261-262
options, viewing, 259-261

www.it-ebooks.info

parameters, 258
searching, 259
sizes, 262
users, creating, 268
verifying, 266
voice message directory, 267
messages
addressing, troubleshooting, 545-547
aging policies, 268-272
alerts, 272-275
case study, 279-280
creating, 271
default, 269-271
optimizing, 271-272
users, applying, 273
archiving, 272
authentication rules, 163
broadcast, 225
call handler settings, 324, 330-331
deployment, 110
centralized, 111
distributed, 112
Mag's Cycle Corporation case study, 113
single-site, 110
designs
preliminary, 13-14
server sizing. See server sizing
distribution lists, 225
expiration, 275
incoming
marking secure, 428
recorded names, deleting, 428
IP phone access, 238-240
Phone View, 240-243
Visual Voicemail. See Visual Voicemail
migrating, 477-478
mobility technologies, 250
case study, 252
Mobile Communicator, 251-252
Personal Communicator, 251
networking, 28-29
intersite, 32-33
intrasite, 29-31
intrasite versus intersite, 34
VPIM, 36-38
notifications, 292-296
devices, 293-294
enabling/disabling, 294
schedules, 296
users, 293
viewing, 295
voicemail ports, 24
outgoing
faxes, deleting, 428
private, 427
secure, 427
subjects, deleting, 428
text, deleting, 428
phone access, 213-214
alternate extensions, 219-220
message actions, 224
message settings, 223
MWIs, 216-219
Phone Menu options, 221-222
playback settings, 224
sending messages, 225
transfer rules, 214216
pilots, configuring, 124-126
planning, 6-7
current network status/design, 7-8
features required, 10-11

www.it-ebooks.info

redundancy, 10
scalability, 9
user requirements, 8-9
ports, 22-24
amount required, determining, 23
audiotext applications, 24
functions, 23
high availability, 24
message notifications, 24
TRaP, 23
product listing, 4
profiles, 126
read receipts
headers, 428
timing, 428
SpeechView
configuring, 522-523
CoS, 527
licensing, 523-524
message actions, 527-529
notifications, 529
overview, 522
security, 522
SMTP Smart Hosts, 524-529
transcription service, 522, 525-527
SRSV (Survivable Remote Site Voicemail), 111,508
storage
directory, 267
quotas, 276-279
requirements, 20-21
Tamicka-Peg Corporation
intersite networking, 35
voicemail example, 2728
undeliverable,278
Unified Messaging Gateway, 6
Unity, 5
ViewMail for Outlook,314
Voicemail Organization, configuring, 363-365
VPIM location settings, 427-428
waiting indicators. *See* MWIs
web access, 226
Connection Personal Call Transfer Rules, 231
Messaging Assistant, 230
Messaging Inbox, 229-230
Microsoft Outlook, 235-238
PCAs, 226-228
RSS feeds, 233-235
Messaging Assistant, 230
greetings, managing, 285
private distribution lists, creating, 308-309
SMS notification devices, 531
Messaging Inbox, 229-230
MIB2 Agent, 455
Micam-Lyn University greetings case study, 290
Microsoft Outlook, voice message access, 235-238
IMAP client, configuration, 237-238
ViewMail plug-in, 235-236
migrate utilities, 477-478
MIME (Multipurpose Internet Mail Extensions), 30
Mobile Communicator, 251252
mobility technologies, 250
case study, 252
Mobile Communicator, 251252
Personal Communicator,251

www.it-ebooks.info

monitoring
CPU/memory performance,451
critical services, 453-456
AMC service, 454
Audit Event service, 454
AXL web service, 456
CallManager serviceability, 454
CallManager serviceability RTMT, 454
categories, 453
CDP, 454
CDP Agent, 454
Certificate Change Notification, 455
Certificate Expiry Monitor, 455
Database Layer Monitor, 455
DB, 454
DB Replicator, 454
DirSync service, 456
DRF Local, 455
DRF Master, 455
Host Resources Agent, 455
Log Partition Monitoring tool, 455
MIB2 Agent, 455
RIS Data Collector, 455
RTMT Reporter Servlet, 455
Serviceability Reporter, 456
SNMP Master Agent, 455
SOAP,456
Syslog Agent, 455
System Application Agent, 456
Tomcat, 455
Tomcat Stats servlet, 455
Trace Collection service, 455
Trace Collection servlet,455
UXL web service, 456
disk usage, 451-453
performance
counters, 460-463
log viewer, 464-465
profile selection, 464
views, saving, 464
ports, 507
server processes, 451
MTAs (Mail Transfer Agents),361
MTU (Maximum Transmission Unit), 45, 56-57
multiple integrations, 4, 109-110
Multipurpose Internet Mail Extensions (MIME), 30
MWIs (message waiting indicators)
CUCM integrations, 124
message aging policies, 272-275
phone systems, 130
phones, 216-219
troubleshooting, 539-541

N

names
message stores, 262
phone systems, 128
system distribution lists, 305
system objects, 373-375
VPIM
contacts, 441
locations, 440-441
Network Time Protocol. *See* NTP
networking, 28-29
Cisco Voicemail Organization, 363-365

www.it-ebooks.info

cluster management, 371-373
cluster pair status, 372-373
manual failback events, 373
primary status, 372
interlocation cross-server features, 401-402
configuring, 406-408
live reply, 405-406
sign-ins, 403-404
transfers, 405
intersite, 32-33
configuring, 399-401
Tamicka-Peg Corporation voice-mail example, 35
versus intrasite, 34
VPIM connections, 37-38
intrasite, 29-31
active-active cluster-pair designs, 29
automatic versus manual, 377
automatically configuring, 378-381
directory synchronization, verifying, 385-389
distribution lists, 391-392
Live Reply, 32
manually configuring, 381-384
MIME over SMTP, 30
single connection sites, 31
single/multiple call processing systems, 29
system objects, 392
users, verifying, 389-391
verifying, 385
voice network maps, 393-396
versus intersite, 34
limitations, 361
live reply, configuring, 410
locations, 362
connectivity, verifying, 365
intrasite links, 362
WANs, 362
phone system trunks, configuring, 411-414
post-networking
considerations, 414-415
tasks case study, 392-393
preparations, 365
current design/software, reviewing, 365
display names, configuring, 365-366
location connectivity, verifying, 365
SMTP domain names, configuring, 365-366
SMTP server configuration, 367-369
sites, connecting, 363
system objects, naming, 373-375
troubleshooting
cross-server features, 552
dial plans, 547-549
replication agents, 552
VPIM, 36, 421
intersite links, 37-38
Jensen Industries case study, 36
multisite design example, 38-39
new features, 2
notifications, 292-296
devices
configuring, 293-294
timing and delay options, 294
enabling/disabling, 294
schedules, 296

www.it-ebooks.info

SNMP, 510
SpeechView, 529
devices, configuring, 530-531
Messaging Assistant SMS device configuration, 531
SMPP providers, 529
SMS store, 529
users, 293
viewing, 295
voicemail ports, 24
NTP (Network Time Protocol)
client configuration, 61
configuring, 46
Nyquist, Harry, 15-16
Nyquist-Shannon Theorem, 15-16

O

Open Virtualization Format (OVF), 93
opening greetings, 321, 341
operating system installation, 66
operators, 160, 321
optimizing message aging policies, 271-272
outgoing call restrictions, 131
outgoing messages
faxes, deleting, 428
private, 427
secure, 427
subjects, deleting, 428
text, deleting, 428
OVF (Open Virtualization Format), 93

P

PAKs (Product Authorization Keys), 69, 97
partitions
assigning to search spaces, 346-348
configuring, 344
default, editing, 350
deleting, 350-354
overview, 341-342
reassigning, 351-353
system call handlers, 324
troubleshooting, 545-547
users, assigning, 348
VPIM locations, 426
passwords
application, configuring, 47, 64
backup administrators, 178
security, 158-159
trivial password checks, 162
troubleshooting, 549
user templates, 175-176
pattern restrictions, 299
PBX IP Media Gateway. *See* PIMG, 106
PCAs (Personal Communications Assistants), 226-228
Connection Personal Call Transfer Rules, 231
Messaging Assistant, 230
Messaging Inbox, 229-230
PCM (pulse code modulation), 17
PCM Linear codec, 17
PDIO (planning, design, implementation, and operate), 6
Pegeramy Corporation case studies
mobility technologies, 252
user imports, 205-207

www.it-ebooks.info

pem files, 490
performance monitoring, 460-464
log viewer, 464-465
monitoring counters, 460-463
profile selection,464
views, saving, 464
Personal Communications Assistants. *See* **PCAs**
Personal Communicator, 251
phase-in migration, 3
phone access, 213-214
alternate extensions, 219-220
message actions,224
message settings, 223
MWIs, 216-219
Phone Menu options, 221-222
playback settings, 224
sending messages, 225
transfer rules, 214-216
phone numbers
alternate extensions, 219-220
conversion case study, 199-200
converting, 198
phone systems
basics, 128
configuring, 115
hunt pilots, verifying, 136
loop detection,130
names, 128
outgoing call restrictions, 131
ports, configuring, 132-135
searching, 128
TRaP, 128
trunk configuration, 411-414
view settings, 131
Phone View application, 240-243
CUCM integration, 240-241
Phone Menu options, 241
users, configuring, 240
PIMG (PBX IP Media Gateway) integrations, 106-109
bandwidth, 109
configuring, 151
devices available, 108
ports, 107
serial connections, 107
Plan, Prepare, Design, Implement, Operate, and Optimize (PPDIOO), 6
planning, design, implementation, and operate (PDIO), 6
planning voice-messaging, 6-7
current network status/design, 7-8
features required, 10-11
redundancy, 10
scalability, 9
user requirements, 8-9
platform overlays, 25-26
intersite networking, 32-33
Tamicka-Peg Corporation voicemail example,35
versus intrasite networking, 34
VPIM connections, 37-38
intrasite networking, 29-31
active-active cluster-pair designs, 29
Live Reply, 32
MIME over SMTP, 30
single connection sites, 31
single/multiple call processing systems, 29
versus intersite networking, 34
overview, 26
virtualization, 26-27

www.it-ebooks.info

VPIM networking, 36
intersite links, 37-38
Jensen Industries case study, 36
multisite design example, 38-39
platforms
administrators, 158
configuring, 64
installation wizard, 52-54
playback settings, 224
ports
configuring, 132-135
CUCM integrations, 117
distribution list activity, 311
groups
CME integrations, 149-150
integrations, 115-116
ports, 116
SIP integration, 144
integrations, 103
monitoring, 139, 507
PIMG, 107
port groups, 116
rPSM, 137-138
SIP integration, 144-145
verifying, 135-136
voicemail, 22-24
amount required, determining, 23
audiotext applications, 24
functions, 23
high availability, 24
message notifications, 24
TRaP, 23
post-greeting recordings, 285, 324, 329-330
applying to users, 291
configuring, 290
playback settings, 292
recording, 291
transfers, 290
voicemail, 290
post-installation configuration, 67
post-networking
considerations, 414-415
tasks case study, 392-393
PPDIOO (Plan, Prepare, Design, Implement, Operate, and Optimize), 6
pre-installation tasks, 45-47
administrator logins, 46
clock synchronization, 46
DHCP, 45
DNS, 46
interface speed and duplex, 45
MTU, 45
NTP, 46
SMTP host configuration, 46
time zones, 45
usernames/passwords, 47
preliminary designs, 13-14
preparations (networking), 365
current design/software, reviewing, 365
display names, configuring, 365-366
location connectivity, verifying, 365
SMTP
domain names, configuring, 365-366
server configuration, 367-369
private distribution lists, 308-310
addressing messages, 310
CoS configuration, 308
creating, 308-309
user configuration, 310
processes
CUC installation, 47-48
servers, monitoring, 451

www.it-ebooks.info

Product Authorization Keys (PAKs), 69
product deployment selection, 50
profiles
selecting, 464
verifying, 136
voicemail, 126
protocols
DHCP, configuring, 45, 57-58
IMAP, 21-22
combining modes, 22
Idle-mode, 22
Microsoft Outlook configuration, 237-238
Non-Idle mode, 22
LDAP
authentication, 200-201
directory configuration, 193-195
filters, configuring, 196-197
phone numbers, converting, 198
setting up, 192-193
synchronization, 190-191
user verification, 198
users, importing, 195-196
MIME, intrasite networking, 30
NTP, configuring, 46
RTPs, 15
SIP (Session Initiation Protocol)
CME integrations, 150-151
integrations, 144-145
trunk integrations, 140-145
Skinny, 3
CME integrations, 150-151
integrations, 104
SMPP, 529
SMTP, 360-361
domain configuration case study, 369-370
domain names, configuring, 365-366, 422-423
fax integration configuration, 517
host configuration, 46, 63-64
interlocation routing, 428
intrasite networking, 30
proxy addresses, 316, 442
server configuration, 367-369
Smart Hosts. See Smart Hosts (SMTP)
VPIM locations, 426
SNMP, configuring, 509-510
community strings, creating, 509-510
master agent restart warning, 510
notifications, 510
requirements, 509
UDPs, 15
VPIM, 2, 36
publishers
active-active cluster-pairs, installing, 77
installing, 81
first node access, 83
first node configuration, 81
installation dialogue, 81-82
pulse code modulation (PCM), 17

Q - R

quality (audio), 19-20
read receipts
headers, 428
timing, 428
real time monitoring, 139.
***See also* RTMT**
Real-Time Monitoring Tool. *See* RTMT
real-time transport protocols (RTPs), 15
recordings
codecs, 18

www.it-ebooks.info

greetings, 284, 326
greeting administrator configuration, 356-357
post greeting. See post-greeting recordings
redundancy
active-active cluster-pairs, 24-25, 77
voice-messaging design, 10
registering product licenses, 97
remote
administrators, 183, 476
phone prefixes, 426
Port Status Monitor (rPSM), 137-138
phone system trunks, configuring, 411-414
VPIM contacts, 429-431
replication agents, 160, 552
reports, 479
CSV format, 484
faxes, 516
HTML format, 482
listing of, 481-482
record limits, 484
Serviceability Report, 481
Users, viewing, 482
viewing, 481
requirements
features, 10-11
message storage, 20-21
SNMP, 509
users, 8-9
voicemail ports, 23
Restore Wizard, 501-502
restores, performing, 501-503
backup devices, selecting, 501
backup files, 502
components, restoring, 502
final warning, 502
status, 503
restriction tables
alternate extensions, 297-298
listing of, 297
viewing, 297
pattern restrictions, 299
RIS Data Collector, 455
roles (users), 181-183
routing
default, 153
direct calls, 153
greeting administrator configuration, 356-357
Visual Voicemail, configuring, 244-245
forwarded calls, 154
patterns, 142-143
rPSM (Remote Port Status Monitor), 137-138
RSS feeds
CoS, 233
voice messages, accessing, 233-235
limitations, 234
RSS readers, configuring, 233
security, 234
RTMT (Real-Time Monitoring Tool), 447
Alert Central, 468
case study, 460
CPU performance, 451
critical services, 453-456
AMC service, 454
Audit Event service, 454
AXL web service, 456
CallManager serviceability, 454

www.it-ebooks.info

CallManager serviceability RTMT, 454
categories, 453
CDP, 454
CDP Agent, 454
Certificate Change Notification, 455
Certificate Expiry Monitor, 455
Database Layer Monitor, 455
DB, 454
DB Replicator, 454
DirSync service, 456
DRF Local, 455
DRF Master, 455
Host Resources Agent, 455
Log Partition Monitoring tool, 455
MIB2 Agent, 455
RIS Data Collector, 455
RTMT Reporter Servlet, 455
Serviceability Reporter, 456
SNMP Master Agent, 455
SOAP services, 456
Syslog Agent, 455
System Application Agent, 456
Tomcat, 455
Tomcat Stats servlet, 455
Trace Collection service, 455
Trace Collection servlet,455
UXL web service, 456
CUC services, 457-460
disk usage, monitoring, 451-453
downloading, 447
Java components, 447
Job Status section, 471
memory performance, 451
options, 447-449
performance, 460-464
log viewer, 464-465
monitoring counters, 460- 463
profile selection, 464
views, saving, 464
ports, 507
Reporter servlet, 455
server processes, 451
serviceability, 456-457
SysLog Viewer, 471-472
system summaries, 449-450
Trace & Log Central, 468-469
version 8.7,447
zooming in/out, 450
RTPs (real-time transport protocols), 15

S

sampling, 15-16
SB-ADPCM (Sub-Band Adaptive Differential Pulse Code Modulation), 17
scalability, 2
server sizing, 15
voice-messaging design, 9
SCCP (Skinny Client Control Protocol). *See* Skinny
schedules, 165-169
backups, 492, 499-500
configuring, 167
default, 166-167
editing, 167
holidays
default, 165-166
new, adding, 166
notifications,296
tasks, viewing, 479

www.it-ebooks.info

search spaces
configuring, 346
default, editing, 350
deleting, 350-354
overview, 342-343
partition assignments, 346-348
reassigning, 351-353
troubleshooting, 545-547
users, assigning, 348
searching
message stores, 259
phone systems, 128
system call handlers, 324
security
administrators, 158-159
configuring, 63
greeting administrators, 356-357
lockout policies, 162
roles, 181-183
RSS feeds, 234
SpeechView, 522
sender-recorded names, 427
sending
quota, 277, 278
voice messages, 225
serial connections, 107
server sizing, 14-15
audio codecs, 15-20
audio quality, 19-20
decoding, 15
defined, 15
G.711, 16
G.722, 16-17
G.726, 17
G.729, 16
iLBC, 17
implementing, 18
line-side, 17-18
listing of, 20
PCM Linear, 17
recording, 18
sampling, 15-16
transcoding, 17-20
clients supported, 21
IMAP support, 21-22
message storage, 20-21
voicemail ports, 22-24
amount required, determining, 23
audiotext applications, 24
functions, 23
high availability, 24
message notifications, 24
TRaP, 23
servers
AXL, configuring, 203
cluster management, 371-373
cluster pair status, 373-372
manual failback events, 373
primary status, 372
cross-server features, 401-402
configuring, 406-408
live reply, 405-406
sign-ins, 403-404
transfers, 405
troubleshooting, 552
CUCM integrations, 116-117
display names, configuring, 365-366
faxes, 514-515
configuring, 516-517
file types supported, 515
preparations, 515
reports, 516
testing, 520
user accounts, 518-519
verifying, 520

www.it-ebooks.info

licensing, 96
live reply, configuring,410
processes, monitoring, 451
restarts, 67
size. *See* server sizing
SMTP domain names, configuring, 365-366
verifying, 71-72
warm standby, 503-506
Serviceability Report, 481
Serviceability Reporter, 456
services
AXL, 456
critical, 453-456
AMC service, 454
Audit Event service, 454
AXL web service, 456
CallManager serviceability, 454
CallManager serviceability RTMT, 454
categories, 453
CDP, 454
CDP Agent, 454
Certificate Change Notification, 455
Certificate Expiry Monitor, 455
Database Layer Monitor, 455
DB, 454
DB Replicator, 454
DirSync service, 456
DRF Local, 455
DRF Master, 455
Host Resources Agent, 455
Log Partition Monitoring tool, 455
MIB2 Agent, 455
RIS Data Collector, 455
RTMT Reporter Servlet, 455
Serviceability Reporter, 456
SNMP Master Agent, 455
SOAP, 456
Syslog Agent, 455
System Application Agent, 456
Tomcat, 455
Tomcat Stats servlet, 455
Trace Collection service, 455
Trace Collection servlet, 455
UXL web service, 456
SOAP, 456
unified messaging service
configuring, 314
features, 2
gateway, 6
overview, 313
user accounts, 315
ViewMail for Outlook, 314
Session Initiation Protocol. See SIP
Shannon, Claude, 15-16
Short Message Peer-to-Peer Protocol (SMPP), 529
Short Message Service (SMS), 529
Simple Mail Transfer Protocol. *See* SMTP
Simple Network Management Protocol. *See* SNMP
single-site messaging deployment, 110
SIP (Session Initiation Protocol)
CME integrations, 150-151
integrations, 144
port configurations, 144-145
port groups, 144
trunk integrations, 140-145
configuring, 141-142
route patterns, 142-143

www.it-ebooks.info

sites
intersite networking, configuring, 363, 399-401
locations, joining
automatically, 378-381
manually, 381-384
sizes
message stores, 262
servers, 14-15
audio codecs. See audio codecs
clients supported, 21
IMAP support, 21-22
message storage, 20-21
voicemail ports, 22-24
Skinny (Skinny Client Control Protocol), 3
CME integrations, 150-151
integrations, 104
Smart Hosts (SMTP)
configuring, 397-398
IP addresses, 398
locations, 398
fax integration configuration, 517
function, 397
SpeechView, 524-529
access lists, 525
CoS, 527
message actions, 527-529
transcription service configuration, 525-527
transcription service preparations, 525
VPIM networking, 421
SMPP (Short Message Peer-to-Peer Protocol), 529
SMS (Short Message Service), 529
SMS store, 529
SMTP (Simple Mail Transfer Protocol), 360-361
domain configuration case study, 369-370
domain names
configuring, 365-366, 422-423
VPIM locations, 426
fax integration configuration, 517
host configuration, 46, 63-64
interlocation routing, 428
intrasite networking, 30
proxy addresses
user accounts, 316
VPIM contacts, 442
server configuration, 367-369
Smart Hosts
configuring, 397-398
function, 397
SpeechView, 524-529
VPIM networking, 421
SNMP (Simple Network Management Protocol), 509-510
configuring, 509-510
community strings, creating, 509-510
master agent restart warning, 510
notifications, 510
requirements, 509
Master Agent, 455
SOAP services, 456
software
installation, 47, 66
top-level licensing, 95
updates, 88-89
during installation, 89-90
Unified OS Administration, 91-92
Unity Connection 1.2, 92

www.it-ebooks.info

Speech Connect, 96
SpeechView
configuring, 522-523
licensing, 523-524
notifications,529
devices, configuring, 530-531
Messaging Assistant SMS device configuration, 531
SMPP providers, 529
SMS store, 529
overview, 522
security, 522
SMTP Smart Hosts, 524-529
access lists, 525
CoS, 527
message actions, 527-529
transcription service configuration, 525-527
transcription service preparations, 525
transcription service, 522, 525-527
users, configuring
CoS, 527
message actions, 527-529
SRSV (Survivable Remote Site Voicemail), 111,508
standard greetings
defined, 281
options, 327-328
overriding, 283
Standard transfer rule, 214
storage
aging policies, 268-272
alerts, 272-275
case study, 279-280
creating, 271
default, 269-271
optimizing, 271-272
users, applying, 273
archiving, 272
expiration, 275
message stores, 257
backing up, 258
delivered message example, 266
disk space, 266-267
editing, 259, 262
membership, 263-267
moving users, 263-264
names, 262
new, creating, 261-262
options, viewing, 259-261
parameters, 258
searching, 259
sizes, 262
user mailboxes, finding, 263
users, creating, 268
verifying, 266
quotas, 276-279
controlling, 276-278
default, 276
editing, 279
full mailboxes, 278
requirements, 20-21
system configuration directory,258
voice message directory,267
Sub-Band Adaptive Differential Pulse Code Modulation (SB-ADPCM), 17
subscribers
active-active cluster-pairs
installing, 77
servers, configuring, 78
installing, 81
first node access, 83
first node configuration, 81
installation dialogue, 81-82

www.it-ebooks.info

Survivable Remote Site Voicemail (SRSV), 111, 508
synchronization
agreements, 193
clock, 46
directory, 385-389
DirSync service, 192, 456
verifying, 385-389
VPIM, 429, 422
LDAP, 190-191
Syslog Agent, 455
SysLog Viewer, 471-472
system
administrators, 183
Application Agent, 456
configuration directory, 258
default recording, 280-281
distribution lists, 300-306
access lists, 305
allvoicemailenabledcontacts, 301
allvoicemailusers, 301
case study, 306
default, 301
editing, 302
membership, 303-304
names, 305
new, creating, 302-303
undeliverablemessages, 301
viewing, 301
installer, 48-49
objects
naming, 373-375
verifying, 392
summaries, 449-450
system call handlers, 321
caller inputs, 328-329
configuring, 322-324
active schedules, 323
caller input, 324
creation times, 322
display names, 322
extensions, 323
greetings, 324
languages, 323
message settings, 324
owners, 324
partitions, 324
phone systems, 323
recorded names, 324
searches, 324
time zones, 323
transfer rules, 324
default, 321-322
greetings, 325-328
message settings, 330-331
new, configuring, 332
owners, 331-332
post greeting recordings, 324, 329-330
templates, 333-334
transfer rules, 325

T

T1 Media Gateway. *See* TIMG
T.37 on-ramp faxing, 520
T.38 fax relay configuration, 521
Tamicka-Peg Corporation case studies
intersite networking, 35
voicemail example, 27-28
tar files, 502
target backup locations, 491
Task Management tool, 478-479
Check Telephony Integration task, 479

www.it-ebooks.info

schedules, reviewing, 479
viewing, 478
Tcl (Toolkit Command Language) script, 520-521
technicians, 183
Telephony Record and Playback (TraP), 128
telephony service, 146
templates
system call handlers, 333-334
users, 172-176
authentication rules, 175
default, 172
new, creating, 173-175
passwords, 175-176
viewing, 173
voicemailusertemplate, 281
testing faxes, 520
text
outgoing messages, deleting, 428
SpeechView
configuring, 522-523
CoS, 527
licensing, 523-524
message actions, 527-529
notifications, 529
overview, 522
security, 522
SMTP Smart Hosts, 524-529
transcription service, 522, 525-527
Tiferam Corporation case studies
cross-server features, 408-410
dial plans, 354-356
display names, configuring, 367
distribution lists, 306, 375-377
message aging/archiving, 279-280
post-networking tasks, 392-393
RTMT, 460
SMTP domains, configuring, 369-370
time zones, configuring, 45, 54, 323
Times to Re-prompt Caller options, 327
TIMG (T1 Media Gateway) integrations, 106-109
bandwidth, 109
CME, configuring, 151
devices available, 108
digital connections, 107
serial connections, 107
timing read receipts, 428
Tomcat service, 455
Tomcat Stats servlet, 455
Toolkit Command Language (Tcl) script file, 520-521
tools
CUC online, 509
integrations, troubleshooting, 136
Port Monitor, 139
RTMT, 447
Alert Central, 468
case study, 460
CPU performance, 451
critical services. See critical services
CUC services, 457-460
disk usage, monitoring, 451-453
downloading, 447
Java components, 447
Job Status section, 471
memory performance,451
options, 447-449
performance. See performance
ports, 507
Reporter servlet, 455

www.it-ebooks.info

server processes, 451
serviceability, 456-457
SysLog Viewer, 471-472
system summaries, 449-450
Trace & Log Central, 468-469
version 8.7, 447
zooming in/out, 450
Task Management, 478-479
Check Telephony Integration task, 479
schedules, reviewing, 479
viewing, 478
Voice Technology Group Subscription, 509
top-level licensing, 95
Trace & Log Central (RTMT), 468-469
Trace Collection service, 455
Trace Collection servlet, 455
transcoding audio codecs, 17-20
transfer rules
Alternate, 215
busy extension, 216
call screening/queuing options, 216
Closed, 215
Connection Personal Call Transfer Rules, 216
cross-server features, 405
editing, 215
greetings, 285
Standard, 214
status, 216
system call handlers, 324, 325
Transfer Action section, 216
troubleshooting, 543-545
viewing, 214
voice messages, 214-216
TRaP (Telephony Record and Playback), 128
trivial password checks, 162
troubleshooting
addressing messages, 545-547
audiotext applications, 550-552
call transfer rules, 543-545
dial plans, 354-356
error greetings, 281
integrations, 136
logins/passwords, 549
MWIs, 539-541
networking
cross-server features, 552
dial plans, 547-549
replication agents, 552
overview, 536
partitions/search scopes, 545-547
tasks, viewing, 478-479
techniques, 537
assessing the situation, 537-538
developing plans/strategies, 538
good procedures, 538
reporting/resolution/documentation, 539
undeliverable messages, 278
VPIM, 555

U

UDPs (User Datagram Protocols), 15
unattended installations, 86-88
Answer File Generator, 86
download instructions, 86
pre-existing configuration information, 88
undeliverable messages, 278

www.it-ebooks.info

undeliverablemessages distribution list, 301
undeliverablemessagesmailbox user,160
unified messaging service
configuring, 314
features, 2
gateway, 6
overview, 313
user accounts, 315
ViewMail for Outlook, 314
Unified OS Administration
login, 73-76
software updates, 91-92
Unity, 5
updates, 3, 88-89
automatic directory, 431-433
during installation, 89-90
Unified OS Administration, 91-92
Unity Connection 1.2, 92
users, 188
User Datagram Protocols (UDPs), 15
users, 64
aliases, 180
applications
administrators, 158
usernames/passwords, 47, 64
authentication rules, 162-163
default, 162
defining, 162
editing, 163
lockout policies, 162
trivial password checks, 162
viewing, 163
voicemail, 163
web applications, 163
backup administrators, 176-178
call handler owners, 324, 331-332
configuring, 176
Administrative XML, 202-205
BAT, 183184
Bulk Edit, 189-190
DirSync service, activating, 192
importing from AXL, 203-205
importing from LDAP, 195196
LDAP authentication, 200-201
LDAP directory configuration, 193-195
LDAP filters, configuring, 196-197
LDAP setup, 192-193
LDAP synchronization/ authentication, 190-191
with mailboxes, 179-181
phone numbers, converting, 198
roles, 181-183
without mailboxes, 177-178
contacts, 160
CoS, 169-172
default, 169
membership, viewing, 172
new, adding, 170-171
creating with BAT, 187
default, 160-161
distribution list membership, 303-304
exporting to CSV files, 184-185
external service accounts, 311
fax accounts, configuring, 518-519
features required, 10-11
importing
AXL, 203-205
case study, 205-207
LDAP, 195-196, 203205
licensing, 96
limitations, 2

www.it-ebooks.info

live reply, configuring,410
locations, 27
logging in, 70
with mailboxes, 159
mailboxes, finding, 263
management role, 183
message aging policies, applying, 273
message stores
creating, 268
membership, 172
moving between, 263-264
migrating, 472-473, 477-478
notifications,293
operators, 160
partition assignments, 348
phone number conversion case study, 199-200
phone system trunks, configuring, 411-414
Phone View application, configuring, 240
platform administrators, 158
private distribution lists, configuring, 310
replication agents, 160
requirements, 8-9
schedules/holidays, 165-169
configuring schedules, 167
default holidays, 165-166
default schedules, 166-167
editing, 167
new holidays, adding, 166
search space assignments, 348
security, 158-159
SMTP proxy addresses, 316
SpeechView, configuring
CoS, 527
message actions, 527-529
templates, 172-176
authentication rules, 175
default, 172
new, creating, 173-175
passwords, 175-176
viewing, 173
undeliverablemessagesmailbox, 160
unified messaging service, configuring, 315
unityconnection, 161
updating, 188
verifying, 189, 198
viewing, 161
without mailboxes, 159
Users report, viewing, 482
UXL web service, 456

V

verifying
active-active cluster-pairs, 83-86
CME integrations, 148-149
directory synchronization, 385-389
distribution lists, 391-392
faxes, 520
hunt pilots, 136
intrasite networking, 385
location connectivity,365
logins, 73-76
administrator, 73
Unified OS administration login, 73-76
message stores, 266
ports, 135-136
profiles, 136
servers, 71-72
system objects, 392

www.it-ebooks.info

users, 189, 198
VPIM licensing, 425
viewing
authentication rules, 163
cluster management status, 506-507
CoS membership, 172
holidays, 165-166
licensing, 94, 98
mailbox quotas, 276
message store options, 259-261
notifications,295
reports, 481
restriction tables, 297
system
distribution lists, 301
summaries, 449-450
Task Management tool,478
transfer rules, 214
user templates, 173
users, 161
ViewMail for Outlook, 235-236,314
virtualization
installation, 92-94
platform overlays, 26-27
Visual Voicemail, configuring, 243-250
Connection Administration, 243-244
CUCM, 247-249
direct routing rules, 244-245
hunt pilots, 243
IP phone subscriptions, 249-250
Java midlets, 245-246
Voice Mail Port Wizard Results, 122
voice messages. ***See also*** **VPIM**
addressing, troubleshooting, 545-547
aging policies, 268-272
alerts, 272-275
case study, 279-280
creating, 271
default, 269-271
optimizing, 271-272
users, applying, 273
archiving, 272
authentication rules, 163
broadcast, 225
call handler settings, 324, 330-331
CUCM integrations, 116-128
CUE, 5
deployment, 110
centralized, 111
distributed, 112
Mag's Cycle Corporation case study, 113
single-site, 110
designs
preliminary, 13-14
server sizing. See server sizing
distribution lists, 225
expiration, 275
incoming
marking secure, 428
recorded names, deleting, 428
IP phone access, 238-240
Phone View, 240-243
Visual Voicemail. See Visual Voicemail
migrating, 477-478
mobility technologies, 250
case study, 252
Mobile Communicator, 251-252
Personal Communicator, 251
networking, 28-29
intersite, 32-33
intrasite, 29-31
intrasite versus intersite, 34
VPIM, 36-38

www.it-ebooks.info

notifications, 292-296
devices, 293-294
enabling/disabling,294
schedules, 296
users, 293
viewing, 295
voicemail ports, 24
outgoing
faxes, deleting,428
private, 427
secure, 427
subjects, deleting, 428
text, deleting, 428
phone access, 213-214
alternate extensions, 219-220
message actions, 224
message settings, 223
MWIs, 216-219
Phone Menu options, 221-222
playback settings, 224
sending messages, 225
transfer rules, 214-216
pilots, configuring, 124-126
planning, 6-7
current network status/design, 7-8
features required, 10-11
redundancy, 10
scalability, 9
user requirements, 8-9
ports, 22-24
amount required, determining, 23
audiotext applications, 24
functions, 23
high availability, 24
message notifications, 24
TRaP, 23
product listing, 4
profiles, 126
read receipts
headers, 428
timing, 428
SpeechView
configuring, 522-523
CoS, 527
licensing, 523-524
message actions, 527-529
notifications, 529
overview, 522
security, 522
SMTP Smart Hosts, 524-529
transcription service, 522, 525-527
SRSV (Survivable Remote Site Voicemail), 111,508
storage
directory, 267
quotas, 276-279
requirements, 20-21
Tamicka-Peg Corporation
intersite networking, 35
voicemail example, 2728
undeliverable,278
Unified Messaging Gateway, 6
Unity, 5
ViewMail for Outlook,314
Voicemail Organization, configuring, 363-365
VPIM, 2
waiting indicators. *See* MWIs
web access, 226
Connection Personal Call Transfer Rules, 231
Messaging Assistant, 230
Messaging Inbox, 229-230

www.it-ebooks.info

Microsoft Outlook, 235-238
PCAs, 226-228
RSS feeds, 233-235
voice network maps, 393-396
Voice Profile for Internet Mail. *See* VPIM
Voice Technology Group Subscription tool, 509
voicemail. See voice messages
voicemailusertemplate, 173, 281
VPIM (Voice Profile for Internet Mail), 2
blind addressing, 420
case study, 433-434
codecs, 418
connectivity,421
contacts, 420
alternative names, 441
automatic directory updates, 431-433
automatically creating, 435-437
blind addressing, 434-435
creating, 429
deleting, 437-438
remote, 429-431
SMTP proxy addresses, 442
Dial IDs, 419
dial plans, 419
directory synchronization, 422
distribution lists, 420-421
DNS, 421
domain names, 421
features, 440-442
alternative names for contacts, 441
alternative names for locations, 440-441
SMTP proxy addresses, 442
licensing, 419, 425
locations, 425-429
alternative names, 440-441
audio format conversions, 427
audio normalization, 427
Dial IDs, 426
directory synchronization, 429
display names, 425
interlocation SMTP routing, 428
IP addresses, 426
message settings, 427-428
new locations, adding,425
partitions, 426
prefixes, 427
remote phone prefixes, 426
SMTP domain names, 426
networking, 421
overview, 418-419
SMTP
domain names, configuring, 422-423
Smart Hosts, 421
troubleshooting, 555
voicemail design, 36
intersite links, 37-38
Jensen Industries case study, 36
multisite design example, 38-39

W

WAN locations, connecting, 362
warm standby servers, 503-506
warning quota, 277
web
applications, authentication rules, 163
voice messages, accessing, 226
Connection Personal Call Transfer Rules, 231

www.it-ebooks.info

Messaging Assistant, 230
Messaging Inbox, 229-230
Microsoft Outlook, 235-238
PCAs, 226-228
RSS feeds, 233-235
websites
Answer File Generator, 86
COBRAS, 92
CUC online tools, 509
integration troubleshooting tools, 136
ViewMail plug-in, 235
wizards
platform installation, 52-54
Restore, 501-502
Voice Mail Port Wizard Results, 122

Z

zooming (RTMT), 450

www.it-ebooks.info