cisco

Lab Manual

CCNA VOICE

ciscopress.com

Brent Sieling

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CCNA Voice Lab Manual

Brent Sieling

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CCNA Voice Lab Manual

Brent Sieling

Copyright© 2013 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

Second Printing: February 2014

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

ISBN-13: 978-1-58713-299-5

ISBN-10: 1-58713-299-0

Warning and Disclaimer

This book is designed to provide information about CCNA Voice. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

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

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Business Operation Manager, Cisco Press
Anand Sundaram

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Development Editor
Ellie Bru

Project Editor
Mandie Frank

Copy Editor
John Edwards

Technical Editor(s)
Brion Washington
Michael H. Valentine

Editorial Assistant
Vanessa Evans

Designer
Mark Shirar

Composition
Tricia Bronkella

Proofreader
Sheri Cain

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Trademark Acknowledgments

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

Corporate and Government Sales

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

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.

©2008 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)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

About the Author

Brent Sieling is an instructor and program director for the two-year Network Specialist Associate Degree at Madison College. He has been teaching networking classes full-time since January 2006 and part-time for three semesters prior to that. He is the lead contact for the Academy Support Center and Instructor Training Center at Madison College's Cisco Networking Academy, providing support to over 30 high schools and technical colleges in the state of Wisconsin. Brent previously worked as a network specialist at the Madison Metropolitan School District, where he managed a network of over 50 schools. Brent currently holds the Cisco Certified Network Associate (CCNA), CCNA Voice, and CCNA Security certifications, and he was previously a Certified Novell Engineer (CNE). He recently completed the Cisco Academy Instructor Trainer Qualification (ITQ) process to become an Academy Instructor Trainer. Brent has been a regular presenter at the Cisco Academy conferences.

About the Contributing Authors

David Bateman is a Certified Cisco Systems instructor with more than 20 years of internetworking experience. David has always enjoyed sharing his knowledge and has been a Cisco instructor for Skyline-ATS since 2000. In addition to teaching he is involved in authoring courses and books including *Configuring Cisco Communication Manager & Unity Connection* released by Cisco Press. David is currently the director of Educational Services for Skyline-ATS. His years of real-world technical and business knowledge allow him to bring a unique perspective to the classroom, where he not only delivers critical technical knowledge but can also explain how technologies can be used to address various business needs.

Brian Morgan, CCIE No. 4865, is a Collaboration Architect with Cisco specializing in Unified Communications and Collaboration technologies. With over 20 years in the networking industry, he has performed in a number of roles, including network consultant, Certified Cisco Systems Instructor, and engineering director for a telecommunications company. When he's not spending time with his family, Brian enjoys working with local high school and college students enrolled in local Cisco Network Academy programs in North Texas.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

About the Technical Reviewers

Michael Valentine has more than 15 years of experience in the IT field, specializing in Cisco networking and VoIP technologies. He is a freelance Cisco Certified Systems Instructor, currently associated with Skyline Advanced Technology Services. His accessible, humorous and effective teaching style has demystified Cisco for hundreds of students since he began teaching in 2002. He has developed courseware and lab guides both for Cisco Systems and third-party clients.

Mike received his Bachelor of Arts from the University of British Columbia and currently holds CCNA, CCNA Voice, CCDA, CCNP, CCVP, and CCSI certifications, among others.

Mike has authored, co-authored, and technically reviewed several Cisco Press titles.

Brion Washington has been working with Cisco VOIP since the 4.x release. His expertise is in Cisco Unified Communications Manager (CUCM) and Voice Gateways. He has authored the *CCVP GWGK Quick Reference* (978-1-58714-355-7), *CCNP Voice TVoice 642-427 Quick Reference* (978-1-58714-365-6), and *CCNP Voice CAPPS 642-467 Quick Reference* (978-1-58714-361-8), and served as a technical editor for multiple others. He currently works as a Senior Network Engineer based on the East coast.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Acknowledgments

I have many people to thank for helping put this book together. Thankfully for me, this is not the Academy Awards, where the orchestra can cut me off if I go on too long.

First is Mary Beth Ray of Cisco Press. I owe her thanks for her willingness to work with a first-time author to produce a lab book for the CCNA Voice certification. I owe her even more thanks for not sending the Cisco Press Ninja Assassins after me when I was late on my deadlines, even though I completely deserved it.

To Ellie Bru, Mandie Frank, and John Edwards of Cisco Press. Ellie and Mandie had the unfortunate task of working with a first-time author, trying to get me to complete everything (and in a readable format). John not only had to correct my writing, but also to translate it into proper English.

To David Bateman and Brian Morgan. Despite my years of experience with Cisco's router-based voice solution, there are parts of the voice world, such as Cisco Unified Presence Server, that I had not dabbled in. Their writing both helped to make this book more complete and kept the deadlines from slipping any further.

To Brion Washington and Michael Valentine. As technical reviewers, they both made sure that I was as accurate as possible in explanations, and more than once caught areas where I made mistakes.

To David Shonkwiler and Ken McCullough. As my dean and department head, respectively, they have made it possible to teach in one of the finest two-year schools in the state of Wisconsin, if not the nation. They have made sure that my students have access to the equipment and resources in the classroom to succeed in their future jobs.

To Cheryl Halle and Curt Chambers. As any instructor will tell you, his or her success is in large part due to the people who provide help, and Cheryl and Curt are the best at running our labs. The labs are so well run that the Cisco Academy has held instructor training qualifications here twice in the past year, and the Academy told us it could not have had an easier time.

There are many students who were guinea pigs for my labs over the past year and worked on my beta versions (and many alpha versions). They had to put up with my hands waving in the air as I explained how cool this stuff was, even the QoS portion. I was able to sneak their names into Appendix B, "IP Addressing and Phone Extensions for Cisco Unified Communications Manager Labs (Chapters 8–14 and 16–17)," along with many of my students who achieved their CCNA certification while at Madison College. However, there are two students who went above and beyond and deserve special recognition: Krzysztof Petrynko and John Endries. They both put in numerous hours checking my labs and giving me valuable feedback.

In addition to dedicating the book to my wife Megan, I also have to thank her for not only keeping things running at home (I promise to start cooking dinner more often now that this is done!), but also for doing the initial proofread of all my writing. (She was the one to point out that I needed to hyphenate *ever-patient* in the dedication.)

Finally, I have to thank Cisco itself and, by extension, the Cisco Networking Academy. There are few companies in the world that would spend millions of dollars to develop and maintain excellent curriculums and then give it to schools at no cost. My former students would not have their great jobs without the fantastic CCNA Exploration curriculum that the Academy offers. I have found great success in teaching the Academy curriculum and learned many new things along the way.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Dedication

This book is dedicated to my ever-patient wife Megan Schliesman and my wonderful daughter Lily (who will be mortified that I mentioned her name).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Contents at a Glance

Introduction xxviii
Hardware Section xxix

Part I: Voice Concepts

Chapter 1 Traditional and Unified Voice 1

Chapter 2 Understanding Cisco Unified Communications Solutions 3

Chapter 3 Establishing Network Connectivity and Understanding IP Phone Registration 5

Part II: Cisco Unified Communications Manager Express (CUCME)

Chapter 4 Introduction to CUCME Administration 23

Chapter 5 Configuring Phones and Users in Cisco Unified Communications Manager Express (CUCME) 37

Chapter 6 Cisco Unified Communications Manager Express (CUCME) Dial Plans and QoS 73

Chapter 7 Cisco Unified Communications Manager Express (CUCME) Productivity Features 151

Part III: Cisco Unified Communications Manager (CUCM)

Chapter 8 Administrative Interfaces 165

Chapter 9 Managing Services, Phones, and Users 169

Chapter 10 CUCM Dial Plan 257

Chapter 11 CUCM Telephony Features 337

Chapter 12 CUCM Mobility Features 363

Part IV: Voicemail and Presence Solutions

Chapter 13 Cisco Unity Connection 381

Chapter 14 Cisco Unified Presence 425

Part V: Management and Troubleshooting

Chapter 15 Troubleshooting Cisco Unified Communications Manager Express (CUCME) 457

Chapter 16 Troubleshooting CUCM 465

Chapter 17 Monitoring Cisco Unity Connection 481

Part VI: Appendixes

Appendix A IP Addressing and Phone Extensions for Cisco Unified Communications Manager Express (CUCME) Labs 489

Appendix B IP Addressing and Phone Extensions for Cisco Unified Communications Manager (CUCM) Labs (Chapters 8–14 and 16–17) 495

Appendix C Building Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUC), and Cisco Unified Presence (CUPS) Servers in VMware Workstation 501

Appendix D Configuring the Cisco Unified Communications Manager Express Router 531

Appendix E PSTN Simulator 547

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Contents

Introduction xxvii

Hardware Section xxix

Part I: Voice Concepts

Chapter 1 Traditional and Unified Voice 1

Lab 1-1: Telephony Terminology 1

Task 1: Matching Items 1

Chapter 2 Understanding Cisco Unified Communications Solutions 3

Lab 2-1: Key Features of Cisco Unified Communications Solutions 3

Task 1: Questions 3

Chapter 3 Establishing Network Connectivity and Understanding IP Phone Registration 5

Lab 3-1: Network Connectivity 5

Task 1: Clear and Cable Devices 6

Step 1-1: Clear Prior Configurations 6

Step 1-2: Cable Router and Switch 6

Task 2: Configure Basic Setup 6

Step 2-1: Configure Basic Setup on the Router 6

Step 2-2: Configure Basic Setup on the Switch 6

Task 3: Configure the Switch 7

Step 3-1: Create the VLANs 7

Step 3-2: Configure the Trunk Port 7

Step 3-3: Configure the Access Ports 8

Step 3-4: Configure the Switch Management Interface 9

Task 4: Configure the Router Subinterfaces 9

Step 4-1: Configure the Data VLAN Subinterface 9

Step 4-2: Configure the Management VLAN Subinterface 9

Step 4-3: Configure the Voice VLAN Subinterface 9

Step 4-4: Activate the Router Interface 9

Task 5: Verification 10

Step 5-1: Verify Switch VLAN Configuration 10

Step 5-2: Verify Switch Port Assignment 10

Step 5-3: Verify Router Subinterface IP Assignment 11

Task 6: DHCP Services 11

Step 6-1: Configure DHCP Pools on the Router 12

Task 7: Test and Cleanup 12

Step 7-1: Test Connectivity 12

Step 7-2: Save the Configurations 12

Step 7-3: (Optional) Explore Power Over Ethernet on the Switch 13

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 3-2: Network Time Protocol 15

Task 1: NTP Services 15

Step 1-1: Load Prior Configurations 15
Step 1-2: (Optional) Configure Local Time Zone 16
Step 1-3: Manually Set the Clock 16
Step 1-4 (Option A): Contact an NTP Server on the Internet 16
Step 1-4 (Option B): Configure Another Cisco Router to Act as an NTP Server 17
Step 1-5: Verify That the Time Is Synchronized 17
Step 1-6: (Optional) Configure the Switch to Get NTP from the Router 21
Step 1-7: Save the Configurations 21

Lab 3-3: Phone Boot/Registration Process 22

Task 1: Questions 22

Part II: Cisco Unified Communications Manager Express (CUCME)

Chapter 4 Introduction to CUCME Administration 23

Lab 4-1: Exploring the Command-Line Interface and Cisco Configuration Professional 23

Task 1: Load Prior Configurations 23

Task 2: Explore Telephony Services 24

Step 2-1: Determine CUCME Version 24

Task 3: Exploring CUCME Using CCP 25

Step 3-1: Test Connectivity Between PC and Router 25
Step 3-2: Configure the Router for CCP Access 25
Step 3-3: Open the CCP Application 26
Step 3-4: Create a Community in CCP 26
Step 3-5: Working with a Community in CCP 27
Step 3-6: Viewing Device Configuration Options in CCP 28
Step 3-7: Establish Unified Communication Functionality in CCP 29
Step 3-8: Deliver Configuration from CCP to the Router 29
Step 3-9: Review Unified Communications Features Summary 30
Step 3-10: Save the Startup Configuration in CCP 31
Step 3-11: Save the Running Configuration to the PC Using CCP 31
Step 3-12: Explore Other Parts of CCP 32

Lab 4-2: Integrated HTML GUI 33

Task 1: Load Prior Configurations 33

Task 2: Configure the Router for Web Access 33

Step 2-1: Enable HTTP Service on the Router 33
Step 2-2: Create a CUCME Web Administrator Account 34
Step 2-3: Use a Web Browser to Connect to the GUI 34

Chapter 5 Configuring Phones and Users in Cisco Unified Communications Manager Express (CUCME) 37

Lab 5-1: Basic Manual Phone Configuration Using the CLI 37

Task 1: Load Prior Configurations 38

Task 2: Configure Telephony-Service 38

Step 2-1: Disable Auto Phone Registration 38
Step 2-2: Establish the Maximum Number of Phones Allowed to Register 38
Step 2-3: Establish the Maximum Number of Directory Numbers (Phone Numbers) 38

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-4: Set the IP Address Used by CUCME 39
Step 2-5: Create the Default Template Files 39
Step 2-6: Inspect the IP Phone Generic Config File 40
Task 3: Configuring Directory Numbers 41
Step 3-1: Create a Dual-Line Ephone-dn 41
Step 3-2: Repeat to Create the Next Three Phone Numbers 41
Task 4: Manually Configure an Ephone and Associate the First Directory Number 42
Step 4-1: Get the MAC Address of the First Phone 42
Step 4-2: Create an Ephone and Assign the MAC Address 42
Step 4-3: Assign the First Directory Number to the First Button on the Phone 43
Step 4-4: Connect the First Phone to the Switch 44
Task 5: Manually Configure a Second Phone 44
Step 5-1: Connect the Second Phone to the Switch 45
Step 5-2: Assign the Second and First Directory Numbers to the Second Phone 45
Step 5-3: Make a Call 46
Step 5-4: Assign Other Extensions to the First Phone 46
Step 5-5: Clear Configuration for the Next Lab 47

Lab 5-2: Advanced Manual Phone Configuration Using the CLI 48
Task 1: Load Prior Configurations 48
Task 2: Configure Telephony-Service 49
Step 2-1: Configure Required Telephony-Service Settings 49
Step 2-2: Configure System Time in Telephony-Service 49
Step 2-3: Configure a Banner Message for Phones with a Display 49
Task 3: Configure Ephone-dns 50
Step 3-1: Add the name Option to an Ephone-dn 50
Step 3-2: Change the Phone Display Header Bar 50
Step 3-3: Change the Text for Each Line Button 51
Step 3-4: Create the Other Ephone-dns 51
Task 4: Configure Ephones 51
Step 4-1: Create an Ephone, and Assign the MAC Address and a Directory Number 51
Step 4-2: Assign the Ephone Model Type 52
Step 4-3: Assign Users to the Phones 52
Step 4-4: Create the Other Ephones 52
Task 5: Test and Save Configuration 53
Step 5-1: Make Calls 53
Step 5-2: Save the Configuration 53

Lab 5-3: Adding Directory Numbers, Phones, and Users with Cisco Configuration Professional (CCP) 54
Task 1: Load Prior Configurations 54
Task 2: Configure Telephony Settings 55
Step 2-1: View Telephony Settings 55
Step 2-2: Edit General Telephony Settings 55
Step 2-3: Edit System Config Telephony Settings 56
Task 3: Configure Extensions 57
Step 3-1: View Extension Settings 57
Step 3-2: Create an Extension 58
Step 3-3: Create More Extensions 60

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 4: Configure Phones and Users 60
Step 4-1: View Phone/User Settings 60
Step 4-2: Create a Phone 60
Step 4-3: Create a User 62
Step 4-4: Create Another Phone/User 62
Task 5: Test and Save Configuration 63
Step 5-1: Make Calls 63
Step 5-2: Examine the Router Configuration 64
Step 5-3: Save the Configuration 64

Lab 5-4: Examine VoIP Protocols 65
Task 1: Load Prior Configurations 65
Task 2: Establish Packet Capture 65
Step 2-1: Configure the Switch for Packet Capture 66
Task 3: Start Wireshark Capture 66
Step 3-1: Examine Phone Boot in Wireshark 66
Step 3-2: Examine a Phone Call in Wireshark 67
Task 4: Play Captured Audio 70
Task 5: Clean Up 72

Chapter 6 Cisco Unified Communications Manager Express (CUCME) Dial Plans and QoS 73

Lab 6-1: (Optional) Configuring Analog Interfaces 73
Task 1: Load Prior Configurations 74
Task 2: Examine the Interfaces in the Router 74
Task 3: Configuring FXS Ports 75
Step 3-1: Call Signaling Selection 75
Step 3-2: Connect an Analog Phone and Make a Call 75
Step 3-3: Call Progress Tones 75
Step 3-4: Description Information 76
Step 3-5: Caller ID Information 76
Step 3-6: Examine Interface Status 77
Step 3-7: Automatically Dialing Phones 77
Task 4: Configuring FXO Ports 77
Step 4-1: Configure Dial Type 77
Step 4-2: Configure Ring Number 78
Step 4-3: Description Information 78
Step 4-4: Connect the FXO Port (Optional) 78
Step 4-5: Redirect Incoming Calls (Optional) 78

Lab 6-2: (Optional) Configuring Digital Interfaces 79
Task 1: Load Prior Configurations 79
Task 2: Examine Resources in the Router 80
Step 2-1: Examine Hardware 80
Step 2-2: Examine Controller Interface 80
Step 2-3: Examine DSP Resources 81
Task 3: Configure CCS (PRI) Settings 82
Step 3-1: Configure ISDN Switch Type 82
Step 3-2: Configure Clock Participation 82
Step 3-3: Configure Controller T1 Settings 82
Step 3-4: Configure PRI Timeslots 83
Step 3-5: Examine the Interfaces 84
Task 4: Configure ISDN Network End 85

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 6-3: Call Legs, Dial Peers, and Wildcards 86

Task 1: Call Legs 86

Step 1-1: Understanding Call Legs 86

Task 2: Introduction to Dial Peers 87

Step 2-1: Call Flow with a Single-Router Dial Peer Exercise 87

Step 2-2: Create POTS Dial Peers 88

Step 2-3: Call Flow for Dual-Router Dial Peers Without Wildcards Exercise 89

Task 3: Introduction to Wildcards in Cisco Unified Communications Manager Express (CUCME) 90

Step 3-1: Call Flow for Dual-Router Dial Peers with Wildcards Exercise 91

Step 3-2: Create Destination Patterns Using Wildcards 92

Task 4: Create POTS and VoIP Dial Peers 93

Lab 6-4: Call Processing, Dial Plans, and Digit Manipulation 95

Task 1: Outbound Call Processing 95

Step 1-1: Examining Dial-Peer Selection 95

Step 1-2: Understanding Dial-Peer Selection 97

Step 1-3: Troubleshooting Dial-Peer Selection with the show dial-peer voice summary Command 99

Step 1-4: Troubleshooting Dial-Peer Selection with Debug 101

Task 2: POTS Dial-Peer Behavior and Digit Manipulation 102

Step 2-1: Examining POTS Dial-Peer Digit Stripping 103

Task 3: Inbound Dial-Peer Selection 106

Step 3-1: Examine Digit Matching for Inbound Calls 106

Task 4: Dial Plans for the PSTN 107

Step 4-1: Understanding Dial Plans 107

Step 4-2: Creating a PSTN Dial Plan for the NANP 108

Lab 6-5: Dial-Peer Configuration Using the CLI 110

Task 1: Load Prior Configurations 111

Task 2: Configure Hardware Used by the Dial Peers 112

Task 3: Configure Secondary Dial Tone 112

Task 4: Configure the PSTN Dial Peers 113

Step 4-1: Configure Emergency Services Calls 113

Step 4-2: Configure Service Code Calls 114

Step 4-3: Configure Local Calls 114

Step 4-4: Configure Long-Distance (Toll) Calls 114

Step 4-5: Configure Toll-Free Calls 115

Step 4-6: Configure Premium-Rate Calls 115

Step 4-7: Configure International Calls 115

Step 4-8: Make Test Calls to the PSTN Simulator 116

Task 5: Inbound Calls 117

Step 5-1: Configure for Inbound Calls 117

Step 5-2: Test Inbound Calls 118

Task 6: Calls over the WAN 119

Step 6-1: Configure a WAN Connection 119

Step 6-2: Configure a Routing Protocol (Optional) 119

Step 6-3: Configure Four-Digit VoIP Dial Peers to Other Pods Using the WAN 119

Step 6-4: Create VoIP Dial Peer for Any Other Pods 120

Step 6-5: Verify Calls to Other Pods Using the WAN 120

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 7: PSTN Failover 120
Step 7-1: Configure a PSTN Failover 120
Step 7-2: Configure a PSTN Failover 121
Step 7-3: Configure Remaining PSTN Failover Dial Peers 121
Step 7-4: Test PSTN Failover 121
Step 7-5: Verify That VoIP Dial Peers Resume Calls When the WAN Is Back Up 121

Lab 6-6: Dial-Peer Configuration Using CCP 122
Task 1: Load Prior Configurations 123
Task 2A: Configure Digital T1/E1/PRI Interface 124
Step 2A-1: Digital Trunks 124
Step 2A-2: T1/E1 Interface 124
Step 2A-3: Deliver Configuration from CCP to the Router 125
Step 2A-4: Deliver Configuration from CCP to the Router 126
Task 2B: Configure Analog FXO/FXS Interfaces 126
Step 2B-1: Analog Trunks 126
Task 3: Configure Secondary Dial Tone 127
Task 4: Create Outgoing Dial Plan 128
Step 4-1: POTS Dial Plans 128
Step 4-2: Import Outgoing Template 128
Step 4-3: Outgoing Dial Plan Summary 129
Step 4-4: Selecting Destination Trunk 130
Step 4-5: Apply Configuration 130
Task 5: Create Outbound POTS Dial Peers 131
Step 5-1: View POTS Dial Peers 131
Step 5-2: Create POTS Dial Peer 132
Step 5-3: Digit Manipulation 132
Step 5-4: Dial Peers Challenge 133
Step 5-5: Make Test Calls to the PSTN Simulator 134
Task 6: Create Incoming Dial Plan 134
Step 6-1: Create Dial Plans Wizard Selection 134
Step 6-2: Incoming Dial Plan Summary 134
Step 6-3: Create Incoming Dial Plan 134
Step 6-4: Test Incoming Dial Plan 135
Task 7: Create VoIP Dial Peers 135
Step 7-1: Configure a WAN Connection 135
Step 7-2: Configure a Routing Protocol (Optional) 136
Step 7-3: View VoIP Dial Peers 136
Step 7-4: Create VoIP Dial Peer 136
Step 7-5: Create VoIP Dial Peer for Any Other Pods 136
Step 7-6: Verify Calls to Other Pods Using the WAN 136
Task 8: PSTN Failover 137
Step 8-1: Configure a POTS Dial Peer for Failover 137
Step 8-2: Configure a POTS Dial Peer for Failover 137
Step 8-3: Digit Manipulation 138
Step 8-4: Configure Remaining PSTN Failover Dial Peers 139
Step 8-5: Test PSTN Failover 139
Step 8-6: Verify That VoIP Dial Peers Resume Calls When the WAN Is Back Up 139

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 6-7: Quality of Service (QoS) 140
Task 1: Questions 144
Task 2: AutoQoS on a Switch (Optional) 144
Step 2-1: Configure a Port for a Cisco Phone 145
Step 2-2: Configure a Port for PC with Cisco IP Communicator 145
Step 2-3: Configure the Uplink to the Router 145
Step 2-4: Examine the Changes to the Switch Config 145
Step 2-5: Verify the QoS Operation 148
Task 3: AutoQoS on a Router (Optional) 149
Step 3-1: Configure the Port Connected to the Switch 149
Step 3-2: Verify the QoS Configuration 149

Chapter 7 Cisco Unified Communications Manager Express (CUCME) Productivity Features 151

Lab 7-1: Configuring the Phone Directory 151
Task 1: Load Prior Configurations 152
Task 2: Populate the Directory 152
Step 2-1: Manually Adding Directory Entries Using the CLI 152
Step 2-2: Manually Adding Directory Entries Using CCP 152
Step 2-3: Enabling the Local Directory on the Phone Display 154

Lab 7-2: Configuring Call Forwarding 156
Task 1: Load Prior Configurations 156
Task 2: Configure Call Forwarding on the Phone 156
Task 3: Configure Call Forwarding on the Router 157
Step 3-1: Configuring Call Forwarding Using the CLI 157
Step 3-2: Configuring Call Forwarding Using the CCP 158
Step 3-3: Infinite Loop Solved 160

Lab 7-3: Configuring Call Detail Records and Accounting 161
Task 1: Load Prior Configurations 161
Task 2: Establish Logging Locally on the Router 162
Task 3: Establish Logging and CDRs to a Syslog Server 163

Part III: Cisco Unified Communications Manager (CUCM)

Chapter 8 Administrative Interfaces 165

Lab 8-1: Exploring the CUCM GUI 165
Task 1: CUCM Administrative Interfaces 166
Task 2: The CCMAdmin Page 168

Chapter 9 Managing Services, Phones, and Users 169

Lab 9-1: Phone Boot Process 169

Lab 9-2: CUCM Services 170
Task 1: Remove DNS Dependencies 171
Step 1-1: Change Server Host Name to IP Address 171
Step 1-2: Change Phone References to IP Address 172
Task 2: Examine Network and Feature Services 173
Step 2-1: Examine Network Services 173
Step 2-2: Examine Feature Services 173

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 3: Activating Feature Services and Using Help 174
Step 3-1: Service Activation Page 174
Step 3-2: Using the Help Menu 175
Step 3-3: Activate Cisco CallManager and Cisco TFTP Services 176
Task 4: Examine CUCM Licenses 176
Step 4-1: View License Unit Report 176

Lab 9-3: Autoregistration for Phones 178

Task 1: Verify That Required Services Are Ready 179
Task 2: Enable Autoregistration 179
Step 2-1: Verify Enterprise Settings for Autoregistration 179
Step 2-2: Enable Autoregistration 179
Task 3: Testing with Phones 180
Step 3-1: Connect Two Phones 180
Step 3-2: Examine the Registered Phones 181
Task 4: Cleanup 182
Step 4-1: Disable Autoregistration 182
Step 4-2: Remove Registered Phones 182

Lab 9-4: Preparing for Phone Registration 183

Task 1: Examine the Default Device Pool 184
Task 2: Communications Manager Groups 184
Example of a Cluster with Three Servers 185
Task 3: Date/Time Groups 187
Step 3-1: Create Central Time Zone Group 188
Step 3-2: Create Eastern Time Zone Group 188
Task 4: Regions 189
Step 4-1: Examine the Default Region Codecs 190
Step 4-2: Create the First Two Regions 190
Step 4-3: Modify Region Relationships 191
Step 4-4: Create a Third Region 192
Task 5: Locations 193
Task 6: Device Pools 194
Step 6-1: Create Madison Device Pool 195
Step 6-2: Create New York Device Pool 195
Step 6-3: Create Chicago Device Pool 196
Task 7: Phone Button Templates 196
Step 7-1: Create Phone Button Template 196
Step 7-2: Modify Phone Button Template 198
Task 8: Softkey Templates 199
Step 8-1: Create Softkey Template 199
Step 8-2: Modify Softkey Template 200
Task 9: Common Phone Profile 202
Task 10: Device Defaults 202
Task 11: Testing 203
Task 12: Cleanup 204

Lab 9-5: Registering Phones Manually 205

Task 1: Manually Register a Phone 205
Step 1-1: Manually Add a Phone 205
Step 1-2: Manually Add a Directory Number 207
Step 1-3: Manually Add More Directory Numbers 209

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Manually Register More Phones 210

Task 3: Test Custom Softkey Templates 210

Lab 9-6: Registering and Updating Phones Using the Bulk Administration Tool (BAT) 212

Task 1: Activate the BAT Service 213

Task 2: Examine a Phone Export File 213

Step 2-1: Export Phone Configurations 213
Step 2-2: Job Scheduler 214
Step 2-3: Download Files 215
Step 2-4: Open the Phone Export File in Microsoft Excel 216

Task 3: Download BAT File to Import Phones 217

Step 3-1: Using the BAT File 217
Step 3-2: Upload the BAT Import File 220

Task 4: Create BAT Template 221

Step 4-1: Create BAT Phone Template 221
Step 4-2: Add Lines to the BAT Phone Template 222

Task 5: Validate Data Import 224

Task 6: Complete Importing Phones 225

Task 7: Verify Phone Import 226

Task 8: Modifying Existing Phones 227

Step 8-1: Find the Phones to Update 227
Step 8-2: Update Phone Parameters 227

Lab 9-7: Adding End Users Manually 229

Task 1: Examine Administrative Users 230

Task 2: Examine User Groups 231

Task 3: Examine Roles 232

Task 4: Create New AXL Group 234

Task 5: Create the New AXL User 235

Task 6: Examine the Default Login Credential Policy 235

Task 7: Manually Create an End User 236

Task 8: Explore End User Web Pages 239

Lab 9-8: Adding End Users with the Bulk Administration Tool (BAT) 241

Task 1: Use BAT to Import End Users 241

Step 1-1: Use BAT Template 241
Step 1-2: Upload the BAT Import File 242
Step 1-3: Create BAT User Template 243
Step 1-4: Insert New Users 244
Step 1-5: Verify User Import 244

Lab 9-9: Adding End Users with LDAP Synchronization 246

Task 1: Set Up Windows Server 247

Step 1-1: Verify Server IP Address 247
Step 1-2: Configure Active Directory Sync Admin Account 247
Step 1-3: Create New Organizational Unit in Windows 250
Step 1-4: Create End Users in Windows 250

Task 2: Activate DirSync Service in CUCM 251

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 3: Configure CUCM LDAP Synchronization 251
Step 3-1: Configure LDAP System 251
Step 3-2: Configure LDAP Directory 252
Step 3-3: Verify New Users 253
Step 3-4: Add CUCM User to Active Directory 254
Step 3-5: Resync LDAP 254
Task 4: Configure CUCM LDAP Authentication 255
Step 4-1: Configure LDAP Authentication 255
Step 4-2: Verification of End-User Passwords 256
Task 5: Clean Up 256

Chapter 10 CUCM Dial Plan 257

Lab 10-1: Call Routing 257
Task 1: Examine CUCM Call-Routing Logic 258
Step 1-1: Understanding CUCM Wildcards 258
Step 1-2: Understanding CUCM Call-Routing Logic 259
Step 1-3: Understanding CUCM Call-Routing Architecture 260
Task 2: Create Devices in CUCM 261
Step 2-1: (Optional) Create a Dummy H.323 Gateway 261
Step 2-2: Prep the Router to Become an MGCP Gateway 262
Step 2-3: Create the MGCP Gateway in CUCM 263
Step 2-4: Activating the MGCP Gateway on the Router 266
Task 3: Create Route Group in CUCM 269
Task 4: Create Route Lists in CUCM 270
Task 5: Create Route Patterns in CUCM to Build a Dial Plan to Match the North American Numbering Plan (NANP) 272
Step 5-1: Creating a Seven-Digit Local Calls Route Pattern 272
Step 5-2: Creating a Ten-Digit Local Calls Route Pattern 275
Step 5-3: Creating an Emergency Services Calls Route Pattern 276
Step 5-4: Creating a Long-Distance Calls Route Pattern 278
Step 5-5: Creating a Premium Services Blocked Calls Route Pattern 279
Step 5-6: Creating a Toll-Free Calls Route Pattern 280
Step 5-7: Creating a Service Codes Calls Route Pattern 281
Step 5-8: Creating an International Calls Route Pattern 282
Step 5-9: Examine the NANP Route Patterns 283

Lab 10-2: Class of Control—Partitions and Calling Search Spaces (CSS) 285
Task 1: Examine Partitions and Calling Search Spaces (CSS) 286
Step 1-1: Examine Partitions 286
Step 1-2: Examine Calling Search Spaces 286
Step 1-3: Examine Partitions and CSS Together 287
Step 1-4: Calculate Partitions and CSS Interactions 290
Step 1-5: Partitions and CSS for SOI 291
Task 2: Create and Assign Partitions 294
Step 2-1: Create Partitions 294
Step 2-2: Assign a Partition 294
Task 3: Create Calling Search Spaces 297
Step 3-1: Create the Mad_Restricted_CSS Calling Search Space 297
Step 3-2: Create the Mad_Guest_CSS Calling Search Space 297
Step 3-3: Create the Mad_Employee_CSS Calling Search Space 298
Step 3-4: Create the Mad_Unrestricted_CSS Calling Search Space 298

https://t.me/learningnets
From the Library of Aliwarman Tarihoran

Task 4: Assign Calling Search Spaces and Partitions 298
Step 4-1: Assign a CSS and Partition to the Directory Numbers 299
Step 4-2: Assign a Partition to a Route Pattern 300
Step 4-3: Assign Partitions to All the Route Patterns 301
Step 4-4: Assign a CSS to a Gateway 302
Step 4-5: Assign a CSS to a Phone 303
Step 4-6: Experiment with Line/Phone CSS Interaction 304
Step 4-7: Challenge: Complete the Testing 305
Step 4-8: Cleanup 305

Lab 10-3: Centralized Cisco Unified Communications Manager (CUCM)–to–Branch Office Call Routing 306

Task 1: Examine Call Admission Control (CAC) 307
Step 1-1: Examine the Settings for Regions and Locations 307
Step 1-2: Examine Call Statistics on a Phone 307
Step 1-3: Change a Phone to the New York Device Pool 308
Step 1-4: Determine Bandwidth Needed for G.729 Calls 309
Step 1-5: Determine Bandwidth Needed for G.711 Calls 310
Step 1-6: Determine Bandwidth Needed for iLBC Calls 311
Step 1-7: Cleanup 312

Task 2: Implement Alternate Automatic Routing (AAR) 312
Step 2-1: Set Up Branch Office Gateway 312
Step 2-2: Enable AAR Service Parameter 315
Step 2-3: Create AAR Groups 315
Step 2-4: Update Device Pools 316
Step 2-5: Configure a Branch Office Phone 317
Step 2-6: Testing 319
Step 2-7: Verify That the AAR CSS Is Working 320
Step 2-8: Branch Office Dial Plan Challenge 321

Task 3: Implement Survivable Remote Site Telephony (SRST) and Call Forward UnRegistered (CFUR) 321
Step 3-1: Configure SRST Reference in CUCM 322
Step 3-2: Apply SRST Reference to Device Pool 323
Step 3-3: Configure Router for SRST 324
Step 3-4: Configure Dial Peers for SRST 325
Step 3-5: Configure Maximum Redirects 326
Step 3-6: Configure CFUR 326
Step 3-7: Test SRST Failover and CFUR Behavior 327

Tips to Complete Branch Office Dial Plan 328

Lab 10-4: Hunt Groups 330

Task 1: Configure Hunt Groups 331
Step 1-1: Configure Sales Agents Line Group 331
Step 1-2: Configure Managers Line Group 332
Step 1-3: Configure Hunt List 332
Step 1-4: Configure Hunt Pilot 334
Step 1-5: Testing 334

Chapter 11 CUCM Telephony Features 337

Lab 11-1: Extension Mobility 337

Task 1: Activate Extension Mobility Services and Configure Service Parameters 338
Step 1-1: Activate Extension Mobility Service 338
Step 1-2: Configure Extension Mobility Service Parameters 338

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Configure Extension Mobility IP Phone Service 340
Step 2-1: Configure the Extension Mobility IP Phone Service 340
Task 3: Create and Associate Device Profiles 341
Step 3-1: Create Default Device Profile 341
Step 3-2: Create Device Profile 341
Step 3-3: Configure Lines for the Device Profile 342
Step 3-4: Associate a Device Profile with a User 343
Step 3-5: Enable Extension Mobility on a Phone 344
Task 3: Validate Extension Mobility 344

Lab 11-2: Call Coverage Features 346
Task 1: Configure Call Park and Directed Call Park 347
Step 1-1: Configure Call Park 347
Step 1-2: Test Call Park 348
Step 1-3: Configure Directed Call Park 348
Step 1-4: Test Directed Call Park 349
Task 2: Configure Call Pickup 349
Step 2-1: Create a Call Pickup Group 349
Step 2-2: Assign a Call Pickup Group to a Phone 349
Step 2-3: Test Call Pickup 350
Task 3: Configure Shared Lines 351
Step 3-1: Create a New Directory Number 351
Step 3-2: Assign Directory Number to Second Phone 351
Step 3-3: Test Shared Lines 352
Task 4: Configure Barge and Privacy 352
Step 4-1: Configure System Parameters for Barge 352
Step 4-2: Disable Barge on a Phone 353
Step 4-3: Testing Barge 354
Task 5: Configure Intercom 354
Step 5-1: Create Intercom Partitions 354
Step 5-2: Create Intercom Numbers 355
Step 5-3: Configure Intercom on First Phone 356
Step 5-4: Configure Intercom on Second Phone 358
Step 5-5: Testing Intercom 359
Step 5-6: Intercom Challenge 359
Task 6: Configure Native Presence 359
Step 6-1: Configure Phone Button Template (BLF Speed Dials) 359
Step 6-2: Enable BLF Speed Dials 360

Chapter 12 CUCM Mobility Features 363

Lab 12-1: Mobile Connect 363
Task 1: Enable Users and Phones for Mobile Connect 364
Step 1-1: Configure User to Use Mobile Connect 364
Step 1-2: Configure Softkey Template 365
Step 1-3: Configure Phone for Mobile Connect 367
Task 2: Create Remote Destinations and Remote Destination Profiles 368
Step 2-1: Create Remote Destination Profile 368
Step 2-2: Create Remote Destinations. 369
Task 3: Configure and Apply Access Lists 371
Step 3-1: Create Allowed Number Access List 372
Step 3-2: Create Blocked Number Access List 373
Step 3-3: Apply Access Lists 374

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 4: Testing Mobile Connect 374
Step 4-1: Mobile Connect—Forwarding to Remote Destination 374
Step 4-2: Mobile Connect—Blocking 375

Lab 12-2: Mobile Voice Access 376

Task 1: Enable MVA 377
Step 1-1: Activate the MVA Service 377
Step 1-2: Configure Service Parameters for MVA 377
Task 2: Configure Users for MVA 377
Step 2-1: Enable MVA for the User 377
Task 3: Configure MVA 378
Step 3-1: Configure MVA Media Resource 378
Step 3-2: Examine IOS Gateway Configuration 379

Part IV: Voicemail and Presence Solutions

Chapter 13 Cisco Unity Connection 381

Lab 13-1: Integrating CUC with CUCM 381

Task 1: Create SCCP Ports for CUCM Connections to CUC 382
Step 1-1: Add Voice Mail Ports Using the Wizard 382
Step 1-2: Add Ports Using the Wizard 383
Step 1-3: Configure Device Information Using the Wizard 384
Step 1-4: Configure Directory Numbers Using the Wizard 384
Step 1-5: Configure Line Group Using the Wizard 385
Step 1-6: Wizard Confirmation 385
Step 1-7: Wizard Summary 385
Step 1-8: Create Hunt List 386
Step 1-9: Create Hunt Pilot 387
Step 1-10: Create Message Waiting Indicator On 388
Step 1-11: Create Message Waiting Indicator Off 389
Step 1-12: Create Voice Mail Pilot 389
Step 1-13: Create Voice Mail Profile 390
Task 2: Configure CUC for SCCP Connection to CUCM 390
Step 2-1: Configure Phone System 390
Step 2-2: Configure Port Group 391
Step 2-3: Configure SCCP Port 392
Step 2-4: Test the CUCM-to-CUC Connection 393
Task 3: Create SIP Trunk for CUCM Connections to CUC 393
Step 3-1: Configure SIP Trunk Security Profile 394
Step 3-2: Configure SIP Trunk 395
Step 3-3: Configure Route Pattern 396
Step 3-4: Create SIP Voice Mail Pilot 397
Step 3-5: Create Voice Mail Profile 398
Step 3-6: Assign SIP Voice Mail Profile to a Phone 399
Task 4: Configure CUC for SIP Connection to CUCM 399
Step 4-1: Configure Phone System 399
Step 4-2: Configure SIP Port Group 400
Step 4-3: Configure SIP Port 400
Step 4-4: Test the CUCM-to-CUC Connection 401
Task 5: Using the Real-Time Monitoring Tool (RTMT) to Examine Voice Mail Call Flow 401
Step 5-1: Download and Install RTMT 401
Step 5-2: Examine Voice Mail Ports Using RTMT 402

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 13-2: Configuring Cisco Unity Connection (CUC) Templates and Manually Adding a User 405

Task 1: CUC Authentication Rules and Class of Service 406

Step 1-1: Examine Authentication Rules 406
Step 1-2: Configure Authentication Rules 407
Step 1-3: Examine Class of Service 408

Task 2: CUC User Template 409

Step 2-1: Examine the User Template 409
Step 2-2: Create a User Template 410

Task 3: Configure CUC Users 412

Step 3-1: Configure User with the Custom Template 412
Step 3-2: Test User Voice Mailbox 414

Task 4: Update CUCM Directory Numbers to Use Voice Mail 414

Step 4-1: Configure Voice Mail on a Directory Number 414
Step 4-2: Configure Voice Mail on a Directory Number 415
Step 4-3: Test Call Forwarding to Voice Mail 416

Lab 13-3: Adding Users to Cisco Unity Connection (CUC) from Cisco Unified Communications Manager (CUCM) and Using the Bulk Administration Tool (BAT) 418

Task 1: Configure CUC to Import Users from CUCM 418

Step 1-1: Activate AXL Web Service on CUCM 419
Step 1-2: Create AXL User Account 419
Step 1-3: Configure AXL Services in CUC 419
Step 1-4: Configure User Accounts in CUCM 420
Step 1-5: Import CUCM Users into CUC 421
Step 1-6: Examine Imported User 421

Task 2: Use BAT to Import Users into CUC 422

Step 2-1: Export Users 422

Chapter 14 Cisco Unified Presence 425

Lab 14-1: Configuring Cisco Unified Presence Server 425

Task 1: Configure CUCM for CUPS Functionality 426

Step 1-1: Activate Services 426
Step 1-2: Add CUPS as an Application Server 426
Step 1-3: Add an AXL Group and User 427
Step 1-4: Add a CTI-Enabled Group 427
Step 1-5: Add a CTI User 428
Step 1-6: Add an IP Phone Messenger User 428
Step 1-7: Add the IP Phone Messenger Service 429
Step 1-8: Subscribe Phones to IP Phone Messenger 430
Step 1-9: Add a SIP Trunk Security Profile 430
Step 1-10: Add SIP Publish Trunk 431
Step 1-11: Enable Users for Presence Functionality 432

Task 2: Configure CUPS Connectivity to CUCM 433

Step 2-1: Access the CUPS Web Administration Page 434
Step 2-2: Upload a License File (Optional) 435
Step 2-3: Activate Services 436
Step 2-4: Add a Presence Gateway 437
Step 2-5: Add CUCM as a Presence Gateway 437
Step 2-6: Activating Desk Phone Control/Microsoft RCC 438
Step 2-7: Enable Users for Desk Phone Control/Microsoft RCC 439
Step 2-8: Activate the IP Phone Messenger 439

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 3: Configure CUPC/Jabber Profile 440
Step 3-1: Configure CUPC Settings 441
Step 3-2: Configure CUPC Voicemail—Voicemail Server 441
Step 3-3: Configure CUPC Voicemail—Mailstore 442
Step 3-4: Configure CUPC Voicemail—Voicemail Profile 443
Step 3-5: Configure CUPC Conferencing (Optional) 444
Step 3-6: Configure CUPC CTI Access 446
Step 3-7a : Configure CUPC CTI Gateway Profile for CUPS Version 8.6.3 or Greater 446
Step 3-7b: Configure CUPC CTI Gateway Profile CUPS Version Prior to 8.6.3 447
Step 3-8: Configure CUPC LDAP Access 448
Step 3-9: Configuring CUPC LDAP Access 449
Step 3-10: Configure a CUPC Audio Profile 450
Step 3-11: Configure a CUPC CCMCIP Profile 450
Step 3-12: Enable User Calendar Integration (Optional) 451
Task 4: Create CSF Devices in CUCM 452
Step 4-1: User/Desk Phone Association 452
Step 4-2: Create CSF Device in CUCM 454

Part V: Management and Troubleshooting

Chapter 15 Troubleshooting Cisco Unified Communications Manager Express (CUCME) 457

Lab 15-1: Troubleshooting Process 457
Task 1: Complete the Troubleshooting Methodology Diagram 458
Task 2: Phone Boot Process 458

Lab 15-2: Troubleshooting CUCME Configuration 459
Task 1: Desired Configuration 459
Task 2: Router Configuration 460
Task 3: Switch Configuration 461

Chapter 16 Troubleshooting CUCM 465

Lab 16-1: Troubleshooting Process 465
Task 1: Complete the Troubleshooting Methodology Diagram 465
Task 2-1: Understand the Phone Boot Process 466
Task 2-2: Playing “What If?” 466
Task 3: Dialed Number Analyzer 469
Step 3-1: Activate Services 469
Step 3-2: Dialed Number Analyzer 469
Task 4: CUCM Reports 473
Step 4-1: Route Plan Report 473
Step 4-2: Cisco Unified Reporting 475
Step 4-3: Call Detail Record Analysis and Reporting 475
Step 4-4: Real Time Monitoring Tool (RTMT) 476
Step 4-5: Disaster Recovery System 479

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Chapter 17 Monitoring Cisco Unity Connection 481

Lab 17-1: Cisco Unity Connection Reports 481

Task 1: Prepare the System 482

Step 1-1: Leave Unheard Messages 482
Step 1-2: Examine Authentication Rule Settings 482
Step 1-3: Lock Out an Account 482
Step 1-4: Adjust Report Configuration 482

Task 2: Cisco Unity Connection Serviceability Page 483

Step 2-1: Access the Cisco Unity Connection Serviceability Page 483
Step 2-2: Examine the Users Report 484
Step 2-3: Examine the User Lockout Report 485
Step 2-4: Examine the Phone Interface Failed Logon Report 485
Step 2-5: Examine the User Message Activity Report 486
Step 2-6: Examine Other Reports 486

Task 3: Real-Time Monitoring Tool and Serviceability Reports Archive 487

Step 3-1: Activate the Cisco Serviceability Reporter Service 487
Step 3-2: Examine RTMT Reports 487

Part VI: Appendixes

Appendix A IP Addressing and Phone Extensions for Cisco Unified Communications Manager Express (CUCME) Labs 489

Appendix B IP Addressing and Phone Extensions for Cisco Unified Communications Manager (CUCM) Labs (Chapters 8–14 and 16–17) 495

Appendix C Building Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUC), and Cisco Unified Presence (CUPS) Servers in VMware Workstation 501

Lab C-1: Build Cisco Unified Communications Manager (CUCM) Image 501

Task 1: Configure and Cable Devices 502

Task 2: Build the Virtual Machine 502

Step 2-1: New Virtual Machine 502
Step 2-2: Choose Install Media 502
Step 2-3a: New Virtual Machine Wizard 503
Step 2-3b: Personalize Linux Install Information 504
Step 2-4: Choose Machine Name and File Location 504
Step 2-5: Specify Disk Capacity 504
Step 2-6: Customize Hardware 505
Step 2-7: Create Virtual Machine 506

Task 3: CUCM Installer 507

Step 3-1: Optional Media Check 507
Step 3-2: Product Selection 507
Step 3-3: Install Verification 508
Step 3-4: Platform Install Wizard 508
Step 3-5: Apply Patch 508
Step 3-6: Basic Install 508
Step 3-7: Time Zone Selection 510
Step 3-8: NIC Configuration 510
Step 3-9: MTU Configuration 510
Step 3-10: DHCP Configuration 511

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-11: Assign IP Address 511
Step 3-12: DNS Client Configuration 512
Step 3-13: Platform Administrator Login 512
Step 3-14: Certificate Information 513
Step 3-15: First Node Configuration 513
Step 3-16: NTP Client Configuration 514
Step 3-17: System Security Password 515
Step 3-18: SMTP Host Configuration 515
Step 3-19: Application User Configuration 516
Step 3-20: Platform Configuration Confirmation 517
Step 3-21: Waiting for the Install to Complete 517

Task 4: VMware Tools Upgrade for Original Install Media 518

Step 4-1: Shutting Down the CUCM Server 518
Step 4-2: Removing Autoinstall ISO 518
Step 4-3: Upgrading VM Tools 518

Task 5: VMware Tools Upgrade for Upgrade Media 520

Step 5-1: Upgrading VM Tools 520
Step 5-2: Shutting Down the CUCM Server 520

Task 6: Entering Descriptions in the System (Optional) 520

Task 7: Tips for Cisco Unified Communications Servers and VMware Workstation 521

Lab C-2: Build Cisco Unity Connection (CUC) Image 522

Task 1: Configure and Cable Devices 522

Task 2: Build the Virtual Machine 522

Step 2-4: Choose Machine Name and File Location 523
Step 2-5: Specify Disk Capacity 523
Step 2-6: Customize Hardware 524
Step 2-7: Create Virtual Machine 524

Task 3: CUC Installer 525

Step 3-2: Product Selection 525
Step 3-11: Assign IP Address 525
Step 3-15: First Node Configuration 526
Step 3-17: System Security Password 526

Task 4: VMware Tools Upgrade for Original Install Media 526

Step 4-2: Removing Autoinstall ISO 526

Lab C-3: Build Cisco Unified Presence Server (CUPS) Image 527

Task 1: Configure and Cable Devices 527

Task 2: Build the Virtual Machine 527

Step 2-2 Choose Install Media 528
Step 2-4: Choose Machine Name and File Location 528
Step 2-5: Specify Disk Capacity 528
Step 2-6: Customize Hardware 528

Task 3: CUPS Installer 528

Step 3-11: Assign IP Address 528
Step 3-15: First Node Configuration 528
Step 3-17: System Security Password 529

Task 7: CUPS Postinstallation Deployment Wizard 529

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Appendix D Configuring the Cisco Unified Communications Manager Express Router 531

Lab D-1: Configuring the CUCME Router 531

Task 1: Obtain the Desired Version of the IOS and CUCME Support Files 531

Step 1-1: Examine Your Router Hardware 532
Step 1-2: Understand CUCME and IOS Version 532
Step 1-3: Understand IOS Feature Sets 533
Step 1-4: Obtain IOS Files 534
Step 1-5: Determine Phone Firmware Files 535
Step 1-6: Download CUCME Support Files 536
Step 1-6: Uncompress the Support Files to the TFTP Directory 537

Task 2: Upload the Files to the Router 537

Step 2-1: Set Up the Router and PC 537
Step 2-2: Back Up All Existing Files to the TFTP Server 537
Step 2-3: Format the Flash 537
Step 2-4: Upload the New IOS 538
Step 2-5: Create Directory Structure 538
Step 2-6: Upload Phone Firmware Files 539
Step 2-8: Upload GUI Files 540
Step 2-9: Verify Files and Placement 541

Task 3: Commands to Upgrade or Downgrade Firmware on the Phones 543

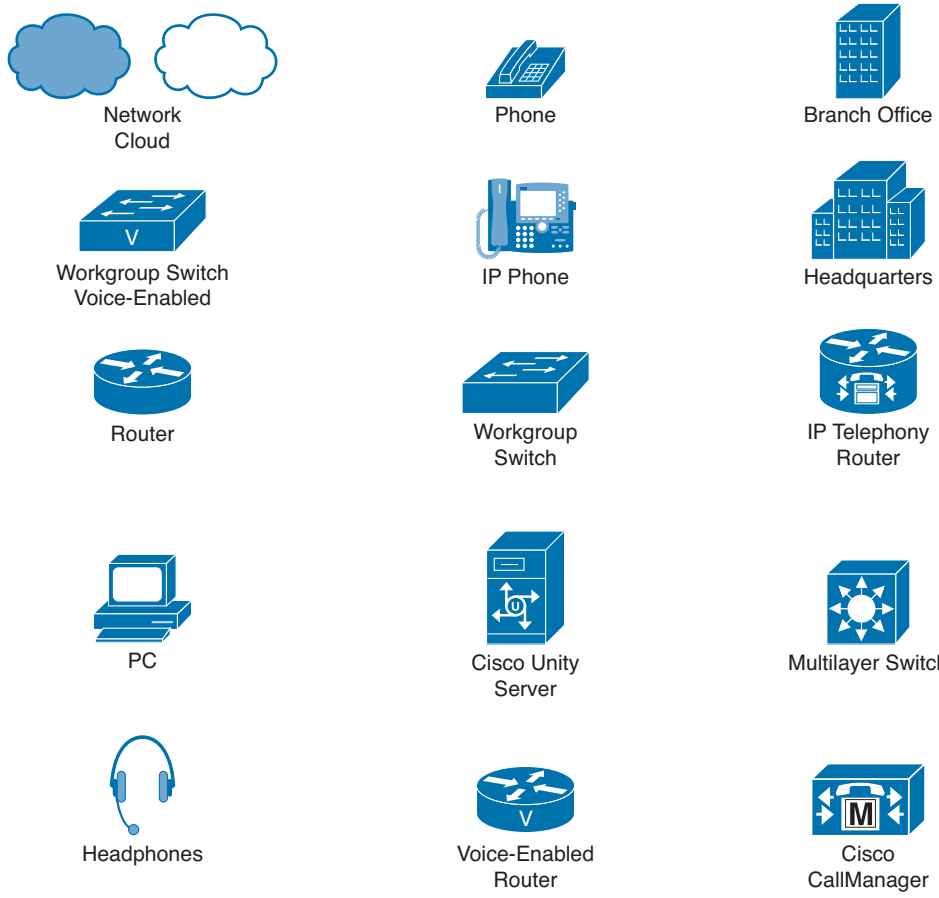
Step 3-1: Allow the Router to Send TFTP Files from Flash 543
Step 3-2: Inform the Phone of the Updated Firmware to Load 544
Step 3-3: Troubleshooting Firmware Loading on the Phones 545

Appendix E PSTN Simulator 547

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Icons Used in This Book



Command Syntax Conventions

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

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

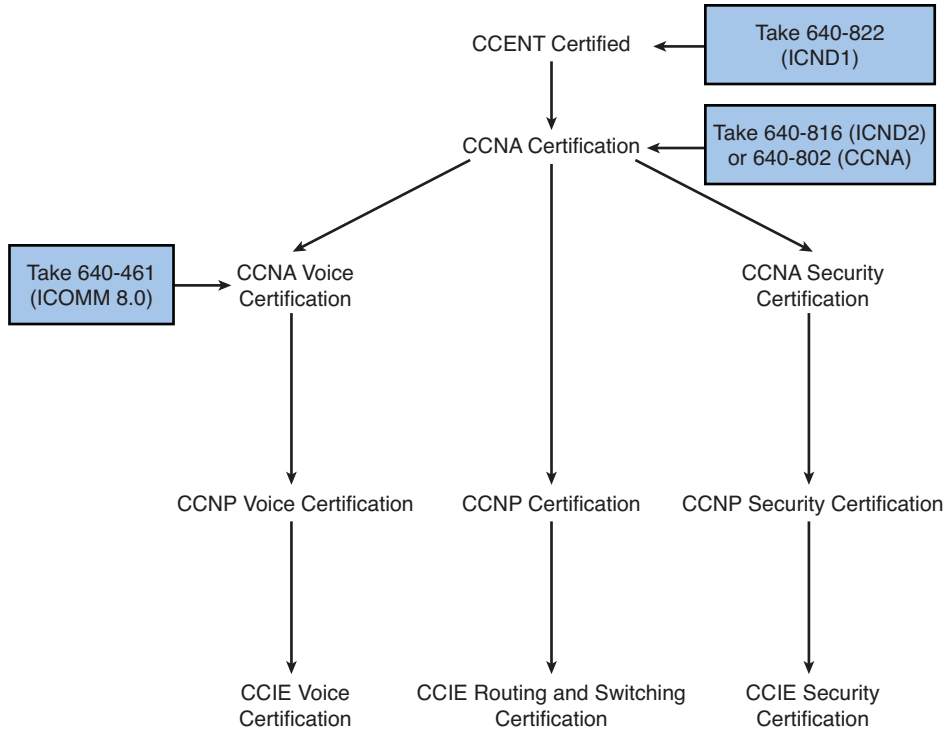
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Introduction

Cisco introduced the CCNA specialty exams in 2008 (CCNA Security, CCNA Voice, and CCNA Wireless) to provide a bridge between the CCNA certification and CCNP-level certifications, allowing networking professionals to get experience in a topic without having to complete the full CCNP-level track. The CCNA specialty exams also provide a common foundation for all the CCNP-level certification exams in a track. Cisco announced a revamped CCNA Voice certification in 2010 that focused more on the Cisco Unified Communications applications. Figure I-1 shows where the current 640-461 CCNA Voice exam fits in with the Cisco certification path.

Figure I-1 Cisco Certifications and CCNA Voice Certification Path



Goals and Methods

While many of the labs in this book can stand on their own, it is expected that this book will be used as a companion to the *CCNA Voice 640-461 Official Certification Guide* from Cisco Press (ISBN 978-1-58720-417-3). The Certification Guide has topics covered on the CCNA Voice certification exam that are not duplicated in this lab book.

Some of the labs (or items in a lab) in this book are marked as optional. In some cases, the lab is designed to match the material in the Certification Guide, but is not required for the CCNA Voice exam (such as Lab 6-1). In other cases, some labs can be completed and require optional hardware to test, but the key concepts can be learned without the hardware.

The goal of this lab book is to help students learn by doing. To that end, these labs contain far more than just step-by-step instructions to complete a task. The ideal scenario is that students understand *why* they are completing each step. When I first started writing labs, they were just simple lists of the commands to complete a task. As an instructor, I found that the minute the student encountered a problem or had something unexpected happen, up went his hand asking for help, as he had no idea

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

what to do. I started to realize that I was just training "typing monkeys," when my goal was to get students to *think* about why they were typing these commands. My labs grew longer as I added more descriptions and details.

Every time I had more than a few students get stuck or encounter a problem in one place, I would add information on how to avoid the problem or how to troubleshoot the issue in the lab. The result is the labs in this book. I found that most students love the detail I have put into the labs, and when they encounter a problem, the solution is often found nearby. However, I still have students in my classroom that just want to rush through a lab and skim it to find the commands that are printed in bold. Usually, by the fifth lab, they start to realize that I have commands that only apply in some circumstances, and the commands will not work in other cases. They learn to read the lab and carefully go through it. My goal is that they don't type commands without knowing what they are doing. They should "own" the process. After a student understands the process, he does not get stuck as easily and is instead able to figure out what to do to solve a problem.

In almost all cases, the labs build on one another for each of the two different Call Agents:

- For Cisco Unified Communications Manager Express (CUCME), the labs should go in order of Appendix D, "Configuring the Cisco Unified Communications Manager Express Router" (if necessary to load the router), Chapters 3–7, and then Chapter 15.
- For Cisco Unified Communications Manager (CUCM), the labs should go in order of Appendix C, "Building Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUC), and Cisco Unified Presence (CUPS) Servers in VMware Workstation" (if necessary to build the servers), Chapters 8–14, Chapter 16, and then Chapter 17.

When proceeding through the labs, it is advisable to save device configurations (or back up servers in the case of CUCM) at the end of each lab.

Hardware Section

For the previous version of the CCNA Voice certification exam, you just needed a router with an IOS that included Cisco Unified Communications Manager Express (CUCME), or CME, as it commonly called, and some phones to learn the material. The current CCNA Voice 640-461 exam is more focused on knowing the functioning and configuration of Cisco Unified Communications applications, such as the Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUC), and Cisco Unified Presence (CUPS). Having access to this software is important to understanding the topics for the certification exam. If you do not have access to the Cisco Unified Communications applications, study the figures included with the labs, as figures for the most common or difficult items to configure were included in the labs. Alternatively, check with your local Cisco Networking Academy, as it has the ability to offer classes using the Cisco Unified Communications applications at academic pricing.

Hardware and Software Used in the Labs

This is a list of equipment used to develop the labs. Use the following equipment to ensure the best compatibility. In a later section, alternatives will be explored.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Recommended Resources

These labs were created using the following equipment:

- Cisco 2811 router, running IOS c2800nm-adventerprisek9_ivs-mz.124-24.T2.bin, with a VWIC2-1MFT-T1/E1 card and a PVDM-16 (16-Channel Packet Voice/Fax DSP Module) installed. Some labs require two of these: one router for the HQ location and one for the branch office.
- Cisco WS-C3560-24PS switch with Power over Ethernet (PoE), running ISO c3560-ipservicesk9-mz.122-53.SE.bin.
- One Cisco router, with two or more VWIC2-1MFT-T1/E1 cards and enough digital signal processor (DSP) resources installed to act as a public switched telephone network (PSTN) simulator. (See Appendix E, "PSTN Simulator," for more details.)
- One or more Cisco 7900 Series IP Phones with three or more line buttons. (The Cisco 7962 is specifically demonstrated.)
- One or more Cisco IP Communicator (CIPC) soft phones running on one or more PCs or virtual machines.
- CUCM version 8.6.2 running in a virtual machine. (See Appendix C for more details.)
- CUC version 8.6.2 running in a virtual machine. (See Appendix C for more details.)
- CUPS version 8.6.3 running in a virtual machine. (See Appendix C for more details.)
- To run the Cisco Unified Communications applications on a PC or server, a machine with 8 or more gigabytes of RAM is required (16 gigs or more are recommended). The speed of the processor(s) on this machine is the biggest factor in how fast the virtual machines will perform. Virtualization software, such as VMware Workstation or ESXi Server, is needed.

Alternative Hardware Resources

While the labs were created using the previously listed equipment, in many cases, other equipment will be adequate.

All VoIP phone systems have a few common elements:

- Call Agents
- Phones
- Power for phones
- Network connectivity

Call Agents

The Call Agent is critical in the VoIP system. It controls all the functions of the phone calls. This lab book will use both Cisco Unified Communications Manager Express (CUCME), or CME as it commonly called, and CUCM for the Call Agent. CME is part of selected versions of the IOS on many, but not all, router models. Additionally, the routers will be needed for the gateways in some of the CUCM labs. As mentioned previously, the CUCM software is essential to understanding the topics in the CCNA Voice certification exam. CUCM version 8.6.2 was used to develop the labs, but any

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CUCM 8.x version should be nearly identical for the purposes of these labs. Earlier versions, such as CUCM 6.x and 7.x can also be used, but they might require adjustments for items that are different.

The following lists are not completely exhaustive but cover the most common router hardware that supports CME.

Recommended router models:

- 2800 ISR Series (2801, 2811, 2821, 2851)
- 3800 ISR Series (3825 and 3845)
- 2900 ISR2 Series (2901, 2911, 2921, 2951)
- 3900 ISR2 Series (3925, 3925E, 3945, 3945E)
- 1861 Router

Models that will work, but are not as desirable (all of these might require RAM and flash upgrades to get the CME version of IOS to run):

- 2600XM Series (2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM)
- 800 Series (891, 892, 887)
- 3700 Series (3725, 3745, 3770)
- 1700 Series (1760, 1751-V)
- 2691 Router
- UC500 Series (UC520, UC540, UC560) (CUCM will not support these as gateways, but they will work for the CME labs.)

To determine the IOS that supports CME, review the information in Appendix D, "Configuring the Cisco Unified Communications Manager Express Router."

Phones

The next items required are the voice endpoints, and there are many options to choose from. Following are the recommended models with comments about each:

- Cisco IP Communicator (also known as CIPC) is a soft phone that runs on Microsoft Windows XP, Vista, and 7, and it will work inside a virtual machine. It requires CME version 4.0 or later to work, so older routers with older versions of CME will not support it. An advantage of CIPC is that it does not require power like a desk phone, because the software runs on the PC or in a VM. A downside to CIPC is that it requires that a microphone and speakers be detected on the hardware, or the software will not launch. But it might be possible to trick the software with older audio drivers to believe that an audio source is present, even if one is not.
- 7900 IP Phone Series (any phone in this series will work, unless you are running an older version of CME). Older versions of the 7900 Series, such as the 7940 and 7960, can be purchased on the refurbished/secondary markets quite cheaply.
- 8900 IP Phone Series (any phone in this series will work, but it will require the newer versions of CME found in IOS 15 or later).
- 9900 IP Phone Series (any phone in this series will work, but it will require the newer versions of CME found in IOS 15 or later).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Power for Phones

(If you are using the CIPC, you can skip this section.) All desk phones require power to function. There are four ways to achieve this:

- The cheapest way to power phones is to use a "power brick" to provide power directly to the phones. (Note: The power supplies for Cisco access points will also deliver the –48V DC required to power the phones.) The model number for the Cisco power brick is CP-PWR-CUBE-3=. These are not commonly used in production environments, as the phone will not work if the power is out.
- Not much more expensive is a power injector, which puts Power over Ethernet (PoE) onto the wires between the switch and the phone. (Note: The PoE injectors for Cisco access points will also work to power the phones.) Power injectors are a common solution in a production environment where only one or two devices need power, as the injector can be plugged into the uninterruptible power supply (UPS) in the wiring closet and keeps the phones working when the power is out. Larger, rack-mount units that support dozens of phones are also sometimes used in production environments when upgrading to a PoE switch is not feasible. The model number is CP-PWR-INJ=.
- A switch that supports PoE (or for some older phones, Cisco-proprietary inline power). This solution is used the most often in production, as the switch should be powered by a UPS in the wiring closet and keeps the phones working when the power is out. In the classroom, students can share a switch for more than one pod by using VLANs and separate trunks to different routers. There are many models of switches that provide PoE, but some of the more common are as follows:
  - WS-C3560-24PS-S (24-port Layer 3 switch that also works for the CCNP material)
  - WS-C3560G-24PS-S (24-port Layer 3 switch with all gigabyte ports)
  - WS-C3560-8PC-S (8-port Layer 3 switch)
  - WS-C2960-24PC-L (24-port Layer 2 switch)
  - WS-C2960-24LT-L (24-port Layer 2 switch, but only eight ports with PoE)
  - WS-C3750-24PS-S (stackable 24-port Layer 3 switch)
  - WS-C3750-48PS-S (stackable 48-port Layer 3 switch)
- A router with a PoE switch module installed. (Note: Some models of routers, such as the 2800 and 2900 Series, *require* upgraded power supplies to support PoE switch modules. Make sure that your router has the upgraded power supply. Examples include the PWR-2801-AC-IP and PWR-2811-AC-IP for the 2801 and 2811 routers.) Also note that not all switch modules supply PoE. The modules that do are as follows:
  - HWIC-4ESW-POE
  - HWIC-4ESW with added ILPM-4 module
  - HWIC-D-9ESW-POE

Network Connectivity

If you are using a PoE switch or router with PoE switch modules, you are all set. If you used soft phones or desk phones with power bricks or injectors, a voice-enabled switch is required. A voice-enabled switch is one that allows voice VLANs to be configured. All the more recent switch models have this, including the 2950, 2960, 3550, 3650, and 3750 Series switches.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Additional Items

Several of the labs use an ISDN PRI connection to another router that is configured as a PSTN simulator (see Appendix E for the details). There are a few options for the PRI cards. Each of these cards will require digital signal processor (DSP) resources. For some routers, the DSPs can be added to the motherboard (2800, 3800, 2900, and 3900 Series), some can get the DSP from an Advanced Integration Module (AIM), and some network modules have slots to add DSPs. Various PRI cards that will work with the labs are as follows:

- VWIC-1MFT-T1 (Single-port voice card that only works as a T1. This will *not* work with the Cisco Configuration Professional software for CME.)
- VWIC-2MFT-T1 (Double-port voice card that only works as a T1. This will *not* work with the Cisco Configuration Professional software for CME.)
- VWIC2-1MFT-T1/E1 (Single-port voice card that will work for T1 or E1 configuration. This will work with the Cisco Configuration Professional software for CME.)
- VWIC2-2MFT-T1/E1 (Dual-port voice card that will work for T1 or E1 configuration. This will work with the Cisco Configuration Professional software for CME.)
- VWIC3-1MFT-T1/E1 (Single-port voice card that will work for T1 or E1 configuration. Note: This only works in newer 2900 or 3900 Series routers.)
- VWIC3-2MFT-T1/E1 (Dual-port voice card that will work for T1 or E1 configuration. Note: This only works in newer 2900 or 3900 Series routers.)
- NM-HDV2 (High-density network module that allows additional Voice/WAN Interface Card (VWIC) and DSP resources to be added to select routers.)
- NM-HDV2-1T1/E1 (High-density network module with a single T1/E1 port that allows additional VWIC and DSP resources to be added to select routers.)
- NM-HDV2-2T1/E1 (High-density network module with dual T1/E1 ports that allows additional VWIC and DSP resources to be added to select routers.)

While Lab 6-1 shows how to configure VIC2-2FXO and VIC2-2FXS analog voice cards, these are *not* necessary for the CCNA Voice certification exam. The only reason to have these interfaces (or similar analog connections) would be to use them to study for the first CCNP Voice certification exam, the 642-437 CVOICE v8.0, which includes analog interfaces.

Special Issues with CUCM and IP Phones

CUCM version 8.0 or higher includes Security by Design, which places a certificate on the phone that authenticates the phone to the TFTP server from which it gets the configuration file. As a result, the phone will not get a configuration from any other TFTP server that does not match the certificate. In a classroom with multiple users, or when going back to use CUCME, the certificate can cause problems with registering to other systems. There are two solutions to this problem:

- **Clearing the networking settings:** This might be enough to get the phone to register. On most phone models, press the **Settings** button and then navigate down to the Network Settings section (but do not enter the Network Settings). Press *** * #** (to unlock the settings) and then press the **Erase** key (you might need to press the **More** softkey to see the **Erase** key). The phone will then reset.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- **Removing the Initial Trust List (ITL) security file from the phone:** It might be necessary to clear the ITL file to upgrade or downgrade the firmware on a phone when switching between CUCM and CME. The easiest solution in a lab is to remove the file manually using the **Settings** button on the phone, as follows:
  - For the 7900 Series phones, press **Settings** and then navigate to **Security > Trust List > ITL File > * * #** (to unlock the settings) **> Erase** (you might need to press the **More** softkey to see the **Erase** key). The phone will then reset.
  - For the 8900/9900 Series phones, press **Settings** and then navigate to **Administrator Settings > Reset Settings > Security Settings**. The phone will then reset.

Search the Cisco support forums at http://supportforums.cisco.com for "Migrating IP Phones Between Clusters with CUCM 8 and ITL Files" for more details on ITL files and Security by Design.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CHAPTER 1

Traditional and Unified Voice

Knowledge of both traditional voice and unified voice terminology is essential before implementing a voice solution.

Lab 1-1: Telephony Terminology

Equipment Required

No equipment is required for this lab.

Learning Objectives

Upon completion of this lab, you will better understand the traditional and unified voice terminology.

Task 1: Matching Items

In Table 1-1, match the item on the left with the definition on the right.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Table 1-1 Telephony Terms

Term	Definition
___ TDM	1. Facility where phone company equipment is located
___ Local loop	2. Used between phone companies to route calls and provide informational signaling
___ Key system	3. Common signaling for home phones in which the circuit to the phone company is open (on-hook) or closed (off-hook)
___ Glare	4. High-complexity audio codec with a bandwidth of 8 kbps used in Cisco IP Phones
___ PVDM	5. Signaling in which signals are sent in the same channel as the voice traffic
___ G.711	6. Connection to the subscriber from the central office switch
___ Central office	7. A common abbreviation for the traditional telephone system
___ CAS	8. Protocol to provide statistical and control information for VoIP calls
___ RTP	9. When outgoing and incoming calls collide on the same phone line
___ Loop start	10. One of the steps in the process of converting an analog signal to a digital number
___ PSTN	11. Hardware modules added to routers to provide resources for analog voice
___ G.729	12. Signaling used more often in corporate business environments to avoid glare
___ DSP	13. Method to create multiple digital channels by assigning time slots on the medium
___ Trunk	14. Signaling that uses a separate, dedicated channel for all signals
___ CO switch	15. Telecommunication equipment owned by a large corporation that allows an internal phone system that can utilize extensions
___ E.164	16. Small-scale telecommunication equipment, commonly used by small businesses
___ SS7	17. Measurement used to compare codecs
___ Ground start	18. Transport protocol for IP-based digital voice
___ RTCP	19. Hardware chips dedicated to converting between analog and digital signals
___ MOS	20. Phone company equipment that provides services to customers, such as call signaling, digit collection, call routing, setup, and teardown
___ Q.931	21. Medium-complexity audio codec with a bandwidth of 64 kbps used in Cisco IP Phones
___ PBX	22. Connections between central office switches and customers that can carry more than one call at a time
___ Quantization	23. Signaling protocol used on ISDN circuits
___ CCS	24. International numbering plan established by the ITU

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CHAPTER 2

Understanding Cisco Unified Communications Solutions

This chapter builds your understanding of key components and features of Cisco Unified Communications solutions.

Lab 2-1: Key Features of Cisco Unified Communications Solutions

Equipment Required

No equipment is required for this lab.

Learning Objectives

Upon completion of this lab, you will better understand Cisco Unified Communications solutions.

Task 1: Questions

Complete all the questions to test your knowledge of Cisco Unified Communications solutions.

Question 2.1

T F The audio streams between two IP Phones must go through the Call Agent (CUCME or CUCM Cluster).

Question 2.2

T F After registering, an IP Phone can make and receive calls, even if the Call Agent (CUCME or CUCM Cluster) is down.

Question 2.3

List seven key features of Cisco Unified Communications Manager (CUCM).

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Question 2.4

List seven key features of Cisco Unity Connection.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

Question 2.5

Explain why, in a larger environment, IP Phones do not typically receive call processing from the CUCM Publisher.

_____

_____

_____

_____

_____

Question 2.6

In Table 2-1, complete the missing information.

Table 2-1 Cisco Messaging Systems

System	Platform	Redundancy?
Cisco Unity		
CUCM Business Edition	Appliance	
Cisco Unity Express		Not supported
Cisco Unity Connection		

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CHAPTER 3

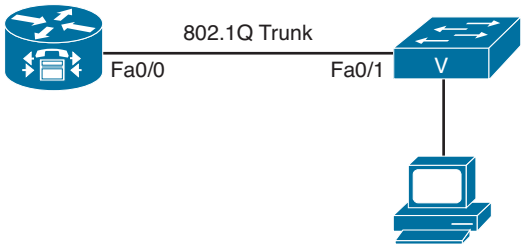
Establishing Network Connectivity and Understanding IP Phone Registration

In both Cisco Unified Communications Manager Express (CUCME) and Cisco Unified Communications Manager (CUCM) environments, phones need to connect to the network to receive services such as IP addresses from DHCP, VLAN assignments for voice traffic, IP information on where to register, and Network Time Protocol (NTP) packets. This chapter focuses on establishing those services.

In this chapter, you will set up a voice network for the fictitious company Shiny Objects Incorporated (SOI). Before phones are connected, you must establish network connectivity and configure needed services.

Lab 3-1: Network Connectivity

Figure 3-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- PC for testing
- Cisco IP Phone (optional, but useful if switch supports Power over Ethernet [PoE])

Learning Objectives

Upon completion of this lab, you will be able to

- Perform basic router and switch configuration
- Configure VLANs to support data, voice, and network management traffic
- Configure VLAN trunking between a router and a switch using subinterfaces
- Configure router-based DHCP pools for voice and data devices

Scenario

SOI would like to establish its new data network with the expectation of using VoIP in the near future.

These instructions refer to the Pod Addressing Table in Appendix A to determine the IP addresses and VLAN numbers used for your pod. Wherever an *x* is shown, substitute the pod number.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Clear and Cable Devices

Because the CCNA is a prerequisite for the CCNA-Voice certification exam, this book assumes that you are familiar with clearing prior configurations.

Step 1-1: Clear Prior Configurations

Clear any prior configuration on the router and switch, and delete the vlan.dat file before reloading both devices.

Step 1-2: Cable Router and Switch

Cable router interface Fast Ethernet 0/0 to switch port Fast Ethernet 0/1, as shown in Figure 3-1. The PC will be connected later.

Task 2: Configure Basic Setup

This task establishes the basic configuration commands on both the router and switch.

Step 2-1: Configure Basic Setup on the Router

Note: Not all devices support the **line vty 0 15** command. If your equipment does not support this command, change it to **line vty 0 4**.

```
Router(config)# hostname RtrPodx
```

For example, Pod 8 would use **hostname RtrPod8**.

```
RtrPodx(config)# no ip domain-lookup
RtrPodx(config)# enable secret class
RtrPodx(config)# line con 0
RtrPodx(config-line)# logging synchronous
RtrPodx(config-line)# exec-timeout 120 0
RtrPodx(config-line)# password cisco
RtrPodx(config-line)# login
RtrPodx(config-line)# line vty 0 15
RtrPodx(config-line)# password cisco
RtrPodx(config-line)# login
RtrPodx(config-line)# exit
```

Note: The **exec-timeout** command shown here is useful in a lab setting. It allows 120 minutes of inactivity before logging you out. (In a production environment, this could be a security risk.)

Step 2-2: Configure Basic Setup on the Switch

```
Switch(config)# hostname SwPodx
```

For example, Pod 3 would use **hostname SwPod3**

```
SwPodx(config)# no ip domain-lookup
SwPodx(config)# enable secret class
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
SwPodx(config)# line con 0
SwPodx(config-line)# logging synchronous
SwPodx(config-line)# exec-timeout 120 0
SwPodx(config-line)# password cisco
SwPodx(config-line)# login
SwPodx(config-line)# line vty 0 15
SwPodx(config-line)# password cisco
SwPodx(config-line)# login
SwPodx(config-line)# exit
```

Task 3: Configure the Switch

For the purposes of security and ease of implementing quality of service (QoS), use VLANs to keep voice traffic separate from other traffic.

Step 3-1: Create the VLANs

Create and name VLANs for data, voice, and network management.

```
SwPodx(config)# vlan x0
SwPodx(config-vlan)# name Data
SwPodx(config-vlan)# vlan x1
SwPodx(config-vlan)# name Management
SwPodx(config-vlan)# vlan x5
SwPodx(config-vlan)# name Voice
SwPodx(config-vlan)# exit
```

Step 3-2: Configure the Trunk Port

Configure the trunk port that connects the switch to the router. Layer 3 switches (such as the Cisco Catalyst 3560) require that the trunking protocol be specified with the **switchport trunk encapsulation** command before the interface can be set as a trunk. If you are using a Layer 2 switch (such as a Cisco Catalyst 2950 or 2960), the command is not needed and will be rejected.

Note: Cisco recommends in the "VLAN Security White Paper," to prevent a double-encapsulated 802.1Q/nested VLAN attack, "always pick an unused VLAN as the native VLAN of all the trunks; don't use this VLAN for any other purpose. Protocols like STP, DTP, and UDLD should be the only rightful users of the native VLAN and their traffic should be completely isolated from any data packets." For this reason, the management VLAN is not the native VLAN in this lab. To improve security, it would be better to create another VLAN as the native VLAN that will remain unused, but to simplify this lab, it is not covered.

```
SwPodx(config)# interface fastethernet 0/1
SwPodx(config-if)# switchport trunk encapsulation dot1q
SwPodx(config-if)# switchport mode trunk
SwPodx(config-if)# exit
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-3: Configure the Access Ports

Almost all Cisco IP Phones are designed with a three-port switch built inside (one physical port connected to the production switch, one physical port for a PC to connect to the phone, and one internal port for the phone itself). This built-in switch saves money in wiring costs, as existing phone cabling might not meet networking standards. This enables an existing computer to be plugged into the phone, and the phone connects to the switch in the wiring closet.

Prior to the introduction of voice VLANs, a trunk connected an IP Phone to the switch to keep the voice and data traffic separate. Current best practice configures the ports connected to phones and PCs to use access mode but adds a secondary voice VLAN. The switch ports use the access VLAN to send data traffic as untagged frames. However, if the switch detects a Cisco IP Phone using Cisco Discovery Protocol (CDP), it will inform the phone of the VLAN used for voice traffic, which will be tagged using 802.1q. This creates a pseudotrunk that allows only the data and voice VLANs on the link.

Note: If CDP is disabled, or if you are using a non-Cisco IP phone, it requires setting the voice VLAN manually on the IP phone; otherwise, the voice traffic will end up on the data VLAN. For this reason, it is recommended that CDP remains enabled for ports that might have Cisco IP Phones connected.

Use the **interface range** command to assign settings. This is the fastest way to assign settings to more than one switch port at a time.

```
SwPodx(config)# interface range fastethernet 0/2 - 24
SwPodx(config-if-range)# switchport mode access
SwPodx(config-if-range)# switchport access vlan x0
SwPodx(config-if-range)# switchport voice vlan x5
SwPodx(config-if-range)# exit
```

Note: Setting the voice VLAN automatically enables **spanning-tree portfast**, so the switch port does not have to wait for Spanning Tree Protocol (STP) and goes active right away. You can verify this with the **show run** command, as shown in Example 3-1.

Example 3-1 Verify That spanning-tree portfast Is Created by the Voice VLAN Assignment

```
SwPod11# show run

<output omitted>

interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 110
 switchport mode access
 switchport voice vlan 115
 spanning-tree portfast

<output omitted>
```

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-4: Configure the Switch Management Interface

Set up an interface to manage the switch remotely.

```
SwPodx(config)# interface vlan x1
SwPodx(config-if)# ip address 10.x1.0.2 255.255.255.0
SwPodx(config-if)# exit
SwPodx(config)# ip default-gateway 10.x1.0.1
```

Task 4: Configure the Router Subinterfaces

Subinterfaces allow the VLANs to cross a trunk link to the router. Each subinterface will be the default gateway for a paired subnet. When using subinterfaces on a router, it is necessary to assign the correct VLAN to the subinterface before an IP address can be entered. Because there are three VLANs, you need three subinterfaces.

Note: As covered in the note in Step 3-2, there is no native VLAN defined on the router.

Step 4-1: Configure the Data VLAN Subinterface

```
RtrPodx(config-if)# interface fastethernet 0/0.x0
RtrPodx(config-subif)# encapsulation dot1Q x0
RtrPodx(config-subif)# description Data VLAN
RtrPodx(config-subif)# ip address 10.x0.0.1 255.255.255.0
```

Step 4-2: Configure the Management VLAN Subinterface

```
RtrPodx(config-subif)# interface fastethernet 0/0.x1
RtrPodx(config-subif)# encapsulation dot1Q x1
RtrPodx(config-subif)# description Management VLAN
RtrPodx(config-subif)# ip address 10.x1.0.1 255.255.255.0
```

Step 4-3: Configure the Voice VLAN Subinterface

```
RtrPodx(config-subif)# interface fastethernet 0/0.x5
RtrPodx(config-subif)# encapsulation dot1Q x5
RtrPodx(config-subif)# description Voice VLAN
RtrPodx(config-subif)# ip address 10.x5.0.1 255.255.255.0
RtrPodx(config-subif)# exit
```

Step 4-4: Activate the Router Interface

```
RtrPodx(config)# interface fastethernet 0/0
RtrPodx(config-if)# no shutdown
```

Note: You might be thinking "What about IPv6?" CUCME does not support IPv6 until version 8.0, which requires router IOS version 15.0 or higher.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 5: Verification

Check the configuration to determine whether it matches what you expect. This will help to avoid future problems.

Step 5-1: Verify Switch VLAN Configuration

Use the **show vlan brief** command to verify the VLAN configuration. This output is from Pod 11; your output will have different VLAN numbers. Notice that Fa0/1 is a trunk port and as such does not have a VLAN assigned to it, so it will not show in the output.

```
SwPod11# show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/1, Gi0/2
110  Data                              active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
111  Management                        active
115  Voice                             active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Step 5-2: Verify Switch Port Assignment

Use the **show interfaces switchport** command to verify the configuration of trunk and access ports. This output is from Pod 11; your output will have different VLAN numbers. Notice that Fa0/1 is a trunk port, while Fa0/2 is a static access port and has a voice VLAN assigned to it.

```
SwPod11# show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none

<output omitted>

Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 110 (Data)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 115 (Voice)

<output omitted>
```

Step 5-3: Verify Router Subinterface IP Assignment

Use the **show ip interface brief** command to verify that the trunk is assigned correctly. This output is from Pod 11; your output will have different subinterface and IP address numbers.

```
RtrPod11# show ip interface brief
Interface                  IP-Address      OK? Method  Status                Protocol
FastEthernet0/0            unassigned      YES unset   up                    up
FastEthernet0/0.110        10.110.0.1      YES manual  up                    up
FastEthernet0/0.111        10.111.0.1      YES manual  up                    up
FastEthernet0/0.115        10.115.0.1      YES manual  up                    up
```

Task 6: DHCP Services

Note: If you are using another source for DHCP, such as a Windows server or a CUCM server, you can skip this task. However, if the DHCP server is in a different subnet than the clients, it is necessary to use the **ip helper-address** command on each router subinterface to forward the DHCP requests to the server. Regardless of the DHCP server platform you use, make sure to configure the DHCP option 150 as discussed in this task.

While phones and PCs can be assigned IP addresses statically, DHCP can automatically assign IP address leases. Additionally, DHCP can provide additional information to clients, allowing them to locate necessary resources on the network at the same time they receive an IP address. Using the router as a DHCP server is a quick way to provide DHCP services to clients.

The DHCP option 150 tells Cisco IP Phones the IP address of the TFTP server with the initial configuration file. When using CUCME, the router is the TFTP server by default. This lab assigns the default gateway IP address as the option 150 address, as there is only one way to reach the call agent in this network.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Note: If there was redundancy in the network, it would be worthwhile to create a loopback interface and set the option 150 address to the loopback address, as that interface is always up.

Step 6-1: Configure DHCP Pools on the Router

Always enter the **ip dhcp exclude address** command before a DHCP pool is created. This avoids IP addresses that should be excluded from being assigned to devices. Enter the **network** statement as the last command in the pool. Otherwise, if devices are connected, they are assigned an IP address by DHCP right after the **network** statement is entered, even if the default gateway and option 150 are not configured. This can make troubleshooting difficult, as the PCs and phones will receive IP addresses, but the phones will not register and the PCs will not communicate outside their own subnet without the default router (gateway) address.

Create DHCP pools for both the data and voice networks. While it might seem that option 150 is irrelevant in data VLANs, with software on a PC able to emulate a phone (such as the Cisco IP Communicator software), it makes sense to include it for both DHCP pools.

```
RtrPodx(config)# ip dhcp excluded-address 10.x0.0.1 10.x0.0.10
RtrPodx(config)# ip dhcp pool Data
RtrPodx(dhcp-config)# default-router 10.x0.0.1
RtrPodx(dhcp-config)# option 150 ip 10.x0.0.1
RtrPodx(dhcp-config)# network 10.x0.0.0 255.255.255.0
RtrPodx(dhcp-config)# exit
RtrPodx(config)# ip dhcp excluded-address 10.x5.0.1 10.x5.0.10
RtrPodx(config)# ip dhcp pool Voice
RtrPodx(dhcp-config)# default-router 10.x5.0.1
RtrPodx(dhcp-config)# option 150 ip 10.x5.0.1
RtrPodx(dhcp-config)# network 10.x5.0.0 255.255.255.0
RtrPodx(dhcp-config)# exit
```

Task 7: Test and Cleanup

Step 7-1: Test Connectivity

Connect a PC to the switch. Verify that the PC is assigned an IP address from the 10.*x*0.0.0 /24 subnet. Verify that the PC can telnet to both the router and the switch management IP addresses. If not, troubleshoot the configuration.

Step 7-2: Save the Configurations

Save the configurations into a text file for both the router and switch. They will be needed for future labs.

Tip: When saving output from the console window, do not forget that some commands are not included and will not be present if pasted back to a device. Common examples include the **no shutdown** command for interfaces and VLAN creation and naming. To avoid problems, add missing commands to the text file or enter a reminder at the top of the text file. An exclamation point (!) at the start of a line makes it a comment for Cisco IOS, and this is an excellent way to add reminders to text output.

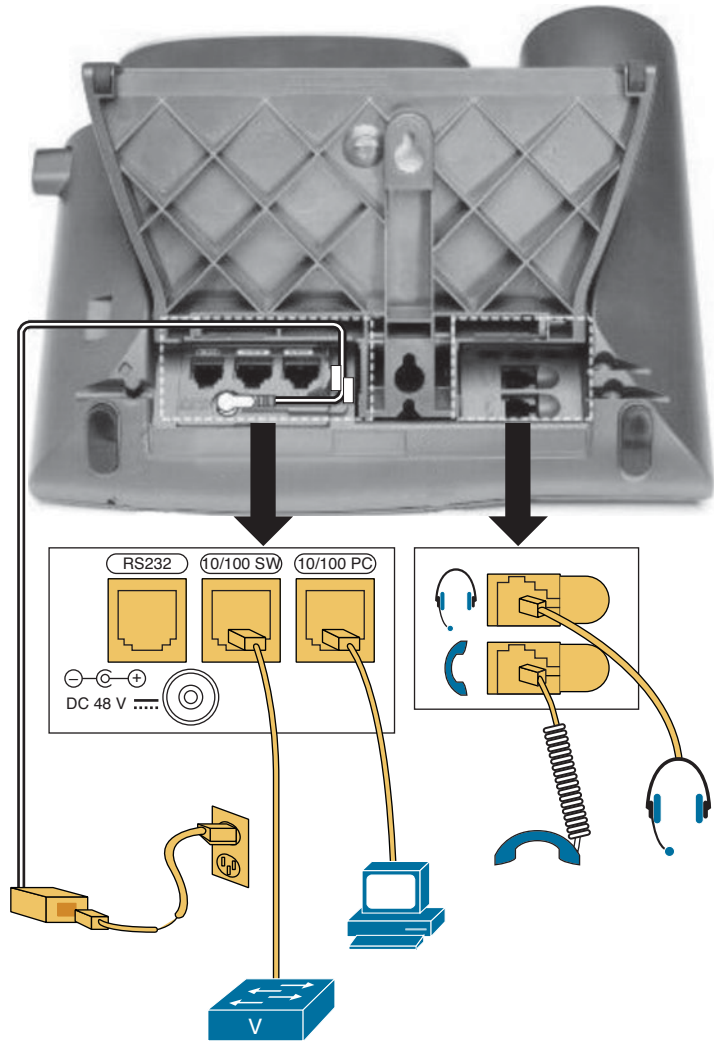
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 7-3: (Optional) Explore Power Over Ethernet on the Switch

If you have a switch that is PoE capable and a Cisco IP Phone or two, monitor the console port of the switch and connect the jack on the phone labeled SW to a switch port. See Figure 3-2 for an example.

Figure 3-2 Cisco IP Phone Connections



If you connect an older Cisco IP Phone (a 7960, for example) that supports only Cisco-proprietary inline power, you might see a message like this on the switch console line:

```
*Mar  1 05:23:55.900: %ILPOWER-7-DETECT: Interface Fa0/3: Power Device detected:
  Cisco PD

*Mar  1 05:23:55.976: %ILPOWER-5-POWER_GRANTED: Interface Fa0/3: Power granted
```

If you connect a newer Cisco IP Phone (a 7975, for example) that supports the IEEE 802.1af standard, you might see a message like this on the switch console line:

```
* Mar  1 05:23:55.858: %ILPOWER-7-DETECT: Interface Fa0/4: Power Device detected:
  IEEE PD

Mar  1 05:23:55.942: %ILPOWER-5-POWER_GRANTED: Interface Fa0/4: Power granted
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

When verifying PoE usage or troubleshooting phone power problems, you can see the existing PoE usage with the **show power inline** command. Knowing the remaining PoE capacity is important, as Cisco sells some switch models that do not have enough PoE to fully power all ports, such as the 24-port Catalyst 2960-24LT-L that supports only eight PoE devices at 15.4 watts.

In this output from Pod 11, there are two Cisco IP Phones attached, consuming 18.3 watts, with 351.7 watts of PoE capacity left on this switch. The 7960 phone (6.3 watts) does not have a PoE class, as it does not support 802.1af, while the 7975 phone (12.0 watts) shows as an IEEE PoE Class 3 device.

```
SwPod11# show power inline
Available:370.0(w)  Used:18.3(w)  Remaining:351.7(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
Fa0/1     auto   off        0.0     n/a                 n/a   15.4
Fa0/2     auto   off        0.0     n/a                 n/a   15.4
Fa0/3     auto   on         6.3     IP Phone 7960       n/a   15.4
Fa0/4     auto   on         12.0    IP Phone 7975       3     15.4
Fa0/5     auto   off        0.0     n/a                 n/a   15.4
Fa0/6     auto   off        0.0     n/a                 n/a   15.4
<output omitted>
```

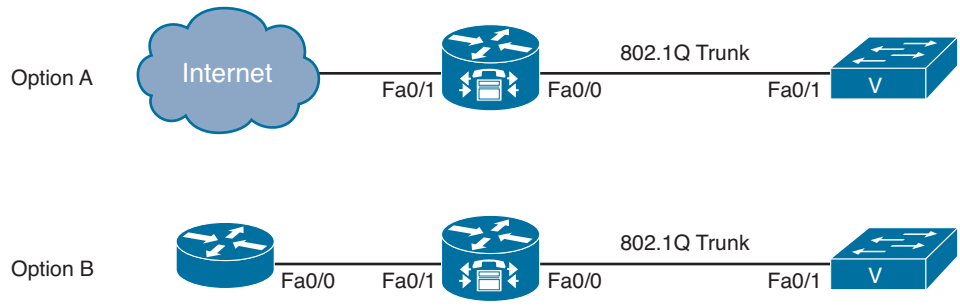
At this point, the phones should be attempting to register and will display a message such as "Registering" or "Configuring CM List" (the message will vary depending on the phone model and the version of firmware on the phone). If the phones show "Configuring IP" for more than a few seconds, the DHCP service is not functioning. The messages displayed on the phones are useful information when troubleshooting.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 3-2: Network Time Protocol

Figure 3-3 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router (and a second Cisco router if Internet access is not allowed from the first router)
- Switch that supports voice VLANs

Learning Objectives

Upon completion of this lab, you will be able to configure Network Time Protocol (NTP).

Scenario

SOI wants its new data network to use NTP to synchronize time for network devices.

NTP is not only important for synchronizing the time in network device event logs, but also for VoIP to show the correct time on the display of the phones and record the correct timestamp on voicemails, among other uses. The best way to keep everything synchronized is to use an NTP server to coordinate time.

This lab has instructions for two options:

- Option A assumes access to a production network that can reach an NTP server on the Internet.
- Option B configures another Cisco router to provide NTP time to simulate an Internet NTP server.

Note: The NTP server should not be a Microsoft Windows server running the W32Time service, as this uses Simple Network Time Protocol (SNTP), which is not as accurate as NTP and will not sync with most Cisco equipment.

These instructions refer to the Pod Addressing Table in Appendix A to determine the IP addresses and VLAN numbers used for your pod. Wherever an *x* is shown, substitute the pod number.

Task 1: NTP Services

Step 1-1: Load Prior Configurations

Use the configuration from Lab 3-1. If necessary, load the configuration for both the switch and router.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 1-2: (Optional) Configure Local Time Zone

NTP is calculated using UTC (Greenwich Mean Time), but you might want to see the time displayed on the router and phones using your local time zone.

Tip: Newer versions of the IOS have the 2007 updated U.S. Daylight Saving Time (DST) start and end dates included. If using an older IOS, or if you have a different DST at your location, you can enter the correct start and end dates as part of the command.

Note: The Cisco IOS does not provide help for time-zone naming conventions. Check Cisco.com for this information.

```
RtrPodx(config)# clock timezone timezone offset-from-GMT
```

For example, U.S. Central Daylight Time would use **clock timezone cdt -6.**

```
RtrPodx(config)# clock summer-time zone recurring
```

For example, U.S. Central Daylight Time would use **clock summer-time cdt recurring.**

Step 1-3: Manually Set the Clock

By manually setting the clock close to the correct time, you reduce the amount of time it takes to synchronize with the NTP server. Ideally, you should be within a minute or two of the correct time.

Use the privileged EXEC mode command **clock set** to manually set time:

```
RtrPodx# clock set hh:mm:ss day month year
```

For example, if the current day is Thursday, August 16, 2012 and the time is 9:40 p.m., you would enter **clock set 21:40:00 16 August 2012**.

Step 1-4 (Option A): Contact an NTP Server on the Internet

(Proceed to Step 1-4 [Option B] if you do not have access to the Internet.)

Configure an interface on the router to reach the Internet. The commands in this step assume that Fast Ethernet 0/1 is cabled to a production network with Internet access and a DHCP server that will assign IP addresses to the router.

```
RtrPodx(config)# interface fastethernet 0/1
RtrPodx(config-if)# ip address dhcp
RtrPodx(config-if)# no shutdown
RtrPodx(config-if)# exit
RtrPodx(config)# ip route 0.0.0.0 0.0.0.0 gateway-of-Fa0/1-network
```

A list of NTP stratum two servers can be found at www.ntp.org (http://support.ntp.org/bin/view/Servers/StratumTwoTimeServers). After selecting one close to you, use the **ntp server** command:

```
RtrPodx(config)# ntp server ntp_server_IP_address
```

Note: Make sure to use the IP address of the NTP server, instead of the Domain Name System (DNS) name, as the router is not configured to translate DNS names.

Skip Step 1-4 (Option B) and go to Step 1-5 to verify NTP operation.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 1-4 (Option B): Configure Another Cisco Router to Act as an NTP Server

(Skip this step if you completed Option A.)

The commands in this step assume that Fast Ethernet 0/1 on the voice router is cabled to another Cisco router. (A serial interface could also be used, but the Ethernet interfaces do not require any additional hardware.)

First, configure the other router to connect to the voice router.

```
Router(config)# hostname NTP_Server
NTP_Server(config)# interface fastethernet 0/0
NTP_Server(config-if)# ip address 192.168.0.1 255.255.255.0
NTP_Server(config-if)# no shutdown
NTP_Server(config-if)# exit
```

Set the time zones and clock on the NTP_Server router to match the VoIP router (as you did in Steps 1-2 and 1-3).

```
NTP_Server(config)# clock timezone timezone offset-from-GMT
NTP_Server(config)# clock summer-time zone recurring
NTP_Server# clock set hh:mm:ss day month year
```

Because you are configuring a "fake" NTP server, it is best to use a higher NTP stratum number to avoid conflicting with real NTP servers. Configure the NTP_Server router to be an NTP time source with the **ntp master** *stratum number* command.

Note: If this configuration is used to build the CUCM server (as shown in Appendix C), the CUCM server will not trust an NTP server with a stratum (distance from the atomic clock) of 7 or higher. To account for each device, such as the voice router (that adds 1 to stratum), the starting value is set to 4.

```
NTP_Server(config)# ntp master 4
```

Configure the VoIP router to connect to the NTP_Server router.

```
RtrPodx(config)# interface fastethernet 0/1
RtrPodx(config-if)# ip address 192.168.0.2 255.255.255.0
RtrPodx(config-if)# no shutdown
RtrPodx(config-if)# exit
RtrPodx(config)# ntp server 192.168.0.1
RtrPodx(config)# end
```

Go to Step 1-5 to verify NTP operation.

Step 1-5: Verify That the Time Is Synchronized

Use the following commands to verify that NTP is working:

```
RtrPodx# show ntp status
RtrPodx# show ntp association
RtrPodx# show ntp association detail
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Note: It can take five to ten minutes to synchronize with the NTP server. To avoid overwhelming NTP servers, the router starts by polling the server every 64 seconds, and it takes several poll intervals for the router to establish confidence in the results.

In Examples 3-2a to 3-2g, the Pod 11 router is shown acquiring NTP time from another router. Your results will vary, but the descriptions will help you understand the various outputs you might see as the router uses NTP to synchronize.

The **show ntp associations** command output start with an "INIT" as the status, while the **show ntp associations detail** command output shows the server as "insane, invalid, unsynced" and the filter error is 16 (showing no polling data).

Example 3-2a Output Showing Pod 11 Router Acquiring NTP Time

```
RtrPod11# show ntp associations
  address          ref clock       st   when   poll reach  delay  offset   disp
 ~192.168.0.1      .INIT.          16      -     64     0  0.000   0.000 16000.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
RtrPod11# show ntp associations detail
192.168.0.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (18:00:00.000 CDT Thu Dec 31 1899)
our mode client, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 16.00
delay 0.00 msec, offset 0.0000 msec, dispersion 16000.00
precision 2**24, version 4
org time 00000000.00000000 (18:00:00.000 CDT Thu Dec 31 1899)
rec time 00000000.00000000 (18:00:00.000 CDT Thu Dec 31 1899)
xmt time 00000000.00000000 (18:00:00.000 CDT Thu Dec 31 1899)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =    16.00   16.00   16.00   16.00   16.00   16.00   16.00   16.00
minpoll = 6, maxpoll = 10
```

After the INIT phase is done (which can take a minute), the router shows the difference between the NTP server time and the time on the router. The router is now establishing the variation in time between the received time and local time. At the point the incrementing "when" counter equals the "poll" number, the NTP server will be queried again.

Example 3-2b Output Showing Pod 11 Router Acquiring NTP Time

```
RtrPod11# show ntp associations
  address          ref clock       st   when   poll reach  delay  offset   disp
 ~192.168.0.1      127.127.1.1     10     11     64     1  0.000 -348980 7937.5
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
RtrPod11# show ntp associations
  address          ref clock       st   when   poll reach  delay  offset   disp
 ~192.168.0.1      127.127.1.1     10     44     64     1  0.000 -348980 7937.5
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

In Example 3-2c, the router is 3,489.807 seconds off from the NTP server time. This phase will take several minutes.

Note: If the root dispersal value is above 1000, the router might not synchronize with the NTP server.

Example 3-2c Output Showing Pod 11 Router Acquiring NTP Time

```
RtrPod11# show ntp associations detail
192.168.0.1 configured, insane, invalid, stratum 10
ref ID 127.127.1.1   , time D22D35B2.32265329 (00:57:06.195 CDT Wed Sep 28 2011)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.30, reach 1, sync dist 7.94
delay 0.00 msec, offset -3489807.6733 msec, dispersion 7937.50
precision 2**24, version 4
org time D22D35B8.CB5A7071 (00:57:12.794 CDT Wed Sep 28 2011)
rec time D22D435A.9A57C7DE (01:55:22.602 CDT Wed Sep 28 2011)
xmt time D22D435A.99DE9D3F (01:55:22.601 CDT Wed Sep 28 2011)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset = -3489.8    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.00   16.00   16.00   16.00   16.00   16.00   16.00   16.00
minpoll = 6, maxpoll = 10
```

The next phase is to accept the time from the NTP server and establish the accuracy of the local clock. Notice that the router is just over 2 milliseconds off from the NTP server. The "filteroffset" and "filtererror" are now 0 for the first poll.

Example 3-2d Output Showing Pod 11 Router Acquiring NTP Time

```
RtrPod11# show ntp associations detail
192.168.0.1 configured, insane, invalid, stratum 10
ref ID 127.127.1.1   , time D22D36A0.3225413B (01:01:04.195 CDT Wed Sep 28 2011)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.21, reach 1, sync dist 7.94
delay 0.00 msec, offset 2.2946 msec, dispersion 7937.50
precision 2**24, version 4
org time D22D36A0.CC349A2D (01:01:04.797 CDT Wed Sep 28 2011)
rec time D22D36A0.CBD66632 (01:01:04.796 CDT Wed Sep 28 2011)
xmt time D22D36A0.CB603CB8 (01:01:04.794 CDT Wed Sep 28 2011)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.00   16.00   16.00   16.00   16.00   16.00   16.00   16.00
minpoll = 6, maxpoll = 10
```

Every 64 seconds, the router polls the NTP server again. You can see the polls show up, as the "filterror" is gradually set to 0 for each new poll.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Example 3-2e Output Showing Pod 11 Router Acquiring NTP Time

```
RtrPod11# show ntp associations
192.168.0.1 configured, insane, invalid, stratum 10
ref ID 127.127.1.1   , time D22D36D2.32254796 (01:01:54.195 CDT Wed Sep 28 2011)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.44, reach 3, sync dist 3.94
delay 0.00 msec, offset 3.1598 msec, dispersion 3937.73
precision 2**24, version 4
org time D22D36DF.CC672189 (01:02:07.798 CDT Wed Sep 28 2011)
rec time D22D36DF.CBD02AD0 (01:02:07.796 CDT Wed Sep 28 2011)
xmt time D22D36DF.CB5A1A5B (01:02:07.794 CDT Wed Sep 28 2011)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.00    0.00   16.00   16.00   16.00   16.00   16.00   16.00
minpoll = 6, maxpoll = 10
```

After enough polls have been completed, the time on the router is NTP synchronized. Your router now considers the NTP server "our master, sane, and valid."

Example 3-2f Output Showing Pod 11 Router Acquiring NTP Time

```
RtrPod11# show ntp associations detail
192.168.0.1 configured, our_master, sane, valid, stratum 10
ref ID 127.127.1.1   , time D22D3756.32286702 (01:04:06.195 CDT Wed Sep 28 2011)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.39, reach 17, sync dist 0.94
delay 0.00 msec, offset 3.1598 msec, dispersion 939.24
precision 2**24, version 4
org time D22D3760.CCE2CF70 (01:04:16.800 CDT Wed Sep 28 2011)
rec time D22D3760.CBD604CE (01:04:16.796 CDT Wed Sep 28 2011)
xmt time D22D3760.CB5F51F8 (01:04:16.794 CDT Wed Sep 28 2011)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.00    0.00    0.00    0.00   16.00   16.00   16.00   16.00
minpoll = 6, maxpoll = 10
```

The asterisk (*) in front of the NTP server IP address shows that the server is synchronized. The **show ntp status** command also shows that the server is synchronized.

Example 3-2g Output Showing Pod 11 Router Acquiring NTP Time

```
RtrPod11# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~192.168.0.1     127.127.1.1     10     21     64   377  0.000  15.598  4.689
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
RtrPod11# show ntp status
Clock is synchronized, stratum 11, reference is 192.168.0.1
nominal freq is 250.0000 Hz, actual freq is 249.9998 Hz, precision is 2**24
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
reference time is D22D3760.CBD604CE (01:04:16.796 CDT Wed Sep 28 2011)
clock offset is 0.0031 msec, root delay is 0.00 msec
root dispersion is 0.94 msec, peer dispersion is 0.44 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000722 s/s
system poll interval is 64, last update was 99 sec ago.
```

Step 1-6: (Optional) Configure the Switch to Get NTP from the Router

For the sake of making sure that all networking devices are synchronized using NTP, the switch should use the router as an NTP source.

Note: To avoid overloading public NTP time servers, common practice has only a few edge devices at a company contact the public NTP servers, and all other company resources contact those edge devices.

```
SwPodx(config)# clock timezone timezone offset-from-GMT
SwPodx(config)# clock summer-time zone recurring
SwPodx(config)# ntp server 10.x1.0.1
```

Step 1-7: Save the Configurations

Save the configurations into a text file for both the router and switch. They will be needed for future labs.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 3-3: Phone Boot/Registration Process

Equipment Required

No equipment is required for this lab.

Learning Objectives

Upon completion of this lab, you will better understand the Cisco IP Phone boot and registration process.

Task 1: Questions

The most important part of solving problems with VoIP solutions is knowing how a properly functioning system should work and comparing it to an existing problem. Cisco IP Phones have multiple steps to complete when connected to the network, and understanding the process from booting to registration will speed resolution of problems.

Question 3.1

List at least three ways that a Cisco IP Phone can receive power.

1. _____
2. _____
3. _____

Question 3.2

What two protocols can Cisco IP Phones use to register to the Call Agent (depending on the phone firmware loaded)?

1. _____
2. _____

Question 3.3

Number the following steps in the order they occur during the phone boot process:

___ The phone downloads the configuration file from the TFTP server.

___ The phone gets IP address information from DHCP, including option 150.

___ The phone registers with one or more Call Agents.

___ The phone receives power, which might involve receiving PoE from the switch.

___ The phone learns the VLAN information from CDP.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

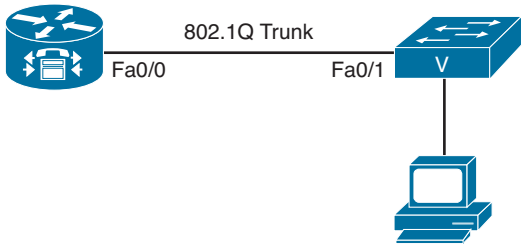
CHAPTER 4

Introduction to CUCME Administration

This chapter explores the three ways to administer Cisco Unified Communications Manager Express (CUCME).

Lab 4-1: Exploring the Command-Line Interface and Cisco Configuration Professional

Figure 4-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- PC with Cisco Configuration Professional (CCP) installed (the lab is based on CCP version 2.5)

Learning Objectives

Upon completion of this lab, you will be able to

- Determine the version of CUCME on the router
- Connect to CUCME with CCP

Scenario

These instructions refer to the Pod Addressing Table in Appendix A to determine the IP addresses and VLAN numbers used for your pod. Wherever an *x* is shown, substitute the pod number.

Task 1: Load Prior Configurations

This lab is based on the configuration from either Lab 3-1 or 3-2. If necessary, load the configuration for both the switch and router, and cable the devices as shown in Figure 4-1.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Explore Telephony Services

It is difficult to determine whether CUCME is available on the router, and what version it is, without knowing specific information about the IOS versions. The best way to determine whether CUCME is available, and the version, is to use the **show telephony-service** command.

This command configures system-level settings for Cisco IP Phones that use the Skinny Client Control Protocol (SCCP). (Session Initiation Protocol [SIP] commands are configured elsewhere.)

Step 2-1: Determine CUCME Version

Enter the **telephony-service** command in privileged EXEC mode. After the service is enabled, you can use the **show telephony-service** command to see the version. In this output, the CUCME version is 7.1. The output also shows many of the default CUCME settings.

Note: If you use the **show telephony-service** command before the service is enabled, you will get the following message:

```
RtrPodx# show telephony-service
telephony-service is not enabled
```

```
RtrPodx(config)# telephony-service
RtrPodx(config-telephony)# end
RtrPodx# show telephony-service
CONFIG (Version=7.1)
====================
Version 7.1
Cisco Unified Communications Manager Express
For on-line documentation please see:
http://www.cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_
  home.html

ip source-address 0.0.0.0 port 2000
ip qos dscp:
 ef (the MS 6 bits, 46, in ToS, 0xB8) for media
 cs3 (the MS 6 bits, 24, in ToS, 0x60) for signal
 af41 (the MS 6 bits, 34, in ToS, 0x88) for video
 default (the MS 6 bits, 0, in ToS, 0x0) for serviceservice directed-pickup
max-ephones 0
max-dn 0
max-conferences 8 gain -6
dspfarm units 0

<output omitted>

keepalive 30 auxiliary 30
timeout interdigit 10
timeout busy 10
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
timeout ringing 180
timeout transfer-recall 0
timeout ringin-callerid 8
timeout night-service-bell 12
caller-id name-only: enable
web admin system name Admin
web admin customer name Customer

<output omitted>
```

Task 3: Exploring CUCME Using CCP

Step 3-1: Test Connectivity Between PC and Router

Verify that the PC is assigned an IP address from the 10.*x*0.0.0 /24 subnet. Verify that the PC can ping the IP address of the router. If not, troubleshoot the configuration.

Step 3-2: Configure the Router for CCP Access

The router needs the following four things before Cisco Configuration Professional (CCP) can connect:

- IP address reachable from the PC. (This was configured in Lab 3-1.)
- A username with privilege level 15 (privileged EXEC access) used to log in from CCP.
- HTTP (and if available, HTTPS) service for CCP to use during discovery.
- Ability to connect to the router's VTY lines using Telnet (and if available, Secure Shell [SSH]).

Enter the following commands for nonencrypted access to the router:

```
RtrPodx(config)# username student privilege 15 secret cisco
RtrPodx(config)# ip http server
RtrPodx(config)# ip http authentication local
RtrPodx(config-line)# line vty 0 15
RtrPodx(config-line)# login local
```

Note: Not all routers and switches support **line vty 0 15**. If that is the case for your equipment, change the command to **line vty 0 4**.

If your router supports encryption (the IOS should have a "k9" as part of the filename), you can add these additional commands to allow secure HTTPS and SSH connections between CCP and the router:

```
RtrPodx(config)# ip http secure-server
RtrPodx(config-line)# line vty 0 15
RtrPodx(config-line)# transport input ssh telnet
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-3: Open the CCP Application

Note: You need to use CCP as an application on the PC. (The CCP Express preinstalled on newer Cisco devices does not support telephony features.) You can download CCP from the Cisco website free of charge.

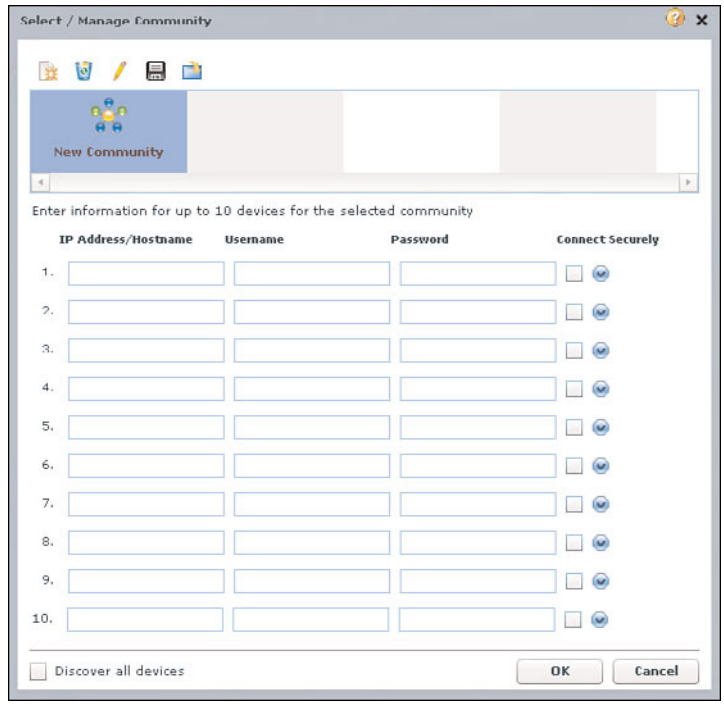
Open the CCP application on your PC.

Tip: During the CCP install, an icon for a demo is created. Make sure to launch the full application, not the demo.

The first time you use CCP, you start out by creating a new community in the Select/Manage Community dialog box (see Figure 4-2). Each community can have up to ten devices.

Note: The images in this book use the latest version available at the time of printing, CCP version 2.5.

Figure 4-2 Creating a Community in CCP



Step 3-4: Create a Community in CCP

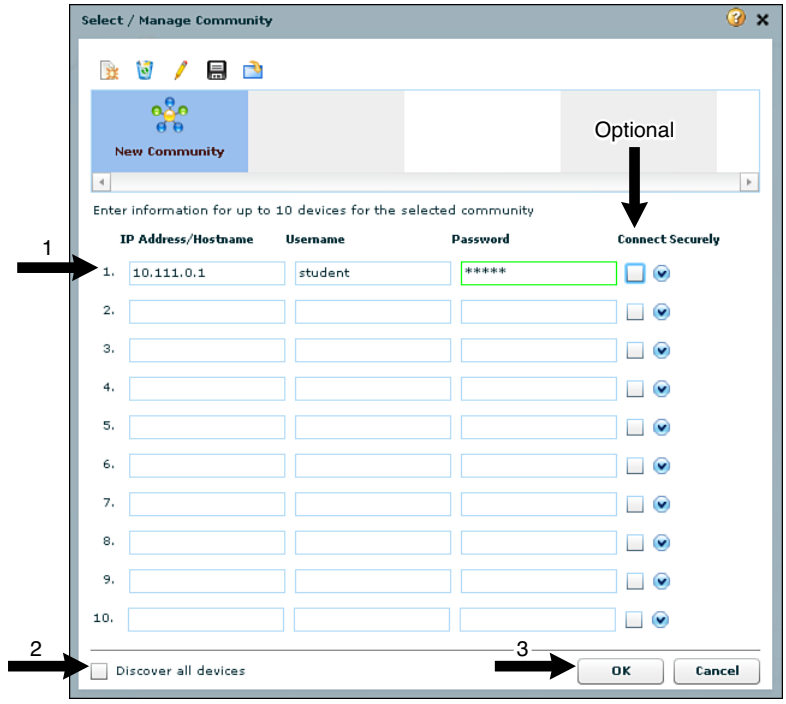
In the first row of fields in the Select/Manage Community dialog box, enter the IP address/host name of the router (the 10.*x*0.0.1 address), the username (student), and the password (cisco).

See Figure 4-3 for an example of the community settings for Pod 11.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 4-3 Example of Pod 11 Community Information



(Optional) If you configured the encryption commands for HTTPS and SSH in Step 3-2, you can check the **Connect Securely** check box. (If you choose this, you will be prompted to accept the certificate in the next step during device discovery. Select **Always**.)

Check the **Discover all devices** check box and click the **OK** button.

Step 3-5: Working with a Community in CCP

After you enter information about devices, CCP shows the Main Application window. The device you just added appears in the Community Information pane. The Discovery Status column should progress from Discovery Scheduled to Discovering to Discovered before the process is complete. It takes several seconds for the discovery to complete.

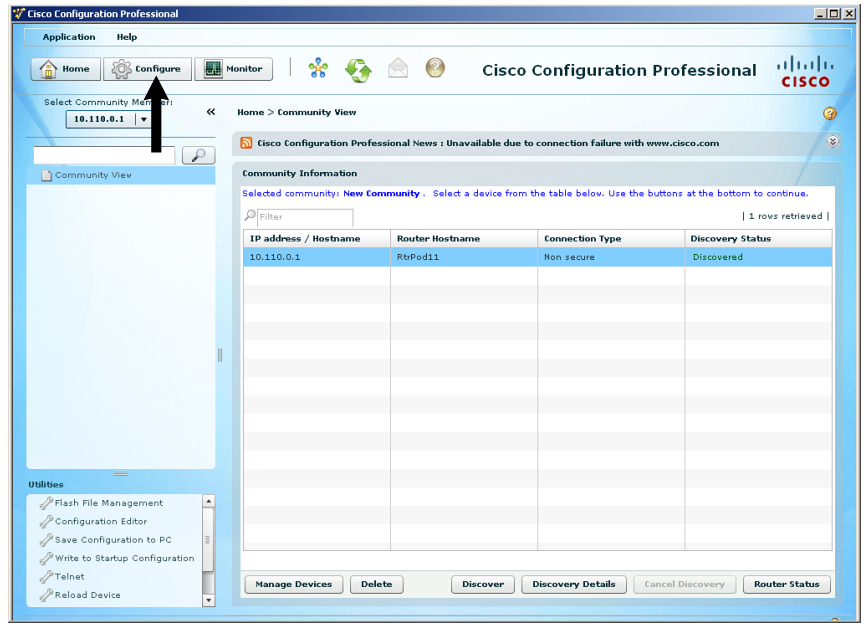
Note: If the Discovery Status column shows "Discovery failed," click the **Discovery Details** button (near the bottom) to find out why. If necessary, click the **Manage Devices** button (near the bottom) to return to the Select/Manage Community window.

See Figure 4-4 for an example of the community settings for Pod 11.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 4-4 Example of Pod 11 Router Discovery



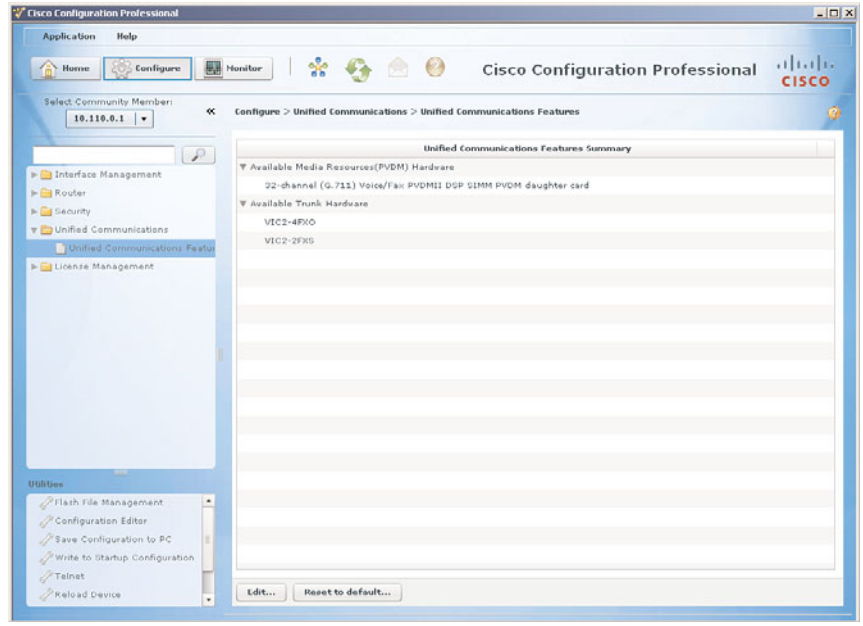
Step 3-6: Viewing Device Configuration Options in CCP

With your router discovered, click the **Configure** button (near the upper-left corner). The pane on the left will show various categories of router configuration options. (The items you see will depend on the IOS you have installed.)

Click the **Unified Communications** folder icon to expand the subitems.

Click the **Unified Communications Features** subitem. In the Unified Communications Features Summary pane on the right is the hardware that CCP has discovered. See Figure 4-5 for an example of the main window. (The output you see can vary from Figure 4-5, based on the hardware installed in your router.)

Figure 4-5 Example of Pod 11 Unified Configuration Features



https://t.me/learningnets

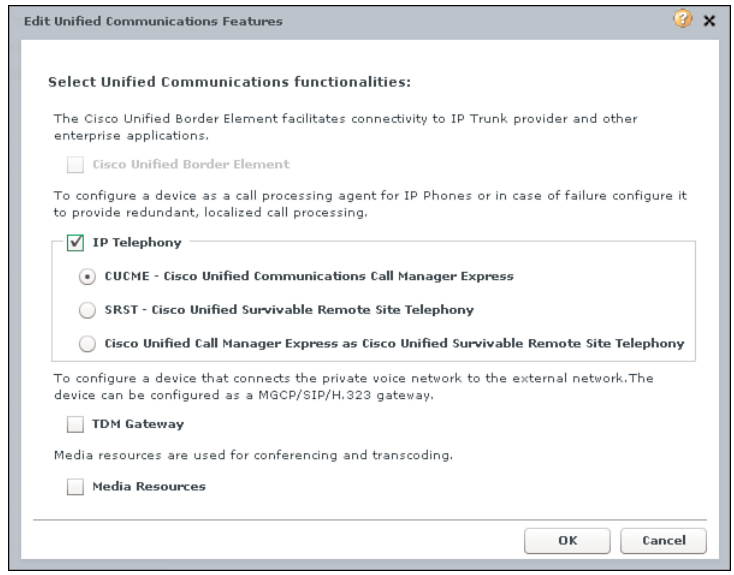
From the Library of Aliwarman Tarihoran

Click the **Edit** button at the bottom of the Unified Communications Features Summary pane. The Edit Unified Communications Features dialog box opens.

Step 3-7: Establish Unified Communication Functionality in CCP

In the Edit Unified Communications Features dialog box, select the **IP Telephony** check box and then click the **CUCME** radio button. See Figure 4-6 for an example of the Edit Unified Communications Features dialog box.

Figure 4-6 Edit Unified Communications Features



Click the **OK** button at the bottom of the Edit Unified Communications Features dialog box.

Step 3-8: Deliver Configuration from CCP to the Router

The Deliver Configuration to Device dialog box opens. CCP has a very handy feature in which it displays the commands before it delivers them to the router. (This not only gives you a chance to verify that the commands are what you wanted, but that the commands listed are also the same commands you could enter at the command-line interface [CLI].)

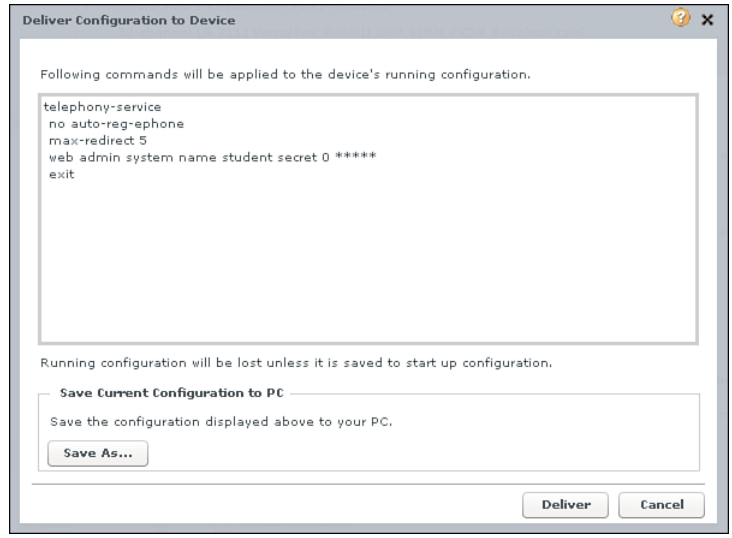
See Figure 4-7 for an example of the Deliver Configuration to Device dialog box.

Click the **Deliver** button to send the commands to the router.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 4-7 Deliver Configuration to Device Dialog Box

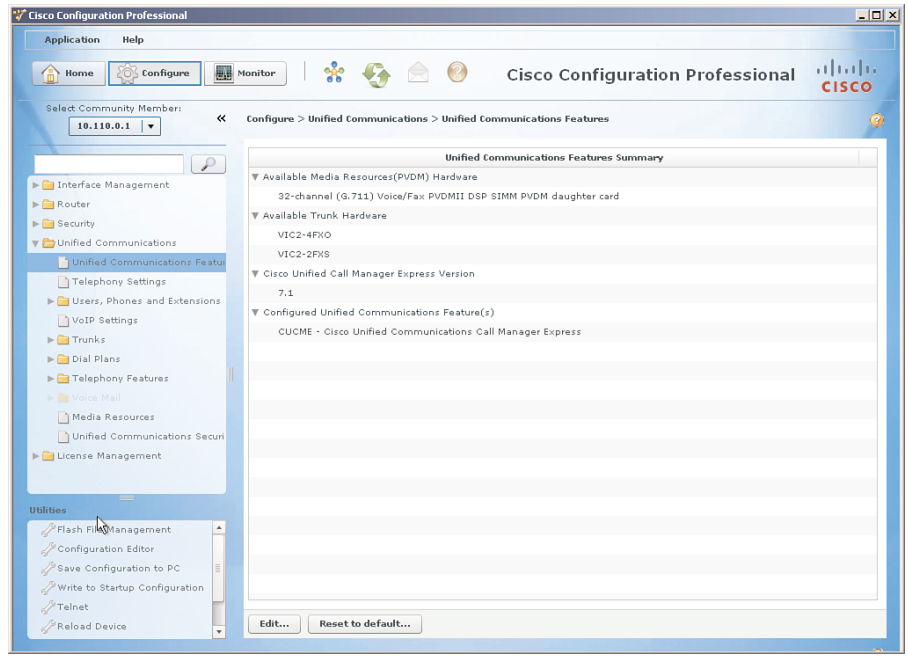


Step 3-9: Review Unified Communications Features Summary

The main window now displays an updated Unified Communications Features Summary pane. You should see CUCME is now active and the version is listed.

See Figure 4-8 for an example of the Unified Communications Features Summary pane.

Figure 4-8 Unified Communications Features Summary Pane



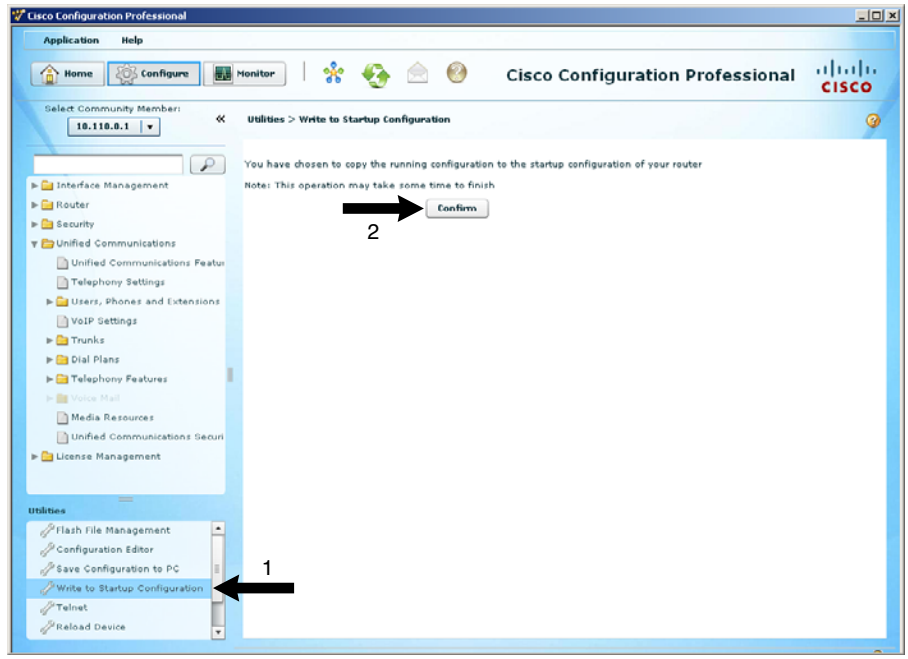
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-10: Save the Startup Configuration in CCP

To save the current configuration to the startup configuration, in the Utilities pane (in the lower-left corner) click the **Write to Startup Configuration** link. See Figure 4-9 for an example of the Write to Startup Configuration pane.

Figure 4-9 Write to Startup Configuration Pane



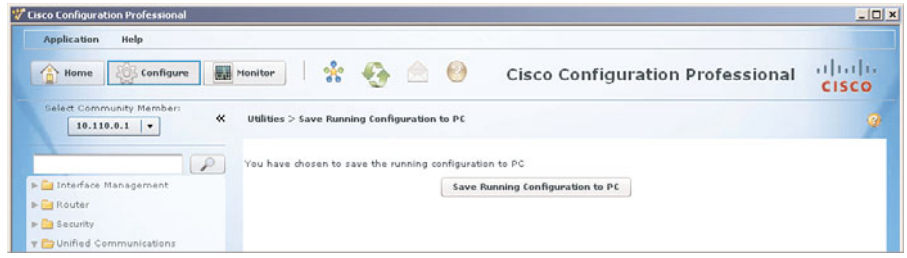
Click the **Confirm** button.

The Information dialog box will open confirming that the configuration was saved. Click the **OK** button.

Step 3-11: Save the Running Configuration to the PC Using CCP

You should keep a copy of the running configuration on the PC for a backup. To save the current configuration to the PC, in the Utilities pane, click the **Save Configuration to PC** link. See Figure 4-10 for an example of the Save Running Configuration to PC pane.

Figure 4-10 Save Running Configuration to PC Pane



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Click the **Save Running Configuration to PC** button.

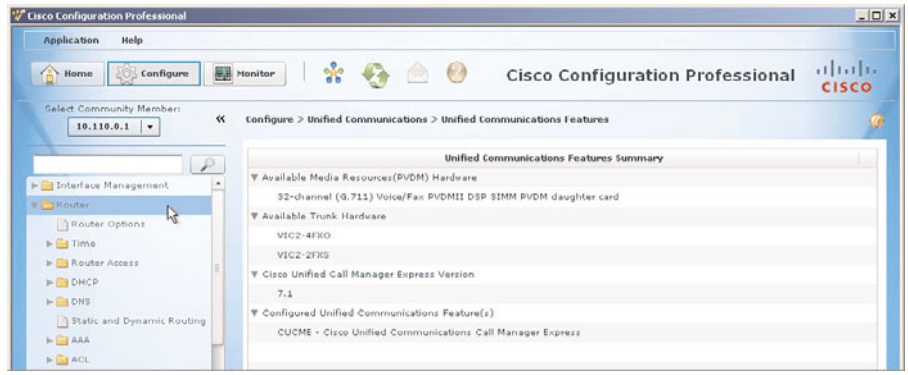
A File Save dialog box opens. After entering the desired filename and navigating to the desired location, click the **Save** button.

Step 3-12: Explore Other Parts of CCP

One major advantage that CCP has over the HTML GUI (covered in Lab 4-2) is that CCP can configure more than just Unified Communications.

Open the **Router** folder icon to expand the subitems (see Figure 4-11). CCP has options (and wizards) to help configure router functions such as DHCP, DNS, ACLs, and more.

Figure 4-11 CCP Router Options

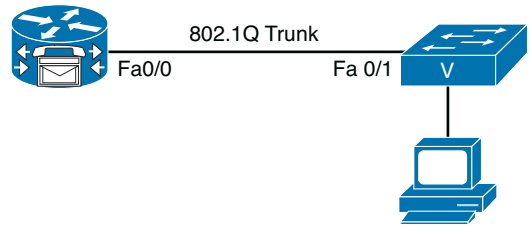


https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 4-2: Integrated HTML GUI

Figure 4-12 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with the GUI files loaded in flash (see Appendix D for details on loading the files)
- Switch that supports voice VLANs
- PC

Learning Objectives

Upon completion of this lab, you will be able to access the HTML GUI on the router.

Scenario

Shiny Objects Inc. (SOI) would like the office manager to add users and phones without having to use the command line for configuration. Ideally, SOI wants to be able to access the configuration from any PC without installing client software.

You can provide SOI with a solution! The integrated HTML GUI is simple enough for nontechnical personnel to use, yet powerful enough to get most phone and user configuration tasks done.

The HTML GUI does have drawbacks, however. The Java and HTML files take up precious flash file space, and the configuration is limited to just common CUCME tasks. In fact, the best use of the HTML GUI is for customer users needing to complete basic configuration tasks.

Task 1: Load Prior Configurations

This lab is based on the configuration from either Lab 3-1 or 3-2. If necessary, load the configuration for both the switch and router, and cable the devices as shown in Figure 4-12.

Task 2: Configure the Router for Web Access

Step 2-1: Enable HTTP Service on the Router

Depending on the IOS version and the router model, the HTTP server might be enabled or disabled. Enable the HTTP server, and if your router IOS supports it, the **ip http secure-server** command to enable HTTPS (SSL). Configure the location of the HTML files in flash, and set the router to use

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

local authentication to log in. Be aware that the IOS is case sensitive when specifying the path to the HTML files.

```
RtrPodx(config)# ip http server
RtrPodx(config)# ip http path <HTML file location path>
RtrPodx(config)# ip http authentication local
```

Note: Some of these commands were entered in Lab 4-1. They are included here again, so this lab is not dependent on Lab 4-1 being completed first.

The **ip http path** command points to the location of the HTML and Java files. If the files are in root of the flash, leave the path with just **flash:**, but if the files are in a subdirectory called (for example) "gui", use **flash:/gui** for the path. Use the **dir** command to verify the file location of the HTML files.

If your router supports encryption (the IOS should have a "k9" as part of the filename), you can add the following command to allow secure HTTPS connections to the router:

```
RtrPodx(config)# ip http secure-server
```

Step 2-2: Create a CUCME Web Administrator Account

Create a CUCME web administrator account to access all the GUI features. In this step, you will create the user named "webadmin" with a password of "webadmin."

Note: If you are using NTP, you should not enable the **time-webedit** command, as this would allow users to potentially override the NTP-learned time.

```
RtrPodx(config)# telephony-service
RtrPodx(config-telephony)# web admin system name webadmin secret 0 webadmin
RtrPodx(config-telephony)# dn-webedit
RtrPodx(config-telephony)# time-webedit
```

Step 2-3: Use a Web Browser to Connect to the GUI

Use the address **http://*<any ip address on your router>*/ccme.html** to connect to the GUI. (For example, pod 11 would use http://10.110.0.1/ccme.html to reach the GUI.) You will then get the login window. Use the webadmin account that you just created to log in. See Figure 4-13 for an example of the login process.

Figure 4-13 HTML GUI Login

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

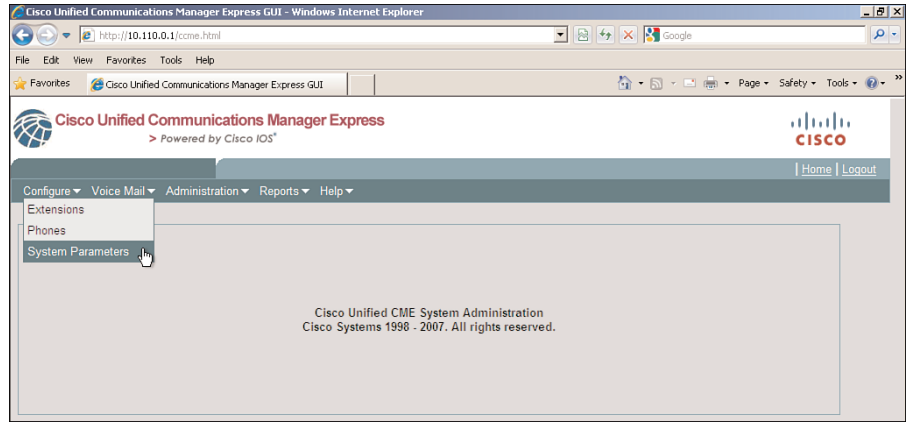
Note: A common mistake is forgetting the /ccme.html at the end of the URL. Without this, you are trying to connect to the basic IOS HTTP server, which is different from the CUCME web service.

After you log in, the main window shows the menu of actions you can perform.

Tip: If you see a blank page after login, the most likely problem is that the HTML files are not at the path specified in the **ip http path** ***<HTML file location path>***command. Remember that the IOS is case sensitive when entering the path. Use the **dir** command to verify the file location of the HTML files.

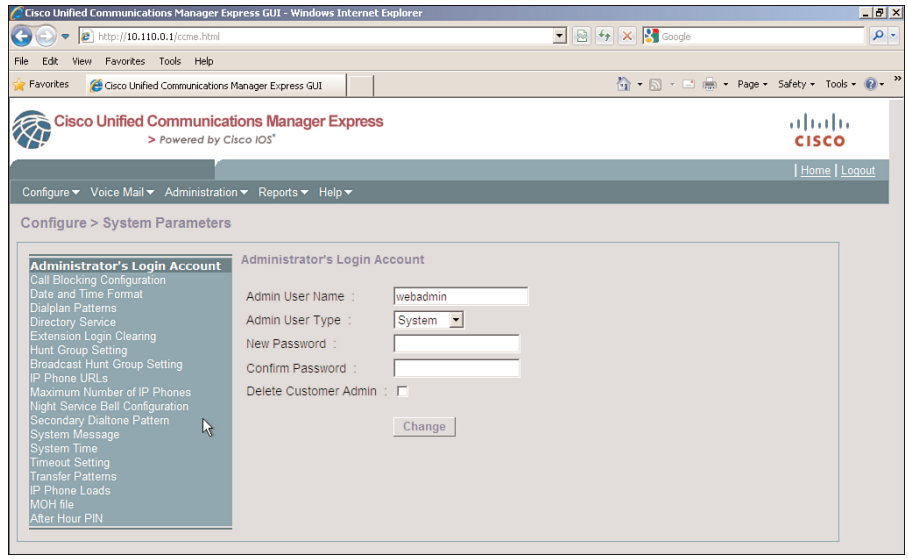
See Figure 4-14 for the Configure menu options.

Figure 4-14 HTML GUI Configure Menu Options



Choose **Configure > System Parameters**. The window will show the various system parameters that can be changed. Figure 4-15 shows the System Parameters window.

Figure 4-15 HTML GUI System Parameters Window



Note: A custom configuration for the HTML GUI is possible that restricts what features are available for users. You can create a custom XML file that allows or restricts features, and then associate the XML file with a user account. See the "Creating a Customized XML File for Customer Administrator GUI" section of the *Cisco Unified Communications Manager Express System Administrator Guide* for more details.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

This page intentionally left blank

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

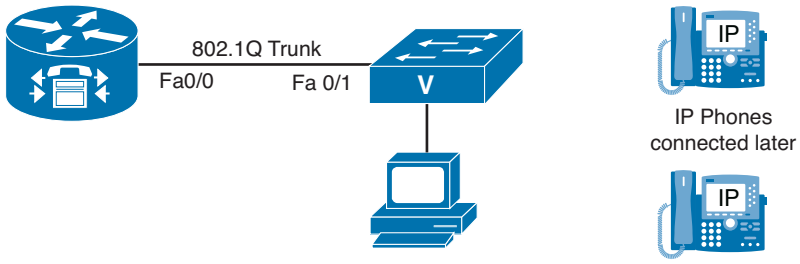
CHAPTER 5

Configuring Phones and Users in Cisco Unified Communications Manager Express (CUCME)

With previous chapters building the foundation for telephony concepts and a network topology, it is time to turn your attention to configuring the Call Agent. You will learn to configure Cisco Unified Communications Manager Express (CUCME) using both the command-line interface (CLI) and Cisco Configuration Professional (CCP).

Lab 5-1: Basic Manual Phone Configuration Using the CLI

Figure 5-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Lab configuration from either Lab 3-1 or 3-2
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)

Learning Objectives

Upon completion of this lab, you will be able to

- Configure telephony services in CUCME
- Manually register phones
- Place phone calls between two phones in the same system

Scenario

Shiny Objects Inc. (SOI) wants to establish internal calls using the new system. These instructions refer to the Pod Addressing Table in Appendix A to determine the phone numbers, IP addresses, and VLAN numbers used for your pod. Wherever an *x* is shown, substitute the pod number.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Load Prior Configurations

This lab is based on the configuration from either Lab 3-1 or 3-2. If necessary, load the configuration for both the switch and router. However, do not connect the phones to the switch until later. Connect a PC to the switch and verify that it can ping the router and switch management addresses. Troubleshoot if necessary.

Task 2: Configure Telephony-Service

Telephony-service configuration mode is where settings that impact the entire CUCME system are configured. There are three settings that must be configured (four in older versions of CUCME) before phones can register, and one optional setting that avoids common phone registration mistakes.

Step 2-1: Disable Auto Phone Registration

Note: Disabling autoregistration of phones is an optional step. However, allowing phones to autoregister can cause problems if MAC addresses are entered incorrectly. Disabling autoregistration eliminates this problem. Versions of CUCME prior to 4.0 (IOS Release 12.4(9)T) don't have this command, so if you are using an earlier version, make sure to double-check the MAC addresses of the phones when registering them.

```
RtrPodx(config)# telephony-service
RtrPodx(config-telephony)# no auto-reg-ephone
```

Step 2-2: Establish the Maximum Number of Phones Allowed to Register

Before any IP phones can register with the system, the maximum number allowed to register must be set. The upper limit of the maximum is dependent on the model of the router; the higher the model number, the more IP Phones CUCME will support. While it might seem best to set the number to the maximum a given router will support, each reservation consumes resources on the router; thus it is better to set the number at slightly above the currently expected number of phones. (The maximum should also be set no higher than the number of licenses purchased.) It can be increased later (up to the maximum supported by the router model) without disrupting operations.

Discover the maximum number of phones that your CUCME router will support by using the question mark (**?**) with the **max-ephones** command:

```
RtrPodx(config-telephony)# max-ephones ?
```

What is the maximum number of phones your system can register? _____

Now set the maximum number of phones to five:

```
RtrPodx(config-telephony)# max-ephones 5
```

Step 2-3: Establish the Maximum Number of Directory Numbers (Phone Numbers)

Before any phones can register with the system, the maximum number of directory numbers must also be set. The upper limit of the maximum is dependent on the model of the router, but it will be higher than the number of phones. (If you consider that directory numbers will be used for intercoms, paging, voicemail numbers, and so on, you can see why there are more numbers allowed than phones.)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Again, each directory number will consume resources on the router; thus it is better to set the number at slightly above the currently expected number of directory numbers needed. As with the phones, it can always be increased later (up to the maximum supported by the router model) without disrupting operations.

Discover the maximum number of directory numbers your CUCME router will support by using the question mark (**?**) with the **max-dn** command:

```
RtrPodx(config-telephony)# max-dn ?
```

What is the maximum number of directory numbers your system can support? _____

Now set the maximum number of directory numbers to ten:

```
RtrPodx(config-telephony)# max-dn 10
```

Step 2-4: Set the IP Address Used by CUCME

Before any phones can register with the system, CUCME needs to know the IP address used to receive requests and respond to IP Phones. The **ip source-address** command tells the system the IP address to use. By default, TCP port 2000 is used, but it can be specified with the **port** option. Any valid IP address on the router can be used, but the address of the voice VLAN interface is the best choice in this case. Remember that wherever an *x* is shown, substitute the pod number.

Note: The best option for the source address is a loopback address, as loopback interfaces are always up. Using a physical interface (or subinterface) address could cause the system to stop responding if that interface is down, even if phones are connected to other interfaces that are up. However, in this configuration, if the interface is down, all phones are disconnected, so a loopback is not necessary.

```
RtrPodx(config-telephony)# ip source-address 10.x5.0.1
```

Note: Older CUCME versions might require you to add the **port 2000** option to the end of the command.

Step 2-5: Create the Default Template Files

With newer versions of CUCME, the system will automatically create the default template files for the phones after all required options are entered. A message will say

```
Updating CNF files
CNF files update complete
```

On older versions of CUCME, it might be necessary to create the template files manually using the **create cnf-files** command in telephony-service mode.

Tip: Sometimes, if a change is made in the Telephony Services section of the config, and the changes do not show on the phones, using the **no create cnf-files** and then the **create cnf-files** commands to manually re-create the template files (followed by restarting the phones) will fix the problem.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-6: Inspect the IP Phone Generic Config File

When phones boot and receive the option 150 address from DHCP, they use that address to contact the TFTP server to get a configuration file. The phone will request an SEP<*phone_MAC_address*>.cnf.xml file that contains the settings the phone should use, which the TFTP should have if the phone is registered. If the phone is not registered, or if the TFTP server does not have the file, the phone will next request the default config file called XMLDefault.cnf.xml. The router is acting as the TFTP server in this lab; normally the router will not respond to TFTP requests. To see what files the router will hand out, and where they are located, use the **show telephony-service tftp-bindings** command. The file we are interested in is the XMLDefault.cnf.xml file.

```
RtrPodx(config-telephony)# end
RtrPodx# show telephony-service tftp-bindings
tftp-server system:/its/united_states/7960-tones.xml alias United_States/7960-
  tones.xml
tftp-server system:/its/united_states/7960-font.xml alias English_United_States/7960-
  font.xml
tftp-server system:/its/united_states/7960-font.xml alias English_United_States/7920-
  font.xml
tftp-server system:/its/united_states/7960-dictionary.xml alias
  English_United_States/7960-dictionary.xml
tftp-server system:/its/united_states/7960-kate.xml alias English_United_States/7960-
  kate.xml
tftp-server system:/its/united_states/7960-kate.xml alias English_United_States/7920-
  kate.xml
tftp-server system:/its/united_states/SCCP-dictionary.xml alias
  English_United_States/SCCP-dictionary.xml
tftp-server system:/its/SEPDEFAULT.cnf alias SEPDefault.cnf
tftp-server system:/its/vrf1/XMLDefault.cnf.xml alias XMLDefault.cnf.xml
tftp-server system:/its/vrf1/ATADefault.cnf.xml alias ATADefault.cnf.xml
```

You can view the file right on the router using the **more** command. If the system has problems finding the file, use the path specified in the output of the previous **show** command. In the output, you see the IP address of the Call Agent (in this case, the CUCME router) and the port number to use.

```
RtrPodx# more system:/its/vrf1/XMLDefault.cnf.xml
<Default>
<callManagerGroup>
<members>
<member  priority="0">
<callManager>
<ports>
<ethernetPhonePort>2000</ethernetPhonePort>
</ports>
<processNodeName>10.115.0.1</processNodeName>
</callManager>
</member>
</members>
</callManagerGroup>
<loadInformation124  model="Cisco IP Phone 7914 14-Button Line Expansion
  Module"></loadInformation124>
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
<loadInformation227  model="Cisco IP Phone 7915 12-Button Line Expansion
  Module"></loadInformation227>
<loadInformation228  model="Cisco IP Phone 7915 24-Button Line Expansion
  Module"></loadInformation228>
<loadInformation229  model="Cisco IP Phone 7916 12-Button Line Expansion
  Module"></loadInformation229>
<loadInformation230  model="Cisco IP Phone 7916 24-Button Line Expansion
  Module"></loadInformation230>
<loadInformation30008  model="Cisco IP Phone 7902"></loadInformation30008>
<loadInformation20000  model="Cisco IP Phone 7905"></loadInformation20000>


<output omitted>
```

Task 3: Configuring Directory Numbers

A directory number (phone number) is represented in Cisco configs as an ephone-dn. (Think *d*irectory *n*umber.) Ephone-dns can be single-line, dual-line, and as of CUCME 4.1, octo-line. The distinction is in the number of simultaneous audio channels (lines) usable per phone button. For example, call waiting and transferring a caller to a third party need two audio channels. (The call transfer needs one channel for the original caller and another to establish the connection to the third party.) For this reason, most desk phones will use dual-line dns. The single-line dn is used for features like intercoms and paging, where dual-lines are not needed. Octo-line dns have eight audio channels per button. You might wonder, "Why not just make them all octo lines?" Each line created consumes resources on the router, so it is best to allocate the correct number of lines to each directory number. Be aware that you cannot later change the number of lines on a dn. To change the number of lines, you have to use the **no** command to remove the entire dn and then re-create it.

Step 3-1: Create a Dual-Line Ephone-dn

The ephone-dns are created in global configuration mode, and each dn is assigned a tag number. The tag number has to be less than the max-dn configured in telephony service, so usually you start with 1.

```
RtrPodx(config)# ephone-dn 1 dual-line
RtrPodx(config-ephone-dn)#
*Sep  9 18:30:43.451: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
*Sep  9 18:30:43.451: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.2, changed state to up
RtrPodx(config-ephone-dn)# number <first_extension_assigned_to_your_pod>
```

For example, Pod 3 would use **number 5060**

Tip: If you make an ephone-dn with an incorrect number of lines (for example, single-line when you wanted dual-line), you have to remove the ephone-dn using the **no ephone-dn** *number* command and re-create it.

Step 3-2: Repeat to Create the Next Three Phone Numbers

Create three more numbers so that there are more to assign for the phones.

```
RtrPodx(config-ephone-dn)# ephone-dn 2 dual-line
RtrPodx(config-ephone-dn)# number <second_extension_assigned_to_your_pod>
RtrPodx(config-ephone-dn)# ephone-dn 3 dual-line
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
RtrPodx(config-ephone-dn)# number <third_extension_assigned_to_your_pod>
RtrPodx(config-ephone-dn)# ephone-dn 4 dual-line
RtrPodx(config-ephone-dn)# number <fourth_extension_assigned_to_your_pod>
RtrPodx(config-ephone-dn)# exit
```

Task 4: Manually Configure an Ephone and Associate the First Directory Number

In a traditional analog or PBX phone system, a directory number (phone number) is associated with a wall jack. Any phone plugged into a wall jack will have the phone number assigned to that jack. Move the phone to another wall jack and the number on the phone changes (unless the line in the jack is manually changed). However, with IP Phones, the phone is identified by the MAC address assigned to it, so it does not matter where in the network the phone is located. As long as the phone can reach the Call Agent, it will be have the same directory numbers. CUCME uses the ephone to connect directory numbers (ephone-dns) to the MAC address of the phone.

Step 4-1: Get the MAC Address of the First Phone

There are three main ways to get the MAC address of a phone:

- **From the box of the IP Phone:** The outside of the box has both the printed MAC address and a bar code. The bar code makes it easier to scan and enter related information (such as extension and username) for bulk importing.
- **From the back of the IP Phone:** (Soft phones use the MAC address of the PC.) Turn the phone over and find the bar code with 12 hex digits. This method can also benefit from using a bar-code scanner to capture the MAC address for bulk import.
- **From the screen of the IP Phone:** Press the Settings button and then navigate to Network Settings to show the MAC address. (The disadvantage of this option is that it requires the phone to be powered on.) Don't use this method if autoregistration in CUCME is still enabled.

No matter which method you use, when entering a MAC address into the router, you need to enter it in the format of three groups of four hex numbers, separated by periods. Thus, a phone with MAC address 1234567890ab would be entered as 1234.5678.90ab in the ephone configuration.

What is the MAC address of the first phone? _____

Step 4-2: Create an Ephone and Assign the MAC Address

Just like the ephone-dns, the ephone requires a tag number that must be less than the max-ephone number defined in telephony-service. After entering config-ephone mode, the **mac-address** command is mandatory before any other command can be issued.

Note: If your CUCME version does not support the **no auto-reg-ephone** command in telephony-service, double-check that the MAC address entered matches the phone. If it is not correct, the phone will autoregister, but not show in the config or get a phone number assigned.

```
RtrPodx(config)# ephone 1
RtrPodx(config-ephone)# mac-address <mac_address_of_your_first_phone>
```

For example, a phone with mac address 1234567890ab would use **mac-address 1234.5678.90ab**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 4-3: Assign the First Directory Number to the First Button on the Phone

The next step is to associate one of the ephone-dns to the ephone. Most Cisco phone models are capable of having more than one line assigned to them, and they use line buttons on the phone for the caller to select the line to use. (See Figure 5-2.)

Figure 5-2 Buttons on a Cisco IP Phone

There are many options when assigning an ephone-dn to a button. The most common option is to use the colon (**:**) to connect the physical button on the phone to the ephone-dn. Use the question mark (**?**) to see the options:

```
RtrPodx(config-ephone)# button ?
  LINE  button-index:dn-index pairs example 1:2 2:5
Configuration line:button with separator feature options:
: normal phone lines
       example    button 1:2 2:5
s silent ring, ringer muted, call waiting beep muted
       example    button 1s2 2s5
b silent ring, ringer muted, call waiting beep not muted
       example    button 1b2 2b5
f feature ring
       example    button 1f2 2f5
       see also 'no dnd feature-ring'
<output omitted>
RtrPodx(config-ephone)# button 1:1
RtrPodx(config-ephone)# end
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

The **button 1:1** command in the example ties the first line button to the extension assigned to the first ephone-dn. If the command had been **button 1:2**, the first line button would have the extension assigned to the second ephone-dn. Likewise, if the command had been **button 5:3**, the fifth line button (counting down the display) would have the extension assigned to the third ephone-dn.

Step 4-4: Connect the First Phone to the Switch

Note: Do not connect other phones at this time.

If using a physical phone, connect the cable from the SW port to the switch. If using a soft phone, make sure that the computer is connected to the switch and start the software. The phone should go through the bootup process and register with CUCME. On the router, you will see a registration status message. In this output, a Cisco phone with MAC address 0022.555e.ef47 and IP address 10.115.0.11 has registered to ephone 1:

```
RtrPodx#

*Sep  7 21:55:15.119: %IPPHONE-6-REG_ALARM: 25: Name=SEP0022555EEF47 Load= SCCP42.8-
  4-2S Last=Initialized

*Sep  7 21:55:15.147: %IPPHONE-6-REGISTER: ephone-1:SEP0022555EEF47 IP:10.115.0.11
  Socket:1 DeviceType:Phone has registered.
```

The phone will then display the number assigned to ephone-dn 1 on the display. If you lift the phone handset, you should hear a dial tone.

Note: If the phone does not register, start troubleshooting using the IP Phone Registration process as a guide. Use the Settings button on the phone to view the networking settings. Questions to ask:

- Is the phone (for physical phones) in a port with the voice VLAN active and assigned? (Soft phones will be in the data VLAN.)
- Is the phone (or PC in the case of soft phones) getting an IP address from DHCP? Use the **show ip dhcp binding** command to verify.
- Is the DHCP option 150 set to an IP address on the router? (For soft phones that don't register, make sure that the option 150 was included in the Data DHCP pool. If necessary, assign the IP address of the Call Agent in the soft phone manually.)
- Are all the required telephony-service items entered and the cnf-files created, as shown in Steps 2-1 to 2-5? Use the **show run** command to verify that the required commands are entered.
- Has the phone previously registered to a CUCM version 8.0 or later system? If so, the phone wants to keep the previous registration and might refuse to register to CUCME. To clear the prior registration settings, see the notes in the hardware section of the Introduction.

If you are still encountering registration problems, try using Wireshark as demonstrated in Lab 5-4 to see where to troubleshoot.

Task 5: Manually Configure a Second Phone

In CUCME, there is an easier way to get the MAC addresses and register a few phones, if you have the **no auto-reg-ephone** command in telephony-service. With autoregistration disabled, you can connect the phone and the phone registration will fail. This allows you to use the **show ephone attempted-registrations** command to get the information.

Note: If your CUCME version does not support the **no auto-reg-ephone** command in telephony-service, skip Step 5-1 and repeat Steps 4-1 and 4-2 for the second IP Phone. Then, proceed to Step 5-2.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 5-1: Connect the Second Phone to the Switch

Connect the second phone to the switch. A message will display on the router console showing a registration alarm. The MAC address is displayed in the output of the alarm, but it is not in the right format. Use the **show ephone attempted-registrations** command to obtain the MAC address in the right format. In the following example, a Cisco 7975 Phone with MAC address 0022.555D.928A attempted to register, but there is no matching ephone config. The output of the **show ephone attempted-registrations** command not only gives the MAC address in the right format, but it also shows the model type of the phone (which is useful to have, as shown in Lab 5-2).

```
RtrPodx#
*Sep  7 22:13:59.770: %IPPHONE-6-REG_ALARM: 25: Name=SEP0022555D928A Load= SCCP75.8-
  4-2S Last=Initialized
RtrPodx# show ephone attempted-registrations
Attempting Mac address:

Num     Mac Address          DateTime                              DeviceType
-------------------------------------------------------------------------------

1       0022.555D.928A       17:16:53 cdt Wed Sep 7 2011       7975

-------------------------------------------------------------------------------
Num     Mac Address          DateTime                              DeviceType
```

You can now copy and paste the MAC address information:

```
RtrPodx# config t
RtrPodx(config)# ephone 2
RtrPodx(config-ephone)# mac-address <mac_address_listed_in_output>
```

Step 5-2: Assign the Second and First Directory Numbers to the Second Phone

Assuming that the second phone has more than one line button, you can assign more than one ephone-dn. The line buttons can be assigned as separate commands, or they can be assigned together as one command. In this output, we assign the first line button to the extension assigned to ephone-dn 2 and the second line button to the extension assigned to ephone-dn 1 (the same directory assigned to ephone 1 button 1).

```
RtrPodx(config-ephone)# button 1:2 2:1
```

However, you might find that the phone has already registered before you type the **button** command and it does not show any extensions on the phone display. While in *config-ephone* mode, you can use either the **restart** or **reset** command to update the phone. The phone will unregister and then reregister.

```
RtrPodx(config-ephone)# restart
restarting 0022.555D.928A
RtrPodx(config-ephone)#
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
*Sep  7 22:34:36.674: %IPPHONE-6-UNREGISTER_NORMAL: ephone-2:SEP0022555D928A
  IP:10.115.0.12 Socket:5 DeviceType:Phone has unregistered normally.

RtrPodx(config-ephone)#

*Sep  7 22:34:38.438: %IPPHONE-6-REG_ALARM: 23: Name=SEP0022555D928A Load= SCCP75.8-
  4-2S Last=Reset-Restart

*Sep  7 22:34:38.466: %IPPHONE-6-REGISTER: ephone-2:SEP0022555D928A IP:10.115.0.12
  Socket:6 DeviceType:Phone has registered.
```

Note: The **restart** command tells the phone to update the configuration. The **reset** command tells the phone to completely reboot, including the full power-up boot process. One hint to remember which does which: The shorter the command, the longer it takes the phone to be back in service.

Step 5-3: Make a Call

Place a call from the first phone to the directory number assigned on ephone-dn 2 (second extension for your pod). When you call from one phone to the other, the display on the ringing phone will show the extension that is called/calling.

Notice that whenever the first phone goes off-hook, the second line button on the second phone goes red, indicating that it is in use. This is because both phones share the same ephone-dn assignment. Unlike an analog home phone, where someone can pick up another extension and join the conversation, only one phone can use an ephone-dn at a time. (Adding other people to the conversation requires conferencing resources, which is beyond the scope of the CCNA Voice exam.)

Step 5-4: Assign Other Extensions to the First Phone

Assuming that the first phone has more than one line button, you can assign additional extensions using the **button** command. You can add additional ephone-dns to unassigned buttons without having to reenter the previous commands. The new assignment is added to the existing configuration. You will assign on the first ephone that line button 2 should use the fourth ephone-dn.

```
RtrPodx(config-ephone)# ephone 1
RtrPodx(config-ephone)# button 2:4
RtrPodx(config-ephone)# restart
RtrPodx(config-ephone)# end
RtrPodx# show run | begin ephone  1   [Note: there are two spaces between the ephone
  and the 1.]
ephone  1
 device-security-mode none
 mac-address 0022.555E.EF47
 button  1:1 2:4


<output omitted>
```

You can verify the phone status using the **show ephone** command. In this output, the directory number and extensions are assigned to line buttons 1 and 2. Notice there is a channel 1 (CH1) and channel 2 (CH2) status of IDLE for both dns, as the ephone-dns were created as dual-line and the phone is not in use.

```
RtrPodx# show ephone
ephone-1[0] Mac:0022.555E.EF47 TCP socket:[1] activeLine:0 whisperLine:0 REGISTERED
  in SCCP ver 20/12 max_streams=5
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:0 reset:0
reset_sent:0 paging 0 debug:0 caps:12
IP:10.115.0.11 52497 7962  keepalive 60 max_line 6 available_line 6
button 1: dn 1  number 5330 CH1   IDLE         CH2   IDLE         shared
button 2: dn 4  number 5333 CH1   IDLE         CH2   IDLE
Preferred Codec: g711ulaw

<output omitted>
```

Now place a call from line button 1 on the second phone to the extension assigned to button 2 of the first phone (extension 5333 in this example), and while the phone is ringing, run the command again. You will notice the status of button 2 CH1 is now RINGING, and at the end of the ephone-1 output, it shows that a call is ringing on line 2.

```
RtrPodx# show ephone
ephone-1[0] Mac:0022.555E.EF47 TCP socket:[1] activeLine:0 whisperLine:0 REGISTERED
  in SCCP ver 20/12 max_streams=5
mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:1 reset:0
  reset_sent:0 paging 0 debug:0 caps:12
IP:10.115.0.11 52497 7962  keepalive 121 max_line 6 available_line 6
button 1: dn 1  number 5330 CH1   IDLE         CH2   IDLE         shared
button 2: dn 4  number 5333 CH1   RINGING      CH2   IDLE
Preferred Codec: g711ulaw
call ringing on line 2

<output omitted>
```

Answer the call and run the command again. The status now shows the call as CONNECTED and the IP addresses of both phones. There are also statistics about the packets of the voice conversation.

```
RtrPodx# show ephone
ephone-1[0] Mac: 0022.555E.EF47 TCP socket:[1] activeLine:2 whisperLine:0 REGISTERED
  in SCCP ver 20/12 max_streams=5
mediaActive:1 whisper_mediaActive:0 startMedia:1 offhook:1 ringing:0 reset:0
  reset_sent:0 paging 0 debug:0 caps:12
IP:10.115.0.11 52497 7962  keepalive 127 max_line 6 available_line 6
button 1: dn 1  number 5330 CH1   IDLE         CH2   IDLE         shared
button 2: dn 4  number 5333 CH1   CONNECTED    CH2   IDLE
Preferred Codec: g711ulaw
Active Call on DN 4 chan 1 :5333 10.115.0.11 20168 to 10.115.0.12 23234 via
  10.115.0.11
G711Ulaw64k  160 bytes no vad
Tx Pkts 710 bytes 122120 Rx Pkts 709 bytes 121948 Lost 0
Jitter 0 Latency 0 callingDn 2 calledDn -1

<output omitted>
```

Step 5-5: Clear Configuration for the Next Lab

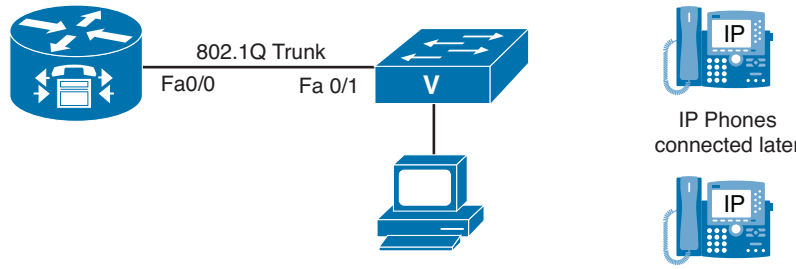
The next lab shows configuring beyond the basics required to make two phones ring. Clear the current configuration and then reload the router.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 5-2: Advanced Manual Phone Configuration Using the CLI

Figure 5-3 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Lab configuration from Lab 3-2
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)

Learning Objectives

Upon completion of this lab, you will be able to

- Configure telephony services in CUCME
- Manually register phones
- Place phone calls between two or more phones in the same system

Scenario

In this lab, SOI wants to establish internal calls using the new system with more than just the basics. These instructions refer to the Pod Addressing Table in Appendix A to determine the phone numbers, IP addresses, and VLAN numbers used for your pod. Wherever an *x* is shown, substitute the pod number.

Task 1: Load Prior Configurations

This lab is based on the configuration from Lab 3-2. Lab 3-2 configures Network Time Protocol (NTP) from the Internet or another router. This lab assumes that the router has the various clock setting commands configured and that NTP is synchronized. If necessary, load the configuration for both the switch and router.

Do not connect the phones to the switch until later. Connect a PC to the switch and verify that it can ping the router and switch management addresses. Troubleshoot if necessary.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Configure Telephony-Service

Telephony-service is where settings that impact the entire CUCME system are configured.

Step 2-1: Configure Required Telephony-Service Settings

If necessary, consult Lab 5-1 for more details on the individual commands. Remember that wherever an *x* is shown, substitute the pod number.

```
RtrPodx(config)# telephony-service
RtrPodx(config-telephony)# no auto-reg-ephone
RtrPodx(config-telephony)# max-ephones 6
RtrPodx(config-telephony)# max-dn 12
RtrPodx(config-telephony)# ip source-address 10.x5.0.1
Updating CNF files
CNF files update complete
```

Note: On older versions of CUCME, it might be necessary to create the template files manually using the **create cnf-files** command in the telephony-service config mode.

Step 2-2: Configure System Time in Telephony-Service

Even with the router's clock showing the correct local time, some phone models will not display the correct time. The **time-zone** command in telephony-service can fix this. (This is not required if you are only using Cisco Unified IP Phone models 7902G, 7905G, 7912G, 7920, 7921, 7935, 7936, 7940, 7960, or 7985G.) Use the **time-zone ?** command to find your time zone.

```
RtrPodx(config-telephony)# time-zone ?
  <1-53>  select timezone name used by IP phones (offset in minutes)
1 Dateline Standard Time -720
2 Samoa Standard Time -660
3 Hawaiian Standard Time -600
4 Alaskan Standard/Daylight Time -540
5 Pacific Standard/Daylight Time -480
6 Mountain Standard/Daylight Time -420
7 US Mountain Standard Time -420
8 Central Standard/Daylight Time -360
9 Mexico Standard/Daylight Time -360
10 Canada Central Standard Time -360
<output omitted>
```

For example, someone in U.S. Central Daylight Time would use **time-zone 8**.

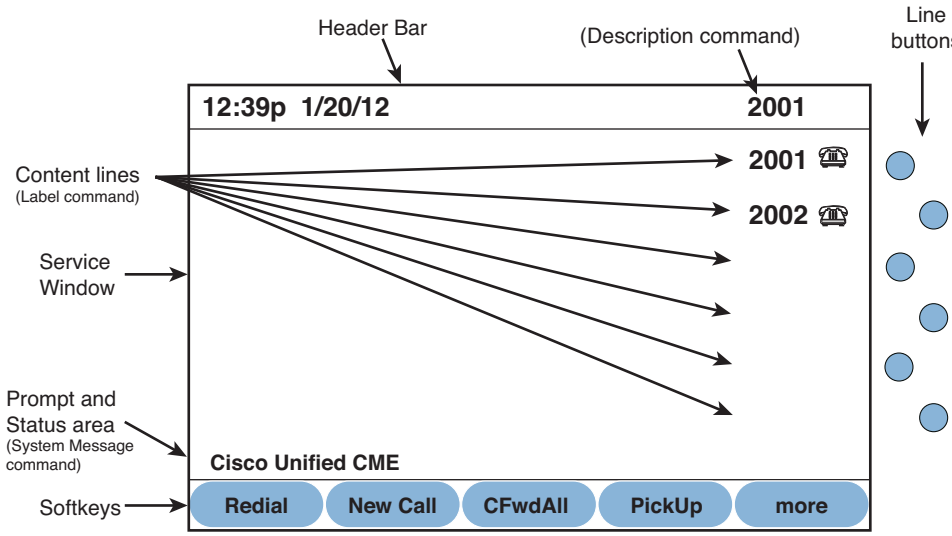
Step 2-3: Configure a Banner Message for Phones with a Display

There are a variety of items on the phone display that can be customized (see Figure 5-4).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 5-4 Cisco Unified IP Phone Display



Having all phones with a display prompt showing the default "Cisco Unified CME" message might not be what you want. Use the **system message** command to change the prompt to show your pod number.

```
RtrPodx(config-telephony)# system message Pod x
```

Task 3: Configure Ephone-dns

As noted in Lab 5-1, ephone-dns can be single-line, dual-line, and as of CUCME 4.1, octo-line. Most phones will use the dual-line option.

Step 3-1: Add the name Option to an Ephone-dn

After the extension is assigned to an ephone-dn, other options can be assigned. One of the most common is the **name** command. This not only shows the name on the display for incoming and outgoing calls, but it also builds the directory that can be used on the phone.

```
RtrPodx(config)# ephone-dn 1 dual-line
RtrPodx(config-ephone-dn)#
*Sep  9 18:30:43.451: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
*Sep  9 18:30:43.451: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.2, changed state to up
RtrPodx(config-ephone-dn)# number <first 4 digit phone number assigned to your pod>
RtrPodx(config-ephone-dn)# name <first name> <last name>
```

For example, I would use: **name Brent Sieling**

Step 3-2: Change the Phone Display Header Bar

At the top of the phone display is the header bar (see Figure 5-4). On the left is the time and date, and on the right is text that shows the extension number on button 1. Use the **description** command on the ephone-dn assigned to button 1 to change the text to whatever you want. If you are used to using the

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

description command for information that only shows in the running config, this is quite a change! The user's name, the full E.164 number, and the phone description (for example, Lobby 2 Intercom) are examples of information that might be displayed in the header bar.

Note that the description only shows on the display if the ephone-dn is attached to button 1 on a phone.

```
RtrPodx(config-ephone-dn)# description Receptionist
```

Step 3-3: Change the Text for Each Line Button

As shown in Lab 5-1, the extension number displays next to each line button. There are reasons you might want to change this to be more descriptive. The **label** command will replace the extension with the text specified. Examples include adding the extension user's name, intercom descriptions, and so on. The label will show on every line button text the ephone-dn is assigned to. Because the **label** command replaces the extension, it might be good practice to include the extension in parentheses at the end of the label. While it is helpful to see the name or purpose of the extension, most people like to also see the extension number in question so that they know the number to dial. Understand that the label only impacts the display on the phone; it does not impact caller ID or the directory information.

```
RtrPodx(config-ephone-dn)# label <user name> (<extension_number>)
```

For example, I would use **label Brent Sieling (5330)**

Step 3-4: Create the Other Ephone-dns

Repeat Steps 3-1 to 3-3 for the other five ephone-dns, using the next five extension numbers assigned to your pod in the Pod Addressing table in Appendix A. Assign names, descriptions, and labels of your choice for each extension.

Task 4: Configure Ephones

Step 4-1: Create an Ephone, and Assign the MAC Address and a Directory Number

With the **no auto-reg-ephone** option set in telephony-service (see Lab 5-1), you can connect the phones to the switch. (If they are all the same model, you might want to connect and register them one at a time.) Use the **show ephone attempted-registrations** command to collect the MAC addresses. (Tip: Use the **do** command to issue the **show ephone attempted-registrations** command while still in configuration mode.)

```
RtrPodx(config)# do show ephone attempted-registrations
RtrPodx(config)# ephone 1
RtrPodx(config-ephone)# mac-address <mac_address_listed_in_output>
RtrPodx(config-ephone)# button 1:1
```

As noted in Lab 5-1, there are other options for the button separator than the colon (**:**). Use the **button** command with the question mark (**?**) to see more details. Useful ones are as follows:

- **f (feature ring):** This produces a "stutter" triple ring. This is useful to distinguish the ring when more than one button is assigned to the phone. For example, a feature ring can be used to easily distinguish whether a caller to your phone is on your line or a coworker's extension on another line button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- **s (silent ring):** This allows you to answer or use a line without having it ring.
- **m (monitor line):** This allow you to monitor the status of an extension, and the button can be used to transfer a call to the extension.

Experiment with them. For example, *button 2f4* assigns button 2 to have a feature ring for ephone-dn 4's extension number.

Step 4-2: Assign the Ephone Model Type

For the router to properly recognize the features on each type of phone, it is necessary to tag each ephone with the model. For example, the directory on the phone will not work without a phone type assigned. Handily, the **show ephone attempted-registrations** command will display the model as well as the MAC address. Note: The Cisco IP Communicator uses the **type CIPC** for the command.

```
RtrPodx(config-ephone)# do show ephone attempted-registrations

Attempting Mac address:

Num    Mac Address         DateTime                          DeviceType
-------------------------------------------------------------------------------

1      001D.705E.ABF1      20:04:37 CDT Sun Jan 1 2012       7962
2      0021.A084.F3A2      23:56:44 CDT Sun Jan 1 2012       7975

-------------------------------------------------------------------------------
Num    Mac Address         DateTime                          DeviceType
```

```
RtrPodx(config-ephone)# type <model_of_your_phone>
```

For example, if ephone 1 is a 7962, use **type 7962**.

Step 4-3: Assign Users to the Phones

For users to log in to the system (for example, to manage their own settings), they need a username and password. Additionally, when using the phone keypad, some features require a PIN. Both of these items are assigned to an ephone.

```
RtrPodx(config-ephone)# username <username> password <password>
RtrPodx(config-ephone)# pin 1234
```

For example, I would use **username bsieling password cisco**

Step 4-4: Create the Other Ephones

Repeat Steps 4-1 to 4-3 for all the other phones you have. Assign the buttons, usernames, and PINs of your choice for each phone.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 5: Test and Save Configuration

Step 5-1: Make Calls

After the phones register, you should immediately notice the differences on the display. Make some calls and observe that the display now shows the name of the calling/called person in addition to the extension. Now you can see the name of the person calling you and not just the extension!

Make sure to call to and from the extensions where you used other options for the button configuration in Step 4-1.

Step 5-2: Save the Configuration

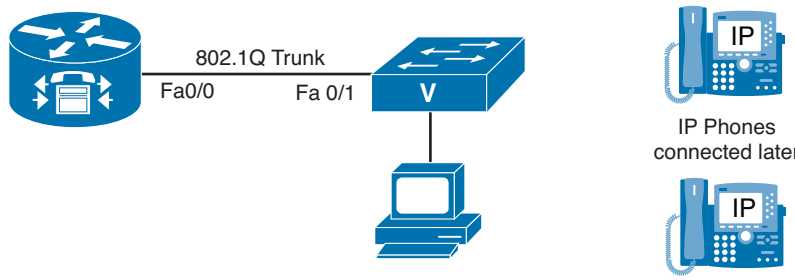
This configuration will be used in later labs, so make sure to copy the router config to a file for later use. The next lab will require the router to be reset to the configuration from Lab 4-1.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 5-3: Adding Directory Numbers, Phones, and Users with Cisco Configuration Professional (CCP)

Figure 5-5 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Lab configuration from Lab 4-1
- PC with Cisco Configuration Professional (CCP) installed (the lab is based on CCP version 2.5)
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)

Learning Objectives

Upon completion of this lab, you will be able to

- Configure telephony services in CUCME
- Register phones and users with CCP
- Place phone calls between two or more phones in the same system

Scenario

SOI would like the office manager to add users and phones without having to use the command line for configuration. Ideally, SOI wants to be able to access the configuration from any PC without installing client software.

Task 1: Load Prior Configurations

This lab is based on the configuration from Lab 4-1 (up through Step 3-10). If necessary, load the configuration for both the switch and router. However, do not connect the phones to the switch until later. Connect a PC to the switch and verify that it can ping the router and switch management addresses. Troubleshoot if necessary.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Configure Telephony Settings

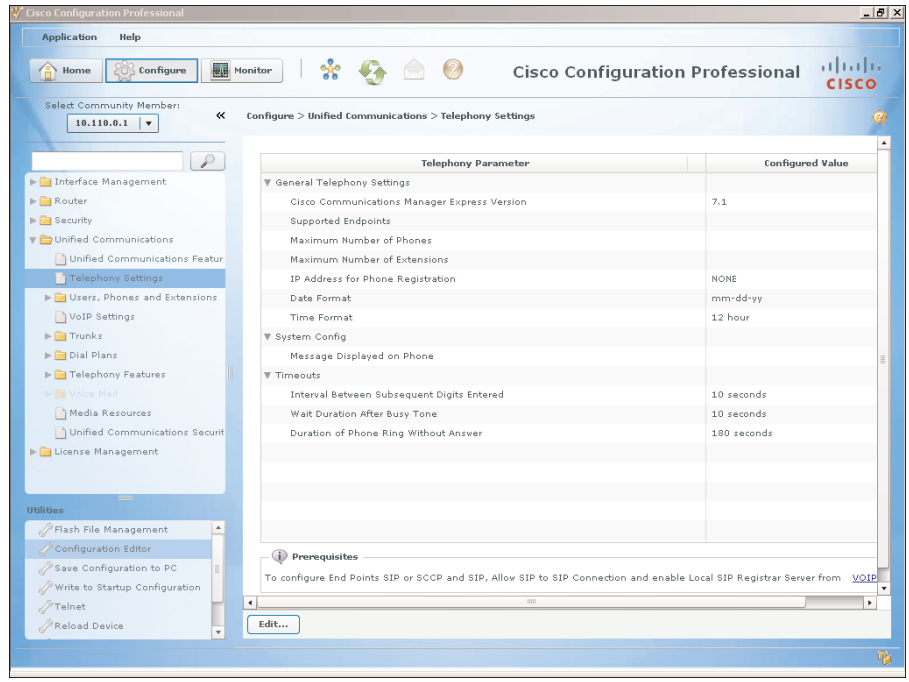
As noted in Labs 5-1 and 5-2, telephony-service (called Telephony Settings in CCP) is where settings that impact the entire CUCME system are configured. There are settings that must be configured before phones can register.

Step 2-1: View Telephony Settings

If Lab 4-1, Step 3-10 is completed, you should have CCP open and in the Configuration portion of CCP. Click the **Unified Communications** folder icon to expand the subitems.

Click the **Telephony Settings** subitem. In the Telephony Settings pane on the right are the current telephony parameters. (See Figure 5-6 for an example of this window.) As you can see, the maximum numbers of phones and extensions are blank, and the IP address for phone registration (**ip source-address** command in the CLI) lists NONE.

Figure 5-6 Telephony Settings



Click the **Edit** button at the bottom of the screen.

Step 2-2: Edit General Telephony Settings

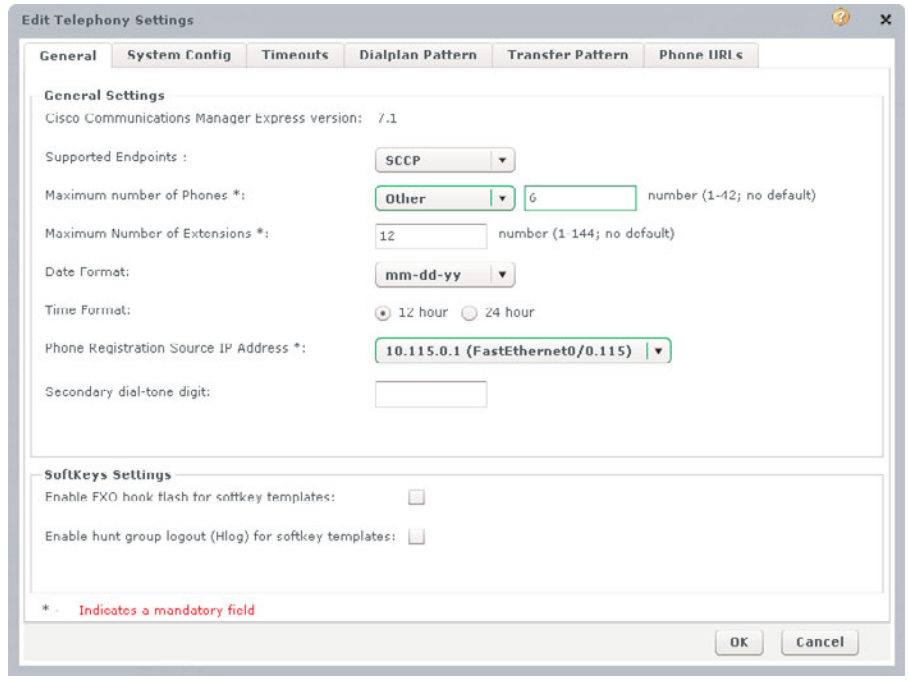
The Edit Telephony Settings window will open with the General tab selected.

1. Click the Maximum Number of Phones pull-down menu to select **Other**.
2. Enter **6** in the Number field (25 and 50 are listed values, as they match common license sizes).
3. Enter **12** for the Maximum Number of Extensions field.
4. Click the Phone Registration Source IP Address pull-down menu to select the voice subinterface IP address (**10.*x*5.0.1**). (See Figure 5-7 for an example of this window.)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 5-7 Edit General Telephony Settings

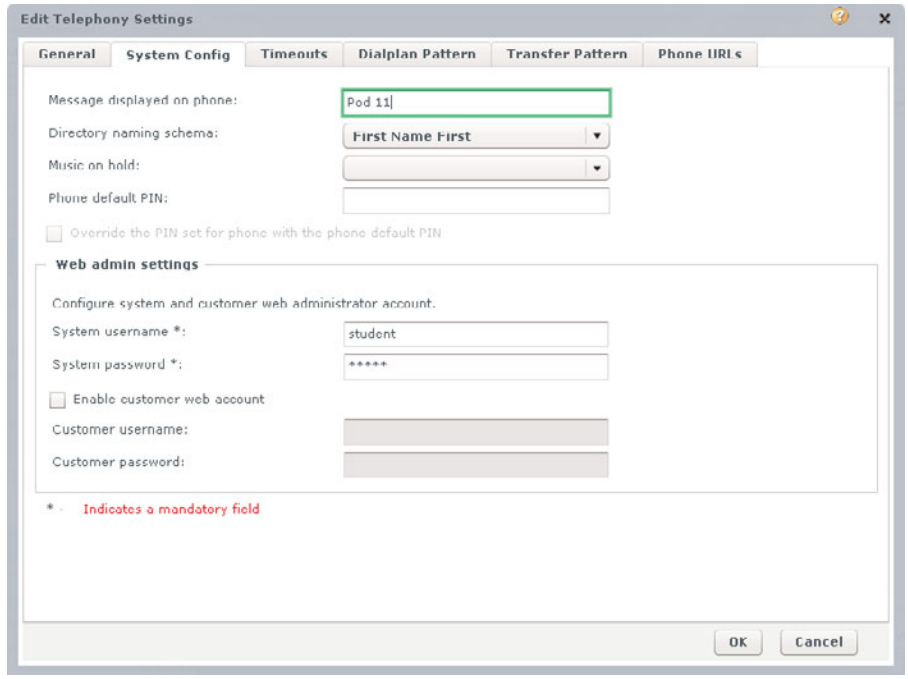


Step 2-3: Edit System Config Telephony Settings

Click the System Config tab in the Edit Telephony Settings window.

1. Enter **Pod *x*** (where *x* is your pod number). (See Figure 5-8 for an example of this window.)

Figure 5-8 Edit System Config Telephony Settings

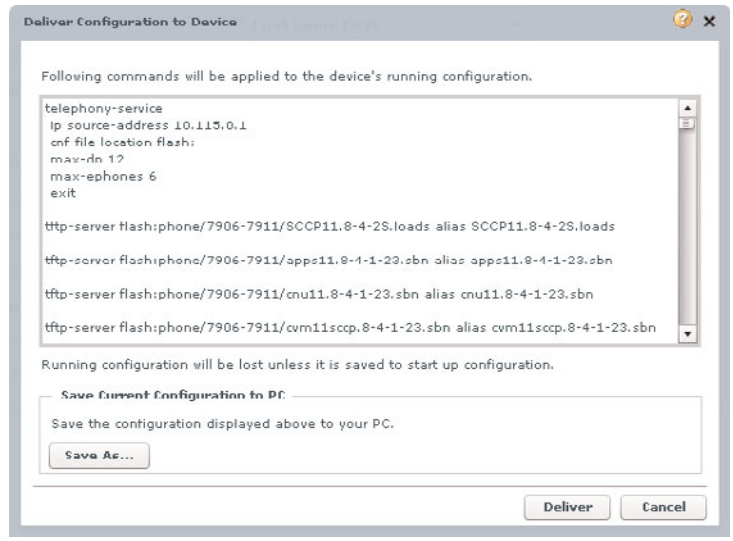


https://t.me/learningnets

From the Library of Aliwarman Tarihoran

2. Click the **OK** button to finish editing the telephony settings.
3. A confirmation dialog box will open warning you that the phone will need to be reset. Click **Yes** to continue.
4. A Deliver Configuration to Device window will open and display the commands that will be applied to the router. (The output might be different based on the phone firmware present on your router.) (See Figure 5-9 for an example of this window.)

Figure 5-9 Deliver Telephony Settings Configuration to Device



5. Click the **Deliver** button. (If an error about create-cnf files is reported, this is okay, as the files take a minute to create. You might then need to click **OK** again to deliver the commands a second time.)

The Telephony Settings window shows the updated values.

Task 3: Configure Extensions

It is easier to create extensions first, so when creating phones, the extensions can be added at that time.

Step 3-1: View Extension Settings

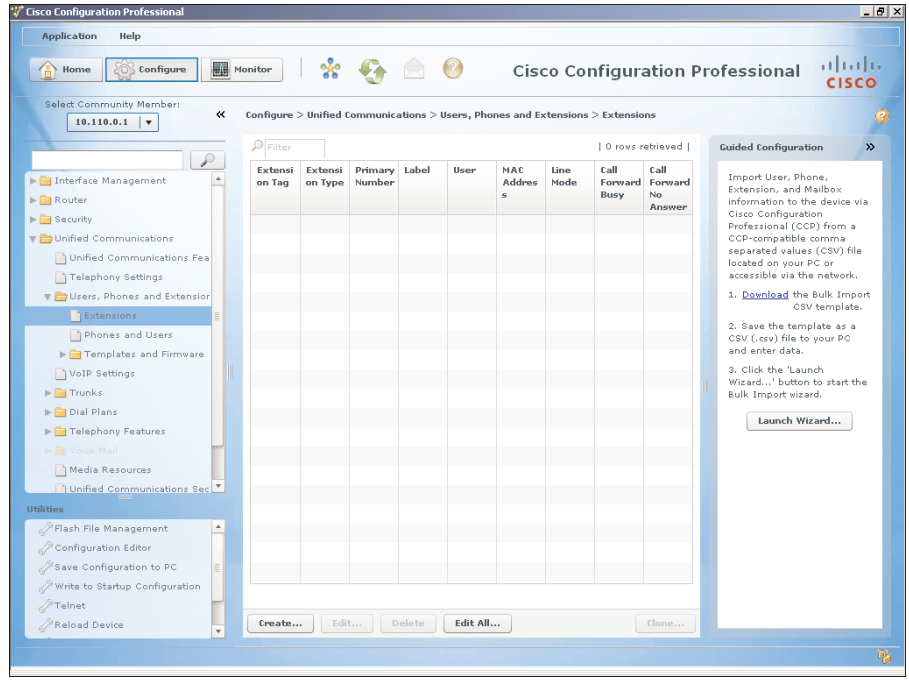
Under the **Unified Communications** folder icon, click the **Users, Phones and Extensions** folder icon to open the subitems.

1. Click the **Extensions** subitem. In the Extensions pane on the right are the current extensions. (See Figure 5-10 for an example of this window.)
2. On the right side is a Guided Configuration pane that allows you to save a spreadsheet file and fill out values for multiple phones and extensions and import them in bulk. Because you will not need this pane, and it is taking up screen space, click the double arrows (>>) to minimize it.
3. Click the **Create** button at the bottom of the window.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 5-10 Extensions



Step 3-2: Create an Extension

The Create Extension window will open with the General feature list selected (on the left).

1. Enter the first extension for your pod in the Primary Number field.
2. Enter your name and, in parentheses, the extension number in the Name to Be Displayed on Phone Line field (this will show on the display next to the line button, the same as the CLI **label** command).
3. Enter **Supervisor** in the Description field (this will show at the top of the phone display, the same as the CLI **description** command). (See Figure 5-11 for an example of this window.)
4. Click the **OK** button to create the first extension.
5. A Deliver Configuration to Device window will open and display the commands that will be applied to the router. (See Figure 5-12 for an example.)
6. Click the **Deliver** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 5-11 General Extensions Settings

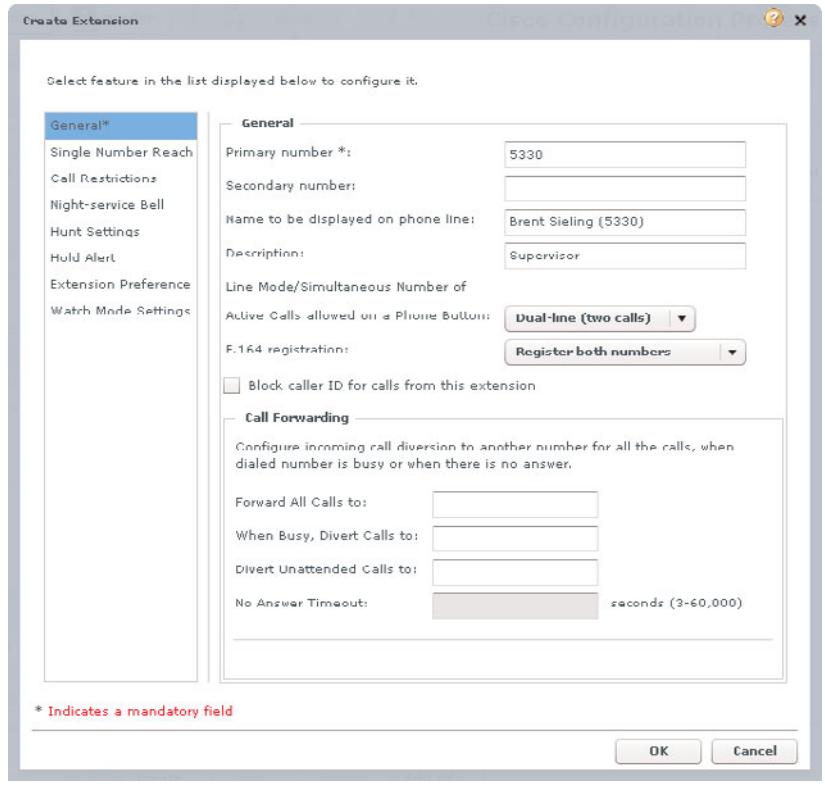
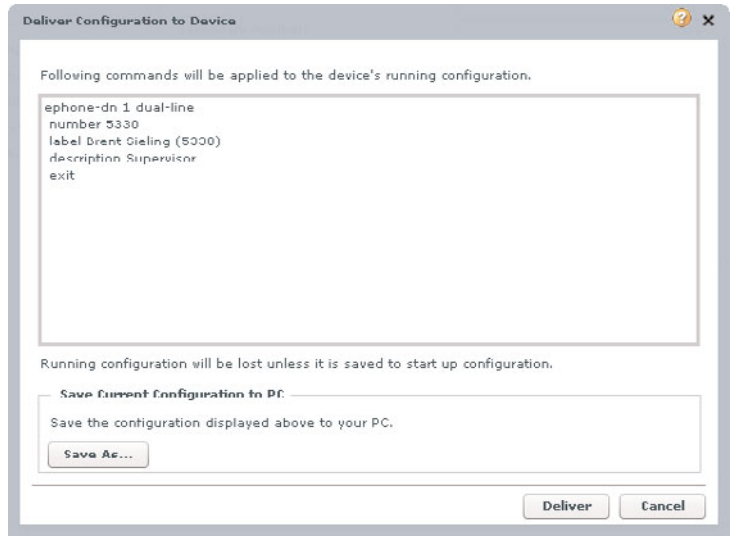


Figure 5-12 Deliver Extension Configuration to Device



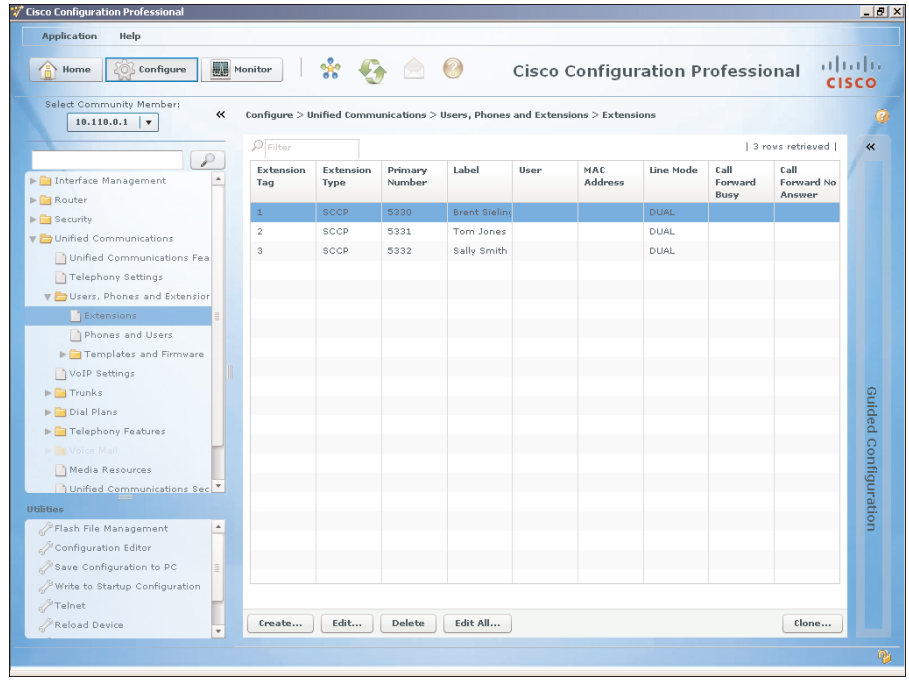
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-3: Create More Extensions

Repeat Step 3-2 to create two additional (or more) extensions. When you are done, the Extensions window should look similar to what is shown in Figure 5-13.

Figure 5-13 Three Extensions



Task 4: Configure Phones and Users

If the extensions are created first, they can be added to the phone during phone creation.

Step 4-1: View Phone/User Settings

Click the **Unified Communications** > **Users, Phones and Extensions** > **Phones and Users** subitem. (See Figure 5-14 for an example of this window.)

Just like in the Extensions window, on the right side is a Guided Configuration pane. Click the double arrows (**>>**) to minimize it.

Click the **Create** button at the bottom of the window.

Step 4-2: Create a Phone

The Create Phone/User window will open to the Phone tab.

1. Click the Phone Model drop-down list to select the model of the first phone.
2. Enter the MAC address of the first phone in the MAC Address field.
3. In the Extensions area, click the first extension number under Available Extensions and then click the Move (**>**) button to place it on Line 1. (See Figure 5-15 for an example of this window.)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 5-14 Phones and Users

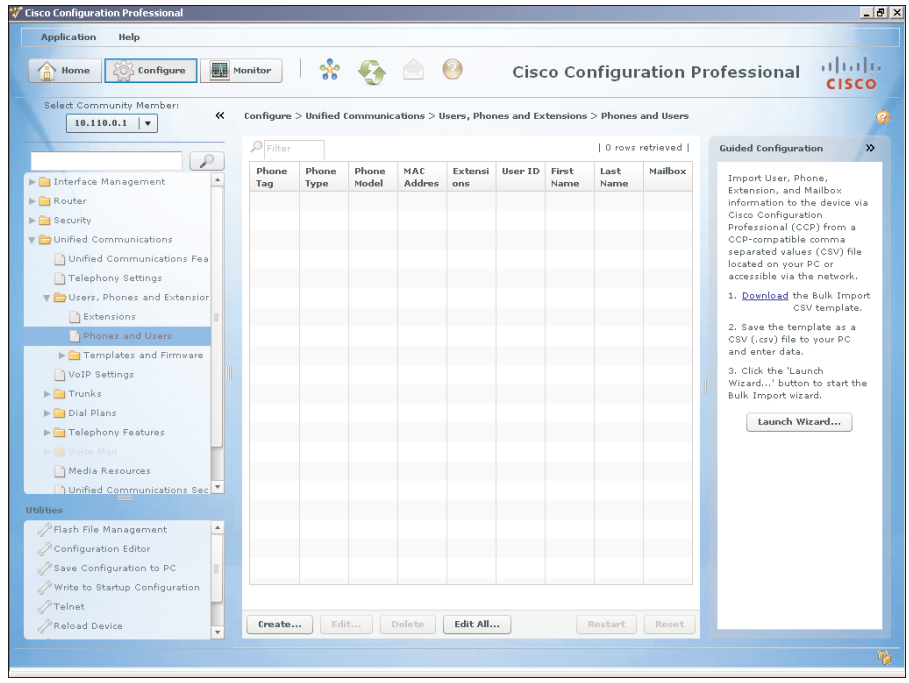
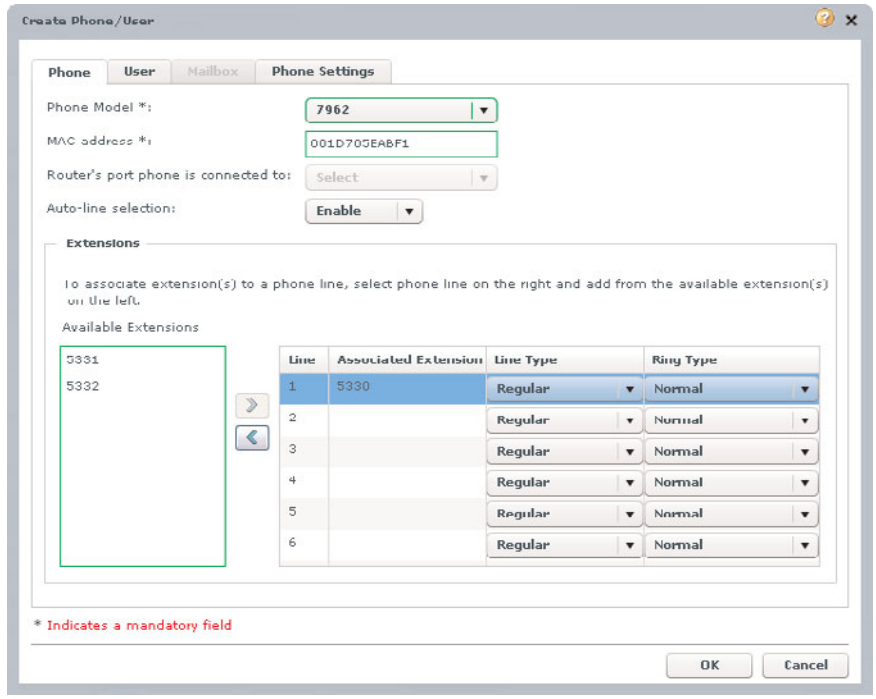


Figure 5-15 Create Phone



https://t.me/learningnets

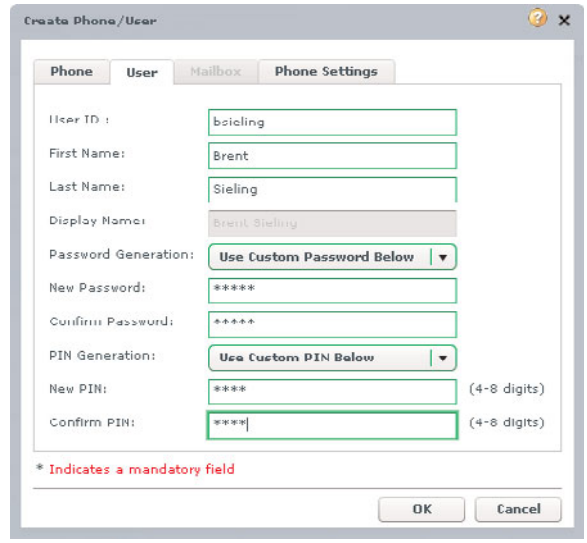
From the Library of Aliwarman Tarihoran

Step 4-3: Create a User

Click the User tab in the Create Phone/User window.

1. Enter a username for yourself in the User ID field.
2. Enter your first name and last name in their respective fields.
3. Click **Use Custom Password Below** from the Password Generation drop-down list.
4. Enter **cisco** for the New and Confirm Password fields.
5. Click **Use Custom PIN Below** from the PIN Generation drop-down list.
6. Enter **1234** for the New and Confirm PIN fields. (See Figure 5-16 for an example of this window.)

Figure 5-16 Create User



7. Click the **OK** button to create the phone and user.
8. A confirmation dialog box will open warning you that the phone will need to be reset. Click **Yes** to continue.
9. A Deliver Configuration to Device window will open and display the commands that will be applied to the router. (See Figure 5-17 for an example.)
10. Click the **Deliver** button.

Step 4-4: Create Another Phone/User

Repeat Steps 4-2 through 4-4 to create another phone and user. When you are done, the Phones and Users window should look similar to what is shown in Figure 5-18.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 5-17 Deliver Phone/User Creation to Device

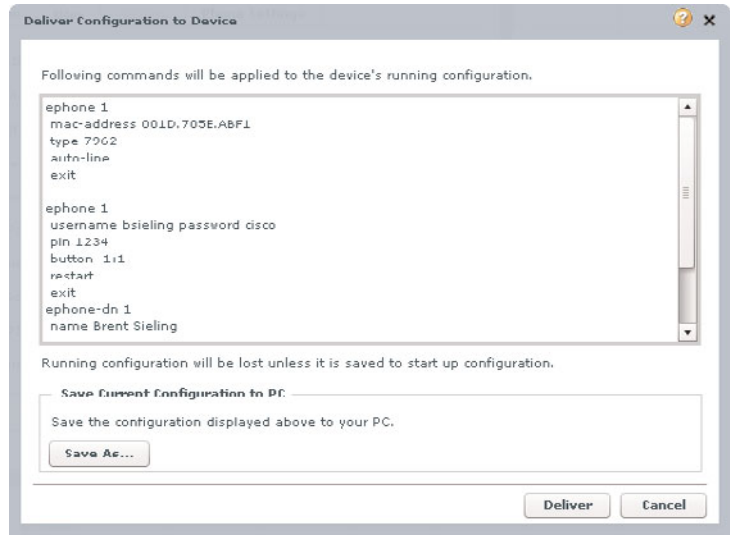
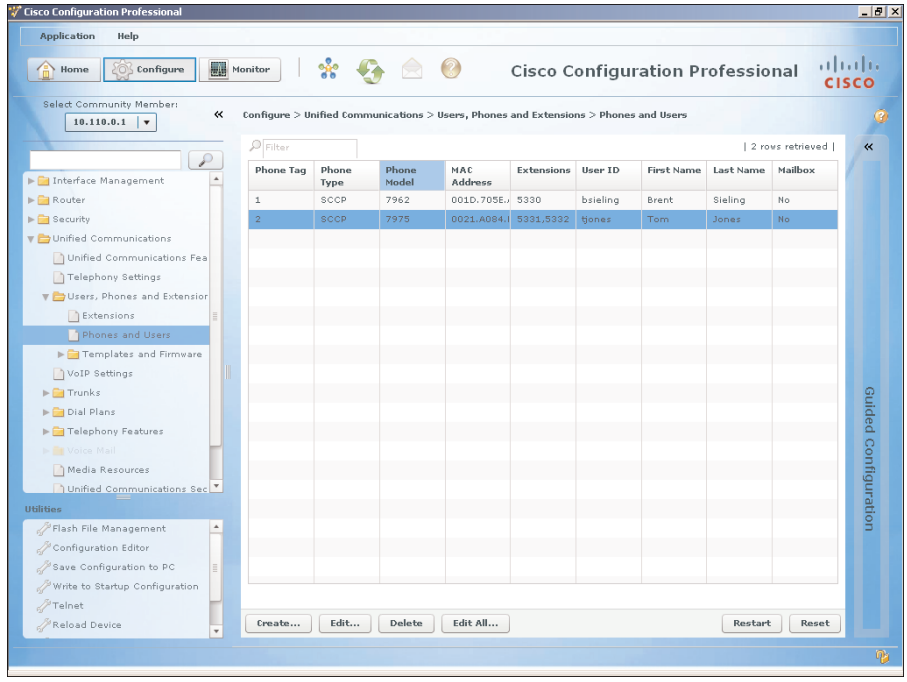


Figure 5-18 Second Phone/User



Task 5: Test and Save Configuration

Step 5-1: Make Calls

Make some calls. The phones should operate in much the same way as they did in Lab 5-2.

https://t.me/learningnets

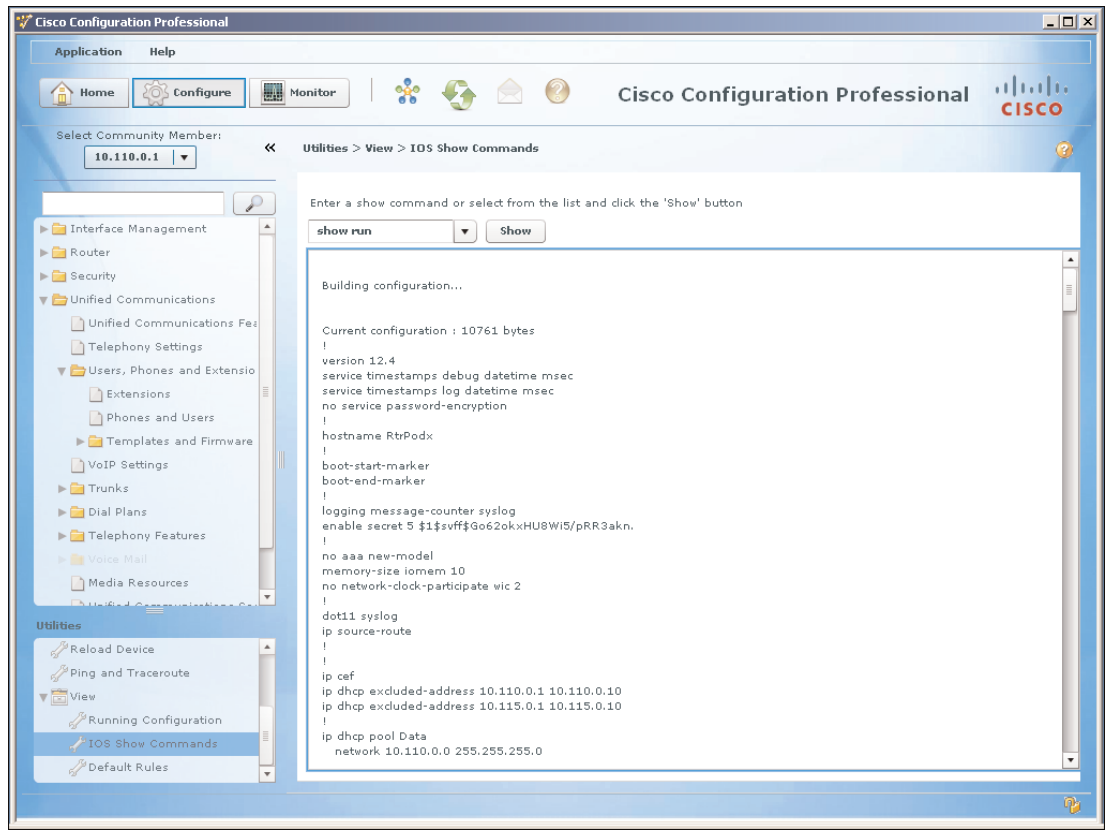
From the Library of Aliwarman Tarihoran

Step 5-2: Examine the Router Configuration

To see the running configuration of the router, in the Utilities pane (at the lower-left corner), scroll down and click the **View** menu folder icon to expand it.

1. Click the **IOS Show Commands** subitem.
2. In the IOS Show Commands pane on the right is a drop-down menu with various **show** commands.
3. Select **show run** from the list (if it is not the default item) and click the **Show** button.
5. The pane will show the output of the router, similar to Figure 5-19. There should be some differences, but also many similarities, to the configuration created in Lab 5-2.

Figure 5-19 CCP Show Run



Step 5-3: Save the Configuration

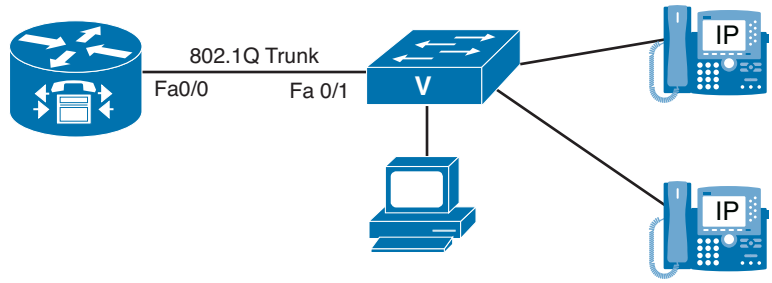
This configuration will be used in later labs, so make sure to copy the router config to a file for later use. To save the current configuration to the PC, in the Utilities pane, click **Save Configuration to PC**. See Lab 4-1, Step 3-11 for more details.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 5-4: Examine VoIP Protocols

Figure 5-20 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Lab configuration from Lab 5-2 or 5-3
- PC with Wireshark installed
- Two or more IP Phones registered (desk phone or soft phone on PC or Windows VM)

Learning Objectives

Upon completion of this lab, you will better understand

- The Skinny Call Control Protocol (SCCP) used for phone signaling
- The Real-Time Transport Protocol (RTP) used for digital voice

Scenario

SOI ran into problems, with some phones not registering, and wants to examine both the phone registration process and the protocols used for digital voice. Wireshark is well suited for this task.

Note: The use of Wireshark to capture packets on a production network without explicit authorization from the network owner can have legal implications.

Task 1: Load Prior Configurations

This lab is based on the configuration from Lab 5-2 or 5-3, and you will need to have two or more IP Phones registered. Troubleshoot if necessary.

Task 2: Establish Packet Capture

If you are using a soft phone (such as the Cisco IP Communicator) and have Wireshark installed on the same PC or VM, you are done with this task. Move on to Task 3.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

If you are planning to capture the traffic of a desk phone, it is necessary to establish the packet capture and forward the packets to the computer where Wireshark is running.

Step 2-1: Configure the Switch for Packet Capture

Cisco switches support the **monitor session** command to forward traffic for packet capture. The **monitor session** command is a CCNP-level topic, so just the basic details will be covered here. For this example, the IP Phone to be captured is in Fast Ethernet 0/3 and the PC with Wireshark is in Fast Ethernet 0/5. (You can use different ports; adjust the commands to match your configuration.) The first step is to tell the switch which port is the source of the packet capture (fa0/3):

```
SwPodx# config t
SwPodx(config)# monitor session 1 source interface fa0/3
```

The next step is to tell the switch which port is the destination of the packet capture (fa0/5):

```
SwPodx(config)# monitor session 1 destination interface fa0/5
```

You can verify that the session is working by using the **show monitor session** command. In this output, you can see that Fa0/3 is the source and Fa0/5 is the destination.

```
SwPodx# show monitor session all
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/3
Destination Ports      : Fa0/5
    Encapsulation      : Native
          Ingress      : Disabled
```

Task 3: Start Wireshark Capture

Start the Wireshark application and set it to capture traffic from the Ethernet interface connected to the switch.

Tip: To stop viewing the Spanning Tree Protocol (STP) messages every two seconds, you can use a filter. The exclamation point (!) followed by a protocol signals Wireshark not to display that protocol. To filter out STP, use **!stp** in the Wireshark filter box. To add other protocols to the filter, use two ampersands together (**&&**) between the protocols. For example, to filter out both STP and ARP, you could use **!stp && !arp** in the filter box. You can also filter traffic by source and destination MAC or IP addresses; search the web for more details.

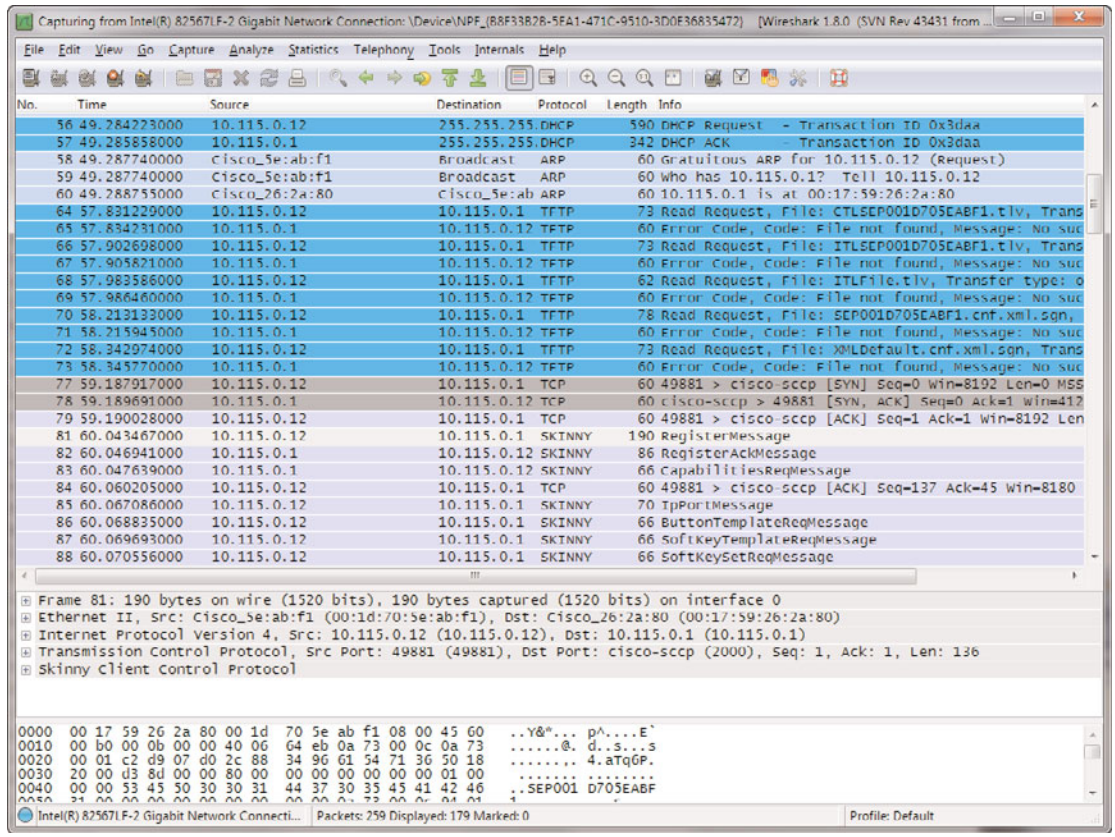
Step 3-1: Examine Phone Boot in Wireshark

To see the phone bootup process, unplug the phone (for soft phones, completely exit the software and start it back up). In Figure 5-21, you can see a partial capture of a desk phone booting. Packets 56 to 58 show the DHCP request for the IP address completing. The phone in packets 64 to 73 contacts the IP address learned from the DHCP option 150 to download files using TFTP. (In this example, the phone has registered previously, so the TFTP error messages are expected.) The phone in packets 81 and beyond uses SCCP (called SKINNY in Wireshark) to register with CUCME and get status information. Packets 86 and beyond show the phone getting information about the button and softkey templates. (There are many more SCCP messages related to the registration that are not shown.)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 5-21 Wireshark Capture of a Desk Phone Booting



After the phone has registered, you see periodic SCCP keep-alive messages. The phone keeps checking every 30 seconds (by default) to verify that the Call Agent is active and responding.

Step 3-2: Examine a Phone Call in Wireshark

With the Wireshark capture running, go off-hook on the monitored phone and dial the extension of the other IP phone. Answer the other phone and talk for a few seconds; then hang up both phones.

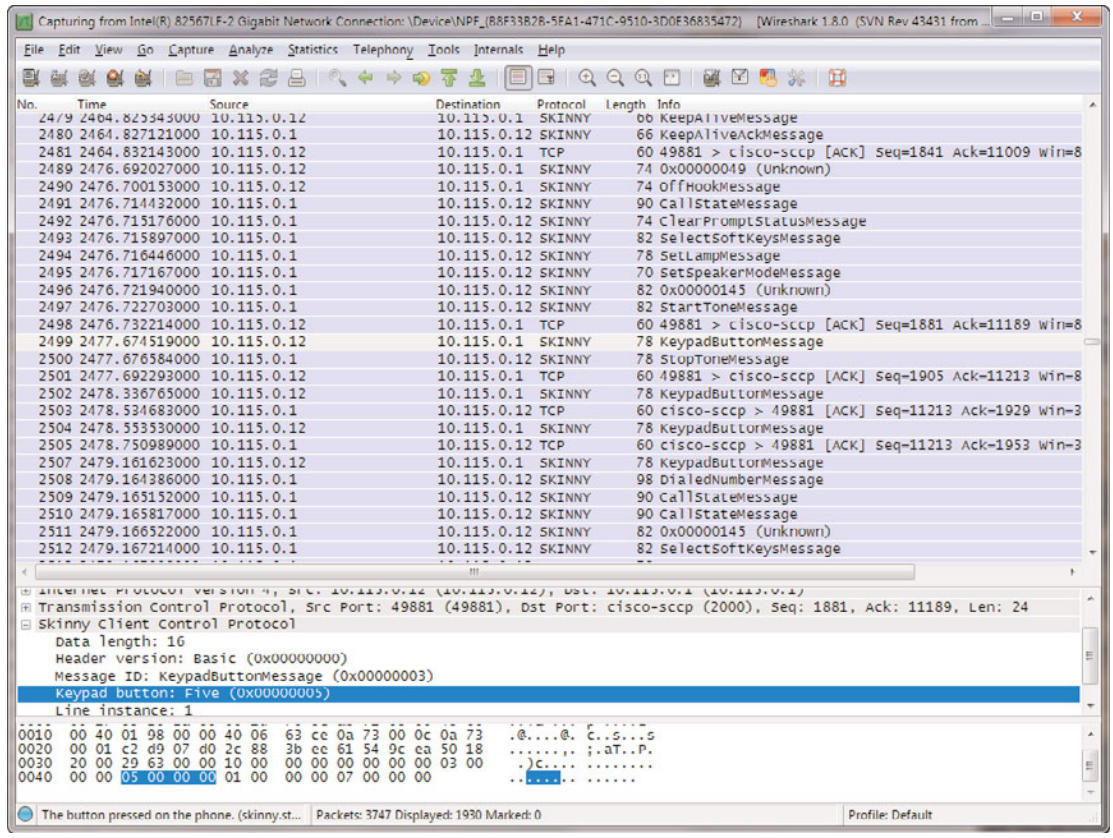
Scroll up in Wireshark to see the start of the SCCP messages for the phone call. In Figure 5-22, packets 2479 and 2480 show the keep-alive messages. Packet 2490 is the message from the phone to CUCME that the phone is now off-hook. Because the SCCP phones are essentially dumb terminals, they have to be told by CUCME to clear the display prompt message (packet 2492); to light the line button lamp green (packet 2494), showing that the line is in use; and to start playing a dial tone (packet 2497). As the phone numbers are dialed, the phone sends an SCCP message for each digit (packet 2499). In the Packet Detail pane, you can see that packet 2499 sent the message to CUCME that 5 was dialed. The phone was then told to stop playing the dial tone (packet 2500). After all the digits are sent to CUCME (packets 2499, 2502, 2504, and 2507), CUCME starts routing the call to the other phone and sends a dialed number confirmation (packet 2508). CUCME informs the phone to play the call ring-out sound (packets 2509 and 2510).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Scroll down in the capture to the packets just before the RTP protocol stream starts. In Figure 5-23, packet 2528 tells the phone to stop playing the callback (the other phone was answered) and start monitoring call statistics (packets 2530 and 2531). The call is two one-way audio streams, so packet 2532 is the start of receiving audio from the other phone while packet 2539 starts the sending audio. In the Packet Detail pane, you see that packet 2539 has selected the G.711 codec with u-law encoding for the audio. From packets 2544 and on, the audio is carried inside RTP packets. In the Info column for the RTP packets, you can see that the audio is G.711 and see the RTP sequence numbers (one for each one-way audio stream) that allow the audio to be reassembled in sequence (because RTP is carried over UDP). There are a lot of these packets! Standard RTP settings send 20 ms of audio per packet, which equals 50 packets per second (times 2 for the other audio stream).

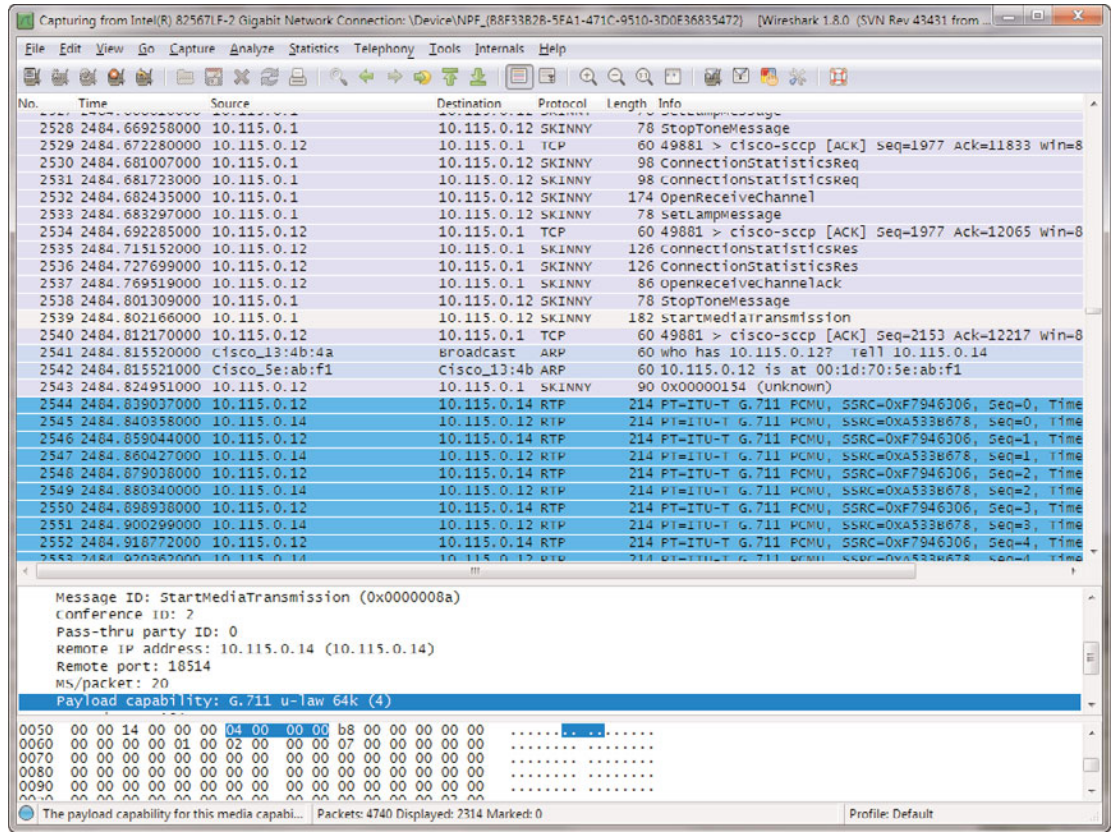
Figure 5-22 Wireshark Capture of Dialing a Phone



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 5-23 Wireshark Capture of a Phone Conversation

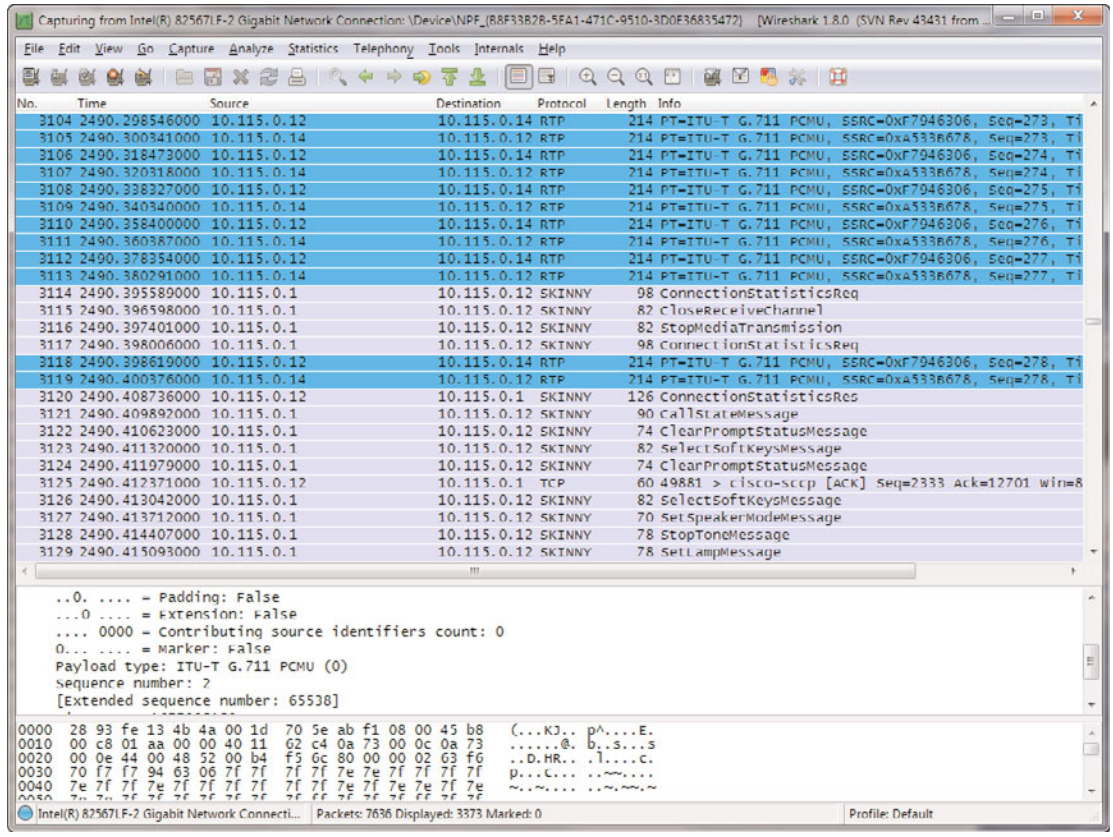


Scroll down in the capture to the packets just after the end of the RTP protocol stream. In Figure 5-24, packet 3115 shows the ending of the conversation with the request to close the receiving audio channel, while packet 3116 signals the end of sending audio. Packets 3121 to 3129 involve CUCME telling the phone to restore the phone state back to on-hook.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 5-24 Wireshark Capture of the End of a Phone Conversation



Task 4: Play Captured Audio

Wireshark has built-in analysis tools for voice traffic. Make another capture of a phone conversation, and make sure to speak into both phone handsets before you hang up. Stop the capture and find the RTP packets. Click one of the RTP packets and select the **Telephony > RTP > Stream Analysis** menu option. The Wireshark RTP Stream Analysis window will open, and you should see both the forward and reverse one-way audio streams. See Figure 5-25 for an example of this window.

Click the **Player** button. The RTP Player window will open. Click the **Decode** button. Select the small check boxes under each audio graph (on the left side). See Figure 5-26 for an example of this window.

If your computer has speakers or headphones, click the **Play** button, and Wireshark will play back the conversation. (Clearly, you can see how using Wireshark in a network without authorization could be a legal problem!)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 5-25 Wireshark RTP Stream Analysis

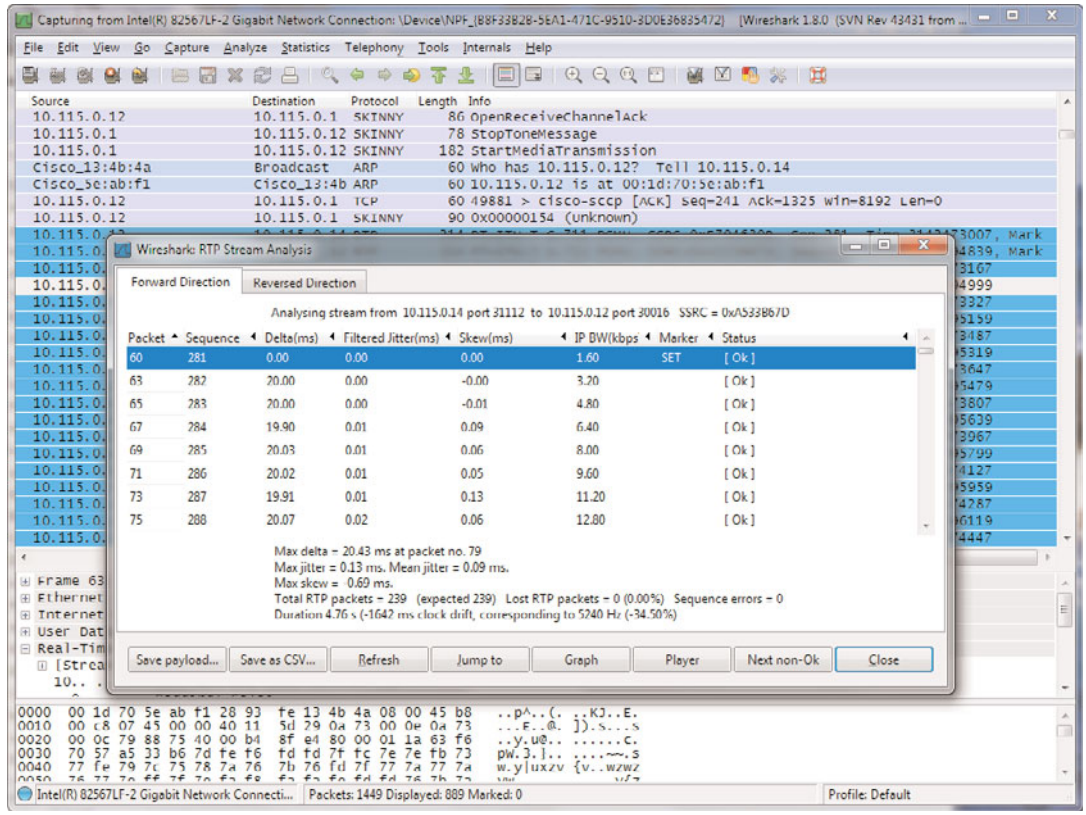
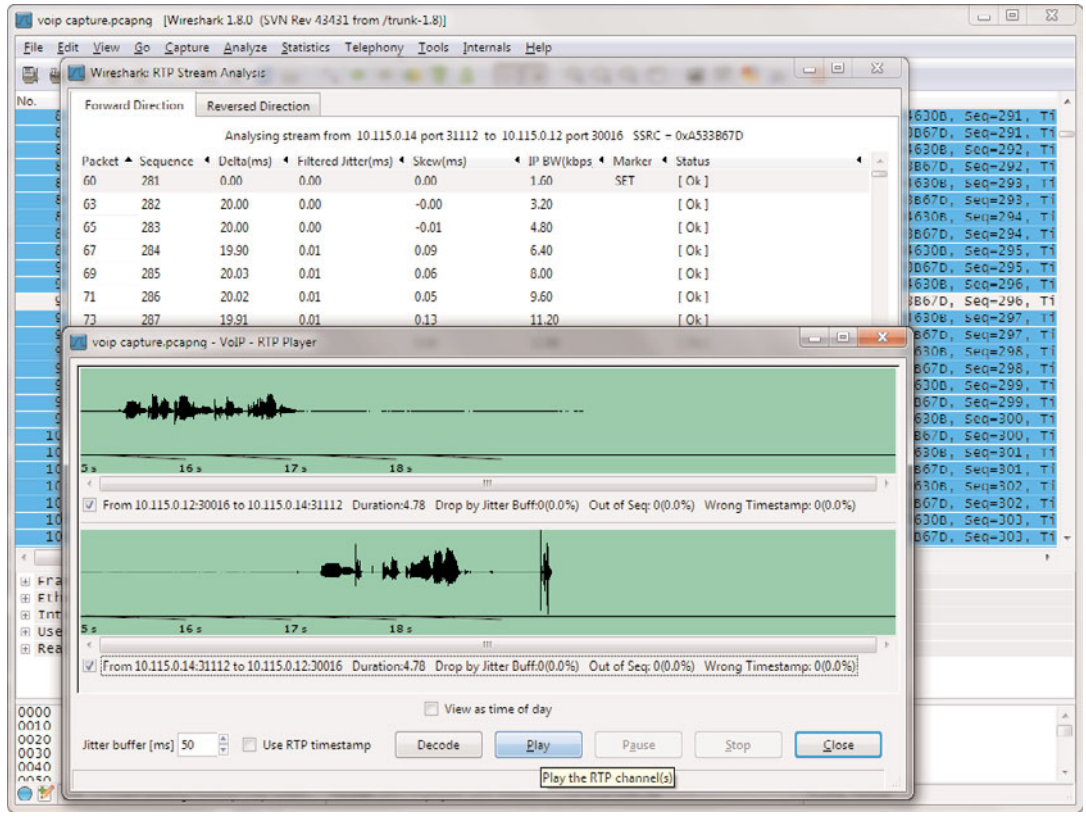


Figure 5-26 Wireshark RTP Player



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 5: Clean Up

There is no need to save the configurations from this lab, but if you do, make sure to remove the **monitor session** commands from the switch before reusing the config. Monitor sessions that are not needed waste CPU resources, and captured traffic is sent to the destination port, which can make troubleshooting difficult if left active.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CHAPTER 6

Cisco Unified Communications Manager Express (CUCME) Dial Plans and QoS

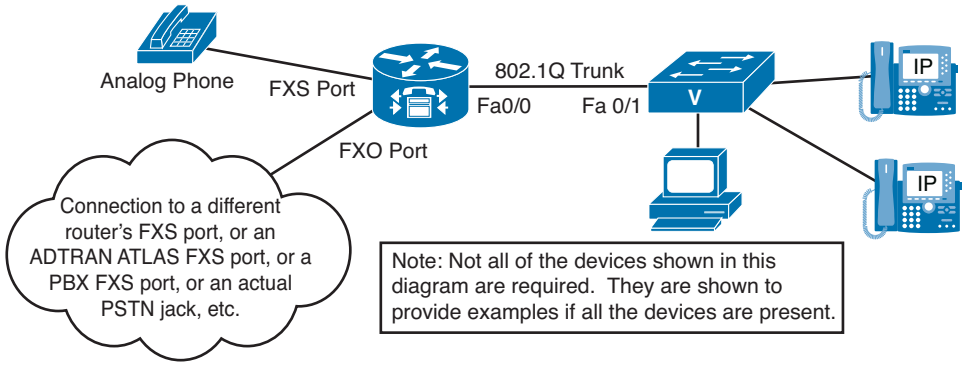
Labs in previous chapters established the ability to call between phones in your company. Now it is time to establish connections to allow phone calls to the public switched telephone network (PSTN) and branch offices. The main focus of this chapter is constructing dial peers (the process of routing phone calls) and exploring quality of service (QoS) concepts and mechanisms.

There are two types of dial peers: Voice over Internet Protocol (VoIP) and plain old telephone service (POTS). Implementing VoIP dial peers only requires an IP connection between two routers. Implementing POTS dial peers requires either analog or digital interfaces. The first two labs are optional and introduce configuring analog and digital interfaces. If you don't have access to these interfaces, just read the labs.

Note: Both analog and digital interfaces require digital signal processor (DSP) resources on the router to function. Check the hardware section in the Introduction for more details.

Lab 6-1: (Optional) Configuring Analog Interfaces

Figure 6-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Lab configuration from either Lab 5-2 or 5-3
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)
- Analog Foreign eXchange Station (FXS) card (optional)
- Analog Foreign eXchange Office (FXO) card (optional)
- Digital signal processor (DSP) resources in the router, which are packet voice DSP modules (PVDM) modules to enable the FXS or FXO ports

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Learning Objectives

Upon completion of this lab, you will be able to

- Configure the basics of analog FXS interfaces
- Configure the basics of analog FXO interfaces

Scenario

Shiny Objects Inc. (SOI) wants to use devices with analog connections, such as analog phones, alarm systems, fax machines, modems, and so on. Connecting analog devices to the router will require either FXS ports in the router or an analog telephone adapter (such as a Cisco ATA 186). This lab will focus on FXS and FXO ports in the router. FXS ports allow the router to act like a central office switch or PBX and provide service to analog phones, including power, collecting dialed digits, responding with call progress tones, and so on.

SOI also wants to connect the system to make and receive phone calls from the PSTN. Analog FXO ports allow the router to act like an analog phone. The router expects to receive power and signaling from the other end and can answer calls, dial digits, and so on.

Task 1: Load Prior Configurations

This lab is based on the configuration from either Lab 5-2 or 5-3. If necessary, load the configuration for both the switch and router. Connect a PC to the switch and verify that it can ping the router and switch management addresses. Connect the VoIP phones and verify that you can call between them. Troubleshoot if necessary.

Task 2: Examine the Interfaces in the Router

Use the **show voice port summary** command to examine the interfaces available in your router. In the output shown, there are four FXO interfaces (in ports 0/0/0 to 0/0/3) and two FXS interfaces (in ports 0/1/0 and 0/1/1). Notice that every ephone-dn created also shows in the output as an EFXS with a virtual port number. The highlighted directory number on virtual port 50/0/1 has two channels (because the directory number was created as dual-line). CUCME automatically creates virtual voice ports for every ephone-dn.

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

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
50/0/1          1      efxs     up    dorm on-hook  idle     y
50/0/1          2      efxs     up    dorm on-hook  idle     y
50/0/2          1      efxs     up    dorm on-hook  idle     y
50/0/2          2      efxs     up    dorm on-hook  idle     y
```

Task 3: Configuring FXS Ports

In most cases, the default options for FXS ports will be fine, but you might want to change some of them. The settings are applied to the individual voice ports, as shown in the output of the **show voice port summary** command. All the commands in the steps for this task demonstrate an FXS port configured in voice port 0/1/0. Change the port number as needed to fit your hardware configuration.

```
RtrPodx(config)# voice-port 0/1/0
RtrPodx(config-voiceport)#
```

Step 3-1: Call Signaling Selection

In Chapter 1, "Traditional and Unified Voice," you learned about ground start and loop start signaling for analog phones. The default for FXS ports is loop start (most common analog devices use loop-start signaling). However, if you need to change the signaling to ground start, you would use the **signal** command in the voice-port configuration.

```
RtrPodx(config-voiceport)# signal ?
  groundStart  Ground Start
  loopStart    Loop Start
```

Step 3-2: Connect an Analog Phone and Make a Call

Connect an analog phone to the port. If you lift the receiver, you should hear a dial tone. (If not, make sure that you are connected to the FXS port, not the FXO ports.) Even without any configuration, the analog phone can make calls. From the analog phone, call the extension of a VoIP phone. The VoIP phone should ring and show "From Unknown Number" on the display. Answer the call to verify that it works as expected. (At this point, there is no way for the VoIP phones to call the analog phone.)

Step 3-3: Call Progress Tones

If you have never left your home country, it might surprise you to learn that the familiar call signaling for things like dial tone and busy signal are not standardized worldwide. The FXS ports default to the standard used in the United States, but they can be changed to match the standard in any country using the **cptone** command in the voice-port configuration.

```
RtrPodx(config-voiceport)# cptone ?
  locale   2 letter ISO-3166 country code
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

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

You might want to try CN (China), DE (Germany), FI (Finland), IN (India), VE (Venezuela), and ZW (Zimbabwe) to hear some of the differences. Use US to return to the default.

Step 3-4: Description Information

While the **description** command should be familiar to anyone who has CCNA-level knowledge, it can be easy to forget. A good use of the **description** command is to indicate the location of the analog device.

```
RtrPodx(config-voiceport)# description Fax Machine in Rm 119 - Jack 119/5
```

Step 3-5: Caller ID Information

The most common commands needed for the FXS ports are those for Caller ID information. The **station-id name** and **station-id number** commands configure the information for use with Caller ID. Use the number assigned in the FXS #1 column from the Pod Addressing table in Appendix A for your phone.

```
RtrPodx(config-voiceport)# station-id name Fax Machine
RtrPodx(config-voiceport)# station-id number number_for_your_FXS
```

Now that Caller ID information is assigned, call from the analog phone to the VoIP phone again. This time, the name and number will show. Despite the Caller ID number showing on the display, there is still no way for the VoIP phones to call the analog phone. To make such calls work requires dial peers, which are discussed in Lab 6-3.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-6: Examine Interface Status

Call from the analog phone to the VoIP phone again, and issue the **show voice port summary** command before hanging up. From the output, you can see that both the analog and VoIP phones are off-hook and in a call. (But from the output shown, you cannot tell that they are talking to each other.)

```
RtrPodx# show voice port summary
                                          IN       OUT
PORT            CH   SIG-TYPE   ADMIN OPER STATUS   STATUS   EC
=============== == ============ ===== ==== ======== ======== ==
0/0/0           --  fxo-ls      up    dorm idle     on-hook  y
0/0/1           --  fxo-ls      up    dorm idle     on-hook  y
0/0/2           --  fxo-ls      up    dorm idle     on-hook  y
0/0/3           --  fxo-ls      up    dorm idle     on-hook  y
0/1/0           --  fxs-ls      up    up   off-hook idle     y
0/1/1           --  fxs-ls      up    dorm on-hook  idle     y
50/0/1          1      efxs     up    dorm off-hook idle     y
50/0/1          2      efxs     up    dorm off-hook idle     y
50/0/2          1      efxs     up    dorm on-hook  idle     y
<output omitted>
```

Step 3-7: Automatically Dialing Phones

In some cases, it is desirable to have a phone automatically call a preconfigured number when the receiver is lifted. Emergency phones and loading dock and lobby phones that connect to after-hours security are examples of this. The ability to forward the calls is configured with the **connection plar** command (PLAR stands for Private Line Automatic Ringdown).

```
RtrPodx(config-voiceport)# connection plar extension_on_voip_phone
```

When the receiver of the analog phone is lifted, the VoIP phone will start ringing. When you are done testing, to avoid unexpected outcomes later, remove the **connection plar** command.

```
RtrPodx(config-voiceport)# no connection plar
```

Task 4: Configuring FXO Ports

In most cases, the default options for FXO ports will be fine, but you might want to change some of them. All the commands in the steps for this task demonstrate an FXO port configured in voice port 0/0/0. Change the port number as needed to fit your hardware configuration.

```
RtrPodx(config)# voice-port 0/0/0
RtrPodx(config-voiceport)#
```

Step 4-1: Configure Dial Type

In most cases, the router will be connected to systems supporting dual-tone multifrequency (DTMF) for dial tones. However, the PSTN in some parts of the world, or a port on a PBX system, might only

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

work with pulse dialing. (Most analog phones sold today still have a tone/pulse switch on them for this reason.) The **dial-type** command allows you to change the default of dtmf to pulse.

```
RtrPodx(config-voiceport)# dial-type ?
  dtmf   touch-tone dialer
  mf     mf-tone dialer
  pulse  pulse dialer
```

Step 4-2: Configure Ring Number

The router defaults to answering on the first ring. If necessary, this can be changed using the **ring number** command to increase the number of rings before the router answers.

```
RtrPodx(config-voiceport)# ring number ?
  <1-10>  The number of rings detected before closing loop
```

Step 4-3: Description Information

A good use of the **description** command might include identifying information for the connection, such as carrier ID, circuit ID, and phone number. This information will help if it is necessary to contact the carrier for troubleshooting.

```
RtrPodx(config-voiceport)# description ATT circuit SD12345 number 555-1212
```

Step 4-4: Connect the FXO Port (Optional)

Using an FXO port is harder to do in a lab (at this point) because the port needs to receive services from another device. While you can connect the FXO port of this router to the FXS port of another router, calls cannot be placed out of the FXS port until dial peers are introduced.

However, if you have access to a live PSTN connection, a preconfigured Adtran Atlas FXS port, or another router FXS port that is preconfigured and can send calls to this port, you can connect it at this time.

Note: If you call the number that is connected to the FXO port, the router will answer and then play a dial tone. This might seem odd, but from the router's perspective, the phone rang and it answered the call. Unlike a person, the router is unable to say, "Hello! Who would you like to speak to?" So it responds with a dial tone to allow the caller to enter the extension. If you dial the extension of an internal phone, the router will direct the call to that phone. This behavior will be fixed in the next step.

Step 4-5: Redirect Incoming Calls (Optional)

Naturally, calling a phone number and hearing a second dial tone without any information is not very caller oriented. The solution to this problem is to tell the router when the phone rings to redirect the call to another number. This number could be the company receptionist, a call center, or an automated attendant that can respond appropriately ("Welcome to Shiny Objects Incorporated. If you know the extension of your party, you can dial it at any time; otherwise press 1 for the company directory, press 2 for . . .").

The ability to forward the calls is configured with the same **connection plar** command used with FXS ports.

```
RtrPodx(config-voiceport)# connection plar extension_on_voip_phone
```

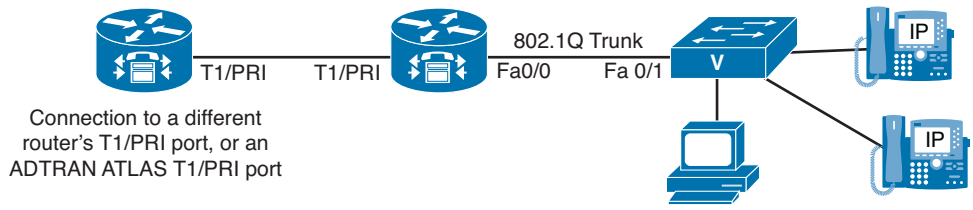
Now any call to the FXO port will be redirected, and the VoIP phone will start ringing.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 6-2: (Optional) Configuring Digital Interfaces

Figure 6-2 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Lab configuration from Lab 5-2, 5-3, or 6-1
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)
- T1/E1/PRI Multiflex Trunk Voice WAN Interface Cards (VWIC) card or Network Module (optional)
- DSP resources in the router (PVDM chips) to enable the Multiflex Trunk
- Another device with a T1/E1/PRI Trunk (optional)

Note: Older digital T1 interfaces such as the DSU-T1 WAN Interface Cards (WICs) will not work for VoIP on the router. To work with VoIP traffic, a Multiflex VIC (Voice Interface Card) that supports both voice and data is required. Check the hardware section of the Introduction for more details. These cards also require DSP resources.

Learning Objective

Upon completion of this lab, you will be able to configure the basics of T1/E1/PRI interfaces.

Scenario

SOI expects to have enough incoming and outgoing calls that it wants to use a digital connection to the PSTN. Not only do digital connections provide a trunk with 23 (PRI), 24 (T1), or 30 (E1) simultaneous calls on a single cable, but they also have enhanced features, such as Direct Inward Dialing (DID), that allow the PSTN to signal the extension that the incoming call should be connected to. As discussed in Chapter 1, there are two types of signaling: common channel signaling (CCS) and channel associated signaling (CAS) (also known as robbed-bit signaling). There are two types of time-division multiplexing (TDM), which impacts the number of channels available. The T1 format is common in the United States and Japan (24 channels), and E1 is common elsewhere (32 channels).

Task 1: Load Prior Configurations

This lab is based on the configuration from Lab 5-2, 5-3, or 6-1. If necessary, load the configuration for both the switch and router. Connect a PC to the switch and verify that it can ping the router and

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

switch management addresses. Connect the VoIP phones and verify that you can call between them. Troubleshoot if necessary.

Task 2: Examine Resources in the Router

Step 2-1: Examine Hardware

Use the **show hardware** command to examine the interfaces available in your router. In the output, you should see the model of your router and the amount of memory installed, followed by a listing of the interfaces installed. You are looking for a line like one (or more) of the following:

- 1 Channelized/Clear T1/PRI port
- 1 Channelized/Clear E1/PRI port
- 1 Channelized (E1 or T1)/PRI module

Note: If you see the last option (E1 or T1), or if you see in the running config a comment that starts with **! card type command needed for**, you have a newer VWIC (such as the VWIC2-1MFT-T1/E1 card) that will support either a T1 or an E1, and you must select which mode before you can complete the later steps.

The command to select a T1 is

RtrPod*x*(config)# **card type t1** *x y*

(*x* is the module slot number and *y* is the subslot number.)

The command to select a E1 is

RtrPod*x*(config)# **card type e1** *x y*

(*x* is the module slot number and *y* is the subslot number.)

For example, to configure a VWIC2-1MFT-T1/E1 card in HWIC slot 2 to be a T1, you would use **card type t1 0 2**, while a network module in slot 1 would use **card type t1 1 0**.

If you have a fixed T1 or E1, this command will not work; it is only needed for the newer combination T1/E1 cards.

Step 2-2: Examine Controller Interface

To achieve the output this lab shows, the T1 or E1 should be connected to another device with a T1 or E1 interface using a T1 crossover cable to keep the interface up. The other device does not have to be configured at this time. After the cable is connected between the systems, the amber Alarm LED will be lit if the two cards are not configured the same, and just the green Carrier Detect LED will be lit if the carrier is present.

Note: A T1 crossover cable is *not* the same as an Ethernet crossover cable. T1 crossover cables have a different pinout. They are not difficult to make if you have cable-making supplies, or they can be purchased premade.

Before configuring the controller, it is useful to examine the current configuration of the interface. In the following output, notice that the controller T1 0/2/0 in this 2811 router has default values for framing of ESF, line coding of B8ZS, and a clock source of Line. Your output can vary, as the same card in a 2621XM router has default values for framing of SF and line coding of AMI.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
RtrPodx# show controllers t1
T1 0/2/0 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Version info Firmware: 20090113, FPGA: 20, spm_count = 0
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  CRC Threshold is 320. Reported from firmware  is 320.
  Data in current interval (454 seconds elapsed):
     2 Line Code Violations, 1 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 1 Line Err Secs, 1 Degraded Mins
     1 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Step 2-3: Examine DSP Resources

DSP resources need to be available in your system to configure the interface. The number of resources can be examined using the **show voice dsp group all** command. (Exception: The 2600XM routers with VOICE-30 or ATM-VOICE-30 AIM cards don't show their DSP resources in the output.) In the following output, the 2811 router has two PVDM2-16 modules installed. Six of the channels are already used for the two FXS and four FXO ports, leaving 26 channels available. A full T1 PRI will need 23 channels. If there are fewer resources available than required, either more DSPs are required or a fractional PRI will need to be configured.

```
RtrPodx# show voice dsp group all
DSP groups on slot 0:
dsp 1:
  State: UP, firmware: 24.3.2
  Max signal/voice channel: 16/16
  Max credits: 240
  num_of_sig_chnls_allocated: 0
  Transcoding channels allocated: 0
  Group: FLEX_GROUP_VOICE, complexity: FLEX
    Shared credits: 240, reserved credits: 0
    Signaling channels allocated: 0
    Voice channels allocated: 0
    Credits used: 0

dsp 2:
  State: UP, firmware: 24.3.2
  Max signal/voice channel: 16/16
  Max credits: 240
  num_of_sig_chnls_allocated: 6
  Transcoding channels allocated: 0
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
  Group: FLEX_GROUP_VOICE, complexity: FLEX
    Shared credits: 240, reserved credits: 0
    Signaling channels allocated: 6
    Voice channels allocated: 0
    Credits used: 0
```

Task 3: Configure CCS (PRI) Settings

The most common signaling for a digital voice trunk is CCS with ISDN PRI as the protocol. The output in this task shows configuring a T1 line as an ISDN PRI.

Step 3-1: Configure ISDN Switch Type

The first step when configuring a PRI is to select the type of switch the service provider uses. For the lab, if connecting to another Cisco router, use the **primary-ni** option.

```
RtrPodx(config)# isdn switch-type ?
  primary-4ess    Lucent 4ESS switch type for the U.S.
  primary-5ess    Lucent 5ESS switch type for the U.S.
  primary-dms100  Northern Telecom DMS-100 switch type for the U.S.
  primary-dpnss   DPNSS switch type for Europe
  primary-net5    NET5 switch type for UK, Europe, Asia and Australia
  primary-ni      National ISDN Switch type for the U.S.
  primary-ntt     NTT switch type for Japan
  primary-qsig    QSIG switch type
  primary-ts014   TS014 switch type for Australia (obsolete)

RtrPodx(config)# isdn switch-type primary-ni
```

Step 3-2: Configure Clock Participation

The **network-clock-participate** command is used to keep multiple interfaces synchronized to the same clock signal. For routers with a VIC, use the following:

```
RtrPodx(config)# network-clock-participate wic x (x is just the wic physical subslot
  number, without any slashes)
```

For routers with a network module, use the following:

```
RtrPodx(config)# network-clock-participate slot x (x is just the physical slot
  number, without any slashes)
```

Note: Some router models require this command, such as the 2800 Series, while routers such as the 2600XM Series do not.

Step 3-3: Configure Controller T1 Settings

The next step is to configure the settings on the T1 controller. (Even though you are configuring the interface as an ISDN PRI, it is still a T1 interface.) The framing, line coding, and clock source should be configured to match the service provider. (The most common settings in the United States are ESF

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

for framing and B8ZS for line coding.) For a connection to a service provider, the clock source should be set to line, but if the router is connected to a PBX, the router might need to provide the clocking, and then the clock source should be internal.

```
RtrPodx(config)# controller t1 x/x/x (slot/subslot/port as identified in the show
  controller T1 command)
RtrPodx(config-controller)# framing esf
RtrPodx(config-controller)# linecode b8zs
RtrPodx(config-controller)# clock source line
```

Step 3-4: Configure PRI Timeslots

There are two limiting factors that control how many timeslots can be allocated. The first is the number of channels the service provider has allocated. With fractional PRI service, the service provider only allocates the number of channels the company pays for. If you allocate more channels than the provider allocated, calls on the extra channels will not complete. The second limit is the amount of DSP resources available in your system, as examined in Step 2-3. For example, if you try to configure all 23 channels of a PRI, but only have enough DSP resources for 16 channels, you will get the following messages:

```
% Not enough DSP resources available to configure pri-group on controller T1 0/2/0
% The remaining dsp resources are enough for 16 time slots.
% For current codec complexity, 1 extra dsp(s) are required to create this voice
  port.
```

Before configuring the timeslots on your system, determine the number of channels that both systems can be configured to use and what resources are available. Use the information in Step 2-3 to determine the number of DSP channels the routers have available. In the following output, the other router (acting as a service provider) has six channels configured, so this router is configured to match it using the **pri-group timeslots** command. When the command is issued, the six channels will be created.

```
RtrPodx(config-controller)# pri-group timeslots 1-6
*Jan 30 08:07:52.845: %LINK-3-UPDOWN: Interface ISDN-VOICE 0/2/0:23(1), changed state
  to up
*Jan 30 08:07:52.845: %LINK-3-UPDOWN: Interface ISDN-VOICE 0/2/0:23(2), changed state
  to up
*Jan 30 08:07:52.845: %LINK-3-UPDOWN: Interface ISDN-VOICE 0/2/0:23(3), changed state
  to up
*Jan 30 08:07:52.845: %LINK-3-UPDOWN: Interface ISDN-VOICE 0/2/0:23(4), changed state
  to up
*Jan 30 08:07:52.849: %LINK-3-UPDOWN: Interface ISDN-VOICE 0/2/0:23(5), changed state
  to up
*Jan 30 08:07:52.849: %LINK-3-UPDOWN: Interface ISDN-VOICE 0/2/0:23(6), changed state
  to up
*Jan 30 08:07:52.861: %ISDN-6-LAYER2UP: Layer 2 for Interface Se0/2/0:23, TEI 0
  changed to up
*Jan 30 08:07:53.817: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:0,
  changed state to down
*Jan 30 08:07:53.821: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:1,
  changed state to down
*Jan 30 08:07:53.821: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:2,
  changed state to down
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
*Jan 30 08:07:53.821: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:3,
  changed state to down
*Jan 30 08:07:53.825: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:4,
  changed state to down
*Jan 30 08:07:53.825: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:5,
  changed state to down
*Jan 30 08:07:53.829: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:23,
  changed state to up
*Jan 30 08:07:54.833: %LINK-3-UPDOWN: Interface Serial0/2/0:23, changed state to up
```

If you encounter any problems, verify that all the steps have been completed correctly.

Step 3-5: Examine the Interfaces

Now that the PRI is configured, examine the changes to the router. Start with the **show isdn status** command to verify that Layer 1 is Active and Layer 2 is Established, as shown in the following output.

```
RtrPodx# show isdn status
Global ISDN Switchtype = primary-ni
ISDN Serial0/2/0:23 interface
        dsl 2, interface ISDN Switchtype = primary-ni
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 2 CCBs = 0
    The Free Channel Mask:  0x800000FF
    Number of L2 Discards = 0, L2 Session ID = 2
    Total Allocated ISDN CCBs = 0
```

Then, look at the output of the **show voice port summary** command. Notice in the following output that the signaling port is 0/2/0:23 with six channels. (While the 24th channel is used for signaling, Cisco starts interface numbering with 0, so it becomes channel 23 in the interface output.)

```
RtrPodx# show voice port summary
                                          IN       OUT
PORT            CH   SIG-TYPE   ADMIN OPER STATUS   STATUS   EC
=============== == ============ ===== ==== ======== ======== ==
0/0/0           --  fxo-ls      up    dorm idle     on-hook  y
0/0/1           --  fxo-ls      up    dorm idle     on-hook  y
0/0/2           --  fxo-ls      up    dorm idle     on-hook  y
0/0/3           --  fxo-ls      up    dorm idle     on-hook  y
0/2/0:23        01  isdn-voice  up    dorm none     none     y
0/2/0:23        02  isdn-voice  up    dorm none     none     y
0/2/0:23        03  isdn-voice  up    dorm none     none     y
0/2/0:23        04  isdn-voice  up    dorm none     none     y
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
0/2/0:23         05  isdn-voice  up    dorm none     none     y
0/2/0:23         06  isdn-voice  up    dorm none     none     y
0/1/0            --  fxs-ls      up    dorm on-hook  idle     y
<output omitted>
```

Task 4: Configure ISDN Network End

Note: This task is only needed on a second router that will be connected to the first. If you are configuring the PSTN simulator in Appendix E, "PSTN Simulator," this command is already included in that configuration.

In the same way that connecting two routers back to back in a lab with a serial cable requires one of them to be the data communications equipment (DCE) and provide the clocking, ISDN needs one of the devices to act as the network end to match the subscriber end. (Configuring a Cisco router to act as the service provider equipment could also be done to provide a connection to a PBX.) There are only a few differences to the configuration previously demonstrated.

Configure the other router's T1 interface as shown in Tasks 2 and 3. Then configure the signaling channel using the serial interface port 23 (for a PRI). For example, if the T1 controller is in port 0/2/0, use the **interface serial 0/2/0:23** command for the signaling interface. Enter the **isdn protocol-emulate network** command to take the role of service provider.

```
OtherRtr(config)# interface serial 0/2/0:23
OtherRtr(config-if)# isdn protocol-emulate network
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 6-3: Call Legs, Dial Peers, and Wildcards

Equipment Required

No equipment is required for this lab.

Learning Objectives

Upon completion of this lab, you will be able to

- Understand the concept of call legs
- Understand POTS and VoIP dial peers
- Create POTS and VoIP dial peers

Scenario

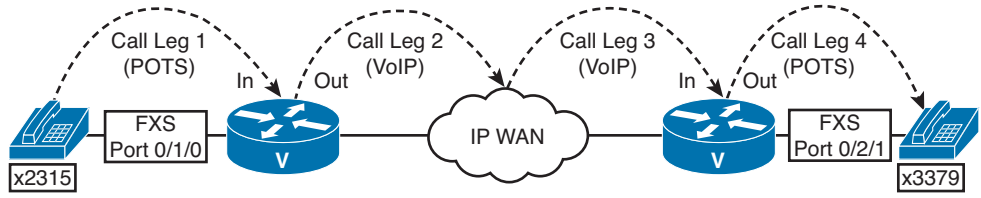
This lab introduces the concepts of call legs, dial peers, and wildcards. Dial peers are the telephony equivalent of static IP routing in data networks; they direct calls to the proper destination. There are two main types of dial peers: POTS and VoIP. The process to create both is covered in this lab, as well as how wildcards can be used to simplify the number of dial peers needed. Before exploring dial peer creation, it is necessary to explore the concepts of dial plans and call legs.

Task 1: Call Legs

Step 1-1: Understanding Call Legs

Anytime a call connects to or exits from a voice gateway, there needs to be a dial peer to direct the call, just as packets in a data network require the use of a routing table. These call connections into or out of the voice gateway are referred to as call legs. There are two types of connections to the voice gateway used in these labs: traditional phone service (plain old telephone service, or POTS) and VoIP. See Figure 6-3 for an illustration of call legs.

Figure 6-3 One-Way Call Legs from One Analog Phone to Another on Separate Routers



Note that with just these four call legs, 2315 can call 3379 and have a conversation, but 3379 cannot call 2315 without an additional four call legs going the other way! With data networks, if PC A can ping to PC B, we can assume that PC B can also ping PC A (unless there are access lists). This logic is not true in voice networks. Just because Caller A can reach Caller B and have a conversation, it does not automatically mean that Caller B can dial Caller A.

In some cases, a dial peer can serve as both the inbound and outbound call legs. In Figure 6-3, the dial peer that creates the outbound call leg to phone 3379 uses the POTS **dial-peer port** command, which allows it to also serve as the inbound call leg from phone 3379.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Introduction to Dial Peers

To make call legs work, we use dial peers. A dial peer is similar in function to a static route statement in data networking, as the dial peer matches a dialed number or numbers and directs the call to its destination. The two types of dial peers used in these labs are POTS and VoIP. The following is an example of both types:

```
dial-peer voice 15 pots
destination-pattern 1234
port 0/1/0

dial-peer voice 6 voip
destination-pattern 5555678
session target ipv4:10.0.10.100
```

Both types of dial peers start with the **dial-peer voice** *tag* command. The tag is a number from 1 to 2147483647 (unique to a gateway) that identifies the individual dial peer. As you can see from the previous output, the tag used does not have any connection to the digits matched. However, in some cases, to organize the dial peers, a tag will be used that is the same as, or identifies, the matching digits. The tag is followed by the **pots** or **voip** keyword. The primary difference between the two will be whether the call is switched to a port or sent to an IP-based network.

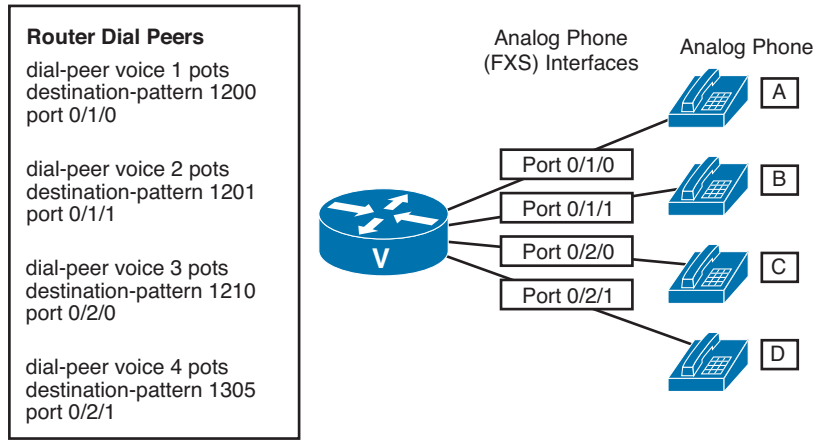
The actual matching of dialed digits is done by the **destination-pattern** command. The destination pattern can be an exact match or, by using wildcards, a range of digits. In both previous outputs, the destination pattern will match a specific dialed number. More details on using wildcards will be provided later in the lab.

The final part of the dial peer is the target. POTS dial peers use the **port** command to identify the analog or digital interface to switch the call to. VoIP dial peers use the **session target** command to direct the call to a remote gateway. Unlike a static route statement, the **session target** command identifies the final destination IP address, not the next-hop IP address.

Step 2-1: Call Flow with a Single-Router Dial Peer Exercise

Use the configuration in Figure 6-4 to complete Table 6-1 by determining the numbers dialed, the dial peers, and the ports used to complete the call. The first two lines are already completed for you.

Figure 6-4 Single Router with Four Analog Phones and Dial Peers



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Table 6-1 Call Completion Table

Calling Phone	Called Phone	Calling Number	Called Number	Dial Peer Used to Reach Destination	Port Used to Reach Destination
A	B	1200	1201	2	0/1/1
D	C	1305	1210	3	0/2/0
C	A				
B	A				
D	B				
A	D				
B	C				
C	D				

Step 2-2: Create POTS Dial Peers

Use the configuration and diagram in Figure 6-5 to complete Table 6-2 by determining the numbers dialed, the dial peers, and the ports used to complete the call. The first configuration is already completed for you.

Figure 6-5 Topology Diagram

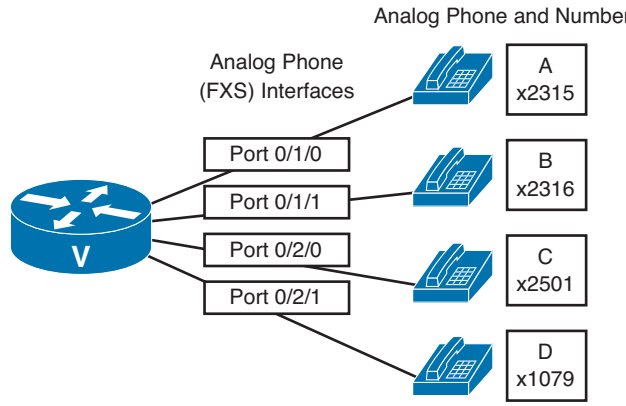


Table 6-2 Dial Peer Configuration

Phone	Dial Peer
A	dial-peer voice 1 pots destination-pattern 2315 port 0/1/0
B	_____ _____ _____

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Phone	Dial Peer
C	_____ _____ _____
D	_____ _____ _____ _____

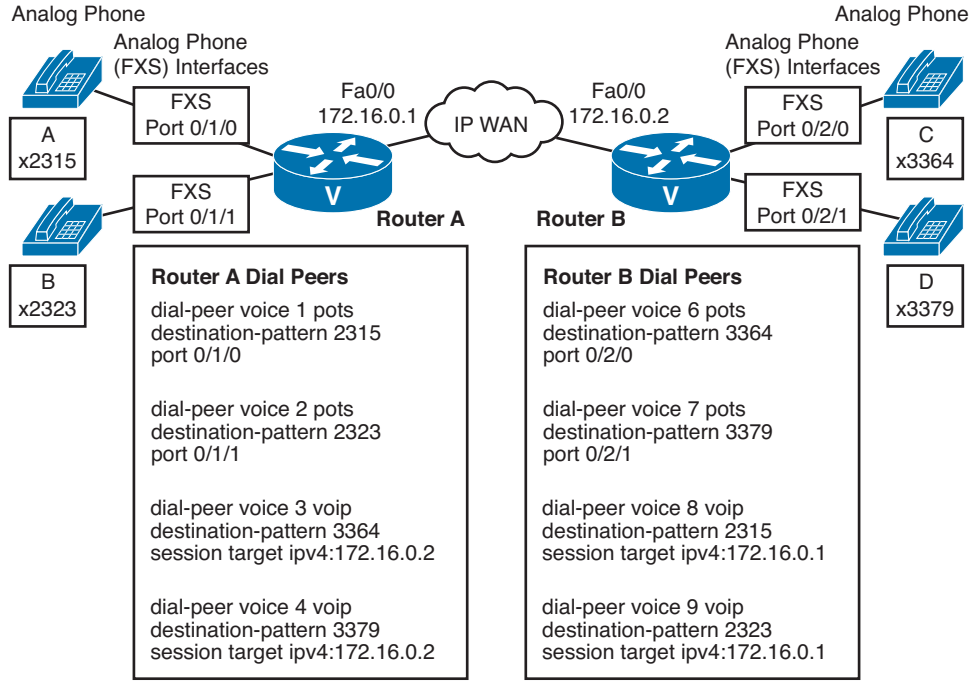
Step 2-3: Call Flow for Dual-Router Dial Peers Without Wildcards Exercise

Use the configuration and diagram in Figure 6-6 to complete Table 6-3 by determining the numbers dialed, the dial peers, and the ports used to complete the call. The first two lines are already completed for you.

Note: Normally, you would not create a separate VoIP dial peer for each remote phone; instead you would use wildcards. Wildcards will be introduced in the next task.

Notice that unlike the POTS dial peers in the previous examples, the VoIP dial peers used here have the IP address of the remote router as the session target. Because the tag used for the dial peer is unique to the router, Router B could have used dial peers 1 to 4 too, but different numbers were used to make determining the answers here easier.

Figure 6-6 Dual-Router Dial Peers (Without Using Wildcards)



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Table 6-3 Call Completion Table

Calling Phone	Called Phone	VoIP Dial Peer (If Used)	POTS Dial Peer Used to Reach Destination	Port Used to Reach Destination
A	B	—	2	0/1/1
B	D	4	7	0/2/1
C	A			
B	C			
D	B			
A	D			
A	C			
C	D	—		

Task 3: Introduction to Wildcards in Cisco Unified Communications Manager Express (CUCME)

Creating a dial peer for every remote phone would quickly become unworkable. Most phones are assigned directory number ranges based on their location. Using wildcards allows us to cover groups of numbers with one statement. There are special characters to help with covering a range (or ranges) of numbers. The most common ones used in CUCME destination patterns are listed in Table 6-4.

Note: The asterisk (*) and pound sign (#) are not wildcards; they are valid digits that can be dialed on a phone, just like the numbers 0 to 9. The pound sign (#) has special meaning in CUCME by signaling that digit collection is done, and the router should process the call without waiting for the interdigit timeout. (This is useful for unknown digit lengths in international calls.)

Table 6-4 Common Wildcards Used in CUCME with the destination-pattern Command

Wildcard	Description
Period (.)	Matches any *single* digit from 0 to 9 and the * key. A **destination-pattern 30..** command would match digits from 3000 to 3099. **A destination-pattern 30.0** command would only match 3000, 3010, 3020, 3030, 3040, 3050, 3060, 3070, 3080, 3090, or 30*0.
Brackets ([])	Match a set or range of numbers for any *single* digit. Individual numbers can be listed or separated by commas. The hyphen (-) is used for a consecutive range. Thus, either [5-8], [5,6,7,8], or [5678] would select numbers from 5 to 8 for a single digit. A **destination-pattern 300[0-3]** command would match 3000 to 3003. Note: The brackets only match a single digit, so it is not possible to match a range of numbers that spans more than a single digit. Thus, 5523 to 5546 *cannot* be matched as 55[23-46], as that pattern would only cover 552, 553, 554, and 556. Likewise, using two brackets to match 5523 to 5546 *cannot* be done as such: 55[2-4][3-6]. That pattern will only match 5523 to 5526, 5533 to 5536, and 5543 to 5546. Each bracket works independently. The only way to match a range such as 5523 to 5546 is to use three separate dial peers, each with a separate destination pattern, such as **(dial-peer 1) destination-pattern 552[3-9]**, **(dial-peer 2) destination-pattern 553.** and **(dial-peer 3) destination-pattern 554[0-6]**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Wildcard	Description
The caret (^)	The caret (sometimes also called a circumflex), when used inside brackets, designates a number to *not* match. A **destination-pattern 300[^0-6] command** would match 3007 to 3009, while a **destination-pattern 300[^0^2]** command would match 3001 and 3003 to 3009. Note that if not in front of a range, the caret should appear in front of every digit to be excluded.
T	Matches any digits up to the maximum length of a dialed string, which is 32 digits. This is very useful when constructing dial peers for international calls, as the number of digits that foreign PSTNs require can vary. However, because the number of digits collected is unknown, the Call Agent must either receive the pound sign (#) to signify the end of the dialed string or wait until the interdigit timeout (10 seconds, by default) before the call is connected. Note: This is usually used with a period before the T, as such: .T Without the period, a phone left off the hook will match no digits and try to dial nothing! By putting the period in front, the dial peer will require at least one digit to be dialed before matching.
Comma (,)	Inserts a one-second delay between dialed digits. (Except when used inside brackets, where it is used as a separator between digits, as noted in the description for the bracket wildcard.)

Note: The wildcards used by CUCME are not entirely the same as the wildcards used in Cisco Unified Communications Manager.

Wildcards can be used together. For example, to match all numbers from 3300 to 3599, you could use this: **destination-pattern 3[3-5]**..

Step 3-1: Call Flow for Dual-Router Dial Peers with Wildcards Exercise

Use the configuration and diagram in Figure 6-7 to complete Table 6-5 to determine the VoIP dial peer used to complete the call. The first three lines are already completed for you. Because the tag used for the dial peer is unique to the router, Router B could have used dial peers 1 to 3 too, but different numbers were used to make determining the answers easier. Note that the VoIP dial peers cover the phone numbers used on both the VoIP and the analog phones on the other pod.

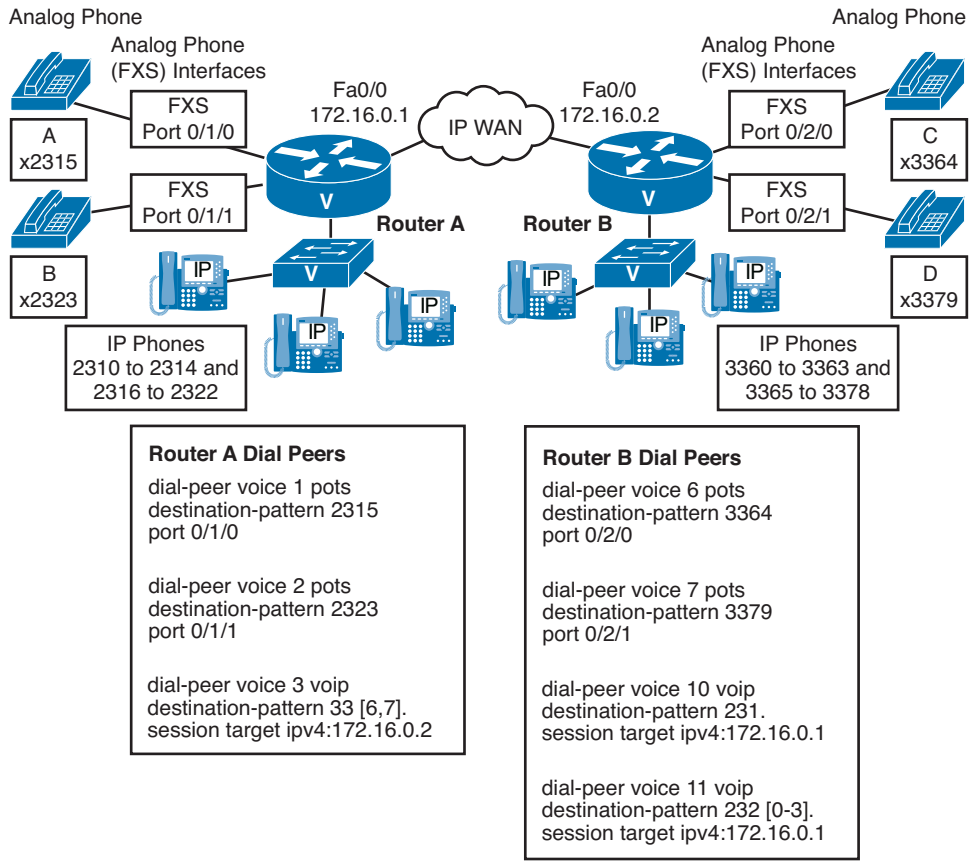
Table 6-5 Call Completion Table

Calling Phone	Called Phone	VoIP Dial Peer (If Used)
2315	2323	—
3363	2317	10
3370	2321	11
2323	3379	
3364	2323	
3366	2315	
3378	2311	

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-7 Dual-Router Dial Peers (Using Wildcards)



Note: In Figure 6-7, Router A can use a single dial peer to reach all the numbers on Router B. However, Router B needs two dial peers. If we used a single dial peer on Router B (for example, **destination-pattern 23[1-2].**), we would match numbers that are not used on Router A, such as 2324 to 2329. As noted in Table 6-4, it is not possible for the brackets to match a range that is more than one digit, so it is necessary to create two dial peers in this case to match the valid numbers on Router A.

Step 3-2: Create Destination Patterns Using Wildcards

Use the information in Table 6-4 and the examples in Figure 6-7 to create destination patterns that match the given numbers in Table 6-6. The first three lines are already completed for you. When using wildcards, there can be more than one way to achieve the same result, as noted in the brackets item in Table 6-4. You only need to do one method, but in some cases, a single destination pattern will not work, as noted in Step 3-1, and you must write all the patterns that are needed. Make sure that your answers do not include numbers that are outside the range.

Table 6-6 Wildcard Pattern Table

Phone Number Range	Destination Pattern That Matches the Range
8740 to 8779	87[4-7]. (could also be 87[4567]. or 87[4,5,6,7]. or 87[4-7][0-9] and so on)
123 to 136	Two patterns are needed: 12[3-9] and 13[0-6]

https://t.me/learningnets

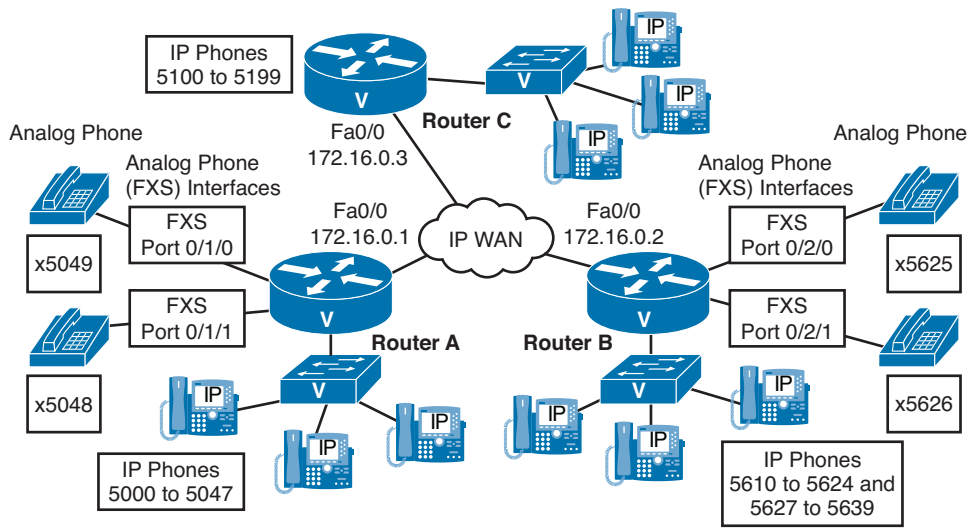
From the Library of Aliwarman Tarihoran

Phone Number Range	Destination Pattern That Matches the Range
5551000 to 5552999	555[12]... (could also be 555[1-2]... or 555[1,2]... or 555[12][0-9][0-9][0-9] and so on)
2000 to 4000	(Hint: Cannot be one pattern)
280 to 285	
4340 to 4389	
6180 to 6190	
54050 to 54199	
946 to 978	

Task 4: Create POTS and VoIP Dial Peers

Use Figure 6-8 to complete Table 6-7 by determining the dial peers, destination patterns, and ports used to call among the three routers. Some of the entries are completed for you. Because the tag used for the dial peer is unique to the router, we are using the same dial-peer tag numbers on all the routers.

Figure 6-8 Three Router Dial Peers (Using Wildcards)



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Table 6-7 Dial Peer Configuration

Source and Destination	Dial Peer(s)
Rtr A to FXS 0/1/0	dial-peer voice 1 pots destination-pattern 5049 port 0/1/0
Rtr A to FXS 0/1/1	dial-peer voice 2 _____
Rtr A to Rtr B	dial-peer voice 3 voip_____
Rtr A to Rtr C	dial-peer voice 4 _____
Rtr B to FXS 0/2/0	dial-peer voice 1 _____
Rtr B to FXS 0/2/1	dial-peer voice 2 _____
Rtr B to Rtr A	dial-peer voice 3 _____
Rtr B to Rtr C	dial-peer voice 4 _____
Rtr C to Rtr A	dial-peer voice 1 _____
Rtr C to Rtr B	dial-peer voice 2 _____

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 6-4: Call Processing, Dial Plans, and Digit Manipulation

Equipment Required

No equipment is required for this lab.

Learning Objectives

Upon completion of this lab, you will be able to

- Understand dial-peer selection
- Understand POTS dial-peer digit-stripping behavior
- Understand basic digit manipulation commands
- Create a dial plan

Scenario

This lab introduces the concepts of call processing, dial plans, and digit manipulation. Before the router can be configured with dial peers, it is necessary to understand some of the rules the router uses for call processing. Additionally, POTS dial peers have specific behaviors for digit stripping that need to be understood. This leads to a discussion of digit manipulation to impact the digit stripping of POTS peers and influence call processing. After understanding these basics, it is time to bring the concepts together into a dial plan that will direct calls to the desired destination.

Task 1: Outbound Call Processing

Step 1-1: Examining Dial-Peer Selection

When a user takes a phone off-hook, the router tells the phone to play a dial tone and then the router starts collecting the digits the user dialed. How the router acts on those dialed digits is fundamental to building a dial plan.

The following rules impact the selection the router makes when collecting digits:

- By default, the router analyzes the outbound digits as they are dialed (digit-by-digit collection) to select the dial peers, rather than collecting all digits first and then selecting the dial peer (en block selection). (One exception is that calls inbound from ISDN trunks use en block dial-peer selection.)
- When a match is found, the router immediately processes the call.
- When more than one match of the same length is found, the most specific destination pattern is selected.
- When two or more destination patterns match on the same digit length (or the exact same number), one of the dial peers is chosen at random. The **preference** command can be used to force a preferred selection order.

To better understand these rules, consider the dial peers in Example 6-1.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Example 6-1 Sample Dial Peers

```
dial-peer voice 1 pots
destination-pattern 911
port 0/1/0

dial-peer voice 2 voip
destination-pattern 91..
session target ipv4:10.1.0.1

dial-peer voice 3 voip
destination-pattern 916.
session target ipv4:10.1.10.1

dial-peer voice 4 voip
destination-pattern 9[1-7]..
session target ipv4:10.1.20.1

dial-peer voice 5 voip
destination-pattern 9[1-7]...
session target ipv4:10.1.30.1

dial-peer voice 6 voip
destination-pattern 9[^1-7]..
session target ipv4:10.1.40.1

dial-peer voice 7 pots
destination-pattern 978.
preference 1
port 0/1/1

dial-peer voice 8 voip
destination-pattern 978.
session target ipv4:10.1.50.1
```

The following paragraphs examine Example 6-1:

1. If a user dials the number 911, rules 1 and 2 require that the digits match dial peer 1, even though it could potentially match dial peers 2 and 4. As a result of this, it is impossible to have longer numbers that start with 911 dialed, such as 9117, 91134, and so on, that match dial peers 2 or 4, because as soon as the three digits are dialed, 911 is matched and dial peer 1 is selected.
2. Now consider a user dialing 9165. The router matches dial peers 2, 3, and 4. This is where rule 3 applies, because there are three dial peers that have the same length (four digits) that could match. The dial peer with the longest match is selected (the periods don't count for match length). In this case, dial peer 3 is the best match, because it has three digits match (the 916), while dial peers 2 and 4 both have two digits matching (both match 91). However, if the first choice is unavailable (down or in use), the router will pick the next best available choice. In this case, both dial peers 2 and 4 match with equal length, and using rule 4, dial peer 2 or 4 is randomly chosen as they both have the same default preference of 0 (which does not show in the configuration). Note that even if dial peers 2, 3, and 4 are unavailable, dial peer 5 will never be selected, as it requires five digits, and the other four-digit dial peers will always match first.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. If a user dials 9889, dial peer 6 is the only match, because the 9[^1-7] excludes any calls starting with 90 to 97, so only four-digit numbers starting with 9800 to 9999 will match.

4. Finally, consider a user dialing 9785. The router would normally randomly select either dial peer 7 or 8 based on rule 4. But with the **preference 1** command on dial peer 7, the router uses dial peer 8, because of the default preference 0 for every dial peer (which does not show in the config). You might ask, "Why even have dial peer 7 if the **preference 1** command causes dial peer 8 to be used?" The **preference** command has the ability to allow orderly failover if dial peers are not available. In Example 6-1, calls should go over the WAN (dial peer 8), but if the WAN fails, the router can select the next-higher-preference dial peer (dial peer 7) that points to another path, thus allowing failover. After the WAN is back in service, dial peer 8 becomes the preferred path for calls again.

Step 1-2: Understanding Dial-Peer Selection

To test your understanding of call processing, in Table 6-8, write the dial peers that will be selected and matched in Example 6-2, based on the dialed digits listed. If more than one dial peer will be randomly chosen, list all of them in the Dial Peer That Is Used column, and if no dial peer matches, write the same thing that the phone display shows: Unknown Number. Assume that all destinations are reachable and interfaces active.

Example 6-2 More Sample Dial Peers

```
dial-peer voice 1 pots
destination-pattern 6772
port 0/1/0

dial-peer voice 2 voip
destination-pattern 67[6-9].
session target ipv4:10.1.0.1

dial-peer voice 3 voip
destination-pattern 6[0-5]..
session target ipv4:10.1.10.1

dial-peer voice 4 voip
destination-pattern 6[5-9]..
session target ipv4:10.1.20.1

dial-peer voice 5 voip
destination-pattern [6-8]...
session target ipv4:10.1.30.1

dial-peer voice 6 voip
destination-pattern [6-8]...
preference 1
session target ipv4:10.1.40.1

dial-peer voice 7 voip
destination-pattern 80..
preference 1
session target ipv4:10.1.50.1
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
dial-peer voice 8 pots
destination-pattern 80..
port 0/1/0

dial-peer voice 9 pots
destination-pattern 611
port 0/1/0
```

Table 6-8 Dial-Peer Results

Dialed Digits	Dial Peers That Match	Dial Peer That Is Used
6773	2, 4, 5 ,6	2
2012	Unknown Number	
6555		
6689		
6233		
6772		
6110		
5772		
6001		
8089		
7772		

Consider the same dial peers and dialed digits, but now include the output in Example 6-3.

Example 6-3 Sample IP Routing Table and Port Summary

```
RtrPodx# show ip route
<output omitted>
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.0.0.0/30 is directly connected, FastEthernet0/1
D       10.1.0.0/24 [90/156160] via 10.0.0.2, 00:36:55, FastEthernet0/1
D       10.1.20.0/24 [90/156160] via 10.0.0.2, 00:36:55, FastEthernet0/1
D       10.1.40.0/24 [90/156160] via 10.0.0.2, 00:36:55, FastEthernet0/1
D       10.1.50.0/24 [90/156160] via 10.0.0.2, 00:36:55, FastEthernet0/1

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

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
0/1/0           --  fxs-ls      down  down on-hook  idle     y
0/1/1           --  fxs-ls      up    dorm on-hook  idle     y
<output omitted>
```

Do any of the dial peers used change for any of the dialed numbers? If so, which dialed numbers are impacted and which dial peers are now used?

Step 1-3: Troubleshooting Dial-Peer Selection with the show dial-peer voice summary Command

There are several commands that can help you troubleshoot dial-peer selection. The **show dial-peer voice summary** command displays the existing dial peers, as shown in Example 6-4. This can be a quick way to check the destination patterns in use, as a call will fail if it cannot match a destination pattern. Notice that the ephone-dns show up in the output. CUCME automatically creates a dial peer for each ephone-dn (they are created with the dollar sign ($) at the end, which is the wildcard to stop matching digits). This is why a VoIP phone can call another VoIP phone without manually creating dial peers.

Example 6-4 show dial-peer voice summary Command

```
RtrPodx# show dial-peer voice summary
dial-peer hunt 0
             AD                                  PRE PASS                 OUT
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN     FER THRU SESS-TARGET     STAT PORT
20001  pots  up   up              5330$             0                            50/0/1
20002  pots  up   up              5331$             0                            50/0/2
20003  pots  up   up              5332$             0                            50/0/3
1      pots  up   up              6772              0                       up   0/1/0
2      voip  up   up              67[6-9].          0  syst ipv4:10.1.0.1
3      voip  up   up              6[0-5]..          0  syst ipv4:10.1.10.1
4      voip  up   up              6[5-9]..          0  syst ipv4:10.1.20.1
5      voip  up   up              [6-8]...          0  syst ipv4:10.1.30.1
6      voip  up   up              [6-8]...          1  syst ipv4:10.1.40.1
7      voip  up   up              80..              1  syst ipv4:10.1.50.1
8      pots  up   up              80..              0                       up   0/1/0
9      pots  up   up              611               0                       up   0/1/0
```

The best way to troubleshoot dial-peer problems is to use the **show dialplan number** command, as shown in Example 6-5. This command shows all the details of each dial peer that matches, in the order that they are selected. As this example shows, dial peer 2 is selected first when 6773 is dialed.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Example 6-5 show dialplan number Command

```
RtrPodx# show dialplan number 6773
Macro Exp.: 6773

VoiceOverIpPeer2
        peer type = voice, system default peer = FALSE, information type = voice,
        description = `',
        tag = 2, destination-pattern = `67[6-9].',
        voice reg type = 0, corresponding tag = 0,
        voice reg type = 0, corresponding tag = 0,
        allow watch = FALSE
        answer-address = `', preference=0,
<output omitted>
Matched: 6773   Digits: 3
Target: ipv4:10.1.0.1

VoiceOverIpPeer4
        peer type = voice, system default peer = FALSE, information type = voice,
        description = `',
        tag = 4, destination-pattern = `6[5-9]..',
        voice reg type = 0, corresponding tag = 0,
        allow watch = FALSE
        answer-address = `', preference=0,
<output omitted>
Matched: 6773   Digits: 2
Target: ipv4:10.1.20.1

VoiceOverIpPeer5
        peer type = voice, system default peer = FALSE, information type = voice,
        description = `',
        tag = 5, destination-pattern = `[6-8]...',
        voice reg type = 0, corresponding tag = 0,
        allow watch = FALSE
        answer-address = `', preference=0,
<output omitted>
Matched: 6773   Digits: 1
Target: ipv4:10.1.30.1

VoiceOverIpPeer6
        peer type = voice, system default peer = FALSE, information type = voice,
        description = `',
        tag = 6, destination-pattern = `[6-8]...',
        voice reg type = 0, corresponding tag = 0,
        allow watch = FALSE
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
        answer-address = `', preference=1,
<output omitted>
Matched: 6773   Digits: 1
Target: ipv4:10.1.40.1
```

Note: There is a lot of output from the **show dialplan number** command. One way to get just the dial-peer tag information is to use CLI output filtering[1] with the pipe character (|). On most keyboards, the pipe is a Shift character for the backslash (\) key. Here is an example of CLI filtering; just replace *number* with the number you want to check:

```
show dialplan number number timeout | i tag = [0-9]+, des
```

If you ran the same command shown in Figure 6-5 with output filtering, the output is much more compact, and it looks like this:

```
RtrPodx# show dialplan number 6773 timeout ¦ i tag = [0-9]+, des
        tag = 2, destination-pattern = `67[6-9].',
        tag = 4, destination-pattern = `6[5-9]..',
        tag = 5, destination-pattern = `[6-8]...',
        tag = 6, destination-pattern = `[6-8]...',
```

[1] Credit for the CLI filtering example goes to Filip Burda at this blog: http://rekrowten.wordpress.com/2011/10/31/longest-number-match-rule-in-cucme/

Step 1-4: Troubleshooting Dial-Peer Selection with Debug

To watch the process the router uses to select the correct dial peers, use the **debug voip dialpeer** command (and the **debug voip dialpeer all** command to get even more detailed output).

Caution: The **debug voip dialpeer** commands should be used only with great caution on a production system. The output generated can overwhelm the console buffer, causing you to lose control of the router.

In the output shown in Example 6-6, the router shows a user dialing 6773. You can see how the router examines each digit as it is dialed until it finds a match, in this case dial peers 2, 4, 5, and 6. Note: To save space, the output was omitted at a point, but it continues for over twice this length.

Example 6-6 debug voip dialpeer Command

```
RtrPodx# debug voip dialpeer
voip dialpeer default debugging is on
RtrPodx#
*Feb 19 22:18:41.963: //-1/xxxxxxxxxxxx/DPM/dpAssociateIncomingPeerCore:
   Calling Number=5330, Called Number=, Voice-Interface=0x4BF57024,
   Timeout=TRUE, Peer Encap Type=ENCAP_VOICE, Peer Search Type=PEER_TYPE_VOICE,
   Peer Info Type=DIALPEER_INFO_SPEECH
*Feb 19 22:18:41.963: //-1/xxxxxxxxxxxx/DPM/dpAssociateIncomingPeerCore:
   Result=Success(0) after DP_MATCH_ORIGINATE; Incoming Dial-peer=20001
*Feb 19 22:18:41.979: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=6, Peer Info Type=DIALPEER_INFO_SPEECH
*Feb 19 22:18:41.979: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=6
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
*Feb 19 22:18:41.979: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Result=Partial Matches(1) after DP_MATCH_DEST
*Feb 19 22:18:41.979: //-1/83B14A988016/DPM/dpMatchPeersMoreArg:
   Result=MORE_DIGITS_NEEDED(1)
*Feb 19 22:18:42.175: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=67, Peer Info Type=DIALPEER_INFO_SPEECH
*Feb 19 22:18:42.175: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=67
*Feb 19 22:18:42.175: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Result=Partial Matches(1) after DP_MATCH_DEST
*Feb 19 22:18:42.175: //-1/83B14A988016/DPM/dpMatchPeersMoreArg:
   Result=MORE_DIGITS_NEEDED(1)
*Feb 19 22:18:42.375: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=677, Peer Info Type=DIALPEER_INFO_SPEECH
*Feb 19 22:18:42.375: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=677
*Feb 19 22:18:42.375: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Result=Partial Matches(1) after DP_MATCH_DEST
*Feb 19 22:18:42.375: //-1/83B14A988016/DPM/dpMatchPeersMoreArg:
   Result=MORE_DIGITS_NEEDED(1)
*Feb 19 22:18:42.575: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=6773, Peer Info Type=DIALPEER_INFO_SPEECH
*Feb 19 22:18:42.575: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=6773
*Feb 19 22:18:42.575: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Result=Success(0) after DP_MATCH_DEST
*Feb 19 22:18:42.575: //-1/83B14A988016/DPM/dpMatchPeersMoreArg:
   Result=SUCCESS(0)
   List of Matched Outgoing Dial-peer(s):
     1: Dial-peer Tag=2
     2: Dial-peer Tag=4
     3: Dial-peer Tag=5
     4: Dial-peer Tag=6
*Feb 19 22:18:42.579: //-1/83B14A988016/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=6773, Peer Info Type=DIALPEER_INFO_SPEECH
<output omitted>
```

Task 2: POTS Dial-Peer Behavior and Digit Manipulation

Before building a dial plan that will involve any POTS dial peers, the default behavior of POTS dial peers needs to be examined, as well as the digit manipulation methods that are used to alter the results. (VoIP dial peers do not strip digits.)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-1: Examining POTS Dial-Peer Digit Stripping

When a call matches a POTS dial peer, by default the router strips the explicitly matched (nonwildcard) digits on the left. Any remaining digits that match a wildcard or are to the right of a wildcard are not stripped. As an example, we have this dial peer:

```
dial-peer voice 1 pots
destination-pattern 555....
port 2/0/0
```

If a user dials 5555439, the result is that the 555 is explicitly matched and stripped, while the 5439 matches the wildcard digits and those digits are sent out the port.

There are two main reasons for this default digit-stripping behavior:

- When constructing a dial plan for a PBX-type environment, an outside access digit (such a dialing a 9 to get an outside line) is needed, or it would be very difficult to dial any number on the PSTN that had the same first digits as your internal extensions, as the calls will complete when the last digit of an extension is dialed. (This is rule 2 of dial-peer selection in Step 1-1.) When using an outside line access digit, this number should not be sent to the PSTN and needs to be stripped.
- When the POTS dial peer points to an FXS port, the analog device has no need of the dialed digits because it is an endpoint. (In contrast, for a digital trunk that connects to the PSTN, the dialed digits are needed to route the call through the PSTN.) (Just for fun, if you have an FXS port, create a dial peer with a destination pattern of seven digits or more, use one of the following digit manipulation commands to keep all the digits, and connect an analog phone to the FXS port. Then dial the number in the destination pattern from an IP Phone. When you answer the ringing analog phone, you will hear the unnecessary dialed digits.)

However, in many cases, we don't want all the digits that are explicitly matched to be stripped. By using digit manipulation commands, you can change the default digit-stripping behavior of POTS dial peers. Table 6-9 shows the common digit manipulations used.

Table 6-9 Common Digit Manipulation Methods on Cisco Routers

Command	Description
Example	
no digit-strip	Turns off digit stripping for a POTS dial peer. Advantage: No digits are stripped. Disadvantage: Outside line access digit is not stripped.

To send a specific seven-digit number range to the PSTN:

```
dial-peer voice 3 pots
destination-pattern 9555....
no digit-strip
port 2/0/0
```

If 95551234 is dialed, 95551234 is sent on.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Command	Description
forward-digits [all | *x*]	**The forward-digits all** command acts just like **no digit strip**. The **forward-digits *x*** command on a POTS dial peer sends on just the *x* number of digits in the destination pattern from the right. Advantage: The **forward-digits *x*** command controls the exact number of digits to be saved; thus the outside line access digit can be stripped while all other digits are sent on. Disadvantage: This is one of the few commands that cannot be removed with the **no** option. To remove the command, use **default forward-digits**.

To send a seven-digit number to the PSTN when a specific ten-digit number range is dialed and 9 is the outside access digit:

```
dial-peer voice 6 pots
destination-pattern 91510555....
forward-digits 7
port 2/0/0
```

If 915105551234 is dialed, 5551234 is sent on.

prefix *digits*	Adds the specified digits to the left, after digit stripping happens in the POTS dial peer. Because the digits to be stripped are known, it is easy to prefix them back while ignoring the outside line access digit. The **prefix** command can also add digits that were not dialed to the start of the dialed digits. Advantage: Can not only replace stripped digits, but also adds additional new digits to the left of the dialed digits. It can also add a one-second delay for every comma (,) added to allow automated systems to answer. Disadvantages: None.

To send a long-distance digit number (1+10 digits) to the PSTN when a specific seven-digit number range is dialed and 9 is the outside access digit:

```
dial-peer voice 4 pots
destination-pattern 9556....
prefix 1510556
port 2/0/0
```

If 95561234 is dialed, 15105561234 is sent on.

Use a wildcard for the first digit (or all the digits) to be saved.	By using a wildcard for the first digit to be saved in the POTS destination pattern, the other remaining digits are not stripped. The wildcard can be as simple as putting a single digit in brackets, for example, [5]55... Advantage: No other method is required to save the digits. Disadvantage: None.

To send the three-digit North American N11 codes (more info at www.nanpa.com/number_resource_info/n11_codes.html) and 9 is the outside access digit:

```
dial-peer voice 8 pots
destination-pattern 9[2-9]11
port 2/0/0
```

If 9311 is dialed, 311 is sent on.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Command	Description
num-exp *match_digits expanded_digits*	Number expansion globally transforms any digits matching the match_digits pattern using the expanded_digits. There can be more replaced digits than the digits matched. Advantage: Transforms digits globally so that they don't need to be applied to every dial peer or ephone-dn. Disadvantage: Transforms digits globally, so you are unable to control which dial peers use the transform.

When callers dial 0 for operator services, redirect the call to an internal support desk at extension 1234:

```
num-exp 0 3344
```

If 0 is dialed, the digits are changed to 3344.

Voice translation profiles	Voice translation profiles allow extremely complex digit manipulation. They can change both the dialed and calling numbers, and are for calls inbound, outbound, or in both directions. Regular expression concepts can be used to save some digits while changing others. Advantage: Extremely powerful and can be applied to individual dial peers or ephone-dns. Can also be used in VoIP dial peers to change digits. Disadvantage: Can be tricky to understand and troubleshoot.

When callers dial 911 for emergency services, redirect the call to an internal security service at extension 1234:

```
voice translation-rule 911
rule 0 /^911$/ /1234/
rule 1 /^9911$/ /1234/
voice translation-profile EMERGENCY
translate called 911
dial-peer voice 17 voip
translation-profile outgoing EMERGENCY
```

If 911 or 9911 is dialed, the digits are changed to 1234.

Note: The details of implementing number expansion and voice translation profiles are not a focus of the CCNA Voice Certification exam and are not covered further in this lab book.

To compare the various digit manipulations, examine a dial peer for emergency services (the number is 911 in North America; elsewhere 112 is the most common). If nothing is done, a destination pattern 911 in a POTS dial peer would have all the digits matched; thus all digits are stripped and no digits are sent to the PSTN. The various methods that are commonly used to resolve this are as follows:

```
destination-pattern 911
no digit-strip
```

or

```
destination-pattern 911
forward digits all
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

or

```
destination-pattern 911
forward digits 3
```

or

```
destination-pattern 911
prefix 911
```

Note: Typically, you use only one method per dial peer. If you mix more than one method on the same dial peer, it can cause unexpected results.

However, if an outside access digit (such as dialing a 9 to get an outside line) is used, some of the previous methods will not work, as they also send the access digit, which causes the PSTN to reject the call. The various methods that are commonly used to resolve this are as follows:

```
destination-pattern 9911
forward digits 3
```

or

```
destination-pattern 9911
prefix 911
```

Note: From a legal and regulatory standpoint, access to emergency service numbers is one of the most critical functions of the phone system. This can cause design issues with your dial plan. To avoid accidental calls (and people hanging up on emergency operators), the approach you take can vary. One of my students worked at a company that changed its outside access line digit from 9 to 8 just to avoid accidental 911 calls. At Madison College where I work, the college does not support dialing 911, only 9911. As a result, for legal reasons, the college needed to notify everyone that 911 alone would not work. To comply, all phones show "Call 9-911 for emergency services" off to the side of the college logo image on the phone displays. Cisco also sells a server product, Cisco Emergency Responder (CER), that offers enhanced ability to track phone locations for emergency response compliance, as well as other functions.

Task 3: Inbound Dial-Peer Selection

After examining the outbound use of the **destination-pattern** command in dial peers, it is necessary to examine how inbound calls are routed. The router uses various methods for inbound calls to match extensions on phones, potentially requiring the incoming number to match the extension length.

Step 3-1: Examine Digit Matching for Inbound Calls

When an incoming phone call is received from the PSTN, the call needs to be matched to an internal extension. One problem that might occur is the number of digits received from the PSTN for the called number being greater than the number of digits used for internal extensions. (For example, the PSTN sends the full ten digits of the phone number, but the company is using four-digit extensions internally.) This results in the call not matching a dial peer because of the difference in the number of digits. There are a few methods to make sure that an incoming call will match a dial peer:

- Ask the PSTN provider to only send in the digits that match your extensions. For example, if customers call 510-555-1234 to reach an inside user at extension 1234, the provider would forward just 1234 as the dialed digits. Not all providers will do this, and this might not be possible

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

if your phone numbers are in more than one exchange or area code, or if the internal extensions do not match the outside numbers.

- When configuring the **number** command in ephone-dn configuration, the secondary *number* keyword allows an additional number to be matched. For example, if the PSTN is sending in ten digits, such as 5105551234, the following command would allow the digits to match internal extension 1234:

```
RtrPodx(config-ephone-dn)# number 1234 secondary 5105551234
```

  Using the secondary keyword on every ephone-dn could be a lot of work.

- Adding the **dialplan-pattern** command in telephony-service configuration mode will automatically create a dial peer for each ephone-dn that matches the extension pattern. For example, if the PSTN is sending in ten digits in the range of 5105551000 to 5105551999, the following command would allow the digits to match all internal extensions that start with 1*xxx*:

```
RtrPodx(config-telephony)# dialplan-pattern 1 5105551... extension-length 4
```

  The dialplan pattern must have at least one of the extension digits listed to work correctly. Thus, if your extension is four digits long, there needs to be three or fewer wildcard digits, and the command does not support the range command wildcard. One other important note: If you ever change the dialplan pattern, you *must* remove the previous one with the **no** command. Overwriting with a new version will not work!

- Use a digit manipulation method to change the incoming digits to match the extensions. Options such as number expansion or voice translation profiles would allow the numbers to be changed to match internal extensions.

Task 4: Dial Plans for the PSTN

Step 4-1: Understanding Dial Plans

Before calls can be placed to local analog phones, remote VoIP phones, and the PSTN, you need to understand dial plans. Dial plans route calls to the correct destination, primarily based on the number dialed by the caller, but this behavior can be modified with digit manipulation as discussed previously. Just like connecting a data network to the Internet requires a valid public IP address, connecting to the PSTN requires using valid phone numbers and following the dial plan of the country you are connecting to.

Note: Cisco Learning Network has a 16-minute quick learning module on Understanding Dial Plans at https://learningnetwork.cisco.com/docs/DOC-1365.

International Telecommunication Numbering Plan

The international numbering plan is defined by E.164 from the International Telecommunication Union (ITU). A full E.164 number is usually written with a + at the front of the number, and must be 15 digits or less. E.164 is comprised of two or three parts:

- **Country code:** One to three digits.
- **National number:** Maximum of 15 digits, minus the length of the country code. Optionally, the national number can be divided into:
  - National destination code
  - Subscriber number

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

North American Numbering Plan

In the United States, the North American Numbering Plan (NANP) further defines the dialing plan used by the PSTN. The NANP is defined as follows:

- **Country code = 1:** (+1 to meet E.164 conventions).
- **Area code = three digits:** The first digit is in the range of 2–9, and the second and third digits are from 0 to 9. The area code defines a geographic region.
- **Central office code = three digits:** The first digit in the range of 2–9, and the second and third digits are from 0 to 9. The central office code also defines a geographic area.
- **Subscriber number = four digits:** A range of 0 to 9 is used for each. This is the unique number for the subscriber.

Note: When talking about local calls in the NANP, there are some variations on the number of digits dialed. For example, in the state of Wisconsin, the 608 area code uses seven digits for local calls and all other calls require 1+10 digits, while the 715 area code (which is in a overlay with the 534 area code) requires ten digits for local calls and all other calls require 1+10 digits.

Step 4-2: Creating a PSTN Dial Plan for the NANP

To create a PSTN dial plan for the NANP, a single dial peer could be used, with 9 as the outside line access, as such:

```
dial-peer voice 1 pots
destination-pattern 9T
port 0/1/0
```

This would work, as the 9 would be stripped off as the access digit, and the T wildcard will collect any number of digits. However, the disadvantage of this method is that for each phone call, the system will wait for the interdigit timeout value (10 seconds by default) or the user will have to press the pound key (#) to signal the end of digit collection. Additionally, there is no way to provide any calling restrictions for numbers that might incur premium rates (1-900 numbers, for example).

A better option is to break down the PSTN dial plan into categories of numbers and build a separate dial peer for each. Sample wildcard patterns for categories of numbers are shown in Table 6-10.

Table 6-10 Sample NANP PSTN Dial Plan

Pattern	Number Type
911	Emergency numbers *
[2-8]11	Service codes (N11) *
[2-9].....	Local calls (seven-digit areas)
[2-9]..[2-9].....	Local calls (ten-digit areas)
1[2-9]..[2-9].....	Long-distance (toll) calls **
1800[2-9].....	Toll-free numbers ** (1-800 numbers. This should also include 888, 877, 866, and 855 area codes to cover all current toll-free numbers.) See www.fcc.gov/guides/toll-free-numbers-and-how-they-work for details.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Pattern	Number Type
1900[2-9].....	Premium-rate numbers ** (1-900 numbers)
011T	International dialing

* You might wonder why this table separates out emergency numbers from the service codes when the pattern [2-9]11 would cover both. There are two main reasons: First, for availability reasons, emergency numbers might use separate, dedicated ports from the exit ports for other voice traffic. Second, if implementing class of restriction (CoR) to control outbound calls (for example, to restrict access to premium-rate numbers [1-900] or international calls to only approved users), emergency numbers must always be accessible. Some service codes (such as 311) are billed back to the caller, so keeping emergency numbers as a separate dial peer avoids restrictions on service codes impacting emergency numbers.

** Toll-free and premium-rate numbers are a subset of the long-distance numbers. If using CoR to control access to long-distance calls, a separate dial peer for toll-free numbers can allow access to those numbers while still restricting long-distance calls. A dial peer for premium-rate numbers can be used to block access to those numbers separate from long-distance and toll-free numbers.

Creating dial peers for the PSTN dial plan shown in Table 6-10 will be covered in the next two labs using the command-line interface (CLI) (Lab 6-5) or the graphical user interface (GUI) (Lab 6-6).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 6-5: Dial-Peer Configuration Using the CLI

Equipment Required

This lab uses the following equipment:

- Two Cisco routers with voice IOS
- Switch that supports voice VLANs
- Lab configuration from Lab 5-2, 5-3, 6-1, or 6-2 (see the scenario for details)
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)

Optional hardware components (see the scenario for details):

- Cisco router configured as a PSTN simulator
- T1/E1/PRI Multiflex Trunk VWIC cards or Network Modules
- Analog Foreign eXchange Station (FXS) cards
- Analog Foreign eXchange Office (FXO) cards
- DSP resources in the routers (PVDM chips) to enable the Multiflex Trunk, FXS, or FXO ports

Learning Objectives

Upon completion of this lab, you will be able to

- Configure dial peers to connect to the PSTN
- Configure dial peers to connect to remote offices using the WAN
- Configure failover for calls to remote offices using the PSTN when the WAN is down

Scenario

Shiny Objects Inc. (SOI) wants to connect to customers using the PSTN and remote branch offices of the company using the WAN. To avoid WAN failure from disabling four-digit dialing between locations, call failover from the WAN to the PSTN needs to be configured.

To allow the variety of hardware that might be available to you, this lab has options for various hardware and notes the impacts each has on the configuration. Listed in order of best case to most limited, the hardware options are as follows:

- **Option 1:** Two (or more) pods with the PSTN simulator (see Appendix E) and an Ethernet connection to simulate the WAN, as shown in Figure 6-9. This option allows you to complete all parts of the lab.
- **Option 2:** One pod with the PSTN simulator (see Appendix E), as shown in Figure 6-10. This will allow you to complete Tasks 2 to 5, but not the WAN links (Task 6) or PSTN failover (Task 7). If you are able to reconfigure the PSTN simulator as another pod, you could complete the WAN links (Task 6) separately.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-9 Topology Diagram Option 1: Two Pods and PSTN Simulator

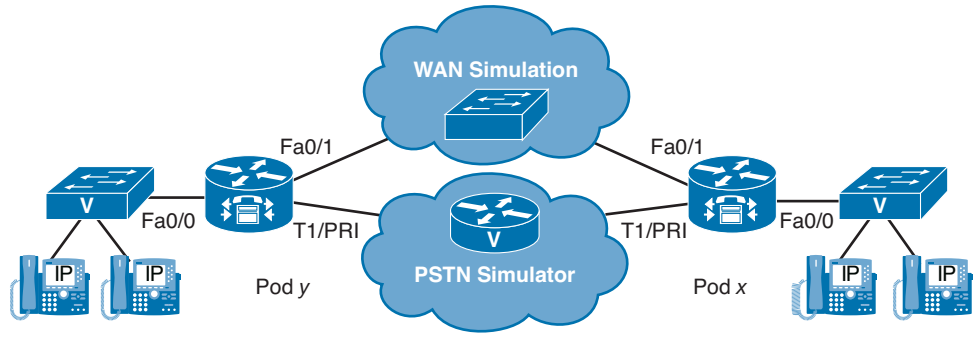
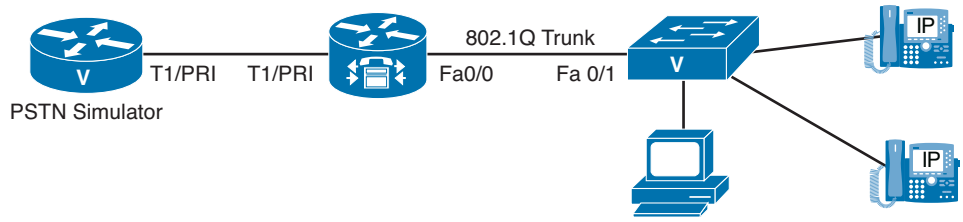
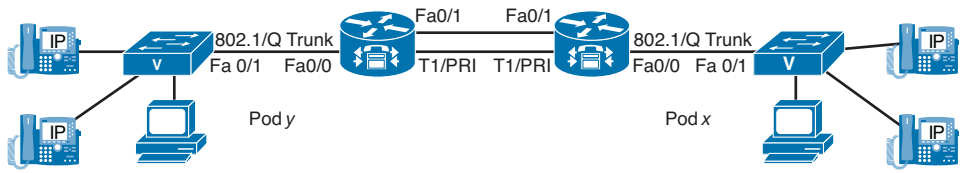


Figure 6-10 Topology Diagram Option 2: One Pod and PSTN Simulator



- **Option 3:** Two pods directly connected with digital or analog interfaces, as shown in Figure 6-11. This will allow you to set up another pod to be a simplistic PSTN simulator so that you can complete Tasks 2 to 4 and 6 to 7, but not the inbound dial peers (Task 5). The biggest limitation is having to use the dial-peer troubleshooting commands to verify that the correct dial peer is being used, as the config shown will send all calls to pod Y to a single phone.

Figure 6-11 Topology Diagram Option 3: Two Pods with Digital Interfaces and Ethernet Connection



Task 1: Load Prior Configurations

This lab is based on the configuration from Lab 5-2, 5-3, 6-1, or 6-2. If necessary, load the configuration for both the switch and router. Connect a PC to the switch and verify that it can ping the router and switch management addresses. Connect the VoIP phones and verify that you can call between them. Troubleshoot if necessary.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Configure Hardware Used by the Dial Peers

Options 1 and 2

If completing option 1 or 2, configure the T1/E1/PRI interfaces to match the PSTN simulator using the instructions in Lab 6-2 and cable all pods using PRI crossover cables to the PSTN simulator. The PSTN simulator in Appendix E is configured for six channels on the PRI; adjust if your configuration is different.

Option 3 Only

If completing option 3, configure the other router to act like pod 2 with at least one IP Phone assigned extension 5030. It will be necessary to set up the other router to accept the incoming calls and direct them to extension 5030.

Use the following commands only if you are completing option 3 and only on the other router acting as pod 2. This configuration assumes that you have configured the PRI interface with six channels and the card is located in VWIC slot 1. Adjust if necessary.

```
Option3Only(config)# ! Allows incoming calls to connect
Option3Only(config)# dial-peer voice 123 pots
Option3Only(config-dial-peer)# description Inbound calls
Option3Only(config-dial-peer)# incoming called-number .
Option3Only(config-dial-peer)# direct-inward-dial
Option3Only(config-dial-peer)# port 0/1/0:23
Option3Only(config-dial-peer)# exit

Option3Only(config)# ! Rule to translate any digits to extension 5030
Option3Only(config)# voice translation-rule 1
Option3Only(cfg-translation-rule)# rule 1 /.+/ /5030/

Option3Only(cfg-translation-rule)# ! Applies the rule to a profile
Option3Only(cfg-translation-rule)# voice translation-profile TenDIGITS
Option3Only(cfg-translation-profile)# translate called 1
Option3Only(cfg-translation-profile)# exit

Option3Only(config)# ! Applies the profile to incoming ISDN calls
Option3Only(config)# voice-port 0/1/0:23
Option3Only(config-voiceport)# translation-profile incoming TenDIGITS
```

Task 3: Configure Secondary Dial Tone

When configuring a PBX-type dial plan, there needs to be an outside line access digit. Many PBX users are used to hearing a slightly different dial tone after dialing this digit, before dialing the intended PSTN number. This secondary dial tone for outside lines can be configured in telephony-service

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

using the **secondary-dialtone** command and assuming that 9 will be used as the outside line access digit:

```
RtrPodx(config)# telephony-service
RtrPodx(config-telephony)# secondary-dialtone 9
RtrPodx(config-telephony)# exit
```

Note: You will not hear the secondary dial tone until you have at least one working dial peer with a destination pattern that starts with a 9. This command only makes the dial tone change when the first digit is 9. It does not eliminate the need for a 9 in each dial-peer destination pattern that will connect to the PSTN.

Task 4: Configure the PSTN Dial Peers

Refer to Table 6-11 for the dial plan to configure the correct dial peers. Refer to Lab 6-4, Task 4-2, for details on the dial plan. Don't forget the requirement to dial a 9 as the outside line access digit when constructing the dial peers. All the dial peers shown in the following steps assume that you have a PRI configured in VWIC slot 2 of the router. Adjust as needed for your hardware.

Table 6-11 NANP PSTN Dial Plan and Test Numbers

Pattern	Number Type	Test Number(s)
911 and 9911	Emergency numbers	911 and 9911
[2-8]11	Service codes (N11)	311, 811, and so on
[2-9].....	Local calls (seven-digit areas)	567-0001
[2-9]..[2-9].....	Local calls (ten-digit areas)	510-567-0001
1[2-9]..[2-9].....	Long-distance (toll) calls	1-333-444-5678
1800[2-9].....	Toll-free numbers. (1-800 numbers—this should also include 888, 877, 866, and 855 area codes to cover all current toll-free numbers.)	1-800-223-4567
1900[2-9].....	Premium-rate numbers (1-900 numbers)	1-900-223-4567
011T	International dialing (011, then country code, then subscriber number)	011-44-88221234 (# key to stop digit collection)

Step 4-1: Configure Emergency Services Calls

As discussed in Lab 6-4, Step 2-1, there are several considerations when creating dial peers for emergency numbers. This step will assume that both 911 and 9911 are needed. There are also several methods to deal with POTS dial-peer digit stripping, as detailed in Lab 6-4, Step 2-1. This step will demonstrate just one of them.

```
RtrPodx(config)# dial-peer voice 911 pots
RtrPodx(config-dial-peer)# description Emergency Services
RtrPodx(config-dial-peer)# destination-pattern 911
RtrPodx(config-dial-peer)# prefix 911
RtrPodx(config-dial-peer)# port 0/2/0:23
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
RtrPodx(config-dial-peer)# dial-peer voice 9911 pots
RtrPodx(config-dial-peer)# description 9+Emergency Services
RtrPodx(config-dial-peer)# destination-pattern 9911
RtrPodx(config-dial-peer)# prefix 911
RtrPodx(config-dial-peer)# port 0/2/0:23
```

Step 4-2: Configure Service Code Calls

To configure N11 calls such as 211 to 811 to dial an outside line, only the 9 for an outside line needs to be removed. Because the brackets [ ] mean that the digits are no longer explicitly matched, that digit and everything thereafter will not be stripped, so there is no need to do anything else for digit stripping. However, you could use the **forward-digits 3** command without harm.

```
RtrPodx(config-dial-peer)# dial-peer voice 411 pots
RtrPodx(config-dial-peer)# description Info Services
RtrPodx(config-dial-peer)# destination-pattern 9[2-8]11
RtrPodx(config-dial-peer)# port 0/2/0:23
```

Step 4-3: Configure Local Calls

As discussed in Lab 6-4, Step 4-1, there are two options for local calls depending on the PSTN area code you are connecting to. Both options for seven- and ten-digit local call are shown, and you should pick one. The PSTN simulator in Appendix E will work with either one. Be aware that if you were to put both dial peers in, the ten-digit dial peer will never be used, as the first seven digits dialed will always match the seven-digit dial peer before the remaining three digits can be dialed, as noted in Lab 6-4, Step 1-1, Rule 2: "When a match is found, the router immediately processes the call." To configure local calls to dial an outside line, only the 9 for an outside line needs to be removed. Because the brackets [ ] mean that the digits are no longer explicitly matched, that digit and everything thereafter will not be stripped, so there is no need to do anything else for digit stripping.

```
RtrPodx(config-dial-peer)# dial-peer voice 97 pots
RtrPodx(config-dial-peer)# description 7 digit local numbers
RtrPodx(config-dial-peer)# destination-pattern 9[2-9].....
RtrPodx(config-dial-peer)# port 0/2/0:23

RtrPodx(config-dial-peer)# dial-peer voice 910 pots
RtrPodx(config-dial-peer)# description 10 digit local numbers
RtrPodx(config-dial-peer)# destination-pattern 9[2-9]..[2-9].....
RtrPodx(config-dial-peer)# port 0/2/0:23
```

Step 4-4: Configure Long-Distance (Toll) Calls

To configure long-distance calls to dial an outside line, only the 9 for an outside line needs to be removed. This dial peer requires that the digit stripping of the 1 digit be fixed, as noted in Lab 6-4, Step 2-1. In this config, the **prefix** command is used to add the 1 back to the dialed digits.

```
RtrPodx(config-dial-peer)# dial-peer voice 9110 pots
RtrPodx(config-dial-peer)# description 1+10 digit long-distance
RtrPodx(config-dial-peer)# destination-pattern 91[2-9]..[2-9].....
RtrPodx(config-dial-peer)# prefix 1
RtrPodx(config-dial-peer)# port 0/2/0:23
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 4-5: Configure Toll-Free Calls

To configure toll-free calls to dial an outside line, only the 9 for an outside line needs to be removed. This dial peer will require that the digit stripping of the explicitly matched digits be fixed. Notice that toll-free numbers are a subset of the long-distance numbers.

```
RtrPodx(config-dial-peer)# dial-peer voice 91800 pots
RtrPodx(config-dial-peer)# description 1800 numbers
RtrPodx(config-dial-peer)# destination-pattern 91800[2-9]......
RtrPodx(config-dial-peer)# prefix 1800
RtrPodx(config-dial-peer)# port 0/2/0:23
```

What are the alternative ways to write this dial peer to prevent POTS dial-peer digit stripping? (There is more than one.) Refer to Lab 6-4, Step 2-1 if necessary.

The dial peer shown only works for 1-800 numbers. To allow all toll-free call area codes currently in the NANP (800, 888, 877, 866, and 855 are toll-free area codes), can the dial peer be modified with wildcards to cover only these area codes? If so, what is the resulting destination pattern? If not, why not?

Step 4-6: Configure Premium-Rate Calls

Use your practice with previous dial peers to create one for premium-rate calls. Notice that premium-rate numbers are a subset of the long-distance numbers. Part of the configuration is already completed for you:

```
RtrPodx(config-dial-peer)# dial-peer voice 91900 pots
```

RtrPod*x*(config-dial-peer)# **description** _____

RtrPod*x*(config-dial-peer)# **destination-pattern** _____

RtrPod*x*(config-dial-peer)# _____

RtrPod*x*(config-dial-peer)# _____

Step 4-7: Configure International Calls

International calls pose an interesting challenge. They have an unknown length, as each country uses different numbering schemes internally. For calls leaving the United States, the digits to signal an international call are 011 (usually written as +011), then the foreign country code, then the area code (if used), then the subscriber number. Thus, a call from the NANP area to a number in Great Britain (country code 44) might look like +011 44 03069 990000.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

The T character can be used in the destination pattern to indicate an unknown length of dialed digits. As noted in Lab 6-3, Task 3, for the T wildcard, there are two ways for the system to determine that the caller is done dialing: Either collect the pound (#) digit to signify the end of the dialed string or wait for the interdigit timeout (10 seconds by default) before the call is connected.

```
RtrPodx(config-dial-peer)# dial-peer voice 9011 pots
RtrPodx(config-dial-peer)# description International calls
RtrPodx(config-dial-peer)# destination-pattern 9011T
RtrPodx(config-dial-peer)# prefix 011
RtrPodx(config-dial-peer)# port 0/2/0:23
RtrPodx(config-dial-peer)# exit
```

Step 4-8: Make Test Calls to the PSTN Simulator

Use the test numbers in Table 6-11 to place calls from an IP Phone to the PSTN simulator. (Don't forget to dial the 9 to get an outside line first.) The PSTN simulator will play a different sound file for each test number listed. Because the PSTN simulator will autoanswer, on the router console you will see the ISDN signaling channel select the first open voice channel to complete the connection, and the number that was sent to the PSTN. In the following output, you can see the call setup and teardown for 911 and 311 calls.

```
RtrPodx(config)#
*Feb 20 01:09:16.747: %ISDN-6-CONNECT: Interface Serial0/2/0:5 is now connected to
  911 N/A
RtrPodx(config)#
*Feb 20 01:09:22.499: %ISDN-6-DISCONNECT: Interface Serial0/2/0:5  disconnected from
  911 , call lasted 5 seconds
RtrPodx(config)#
*Feb 20 01:09:29.235: %ISDN-6-CONNECT: Interface Serial0/2/0:5 is now connected to
  311 N/A
RtrPodx(config)#
*Feb 20 01:09:32.435: %ISDN-6-DISCONNECT: Interface Serial0/2/0:5  disconnected from
  311 , call lasted 3 seconds
```

To watch the process the router uses to select the correct dial peer, use the **debug voip dialpeer** command.

Caution: The **debug voip dialpeer** commands should be used only with great caution on a production system. The output generated can overwhelm the console buffer, causing you to lose control of the router.

In the segment of the following output, you can see that the number 918002234567 matches both the toll-free dial peer (tag 91800) and the long-distance dial peer (tag 9110). The toll-free dial peer will be selected first (as long as it is up), as more digits match it (six digits match) versus the long-distance dial peer (four digits match).

```
<output omitted>
*Feb 20 01:40:15.295: //-1/AA68A02D8079/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=918002234567
*Feb 20 01:40:15.295: //-1/AA68A02D8079/DPM/dpMatchPeersCore:
   Result=Success(0) after DP_MATCH_DEST
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
*Feb 20 01:40:15.295: //-1/AA68A02D8079/DPM/dpMatchPeersMoreArg:
   Result=SUCCESS(0)
   List of Matched Outgoing Dial-peer(s):
     1: Dial-peer Tag=91800
     2: Dial-peer Tag=9110
*Feb 20 01:40:15.299: //-1/AA68A02D8079/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=918002234567, Peer Info Type=DIALPEER_INFO_SPEECH
<output omitted>
```

Task 5: Inbound Calls

Step 5-1: Configure for Inbound Calls

To allow inbound calls from the PSTN, two things need to occur: A dial peer must collect the called digits sent from the provider over the PRI trunk, and the digit length must match the internal dial peers.

A dial peer is created using the **incoming called-number** command to match the Dialed Number Identification Service (DNIS) from the trunk. Then the **direct-inward-dial** command uses the Direct Inward Dialing (DID) digits from the trunk to try to match dial peers (hopefully internal extensions).

```
RtrPodx(config)# dial-peer voice 123 pots
RtrPodx(config-dial-peer)# description Inbound calls
RtrPodx(config-dial-peer)# incoming called-number 5105555...
RtrPodx(config-dial-peer)# direct-inward-dial
RtrPodx(config-dial-peer)# port 0/2/0:23
RtrPodx(config-dial-peer)# exit
```

The PSTN simulator is configured to send the full ten-digit number inbound (even if the call was dialed as a seven-digit local number to reach your pod). Because your internal extensions are only four digits, the calls will fail unless incoming digits match the extensions. As discussed in Lab 6-4, Step 3-1, there are a few methods to address this. The fastest option to implement is the **dialplan-pattern** command in telephony-service.

Caution: If you ever change the dialplan pattern, you must remove the previous one with the no command. Overwriting with a new version will not work!

```
RtrPodx(config)# telephony-service
RtrPodx(config-telephony)# dialplan-pattern 1 5105555... extension-length 4
```

Note: While the **dialplan-pattern** command will automatically create full ten-digit dial peers from the ephone-dn extensions, it will not do the same for any dial peers that point to FXS ports. That is, if you have a POTS dial peer that sends extension 1234 to an FXS port, to make it reachable from the PSTN, a second POTS dial peer is needed with a destination pattern that matches the expected number of digits (5105551234, in this case).

After the **dialplan-pattern** command is issued, you can enter the **show dial-peer voice summary** command to see the new ten-digit dial peers created for each four-digit extension.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
RtrPodx# show dial-peer voice summary
dial-peer hunt 0
             AD                                      PRE PASS                 OUT
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN       FER THRU SESS-TARGET     STAT PORT
20001  pots  up   up             5330$              0                             50/0/1
20002  pots  up   up             5331$              0                             50/0/2
20003  pots  up   up             5332$              0                             50/0/3
911    pots  up   up   911       911                0                        up
0/2/0:23
9911   pots  up   up   911       9911               0                        up
0/2/0:23
<output omitted>
20004  pots  up   up             5105555330$        0                             50/0/1
20005  pots  up   up             5105555331$        0                             50/0/2
20006  pots  up   up             5105555332$        0                             50/0/3
```

Step 5-2: Test Inbound Calls

Call the extension on the other IP Phone in your pod using the full local and long-distance numbers. (Don't forget to dial the 9 to get an outside line first.) Make sure that you answer the call or the voice channels are not used. Notice that when the PRI has six channels, the outgoing call uses channel 0/2/0:5 and the incoming call uses channel 0/2/0:0. Put the call on hold and use another line to make another call. This time, the outgoing call uses channel 0/2/0:4 and the incoming call uses channel 0/2/0:1.

```
RtrPodx#
*Feb 20 04:39:47.498: %ISDN-6-CONNECT: Interface Serial0/2/0:0 is now connected to
  5105555330 N/A
*Feb 20 04:39:47.506: %ISDN-6-CONNECT: Interface Serial0/2/0:5 is now connected to
  5555331 N/A
RtrPodx#
*Feb 20 04:39:52.214: %ISDN-6-DISCONNECT: Interface Serial0/2/0:0  disconnected from
  5105555330 , call lasted 4 seconds
*Feb 20 04:39:52.238: %ISDN-6-DISCONNECT: Interface Serial0/2/0:5  disconnected from
  5555331 , call lasted 4 seconds
RtrPodx#
```

If your calls do not work, first verify that your outbound calls to local or long-distance numbers on the PSTN simulator work. Then verify that the inbound dial peer is correct and use the **show dial-peer voice summary** command to display dial peers that match the extension you are trying to call.

If you have more than one pod, call either the full local or long-distance number of an IP Phone in the other pod. Make sure that you answer the call, or the voice channels are not used. To verify inbound calls, call from a phone in the other pod back to an IP Phone in your pod.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 6: Calls over the WAN

An Ethernet connection will be used to simulate the WAN connection to allow all pods to connect together. If you have just two pods, connect them with a crossover cable. If you have three or more, connect them using a switch.

Step 6-1: Configure a WAN Connection

Use the 10.0.0.0 /24 network for the WAN, and configure the Fast Ethernet 0/1 interface with IP address 10.0.0.*x* /24 (where *x* is the pod number).

```
RtrPodx(config)# interface fa0/1
RtrPodx(config-if)# ip address 10.0.0.x 255.255.255.0 (where x is the pod number)
RtrPodx(config-if)# exit
```

Step 6-2: Configure a Routing Protocol (Optional)

Because all the routers will be directly reachable, a routing protocol is not really necessary, but if this were a corporate WAN, the PCs should be able to ping each other.

```
RtrPodx(config)# router eigrp 119
RtrPodx(config-router)# no auto-summary
RtrPodx(config-router)# network 10.0.0.0
RtrPodx(config-router)# exit
```

Step 6-3: Configure Four-Digit VoIP Dial Peers to Other Pods Using the WAN

Careful crafting of the destination pattern is necessary to send the correct numbers to the right pod. You will need to craft a separate dial peer for each pod. The following output shows how to reach pod 21, using the extensions shown in the Pod Addressing Table in Appendix A. With VoIP dial peers, there is no digit stripping like there is with POTS dial peers, so there is no need for **prefix** or **forward-digits** commands.

```
RtrPodx(config)# dial-peer voice 5660 voip
RtrPodx(config-dial-peer)# description WAN calls to Pod 21
RtrPodx(config-dial-peer)# destination-pattern 56[6-8].
RtrPodx(config-dial-peer)# session target ipv4:10.0.0.21
RtrPodx(config-dial-peer)# exit
```

What would the complete dial peer be if a pod had numbers 8200 to 8259 at IP address 172.16.31.10?

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 6-4: Create VoIP Dial Peer for Any Other Pods

Repeat Step 6-3 to create a VoIP dial peer for all other pods. (There is no need to create a dial peer for the extensions in your own pod, as the ephone-dns already create dial peers for them.)

Step 6-5: Verify Calls to Other Pods Using the WAN

Verify that you can call extensions in other pods by dialing just the four-digit extension. Troubleshoot if necessary before moving on to the next task.

Task 7: PSTN Failover

After users get accustomed to dialing four-digit extensions for other people in the company, a WAN failure will result in call failure, even though the PSTN connection is still working. PSTN failover allows the users to successfully dial the four-digit internal extensions even when the WAN is down; the calls are redirected using the PSTN.

Step 7-1: Configure a PSTN Failover

As noted in Lab 6-4, Step 1-1, Rule 4, when two dial peers have the exact same destination pattern, they are selected at random. However, this can be controlled using the **preference** command. The higher the preference value, the less desirable the dial peer is. All dial peers have a default preference of 0, but this does not show in the running configuration. By creating a POTS dial peer that has the exact same destination pattern as the VoIP dial peer, but assigning a preference greater than 0, the VoIP dial peer will be preferred as long as the WAN is up. If the WAN fails, the router then looks for duplicate destination patterns with higher preferences. The only other thing to remember is that simply sending the remaining digits (after the default POTS digit-stripping behavior) will not be enough for the PSTN to route the call. This is where the **prefix** command is so useful. Not only can the stripped digits be preserved, but the other digits needed to complete the call can also be added to make a routable PSTN number (the same as if the call was dialed directly on a phone through the PSTN). For example, to continue with the VoIP dial peer for pod 21 in Step 6-3, and assuming that pod 21 is reachable with seven-digit dialing in the same exchange as your pod, the following dial peer will allow failover to that pod. The leading 56 will be stripped by the normal POTS dial-peer behavior, and the **prefix** command adds the 555 exchange and restores the stripped 56 digits. Notice that the destination pattern is exactly the same as the one in the VoIP dial peer. Also note that a 9 is not needed for the prefix of this dial peer, because the call will be sent directly to the PRI, and not matched to another dial peer first.

```
RtrPodx(config)# dial-peer voice 5555660 pots
RtrPodx(config-dial-peer)# description PSTN failover calls to Pod 21
RtrPodx(config-dial-peer)# destination-pattern 56[6-8].
RtrPodx(config-dial-peer)# prefix 55556
RtrPodx(config-dial-peer)# preference 1
RtrPodx(config-dial-peer)# port 0/2/0:23
RtrPodx(config-dial-peer)# exit
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 7-2: Configure a PSTN Failover

If a pod had numbers 608-555-8200 to 608-555-8259, what would the failover dial peer be?

Step 7-3: Configure Remaining PSTN Failover Dial Peers

Repeat Step 7-1 to create a POTS failover dial peer for all other pods.

Step 7-4: Test PSTN Failover

Note: If the router knows that the IP address is unreachable (for example, the local interface is down), the call fails over immediately to the next-higher-preference dial peer. However, if the router is not sure that the route is down (for example, the remote interface is down, but connected through a switch or cloud, so the local interface is still up), the router will wait ten seconds by default before failover to ensure that there is no other path.

Shut down the Fa0/1 interface or disconnect the cable and attempt to dial the same extensions you did in Step 6-4. Verify that you can call each of the other pods (and that they can call you) using four digits. You can also verify that the PSTN is used, for if the call is answered, the console will show the PRI channel-in-use messages. If you are having problems with the failover dial peer, first verify that you can directly call the other pod using a local or long-distance number on a VoIP phone to confirm that the PSTN calls are working.

Step 7-5: Verify That VoIP Dial Peers Resume Calls When the WAN Is Back Up

Reenable the WAN interface (and make sure that the other pod has its WAN connection up, too) and attempt to dial the same extensions you did in Step 6-4. Verify that you can call each of the other pods (and that they can call you) using four digits over the WAN.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 6-6: Dial-Peer Configuration Using CCP

Equipment Required

This lab uses the following equipment:

- Two Cisco routers with voice IOS
- Switch that supports voice VLANs
- Lab configuration from Lab 5-2, 5-3, 6-1, or 6-2 (see the scenario for details)
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)

Optional hardware components (see the scenario for details):

- Cisco router configured as PSTN simulator
- T1/E1/PRI Multiflex Trunk VWIC cards or Network Modules (see the scenario for details)
- Analog Foreign eXchange Station (FXS) cards
- Analog Foreign eXchange Office (FXO) cards
- DSP resources in the routers (PVDM chips) to enable the Multiflex Trunk and FXS or FXO ports

Learning Objectives

Upon completion of this lab, you will be able to

- Configure dial peers to connect to the PSTN
- Configure dial peers to connect to remote offices using the WAN
- Configure failover for calls to remote offices using the PSTN when the WAN is down

Scenario

SOI wants to connect to customers using the PSTN, and to remote branch offices of the company using the WAN. To avoid WAN failure from disabling four-digit dialing between locations, call failover from the WAN to the PSTN needs to be configured.

Note: Cisco has recorded screen casts for configuring various items using CCP at www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note: For T1/E1 connectivity, CCP currently supports only voice interface cards VWIC2-1MFT-T1/E1 and VWIC2-2MFT-T1/E1 and network modules NM-HDV2-1T1/E1 and NM-HDV2-2T1/E1. Older Multiflex cards, such as the VWIC-1MFT-T1, VWIC-1MFT-E1, VWIC-2MFT-T1, and VWIC-2MFT-E1, are not recognized and cannot be configured in CCP.

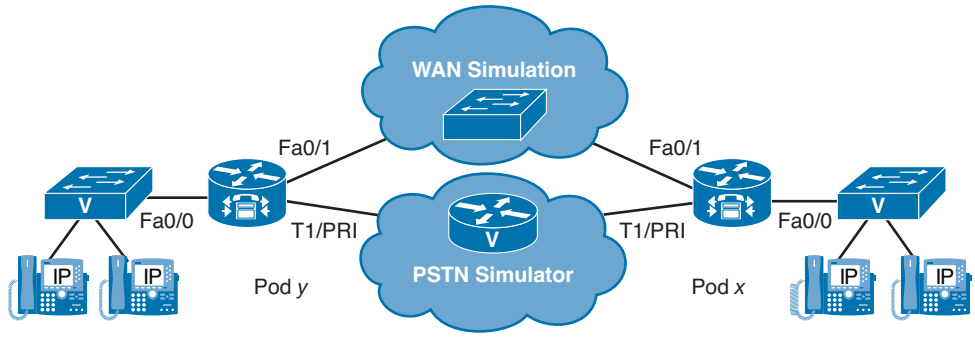
This lab has options for various hardware and notes the impacts each has on the configuration. Listed in order of best case to most limited, the hardware options are as follows:

- **Option 1:** Two (or more) pods with the PSTN simulator (see Appendix E) and an Ethernet connection to simulate the WAN, as shown in Figure 6-12. This option allows you to complete all parts of the lab.

https://t.me/learningnets

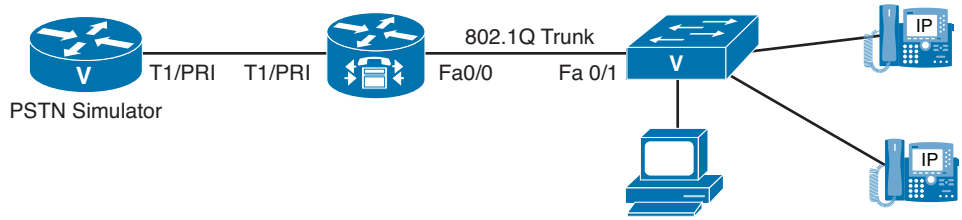
From the Library of Aliwarman Tarihoran

Figure 6-12 Topology Diagram Option 1: Two Pods and PSTN Simulator



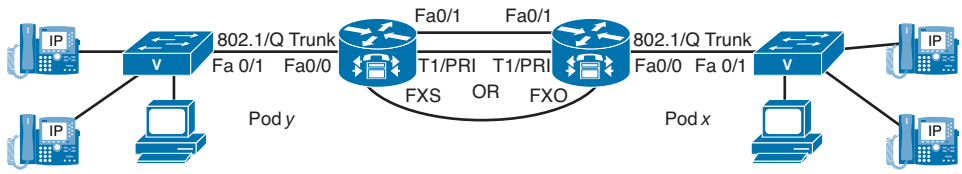
- **Option 2:** One pod with the PSTN simulator (see Appendix E), as shown in Figure 6-13. This will allow you to complete Tasks 2 to 7, but not test the VoIP dial peers (Task 7) or PSTN failover (Task 8). If you are able to reconfigure the PSTN simulator as another pod, you could complete the WAN links (Task 7) separately.

Figure 6-13 Topology Diagram Option 2: One Pod and PSTN Simulator



- **Option 3:** Two pods directly connected with digital or analog interfaces, as shown in Figure 6-14. This will allow you to set up another pod to be a simplistic PSTN simulator so that you can complete Tasks 2 to 7, but not be able to test the PSTN dial peers (Tasks 4 and 5). Additionally, if you are using FXO-to-FXS interfaces, you will not be able to test Task 6 (inbound dial peers).

Figure 6-14 Topology Diagram Option 3: Two Pods with Digital Interfaces and Ethernet Connection



Task 1: Load Prior Configurations

This lab is based on the configuration from Lab 5-2, 5-3, 6-1, or 6-2. If necessary, load the configuration for both the switch and router. Connect a PC to the switch and verify that it can ping the router and switch management addresses. Connect the VoIP phones and verify that you can call between them. Troubleshoot if necessary.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2A: Configure Digital T1/E1/PRI Interface

If you are using a T1/E1/PRI interface (see the note in the scenario) that has not been configured, follow these directions. If you are using analog FXO with FXS interfaces, skip ahead to Task 2B.

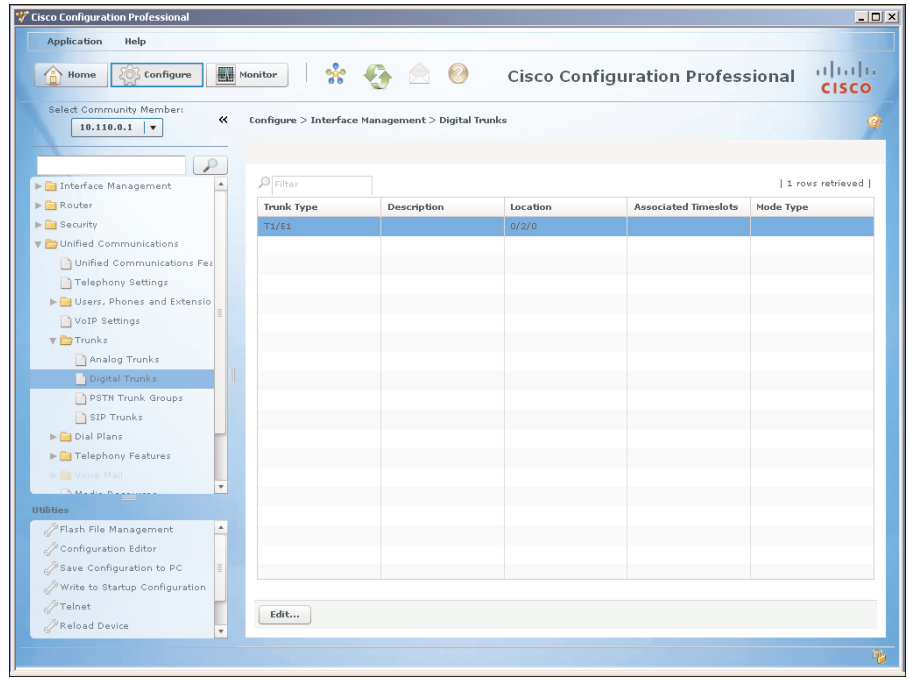
Step 2A-1: Digital Trunks

Use the community created in Lab 4-1, Step 3 to connect to the router. With the router discovered, click **Configure**. The pane on the left will show various categories of router configuration options. (The items you see will depend on the IOS you have installed.)

Click the **Unified Communications** folder icon to expand the subitems.

Click the **Trunks** folder icon to expand the subitems, and click the **Digital Trunks** subitem. In the Digital Trunks pane on the right is a table showing any T1/E1 interfaces. See Figure 6-15 for an example of this window. If you do not see any items, verify that you have a compatible interface and check the note in the scenario.

Figure 6-15 Digital Trunks



Click to highlight the desired trunk (if there is more than one) and then click the **Edit** button at the bottom of the window.

Step 2A-2: T1/E1 Interface

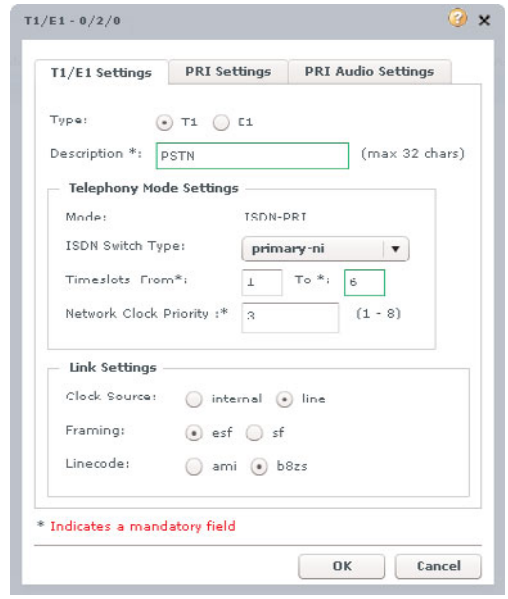
The T1/E1 Interface window will open to the T1/E1 Settings tab.

1. Select the Type radio button to change between **T1** or **E1** (if needed).
2. Enter **PSTN** in the Description field.
3. Change the **Timeslots To** field if needed. (The PSTN simulator in Appendix E is configured for six channels on the PRI.) See Figure 6-16 for an example of this window.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-16 Digital T1/E1 Settings



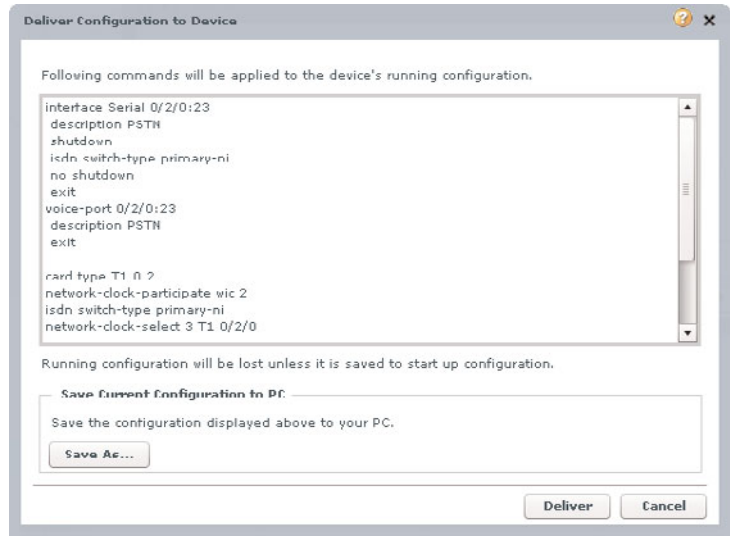
Note: If you are configuring Option 3 only, configure the PRI the same on the remote pod, but then click the **PRI Settings** tab and change the Clock Type radio button to **Source (Network or NT)** for the remote pod only. This is the same as the CLI commands shown in Lab 6-2, Task 4.

4. Click **OK**.

Step 2A-3: Deliver Configuration from CCP to the Router

The Deliver Configuration to Device dialog box opens. See Figure 6-17 for an example of this window.

Figure 6-17 Deliver Configuration to Device Dialog Box



Click **Deliver** to send the commands to the router.

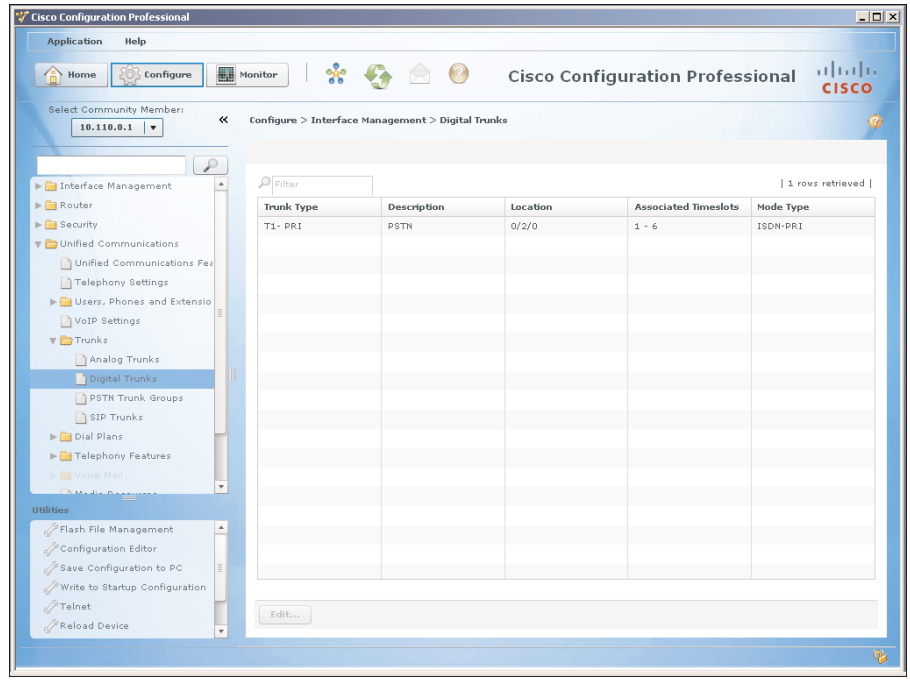
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2A-4: Deliver Configuration from CCP to the Router

The Digital Trunks window shows the configured T1 or E1, as shown in Figure 6-18.

Figure 6-18 Digital Trunks Configured



Cable all pods using PRI crossover cables to the PSTN simulator (Option 1 or 2) or to the other pod (Option 3). See the note about T1 crossover cables in Lab 6-2, Step 2-2.

Task 2B: Configure Analog FXO/FXS Interfaces

If you are using a T1/E1/PRI interface, skip ahead to Task 3. If you are using analog FXO with FXS interfaces, follow these directions.

Step 2B-1: Analog Trunks

Use the community created in Lab 4-1, Step 3 to connect to the router. With the router discovered, click **Configure**. The pane on the left will show various categories of router configuration options. (The items you see will depend on the IOS you have installed.)

Click the **Unified Communications** folder icon to expand the subitems.

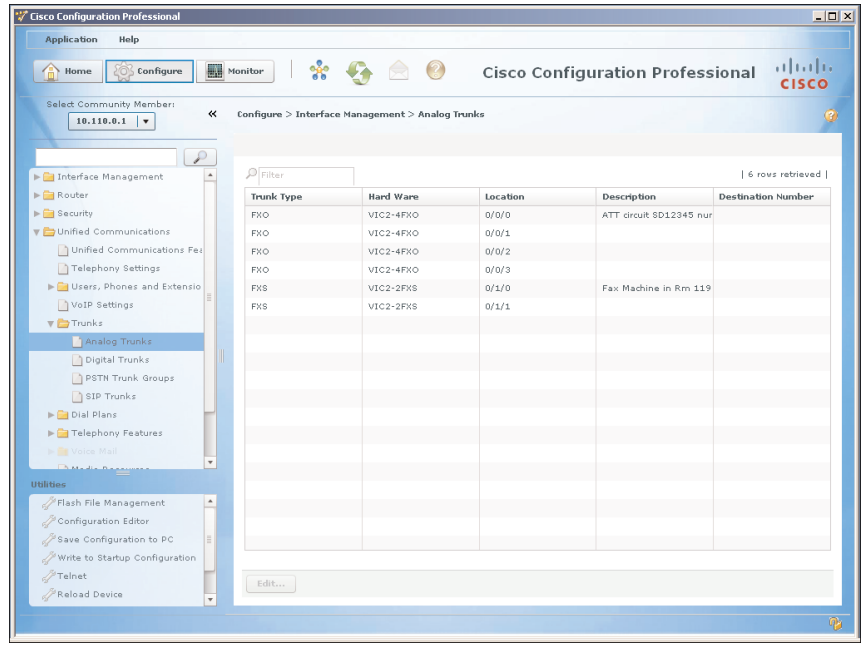
Click the **Trunks** folder icon to expand the subitems, and click the **Analog Trunks** subitem. In the Analog Trunks pane on the right is a table showing any FXO and FXS interfaces. See Figure 6-19 for an example of this window.

There should be no configuration necessary, other than adding a description, as noted in Lab 6-1.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-19 Analog Trunks

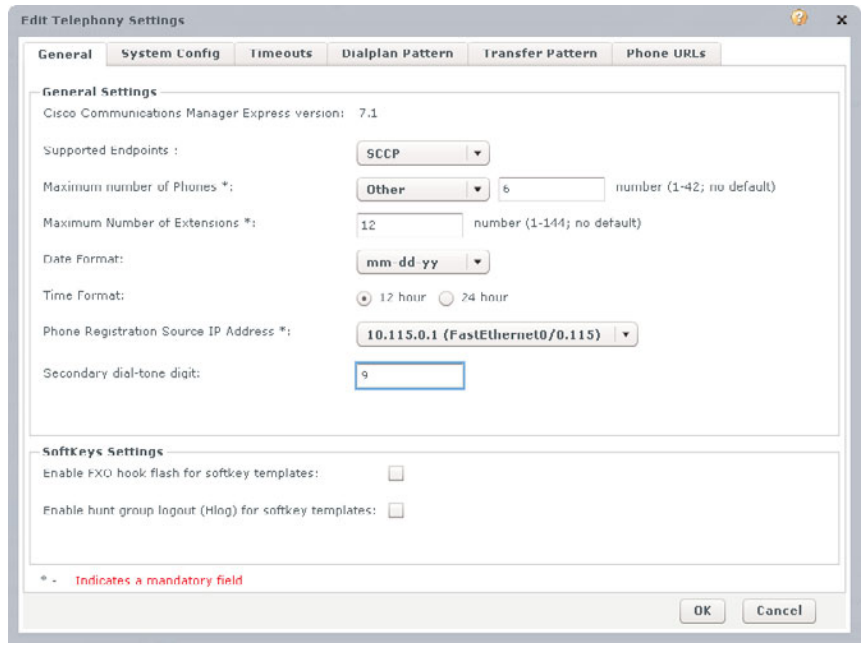


Task 3: Configure Secondary Dial Tone

When configuring a PBX-type dial plan, there needs to be an outside line access digit. Many PBX users are used to hearing a slightly different dial tone after dialing this digit, before dialing the intended PSTN number. This secondary dial tone for outside lines can be configured under the **Unified Communications > Telephony Settings** subitem.

Click the **Edit** button to open the Edit Telephony Settings dialog box. Enter **9** in the Secondary Dial-Tone Digit field. See Figure 6-20 for an example of this window.

Figure 6-20 Edit Telephony Settings



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Click the **OK** button, and the Deliver Configuration to Device dialog box opens. Click **Deliver** to send the commands to the router.

Task 4: Create Outgoing Dial Plan

CCP is able to import templates to quickly create dial plans for various countries. After importing a country-specific set of dial peers, you can customize them to suit your needs.

Table 6-12 lists the desired dial plan to be implemented.

Table 6-12 NANP PSTN Dial Plan and Test Numbers

Pattern	Number Type	Test Number(s)
911 and 9911	Emergency numbers	911 and 9911
[2-8]11	Service codes (N11)	311, 811, and so on
[2-9].....	Local calls (seven-digit areas)	567-0001
[2-9]..[2-9].....	Local calls (ten-digit areas)	510-567-0001
1[2-9]..[2-9].....	Long-distance (toll) calls	1-333-444-5678
1800[2-9].....	Toll-free numbers. (1-800 numbers—this should also include 888, 877, 866, and 855 area codes to cover all current toll-free numbers.)	1-800-223-4567
1900[2-9].....	Premium-rate numbers (1-900 numbers)	1-900-223-4567
011T	International dialing (011, then country code, then subscriber number)	011-44-88221234 (# key to stop digit collection)

Step 4-1: POTS Dial Plans

Under the **Unified Communications > Dial Plans > POTS** subitem, in the Create Dial Plans tab, click the **Import Outgoing Dial Plan Template** radio button. See Figure 6-21 for an example of this window.

Click the **Launch selected task** button at the bottom of the window.

Step 4-2: Import Outgoing Template

The Configure Outgoing Dial Plans dialog box will open to Step 1 – Select File. Click the **Browse** button, and navigate to the templates folder (default location is C:\Program Files\Cisco Systems\CiscoCP\template\OutgoingDialPlan).

1. Click the name of the template for your country (**NorthAmerica.csv** for this lab).
2. Click **Open**.
3. Leave the **Delete all existing Dialing Restrictions and Outgoing Dial Plans before applying new records** check box selected. See Figure 6-22 for an example of this window.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-21 POTS Dial Plans

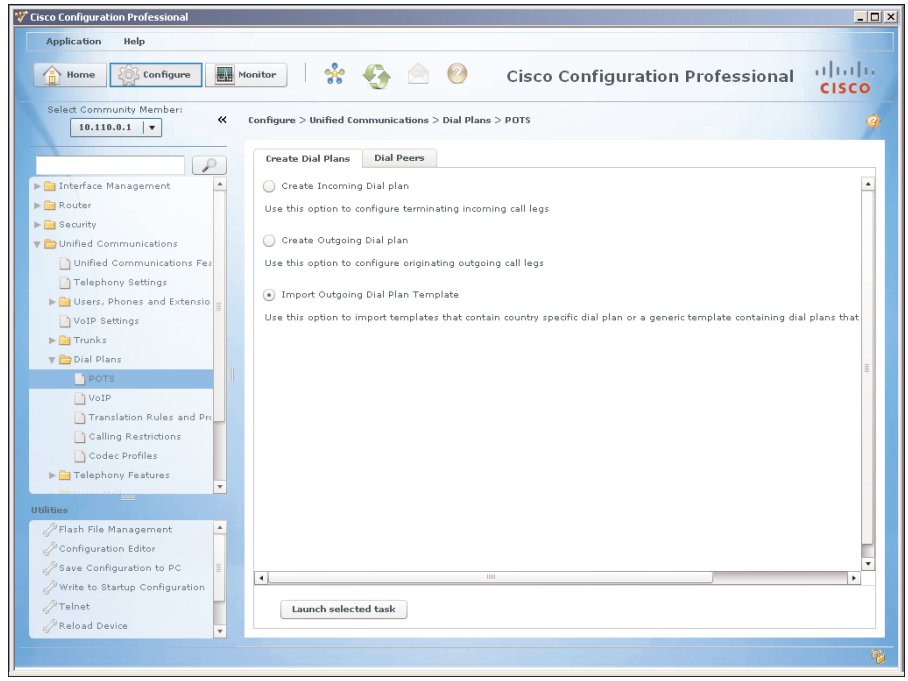
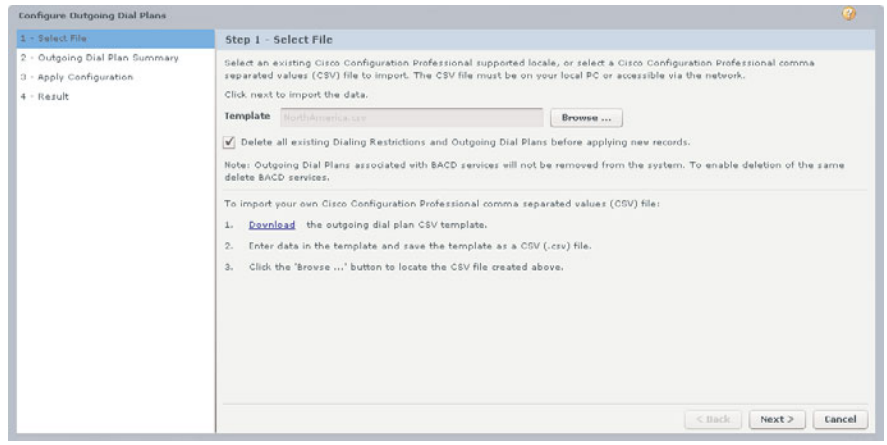


Figure 6-22 Import Outgoing Dial Plan Template—Select File



4. Click the **Next** button at the bottom of the dialog box.
5. A confirmation dialog box will open. Click **Yes**.

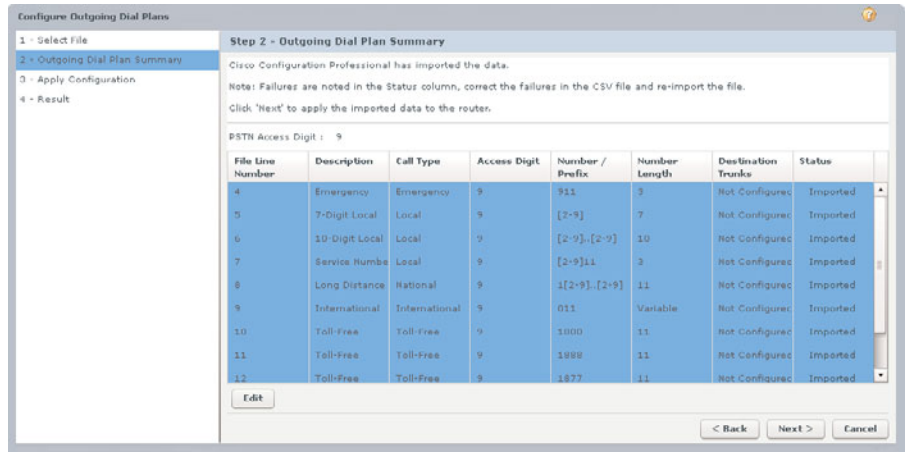
Step 4-3: Outgoing Dial Plan Summary

The Step 2 – Outgoing Dial Plan Summary dialog box shows the dial peers that will be created. Notice that all the dial peers have Not Configured in the Destination Trunks fields. To save time selecting the trunk, click the first dial peer and then scroll down and press Ctrl+Shift while clicking on the last dial peer to change all of them at once. See Figure 6-23 for an example of this window.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-23 Import Outgoing Dial Plan Template—Summary

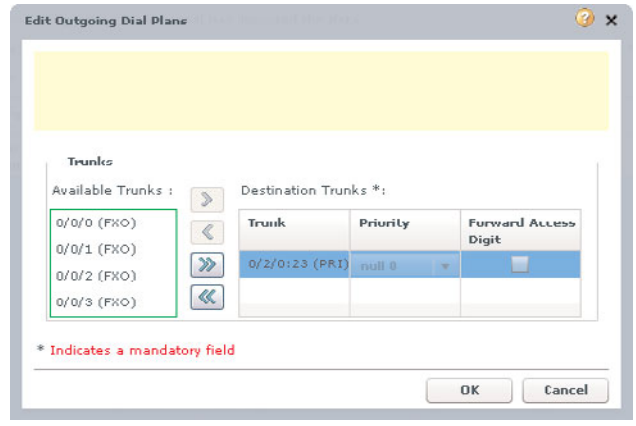


Click the **Edit** button at the bottom of the dialog box.

Step 4-4: Selecting Destination Trunk

The Edit Outgoing Dial Plans dialog box shows a list of available trunks. Under the Available Trunks, click the PRI interface (or one of the FXO interfaces if completing Option 3 with FXO ports) and then click the arrow (>) button to move the selection to the Destination Trunks list. See Figure 6-24 for an example of this window.

Figure 6-24 Edit Outgoing Dial Plans



Click the **OK** button to return to the Outgoing Dial Plan Summary dialog box.

In the Outgoing Dial Plan Summary dialog box, click the **Next** button at the bottom.

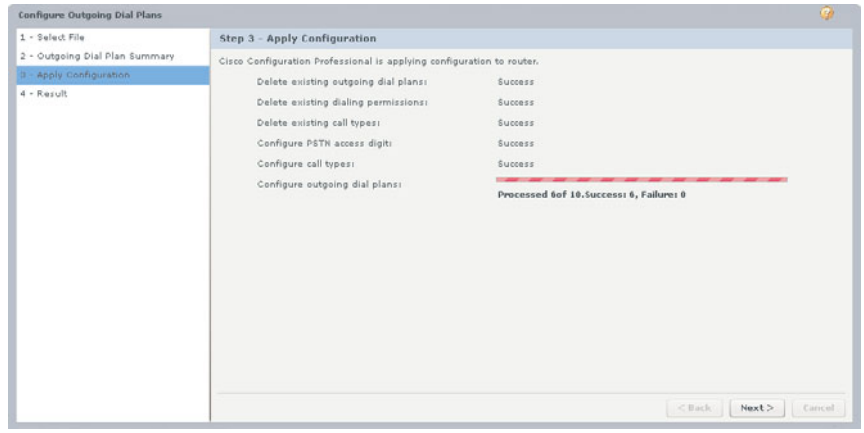
Step 4-5: Apply Configuration

The Step 3 – Apply Configuration dialog box will process the configuration changes. Do not be alarmed if the progress bar does not show all items processed, as long as there are no failures. See Figure 6-25 for an example of this window.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-25 Apply Configuration



Click the **Next** button at the bottom of the dialog box.

The Step 4 – Result dialog box will open. Click the **Finish** button.

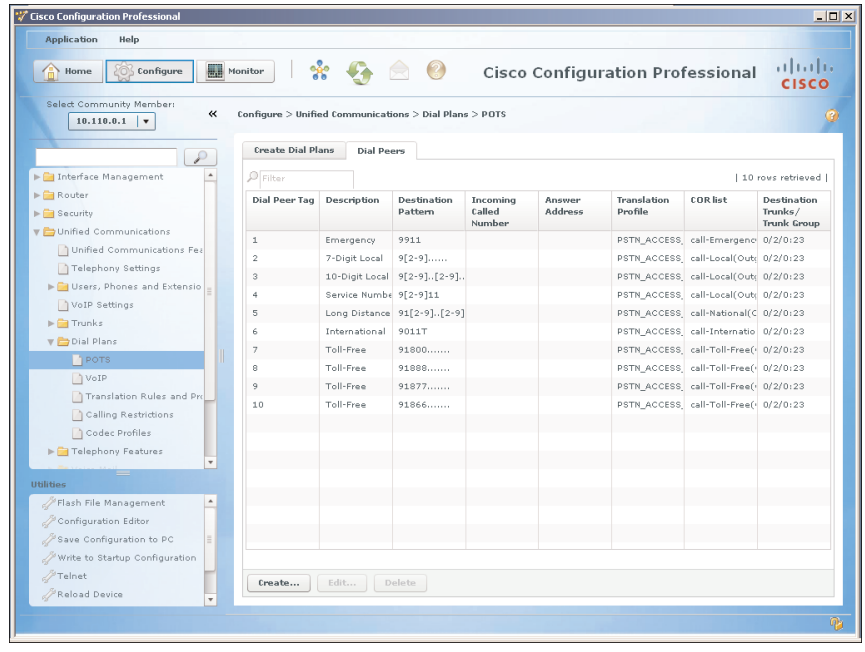
Task 5: Create Outbound POTS Dial Peers

After importing a country-specific set of dial peers, you can customize them to suit your needs. As seen in Table 6-12, the dial peer for 911 (without the access digit), the 855 toll-free area code, and the premium-rate (1-900) numbers are not included in the template. It is also good to know how to manually add and edit dial peers without using the wizard.

Step 5-1: View POTS Dial Peers

Under the **Unified Communications > Dial Plans > POTS** subitem, click the **Dial Peers** tab, which lists all the existing dial peers. See Figure 6-26 for an example of this window.

Figure 6-26 Dial Peers



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Click the **Create** button at the bottom of the dialog box.

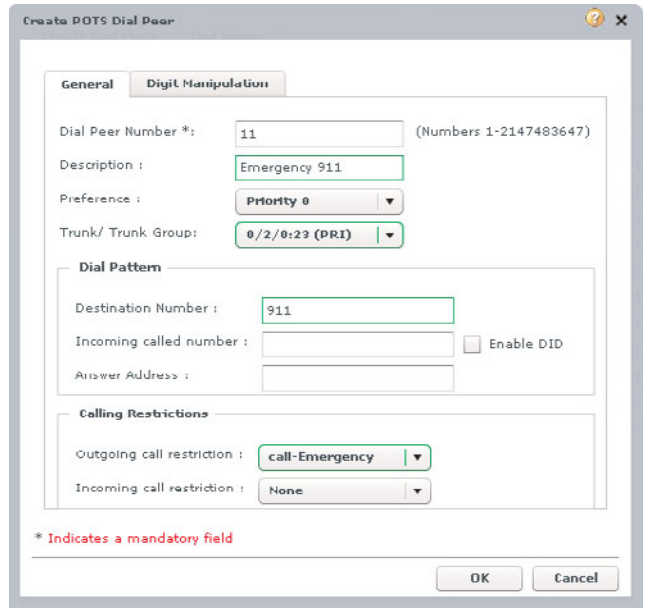
Step 5-2: Create POTS Dial Peer

The Create POTS Dial Peer dialog box will open to the General tab. Use the following steps to create a dial peer for the 911 calls.

1. Enter **Emergency 911** in the Description field.
2. Select the PRI interface (or one of the FXO interfaces if completing Option 3 with FXO ports) from the Trunk/Trunk Group pull-down menu.
3. Enter **911** in the Destination Number field.
4. Select **call-Emergency** from the Outgoing Call Restriction pull-down menu.

See Figure 6-27 for an example of this window.

Figure 6-27 Create POTS Dial Peer General Tab



Step 5-3: Digit Manipulation

As discussed in Lab 6-4, Task 2, POTS dial peers have digit stripping by default. CCP automatically configures the dial peer to strip only the outside line access digit. However, in this case, the goal is to configure 911 without an access digit. If you just left the default configuration, the 9 would be stripped and only the 11 would be sent to the PSTN. Click the **Digit Manipulation** tab to see the defaults. Click to deselect the **Enable Digit Strip** check box. See Figure 6-28 for an example of this window.

Click the **OK** button, and the Deliver Configuration to Device dialog box opens. See Figure 6-29.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-28 Create POTS Dial Peer Digit Manipulation Tab

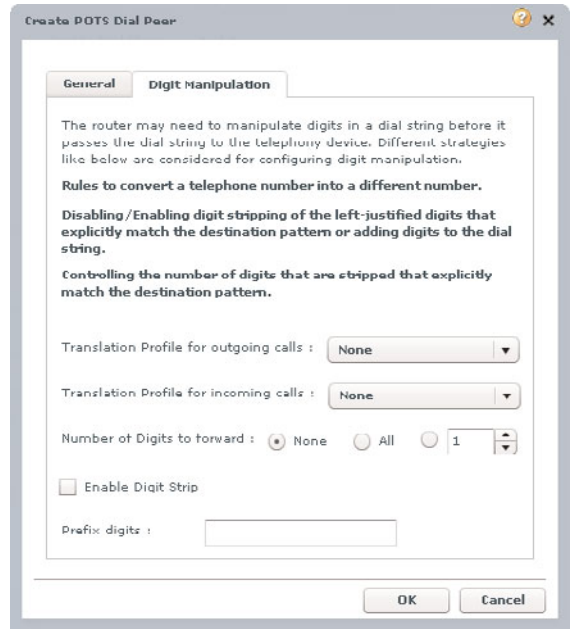
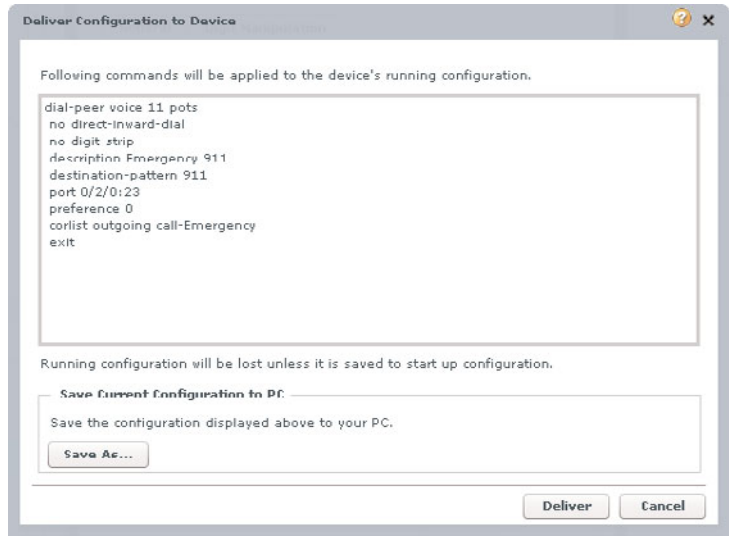


Figure 6-29 Deliver Configuration to Device Dialog Box



Click **Deliver** to send the commands to the router.

Step 5-4: Dial Peers Challenge

Create dial peers for the 855 toll-free area code and the premium-rate (1-900) numbers. Examine the 1-800 dial peer and Steps 5-1 through 5-3 to help you create the two dial peers that match only those numbers.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 5-5: Make Test Calls to the PSTN Simulator

Use the test numbers in Table 6-12 to place calls from an IP Phone to the PSTN simulator. (Don't forget to dial the 9 to get an outside line first.) The PSTN simulator will play a different sound file for each test number listed.

Task 6: Create Incoming Dial Plan

CCP has a wizard to quickly create an incoming dial plan.

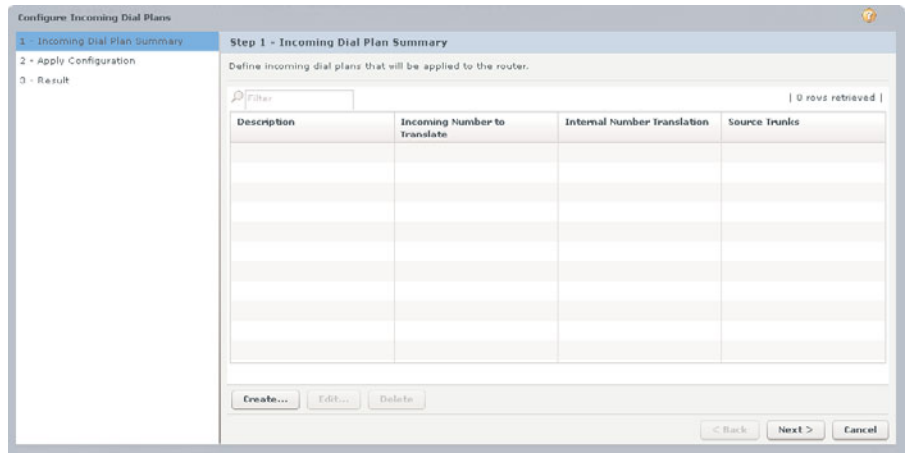
Step 6-1: Create Dial Plans Wizard Selection

Under the **Unified Communications > Dial Plans > POTS** subitem is the **Create Dial Plans** tab. Click the **Create Incoming Dial plan** radio button (if it is not already selected), and click the **Launch selected task** button at the bottom of the window.

Step 6-2: Incoming Dial Plan Summary

The Configure Incoming Dial Plans dialog box will open to Step 1 – Incoming Dial Plan Summary. Click the **Create** button. See Figure 6-30 for an example of this window.

Figure 6-30 Incoming Dial Plan Summary



Step 6-3: Create Incoming Dial Plan

The Create Incoming Dial Plan dialog box will open.

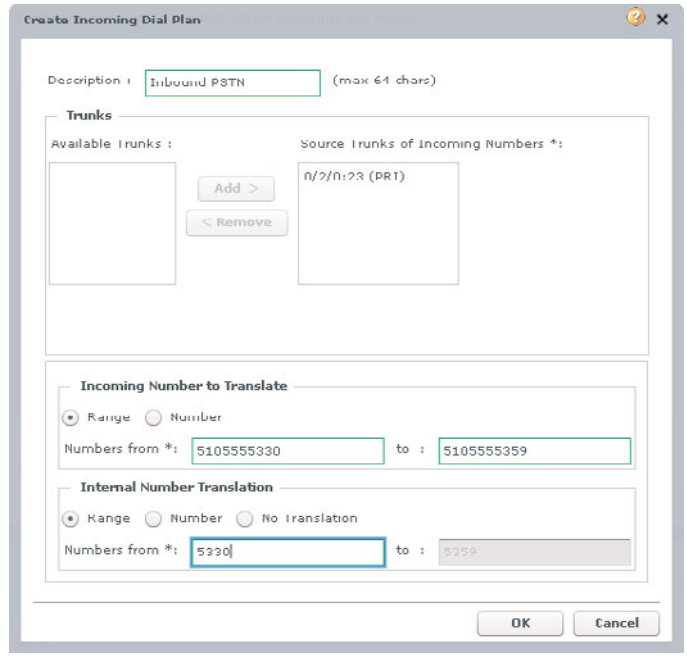
1. Enter **Inbound PSTN** in the Description field.
2. Under the Available Trunks, click the PRI interface and then click the **Add** button to move the selection to the Source Trunks of Incoming Numbers list.
3. Enter the full range of phone PSTN numbers for your pod (see the Pod Addressing Table in Appendix A) in the Numbers From and To fields, under Incoming Number to Translate. (If you are using the PSTN simulator, the numbers should be ten digits long.)
4. Enter the first four-digit extension for your pod in the Numbers From field, under Internal Number Translation.

See Figure 6-31 for an example of this window, showing the Pod 11 configuration.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-31 Create Incoming Dial Plan



5. Click **OK**.
6. The Step 1 – Incoming Dial Plan Summary dialog box shows the dial plan that will be created. Click **Next**.
7. The Step 2 – Apply Configuration screen shows the status of the configuration changes. Click **Next**.
8. At the Step 3 – Results screen, click **Finish**.
9. Back at the POTS window, click the **Dial Peers** tab to see the new inbound dial peer created.

Step 6-4: Test Incoming Dial Plan

Call the extension on the other IP Phone in your pod using the full local and long-distance numbers. (Don't forget to dial 9 to get an outside line first.) The other extension should ring, even though dialed as a local or long-distance number. If not, troubleshoot as necessary.

Task 7: Create VoIP Dial Peers

To send calls over an IP-based network, VoIP dial peers are used. VoIP dial peers are ideal for calls between locations over a WAN. (If completing Option 2, you can create the VoIP dial peers, but you will not be able to test them unless you reconfigure the PSTN simulator to be another pod.)

Step 7-1: Configure a WAN Connection

An Ethernet connection will be used to simulate the WAN connection to allow all pods to connect together. If you have just two pods, connect them with a crossover cable. If you have three or more, connect them using a switch.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

The WAN connection on Fast Ethernet 0/1 can be configured using CCP in the **Interface Management > Interfaces and Connections** subitem. To save time, the CLI will be used instead.

Use the 10.0.0.0 /24 network for the WAN, and configure the Fast Ethernet 0/1 interface with IP address 10.0.0.*x* /24 (where *x* is the pod number).

```
RtrPodx(config)# interface fa0/1
RtrPodx(config-if)# ip address 10.0.0.x 255.255.255.0 (where x is the pod number)
RtrPodx(config-if)# exit
```

Step 7-2: Configure a Routing Protocol (Optional)

Because all the devices will be directly reachable, a routing protocol is not really necessary, but if this was a corporate WAN environment, a routing protocol (or static routing) would be necessary. In either case, the PCs should be able to ping each other. The routing protocol can be configured using CCP in the **Router > Static and Dynamic Routing** subitem. To save time, the CLI will be used instead.

```
RtrPodx(config)# router eigrp 119
RtrPodx(config-router)# no auto-summary
RtrPodx(config-router)# network 10.0.0.0
RtrPodx(config-router)# exit
```

Step 7-3: View VoIP Dial Peers

Click the **Unified Communications > Dial Plans > VoIP** subitem. Click the **Create** button at the bottom of the pane.

Step 7-4: Create VoIP Dial Peer

The Create VoIP Dial Peer dialog box will open to the General tab.

1. Enter a description for the dial peer (use the name of the remote pod this dial peer will connect to).
2. Enter the IP address of the remote pod in the Remote Site field.
3. Enter the four-digit extension range of the remote pod (using wildcards) in the Destination Number field. Careful crafting of the destination pattern is necessary to send the correct numbers to the right pod. (The extensions to reach Pod 2 were used in the example in the figure.)

See Figure 6-32 for an example of this window.

Unlike POTS dial peers, VoIP dial peers do not have automatic digit stripping, so there is no need to use the Digit Manipulation tab. Click the **OK** button, and the Deliver Configuration to Device dialog box opens. Click **Deliver** to send the commands to the router.

Step 7-5: Create VoIP Dial Peer for Any Other Pods

Repeat Step 7-4 to create a VoIP dial peer for all other pods. (There is no need to create a dial peer for the extensions in your own pod, as the ephone-dns already create dial peers for them.)

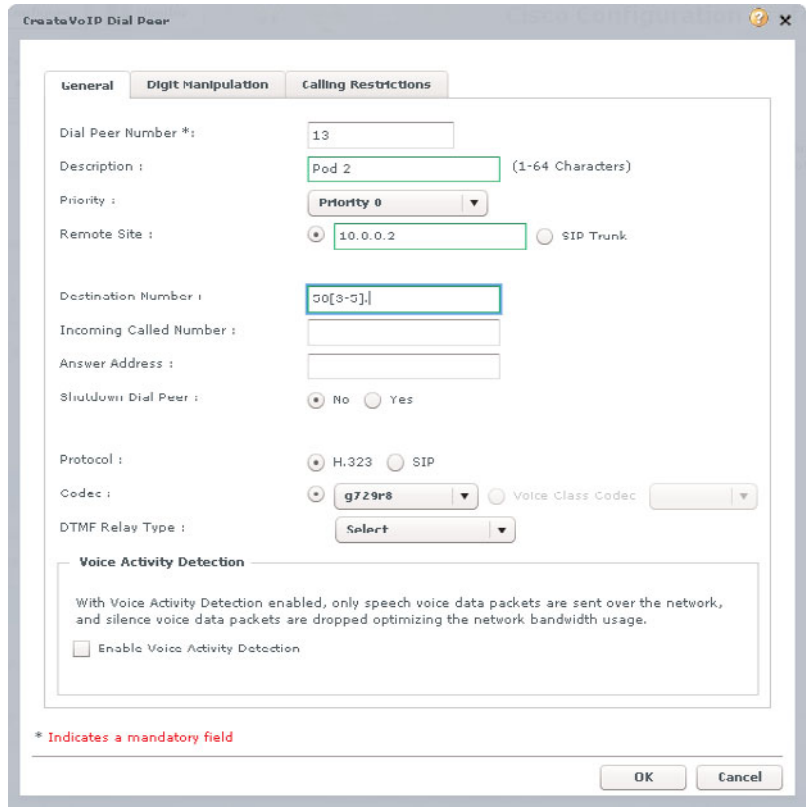
Step 7-6: Verify Calls to Other Pods Using the WAN

Verify that you can call extensions in other pods by dialing just the four-digit extension. Troubleshoot if necessary before moving on to the next task.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-32 Create VoIP Dial Peer Example



Task 8: PSTN Failover

As noted in Lab 6-5, after users get accustomed to dialing four-digit extensions for other people in the company, a WAN failure will result in call failure, even though the PSTN connection is still working. PSTN failover allows the users to successfully dial the four-digit internal extensions even when the WAN is down; the calls are redirected using the PSTN. As noted in Lab 6-4, Step 1-1, Rule 4, when two dial peers have the exact same destination pattern, they are selected at random. However, this can be controlled using the **preference** command. The higher the preference value, the less desirable the dial peer is. All dial peers have a default preference of 0. By creating a POTS dial peer that has the exact same destination pattern as the VoIP dial peer, but assigning a preference greater than 0, the VoIP dial peer will be preferred as long as the WAN is up. If the WAN fails, the router then looks for duplicate destination patterns with higher preferences.

Step 8-1: Configure a POTS Dial Peer for Failover

Under the **Unified Communications > Dial Plans > POTS** subitem, click the **Dial Peers** tab, which lists all the existing dial peers. Click the **Create** button at the bottom of the dialog box.

Step 8-2: Configure a POTS Dial Peer for Failover

The Create POTS Dial Peer dialog box will open to the General tab.

1. Enter a description for the dial peer (add **Failover** to the name of the remote pod this dial peer will connect to).
2. From the Preference pull-down menu, select **Priority 1**.

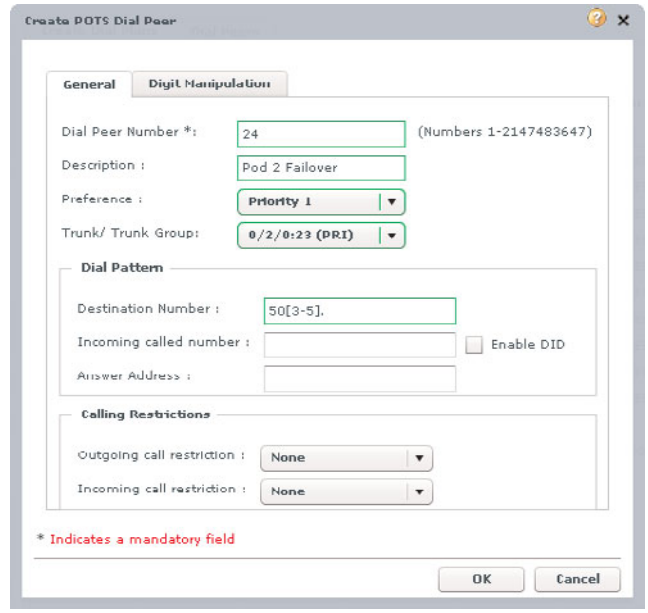
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. Select the PRI interface (or one of the FXO interfaces if completing Option 3 with FXO ports) from the Trunk/Trunk Group pull-down menu.
4. Enter the four-digit extension range (using wildcards) of the remote pod in the Destination Number field. Note: This should be exactly the same as was used in the VoIP dial peer in Step 7-4.

See Figure 6-33 for an example of this window.

Figure 6-33 Create Failover POTS Dial Peer Example



Step 8-3: Digit Manipulation

The only other thing to remember is that simply sending the remaining digits (after the default POTS digit-stripping behavior) will not be enough for the PSTN to route the call. This is where the **prefix** command is so useful. Not only can the stripped digits be preserved, but the other digits needed to complete the call can also be added to make a routable PSTN number (the same as if the call was dialed directly on a phone through the PSTN).

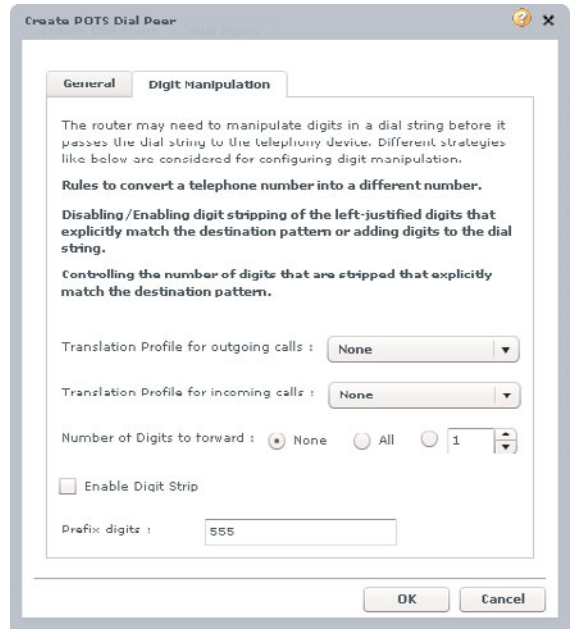
Click the **Digit Manipulation** tab.

Deselect the **Enable Digit Strip** check box (which will preserve the 50 from being stripped), and in the Prefix Digits field, enter the necessary digits to allow the call to complete over the PSTN. For example, Pod 2 is at numbers 5555030 to 5555059, and the 5030 to 5059 is part of the dial peer. But to create a seven-digit local number the exchange needs to be added. In this case, the prefix digits would be 555. Note that a 9 is not needed for the prefix of this dial peer, because the call will be sent directly to the PRI and not matched to another dial peer first. See Figure 6-34 for an example of this window.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-34 Failover POTS Digit Manipulation Example



Click the **OK** button, and the Deliver Configuration to Device dialog box opens. Click **Deliver** to send the commands to the router.

Step 8-4: Configure Remaining PSTN Failover Dial Peers

Repeat Steps 8-2 and 8-3 to create a POTS failover dial peer for all other pods.

Step 8-5: Test PSTN Failover

Note: If the router knows that the IP address is unreachable (for example, the local interface is down), the call fails over immediately to the next-higher-preference dial peer. However, if the router is not sure that the route is down, (for example, the remote interface is down, but connected through a switch or cloud, so the local interface is still up), the router will wait ten seconds by default before failover to ensure that there is no other path.

Shut down the Fa0/1 interface or disconnect the cable and attempt to dial the same extensions you did in Step 7-6. Verify that you can call each of the other pods (and that they can call you) using four digits. If you are having problems with the failover dial peer, first verify that you can directly call the other pod using a local or long-distance number on a VoIP phone to confirm that the PSTN calls are working.

Step 8-6: Verify That VoIP Dial Peers Resume Calls When the WAN Is Back Up

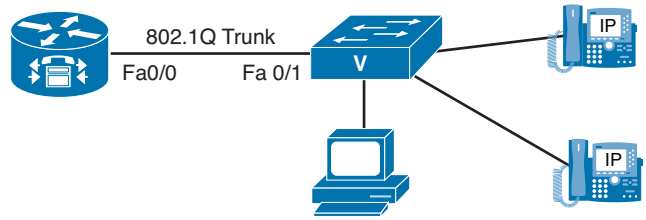
Reenable the WAN interface (and make sure that the other pod has its WAN connection up, too) and attempt to dial the same extensions you did in Step 8-5. Verify that you can call each of the other pods (and that they can call you) using four digits over the WAN.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 6-7: Quality of Service (QoS)

Figure 6-35 Optional Topology Diagram



Equipment Required (Optional)

No equipment is required for this lab, but the following optional equipment can be used:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Lab configuration from Lab 5-2, 5-3, 6-1, or 6-2
- One or more IP Phones (desk phone or soft phone on PC or Windows VM)

Learning Objectives

Upon completion of this lab, you will be able to

- Understand the reasons for quality of service (QoS)
- Understand QoS mechanisms
- (Optional) Configure AutoQoS on Cisco routers and switches

Scenario

Shiny Objects Inc. (SOI) understands that mixing voice traffic with data can cause problems for the voice traffic. This is one reason the voice traffic is in a separate VLAN. However, there are plenty of places in a network where the voice and data traffic are not separated (such as soft phones on the PC). If real-time video traffic is added to the network, the demands for quality of service (QoS) become even greater. The first step to QoS is to understand the requirements of different categories of traffic. The most basic division of traffic is voice, video, and data. (Data traffic can be further divided into a variety of categories, such as business-critical, transactional, network management, bulk, and so on.) As shown in Figure 6-36, voice traffic consists of small regular frames, while video traffic takes up large amounts of bandwidth and data traffic can be highly variable.

Table 6-13 lists the requirements of each traffic category. Knowing the requirements is critical to creating an appropriate QoS policy.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-36 Network Traffic Characteristics

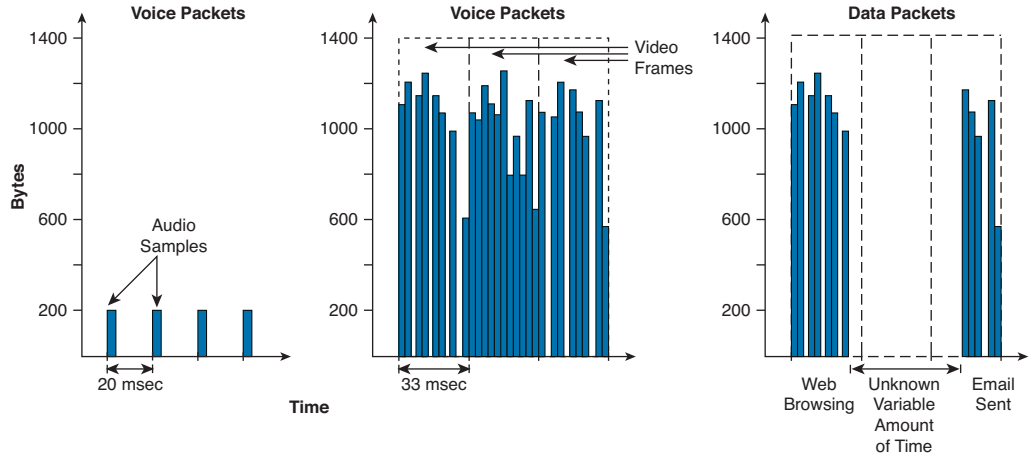


Table 6-13 Network Traffic Requirements

	Voice Traffic	Video Traffic	Data Traffic
Bandwidth requirements	Low	High	Low to High
Smooth or bursty	Smooth	Bursty	Both
Benign or greedy	Benign	Greedy	Both
Drop sensitivity	High (<1% lost)	High (<1% lost)	Medium to Low
Delay sensitivity	High (<150 ms)	High (<150 ms)	Low
Jitter sensitivity	High (<30 ms)	High (<30 ms)	Low
Traffic mechanisms	UDP priority	UDP priority	TCP retransmits

There are three main QoS mechanisms:

- **Best Effort:** No special QoS considerations.
- **Integrated Services (IntServ):** Uses the Resource Reservation Protocol (RSVP) to reserve bandwidth prior to the traffic flow starting.
- **Differentiated Services (DiffServ):** The most common method for QoS. With DiffServ, each device can be configured to respond to traffic using a variety of mechanisms and separate traffic into various classes.

DiffServ QoS Mechanisms

The main tools of DiffServ QoS are

- **Classification:** Each packet examined by a QoS mechanism needs to be classified. Classes of traffic can be as simple as bronze, silver, or gold or as detailed as necessary.
- **Marking:** Closely linked to classification is marking. Ideally, packets are marked once based on classification, and then only the marking needs to be examined by devices farther along the data path. (Of course, later devices can remark the traffic based on their own classification.) Marking can be done in the Layer 2 frame or the Layer 3 packet (or both).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- **Congestion management:** Each interface needs a queuing mechanism for prioritizing the packets. There are a variety of queuing mechanisms, some of which depend on the IOS version, type of device, and interface protocol.
- **Congestion avoidance:** By dropping low-priority traffic (especially TCP traffic), interfaces can avoid overflowing their buffers.
- **Traffic policing and shaping:** Enforces a rate limit by dropping (policing) or delaying (shaping) traffic that exceeds limits.
- **Link efficiency:** Improves bandwidth efficiency through compression, link fragmentation, and interleaving. (Mostly used for slower-speed interfaces and WAN links.)

Queuing Mechanisms (Congestion Management)

Each interface has to prepare packets or frames to be sent out. The mechanisms used to hold the data before transmission vary, but here are the basics of the most common ones:

- **First-In, First-Out (FIFO):** The default for all interfaces with speeds greater than 2 Mbps. This provides no prioritization of traffic.
- **Weighted Fair Queuing (WFQ):** The default for all interfaces with speeds less than 2 Mbps. Traffic is automatically put into different queues before going to the exit interface. Because all the traffic from the same flow will end up in the same queue, traffic flows with high bandwidth will fill the queue and not impact other traffic in other queues. One downside of this mechanism is the lack of control over the traffic allocation.
- **Class-Based Weighted Fair Queuing (CBWFQ):** This mechanism allows user-defined classes of traffic to be put into queues. Thus, voice traffic can be separated from data traffic; however, it still can have unacceptable delay and jitter.
- **Low Latency Queuing (LLQ):** Adds a priority queue on top of CBWFQ (see Figure 6-37). This gives traffic like voice (and video) priority over data traffic, providing low latency and minimizing jitter. Data traffic goes into the CBWFQ mechanism. LLQ is the Cisco-preferred queuing mechanism when voice and video traffic are present.
- **Weighted Round Robin (WRR) and Shaped Round Robin (SRR):** Common methods on Cisco switches that match a set number of hardware queues to prioritizing traffic.

Note: These descriptions are just the basics. QoS is covered in far more detail in the CVOICE Certification exam.

Trust Boundaries

The ideal scenario involves classifying and marking traffic as close to the point of entry to the network as possible. The other devices upstream can queue traffic based on the trusted markings and not have to classify every time. This involves creating a "trust boundary." For example, as shown in Figure 6-38, if a Cisco IP Phone has a computer connected to it, we want the switch to trust the markings from the phone (discovered through CDP), so the phone remarks any traffic from the PC. If the PC is connected directly to the switch, the markings should not be trusted and the switch should remark traffic.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 6-37 LLQ Architecture

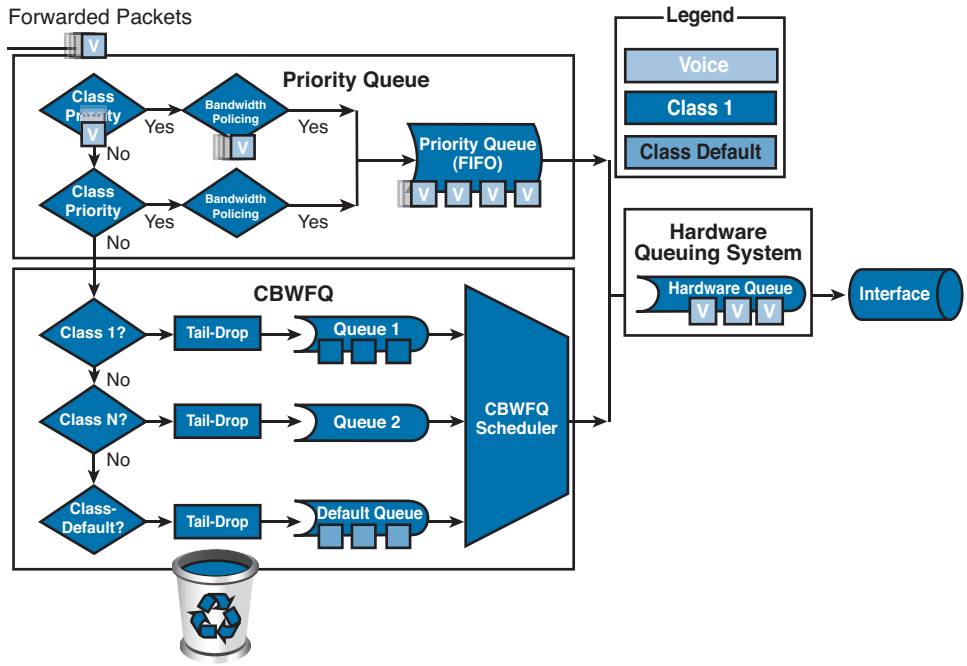
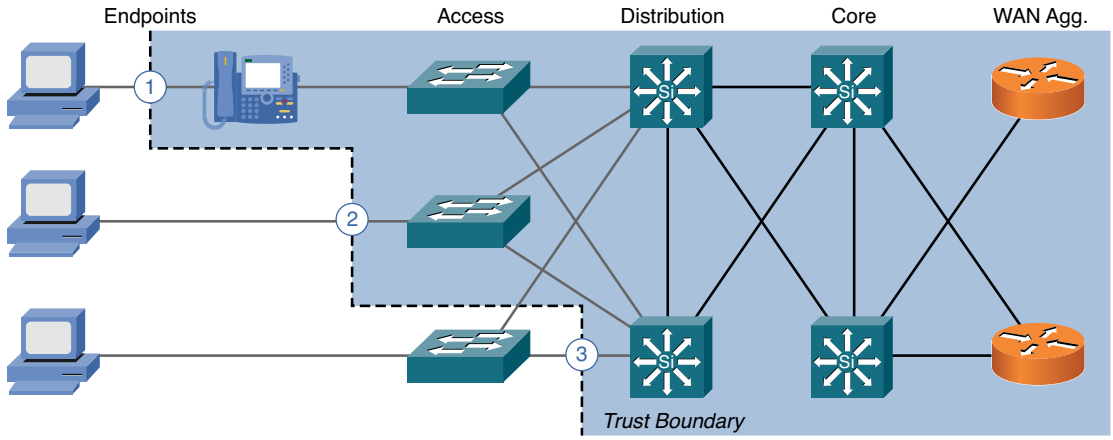


Figure 6-38 Possible QoS Trust Boundaries



AutoQoS

Correctly implementing QoS can be a difficult task. Luckily, Cisco has created an easier way to implement QoS called AutoQoS. AutoQoS applies a template based on the best practices Cisco has found for QoS. Even if you want to design a custom QoS solution, starting with AutoQoS can standardize the starting configuration, and the configuration from AutoQoS can be easily modified to fit the desired goal.

Technically, there are two types of AutoQoS: AutoQoS for VoIP and AutoQoS for Enterprise. This lab will only focus on the AutoQoS for VoIP.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Questions

To test your knowledge of QoS, complete all the questions without looking back at the previous material.

Question 6.1

T F Both voice and video traffic have constant, smooth streams of packets, while data traffic is bursty in nature.

Question 6.2

T F End-to-end packet delay for voice needs to be less than 30 ms.

Question 6.3

T F Congestion avoidance aims to drop packets to prevent interface queues from filling up.

Question 6.4

Complete the traffic requirements.

	Video Traffic	Data Traffic	Voice Traffic
Jitter sensitivity			
Benign or greedy			
Bandwidth requirements			
Drop sensitivity			
Traffic mechanisms			
Delay sensitivity			
Smooth or bursty			

Task 2: AutoQoS on a Switch (Optional)

Note: The results of AutoQoS vary greatly based on the type and model of device, interface applied to, and IOS version. The following output might not match what you see on your equipment.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-1: Configure a Port for a Cisco Phone

As mentioned previously, establishing a trust boundary is important. Cisco switches have an AutoQoS configuration that uses CDP to detect whether a Cisco phone is connected and trust the markings, but not if a PC is attached. Use the **auto qos voip cisco-phone** command on an interface where a Cisco phone is connected. (This example assumes that a Cisco desk phone will be connected to Fa0/5.)

```
SwPodx(config)# interface fastethernet 0/5
SwPodx(config-if)# auto qos voip cisco-phone
SwPodx(config-if)# exit
```

Step 2-2: Configure a Port for PC with Cisco IP Communicator

What if a PC is connected running the Cisco IP Communicator? As is turns out, the soft phone also installs a CDP driver! However, the phone traffic is on the same VLAN as the data traffic, not isolated like the Cisco desk phone. Cisco has a variation on the AutoQoS configuration for this situation: the **auto qos voip cisco-softphone** command. (This example assumes that a PC with Cisco IP Communicator will be connected to Fa0/6.)

```
SwPodx(config)# interface fastethernet 0/6
SwPodx(config-if)# auto qos voip cisco-softphone
SwPodx(config-if)# exit
```

Step 2-3: Configure the Uplink to the Router

Any port that is connected to a trusted device (for example, the router or another switch) should be configured to trust the QoS markings. This is done with the **auto qos voip trust** command. Assuming that the router is connected to Fa0/1, this will trust all markings on packets from the router.

```
SwPodx(config)# interface fastethernet 0/1
SwPodx(config-if)# auto qos voip trust
SwPodx(config-if)# exit
```

Note: At this point, all other switch ports are untrusted. The **auto qos voip cisco-phone** command is commonly applied to all end-user interfaces, because it trusts a Cisco phone but does not trust a PC directly connected to the switch port.

Step 2-4: Examine the Changes to the Switch Config

There are two main changes to the switch. These are discussed in the following paragraphs.

First are the commands that configure global settings. As you can see in the following output, this switch is using Shaped Round Robin (SRR) queuing. Don't worry too much about understanding the details of each of these commands.

```
SwPodx# show run
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
!
<output omitted>

mls qos map policed-dscp  24 26 46 to 0
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
<output omitted>

class-map match-all AutoQoS-VoIP-RTP-Trust
 match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
 match ip dscp cs3  af31
!
!
policy-map AutoQoS-Police-SoftPhone
 class AutoQoS-VoIP-RTP-Trust
  set dscp ef
  police 320000 8000 exceed-action policed-dscp-transmit
 class AutoQoS-VoIP-Control-Trust
  set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
policy-map AutoQoS-Police-CiscoPhone
 class AutoQoS-VoIP-RTP-Trust
  set dscp ef
  police 320000 8000 exceed-action policed-dscp-transmit
 class AutoQoS-VoIP-Control-Trust
  set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
!
```

Second are the commands for the individual interfaces. In each interface you can see the type of AutoQoS configured.

```
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust cos
 auto qos voip trust

<output omitted>

interface FastEthernet0/5
 switchport access vlan 110
 switchport mode access
 switchport voice vlan 115
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
 service-policy input AutoQoS-Police-CiscoPhone
!
interface FastEthernet0/6
 switchport access vlan 110
 switchport mode access
 switchport voice vlan 115
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 auto qos voip cisco-softphone
 spanning-tree portfast
 service-policy input AutoQoS-Police-SoftPhone
```

Step 2-5: Verify the QoS Operation

To see that AutoQoS properly detects and trusts the Cisco phones, fist connect a PC (that is not running IP Communicator) to Fa0/5 and use the **show mls qos interface fastEthernet 0/5** command to view the QoS status. In this case, the PC is not trusted.

```
SwPodx# show mls qos interface fastEthernet 0/5
FastEthernet0/5
Attached policy-map for Ingress: AutoQoS-Police-CiscoPhone
trust state: not trusted
trust mode: trust cos
trust enabled flag: dis
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: cisco-phone
qos mode: port-based
```

Now connect a Cisco desk phone to Fa0/5. You might see a status message on the console showing that the Cisco phone is trusted. The **show mls qos interface fastEthernet 0/5** command also shows that the IP phone is trusted.

```
*Mar  1 05:27:47.419: %SWITCH_QOS_TB-5-TRUST_DEVICE_DETECTED: cisco-phone detected on
port Fa0/5, port's configured trust state is now operational.
SwPodx# show mls qos interface fastEthernet 0/5
FastEthernet0/5
Attached policy-map for Ingress: AutoQoS-Police-CiscoPhone
trust state: trust cos
trust mode: trust cos
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: cisco-phone
qos mode: port-based
```

Task 3: AutoQoS on a Router (Optional)

Note: The results of AutoQoS vary greatly based on the type and model of device, interface applied to, and IOS version. The following output might not match what you see on your equipment.

Step 3-1: Configure the Port Connected to the Switch

In the same way that the switch was configured to trust the markings from the router, the router should be set to trust the markings from the switch. The same **auto qos voip trust** command is used. (The router's built-in interfaces do not have the **cisco-phone** or **cisco-softphone** options.) Note that you might see an RMON trap message on the console, and this is not a problem.

```
RtrPodx(config)# interface fa0/0
RtrPodx(config-if)# auto qos voip trust
RtrPodx(config-if)# exit
*Mar 20 06:21:42.290: %RMON-5-FALLINGTRAP: Falling trap is generated because the
  value of cbQosCMDropBitRate.34.5364641 has fallen below the falling-threshold value 0
```

Step 3-2: Verify the QoS Configuration

The **show auto qos** command will show the QoS configuration commands on the router:

```
RtrPodx# show auto qos
 !
 policy-map AutoQoS-Policy-Trust
  class AutoQoS-VoIP-RTP-Trust
     priority percent 70
  class AutoQoS-VoIP-Control-Trust
     bandwidth percent 5
  class class-default
     fair-queue
 !
 class-map match-any AutoQoS-VoIP-RTP-Trust
  match ip dscp ef
 !
 class-map match-any AutoQoS-VoIP-Control-Trust
  match ip dscp cs3
  match ip dscp af31
 !
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice Drops"
  owner AutoQoS
 rmon alarm 33333 cbQosCMDropBitRate.34.5364641 30 absolute rising-threshold 1 33333
  falling-threshold 0 owner AutoQoS
 rmon alarm 33334 cbQosCMDropBitRate.50.14618161 30 absolute rising-threshold 1 33333
  falling-threshold 0 owner AutoQoS


FastEthernet0/0 -
 !
 interface FastEthernet0/0
  service-policy output AutoQoS-Policy-Trust
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

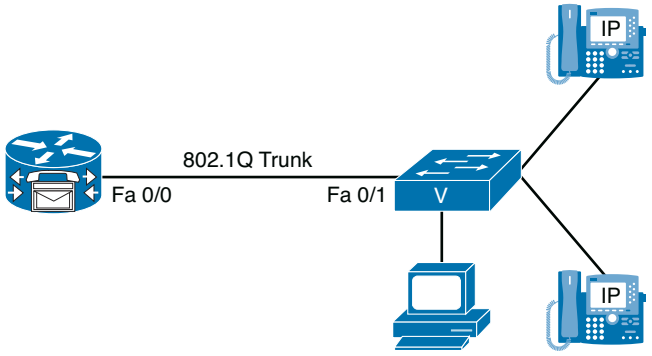
CHAPTER 7

Cisco Unified Communications Manager Express (CUCME) Productivity Features

Labs in previous chapters established the ability to call between phones in a company and to the public switched telephone network (PSTN). The next step is to add features that improve the functioning of the system and enhance the users' experience. CUCME, as a small to medium business solution, has numerous features that provide functionality comparable to a full-fledged PBX. However, the CCNA Voice Certification exam does not require extensive experience with CUCME, so this chapter will focus on just two features: the local directory and call forwarding, and the system reporting capabilities of call detail records (CDR) and call accounting.

Lab 7-1: Configuring the Phone Directory

Figure 7-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Lab configuration from Lab 5-2, 5-3, 6-5, or 6-6
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)

Learning Objectives

Upon completion of this lab, you will be able to

- Create a directory of phone users
- Configure the directory to show on the phone display

Scenario

Shiny Objects Inc. (SOI) wants to get rid of its photocopied company directory and use a directory that is easy to update whenever there is a change at the office. Using the phone directory on the phone display will allow this.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Load Prior Configurations

This lab is based on the configuration from Lab 5-2, 5-3, 6-5, or 6-6. If necessary, load the configuration for both the switch and router. Connect a PC to the switch and verify that it can ping the router and switch management addresses. Connect the VoIP phones and verify that you can call between them. Troubleshoot if necessary.

Note: This lab will show both the CLI and Cisco Configuration Professional (CCP) software methods to complete the tasks. If you want to use CCP, make sure that you start with a configuration that has the commands to enable CCP access included. (Refer to Lab 4-1, Task 3 for details.)

Task 2: Populate the Directory

There are two methods to add names to the CUCME user directory. The first method is by using the **name** command when configuring each ephone-dn, as shown previously in Lab 5-2, Step 3-1 or Lab 5-3, Step 3-2. This is the best method to add user names to the directory, as it also builds the caller ID information for calls. If necessary, review those steps again to make sure that you have names assigned to each ephone-dn.

The second method is to manually add names and numbers to the directory. This is useful to add items to the directory for devices that don't use ephone-dns (for example, a fax machine connected to an FXS port) or even users outside of the system (for example, adding contractors to the directory).

SOI would like to add the phone number for the fax machine (use the number assigned in the FXS #1 column from the Pod Addressing Table in Appendix A) and the contracted accountant (at phone number 555-6000) to the company directory.

Step 2-1: Manually Adding Directory Entries Using the CLI

The **directory entry** command in telephony-service configuration mode allows you to manually add entries to the directory. Each entry has a tag number, the directory number associated with the name, the **name** keyword, and the actual name for the entry. A common mistake is forgetting that the command requires the **name** keyword prior to the actual name. (Don't forget that if you are dialing an outside number, you need to include the outside line access digit, the same as if you were dialing on a phone.)

```
RtrPodx(config)# telephony-service
RtrPodx(config-telephony)# directory entry ?
  <1-250>  Directory entry tag
  clear    clear all directory entries
RtrPodx(config-telephony)# directory entry 1 5358 name Fax Machine
RtrPodx(config-telephony)# directory entry 2 95556000 name Accountant
```

Step 2-2: Manually Adding Directory Entries Using CCP

Use the community created in Lab 4-1, Steps 3-4 to connect to the router. With the router discovered, click **Configure**. The pane on the left will show various categories of router configuration options. (The items you see will depend on the IOS you have installed.)

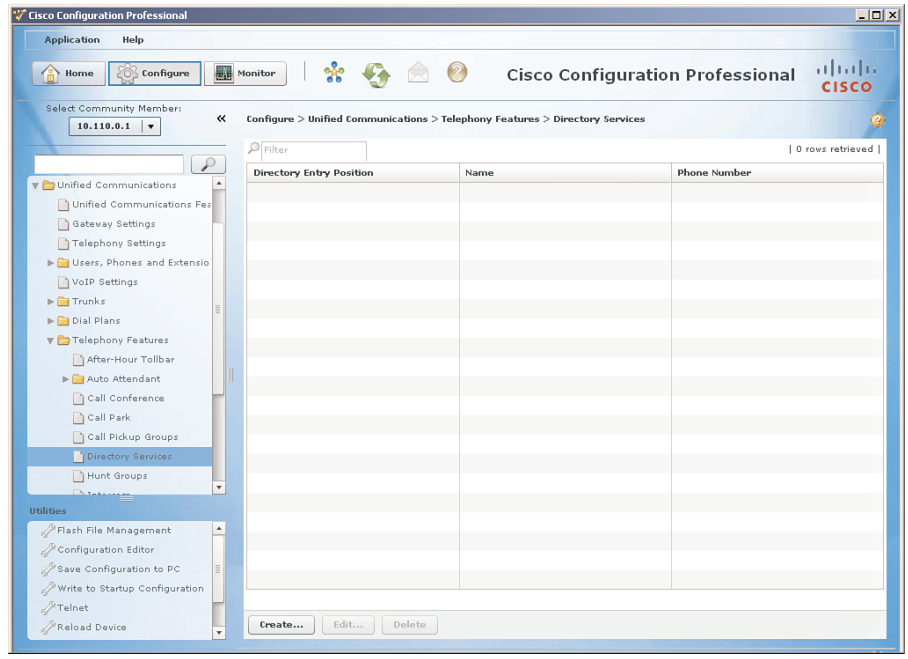
1. Click the **Unified Communications** folder icon to expand the subitems.
2. Click the **Telephony Features** folder icon to expand the subitems.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. Click the **Directory Services** subitem. In the Directory Services pane on the right is a table showing manually entered directory entries. (See Figure 7-2 for an example of this window.) (If you just completed Step 2-1, you might need to refresh to see those entries; otherwise, this will be blank. If necessary, delete the entries created with the CLI in Step 2-1 to re-create them using CCP.)

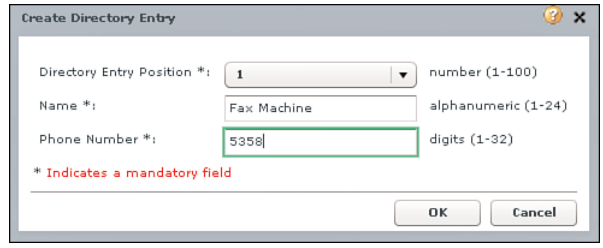
Figure 7-2 Directory Services Pane



4. Click the **Create** button at the bottom of the pane to add a new entry.

5. The Create Directory Entry dialog box opens. The Directory Entry Position drop-down list will default to the next usable number. Enter **Fax Machine** in the Name field and the FXS Port #1 directory number, and click the **OK** button. (See Figure 7-3 for an example of this dialog box.)

Figure 7-3 Create Directory Entry Dialog Box

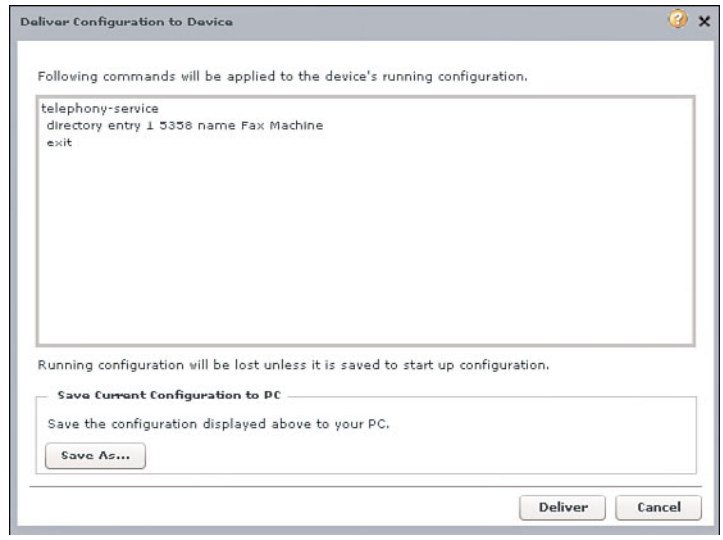


6. The Deliver Configuration to Device window will open and display the commands that will be applied to the router. (See Figure 7-4 for an example.)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 7-4 Deliver Configuration Confirmation Dialog Box



7. Click the **Deliver** button.
8. Repeat this step to add the Accountant to the directory.

Step 2-3: Enabling the Local Directory on the Phone Display

For the local directory to show on the phones, three things are needed:

- Directory entries.
- HTTP service enabled on the router.
- Each ephone needs to have the model type configured.

The more current IOS versions have unneeded services disabled by default for improved security (including the http service). The directory on the phone uses http to communicate with the router to get the directory information. (If you are using CCP, the http service has already been enabled.) If necessary, turn on the service using the **ip http server** command:

```
RtrPodx(config)# ip http server
```

The **type** command identifies the features of the phone model to CUCME, and is required for the Directories button on the phone to show the local directory. This was configured previously in Lab 5-2, Step 4-2 or Lab 5-3 (CCP requires you to select the model before adding a phone). If necessary, review those steps again to make sure that each ephone has the type assigned.

With those steps complete, press the Directories button on the phone (see Figure 7-5) to see the various services, such as Missed Calls, Received Calls, Speed Dials, and so on.

Note: If the Local Directory does not show on the phone, verify the previous steps were completed successfully. Additionally, verify the firmware on the IP Phone is correct for the version of CUCME. For example, if the phones have their firmware updated by CUCM 8.6 (as shown in Chapter 9) the updated firmware will not show the Local Directory for CUCME version 7.1. In this case, it would be necessary to downgrade the firmware to the correct version before CUCME shows the Local Directory on the phone.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 7-5 Browsing Phone Directories

Use the navigation buttons (or press the number to the left of the name) to select the Local Directory. You can press the Submit softkey to see the first 32 directory entries, or use the keypad on the phone to enter part of a first or last name to search for it. (On the IP Communicator soft phone, you can also use the keyboard to type the name.)

Use the navigation buttons (or press the number to the left of the name) to select the entry you want (see Figure 7-6). The entry can be called by pressing the Dial softkey.

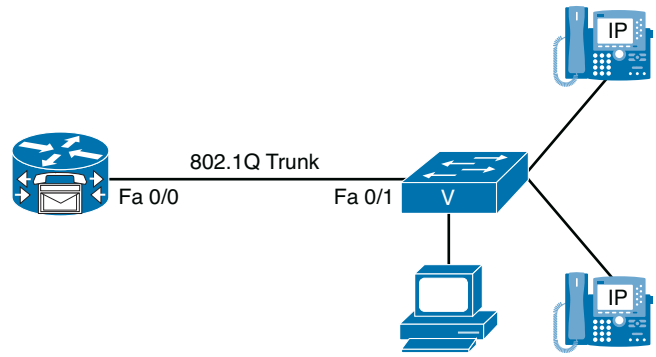
Figure 7-6 Local CUCME Directory

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 7-2: Configuring Call Forwarding

Figure 7-7 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Lab configuration from Lab 5-2, 5-3, 6-5, 6-6, or 7-1
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)

Learning Objectives

Upon completion of this lab, you will be able to

- Configure phone calls to be redirected using the phone display
- Configure phone calls to be redirected when the phone is busy or not answered

SOI wants to have calls redirected by the user from the phone and automatically forwarded when the phone line is busy or not answered.

Task 1: Load Prior Configurations

This lab is based on the configuration from Lab 5-2, 5-3, 6-5, 6-6, or 7-1. If necessary, load the configuration for both the switch and router. Connect a PC to the switch and verify that it can ping the router and switch management addresses. Connect the VoIP phones and verify that you can call between them. Troubleshoot if necessary.

Note: This lab will show both the CLI and Cisco Configuration Professional (CCP) software methods to complete the tasks. If you want to use CCP, make sure that you start with a configuration that has the commands to enable CCP access included. (Refer to Lab 4-1, Task 3 for details.)

Task 2: Configure Call Forwarding on the Phone

Cisco IP Phones have a softkey on the phone display to allow calls to be forwarded to another number. The phone user presses the CFwdAll softkey on the display, dials the extension that calls should

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

be redirected to, and then presses the EndCall softkey. The display shows a moving arrow in the upper right, and the Status bar shows the extension that the calls are forwarded to (see Figure 7-8).

Figure 7-8 Forwarding Calls from the Cisco IP Phone

While the forwarding is active, any calls to the extension will not ring on this phone, but are redirected to the specified extension. Make a call from another phone to the extension that is forwarded, and you will see that the phone display shows that the call is forwarded.

To cancel the call forwarding, press the CFwdAll key again.

Task 3: Configure Call Forwarding on the Router

Allowing users to forward their own phones is great, as long as they remember to do so. Configuring call forwarding on the router allows you to establish configurations such as forwarding a call when it is not answered after a few rings, or when the phone is busy.

Step 3-1: Configuring Call Forwarding Using the CLI

The **call-forward** command has a variety of options, such as forwarding all calls or forwarding calls automatically after hours, but the two most common options are forwarding calls when the phone is busy and forwarding calls that are not answered after a set amount of time. The call forward when not answered (**call-forward noan**) option allows calls to be sent to voicemail, an operator, or an auto-attendant.

Set ephone-dn 1 to forward calls to another extension when the ephone-dn is busy and when the ephone-dn is not answered for 12 seconds.

```
RtrPodx(config)# ephone-dn 1
RtrPodx(config-ephone-dn)# call-forward ?
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
  all             forward all calls
  busy            forward call on busy
  max-length      max number of digits allowed for CFwdAll from IP phone
  night-service   forward call on activated night-service
  noan            forward call on no-answer
RtrPodx(config-ephone-dn)# call-forward busy extension_of_ephone_dn_two
RtrPodx(config-ephone-dn)# call-forward noan extension_of_ephone_dn_two timeout 12
```

Now when you call from another phone to the first extension, count the number of rings. After about three rings, the call will forward to directory number two.

Tip: Cisco IP Phones don't use the traditional six seconds between rings that the PSTN uses; the IP Phones have approximately four seconds between rings. You can use the four seconds to estimate the time to set the call forward value. However, if a user asks for the phone to ring five times before forwarding to voicemail, don't just plug 20 (5 rings times 4 seconds) into the command. To make the user happy, test it! Verify that it gives him not four, not six, but five full rings.

Testing the forward when busy (**call-forward busy**) option is harder, as the ephone-dn was created as dual-line, and as a result, the second incoming call is treated as call waiting. Both channels of the dial-line would have to be in use before the **call-forward busy** option takes effect.

Step 3-2: Configuring Call Forwarding Using the CCP

Use the community created in Lab 4-1, Steps 3-4 to connect to the router. With the router discovered, click **Configure**. The pane on the left will show various categories of router configuration options. (The items you see will depend on the IOS you have installed.)

1. Click the **Unified Communications** folder icon to expand the subitems.
2. Click the **Users, Phones and Extensions** folder icon to expand the subitems.
3. Click the **Extensions** subitem.
4. On the right side is a Guided Configuration pane that is not needed and is taking up screen space, so click the double arrows (**>>**) to minimize it.
5. Click the row for **Extension Tag 2**. (See Figure 7-9 for an example of this window.)
6. Click the **Edit** button. The Edit Extension window will open. Under the General Options on the left, the bottom of the pane on the right shows the call forwarding.
7. Enter the extension of the first ephone-dn in the When Busy, Divert Calls, and Divert Unattended Calls fields.
8. Enter **16** for the No Answer Timeout field, which should give about four rings before redirecting the call. (See Figure 7-10 for an example of this dialog box.)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 7-9 CCP Extensions Pane

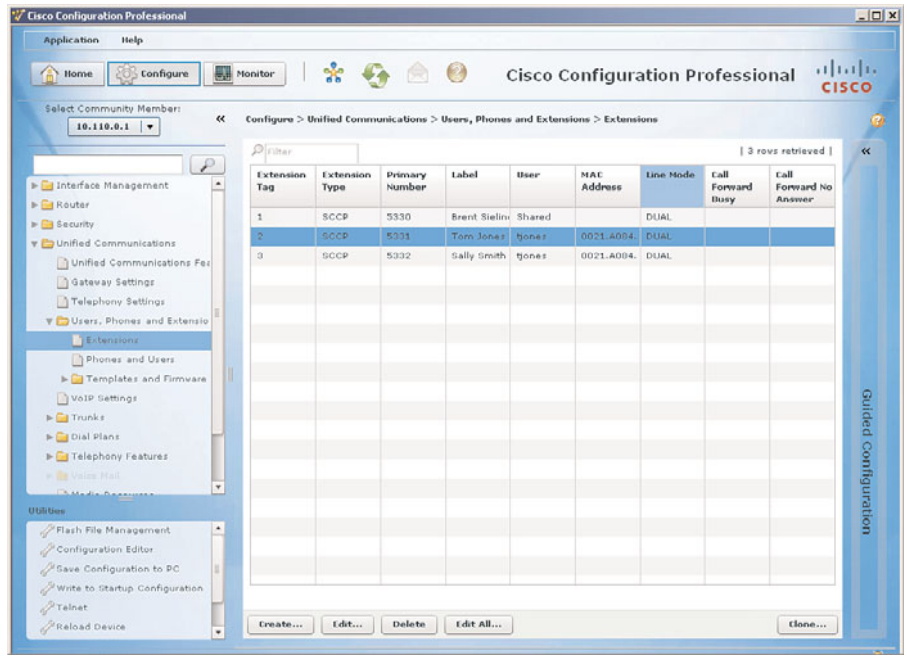
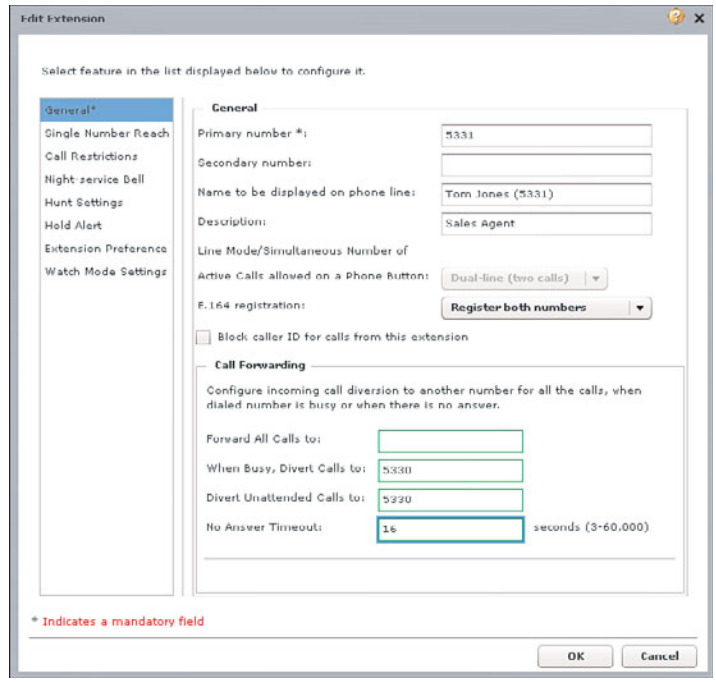


Figure 7-10 CCP Edit Extension Window

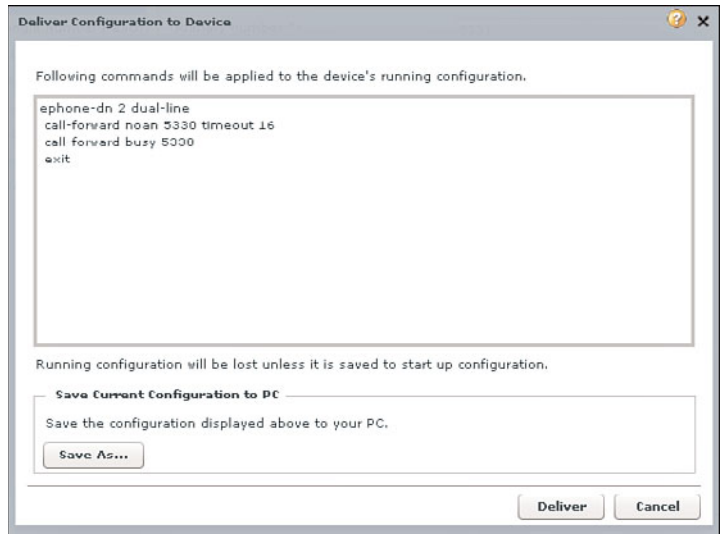


9. Click the **OK** button. The Deliver Configuration to Device window will open and display the commands that will be applied to the router. (See Figure 7-11 for an example.)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 7-11 Deliver Configuration Confirmation Dialog Box



10. Click the **Deliver** button.

Step 3-3: Infinite Loop Solved

Now that we have configured ephone-dn 1 to forward to ephone-dn 2 when not answered, and ephone-dn 2 to forward to ephone-dn 1 when not answered, does an incoming call bounce back and forth between the two phones forever? The answer is no. This problem is solved by the **max-redirect** command in telephony-service that sets the number of redirects before a call is disconnected. You should be aware of this value, because if a call is forwarded too many times, it will be dropped. The current value can be found with the **show telephony-service** command.

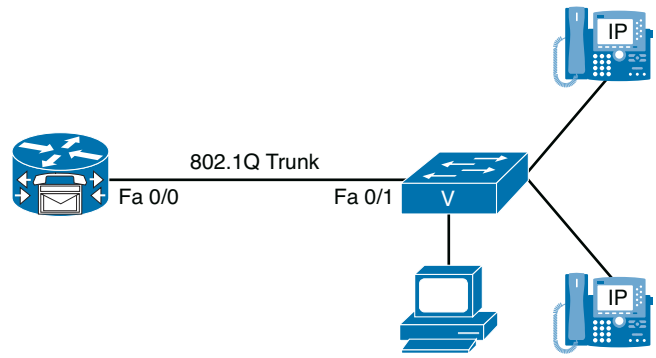
```
RtrPodx# show telephony-service
CONFIG (Version=7.1)
====================
Version 7.1
Cisco Unified Communications Manager Express
<output omitted>
max-redirect 5
<output omitted>
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 7-3: Configuring Call Detail Records and Accounting

Figure 7-12 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Lab configuration from Lab 5-2, 5-3, 6-5, 6-6, 7-1, or 7-2
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)
- PC running Syslog software (such as Kiwi Syslog Daemon)

Learning Objectives

Upon completion of this lab, you will be able to

- Examine call records on the router
- Send call detail records and accounting to a syslog server

Scenario

SOI needs to get information about calls placed on its phones. There might be a number of reasons for this, such as disputing with the service provider over billing, investigating improper use of long-distance and international calls, breaking billing costs out to department or user levels, and troubleshooting. Two related logging systems can provide this information: system event logging and call detail records (CDR). System event logging helps troubleshoot any number of problems with the networking gear, while call detail records contain information about each call going through the system. These messages can be sent to a local buffer on the device and to a syslog server.

Task 1: Load Prior Configurations

This lab is based on the configuration from Lab 5-2, 5-3, 6-5, 6-6, 7-1, or 7-2. If necessary, load the configuration for both the switch and router. Connect a PC to the switch and verify that it can ping the router and switch management addresses. Connect the VoIP phones and verify that you can call between them. Troubleshoot if necessary.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Establish Logging Locally on the Router

While troubleshooting on a router, it can be handy to view the logs of recent events to gather information. All the event messages that show on the console can be sent to a local logging facility on the device, which is disabled by default.

Although not absolutely necessary, having correct timestamps on events makes troubleshooting easier and is essential if the logs might ever be used for legal purposes. Enabling Network Time Protocol (NTP) (as shown in Lab 3-2) allows the device to have accurate time. The timestamps for system events can then be set to use the local time zone using the **service timestamps** command with the **localtime** keyword.

To enable logging, the size of the buffer to store messages (which impacts memory usage) must be determined using the **logging buffered** command:

```
RtrPodx(config)# service timestamps log datetime msec localtime
RtrPodx(config)# logging buffered 512000
```

Now that logging is established, generate a log message by restarting an IP Phone:

```
RtrPodx(config)# ephone 1
RtrPodx(config-ephone)# restart
restarting 001D.705E.ABF1
Feb 26 18:37:22.779: %IPPHONE-6-UNREGISTER_NORMAL: ephone-1:SEP001D705EABF1
 IP:10.115.0.11 Socket:5 DeviceType:Phone has unregistered normally.
Feb 26 18:37:24.495: %IPPHONE-6-REG_ALARM: 23: Name=SEP001D705EABF1 Load= SCCP42.8-4-
  2S Last=Reset-Restart
Feb 26 18:37:24.535: %IPPHONE-6-REGISTER: ephone-1:SEP001D705EABF1 IP:10.115.0.11
 Socket:2 DeviceType:Phone has registered.
RtrPodx(config-ephone)# end
```

Use the **show logging** command to see the same ephone unregister and registration messages in the buffer:

```
RtrPodx# show logging
Syslog logging: enabled (0 messages dropped, 4 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 92 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 5 messages logged, xml disabled,
                     filtering disabled
    Logging Exception size (4096 bytes)
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped

    Trap logging: level informational, 96 message lines logged

Log Buffer (512000 bytes):

Feb 26 18:36:57.311: %SYS-5-CONFIG_I: Configured from console by console
Feb 26 18:37:22.779: %IPPHONE-6-UNREGISTER_NORMAL: ephone-1:SEP001D705EABF1
  IP:10.115.0.11 Socket:5 DeviceType:Phone has unregistered normally.
Feb 26 18:37:24.495: %IPPHONE-6-REG_ALARM: 23: Name=SEP001D705EABF1 Load= SCCP42.8-4-
  2S Last=Reset-Restart
Feb 26 18:37:24.535: %IPPHONE-6-REGISTER: ephone-1:SEP001D705EABF1 IP:10.115.0.11
  Socket:2 DeviceType:Phone has registered.
Feb 26 18:38:10.947: %SYS-5-CONFIG_I: Configured from console by console
RtrPodx#
```

The logging buffer will get the same messages the console receives, and it will show messages regarding calls that use the ISDN PRI. (If you configured Lab 6-5 or 6-6, you can test this by making a call to the PSTN.) In this example, the router shows that 911 was called, and the call lasted seven seconds:

```
Feb 26 18:43:25.163: %ISDN-6-CONNECT: Interface Serial0/2/0:5 is now connected to 911
  N/A
Feb 26 18:43:31.335: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:5,
  changed state to up
Feb 26 18:43:32.791: %ISDN-6-DISCONNECT: Interface Serial0/2/0:5  disconnected from
  911 , call lasted 7 seconds
```

However, these messages are the result of the ISDN PRI interface activity. If you make a call between IP Phones, there are no logged messages. This is where CDRs enter the picture.

Task 3: Establish Logging and CDRs to a Syslog Server

There are advantages to having logging messages sent to an external syslog server. On a syslog server, scripts can be used to filter the output, and there is no risk of losing the records when the device loses power. Additionally, the CDRs can be sent to a syslog server (RADIUS and FTP are two other options) for detailed billing information and call tracing. Establishing CDRs is done with the **dial-control-mib** command, with the maximum number of entries to retain using the **max-size** keyword and how long to keep the records using the **retain-timer** keyword. The **gw-accounting syslog** command tells the system to send CDRs to a syslog server, and the **logging** command specifies the IP address of the syslog server.

```
RtrPodx(config)# dial-control-mib max-size 500
RtrPodx(config)# dial-control-mib retain-timer 10080
RtrPodx(config)# gw-accounting syslog
RtrPodx(config)# logging IP_address_of syslog_server
RtrPodx(config)# exit
```

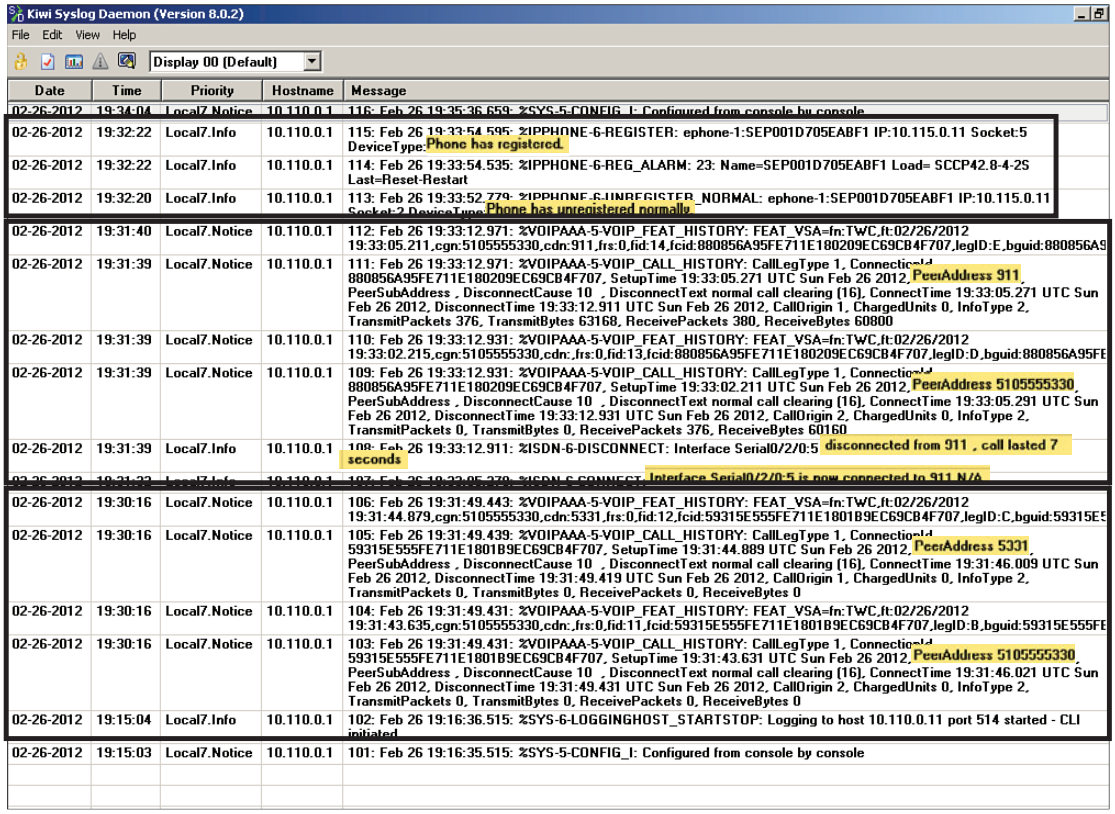
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Now make a call from IP Phone 1 to IP Phone 2. The syslog server should receive the CDR, as shown in the bottom box in Figure 7-13. If you completed Lab 6-5 or 6-6 and make a call to 911, not only do you see the ISDN PRI messages but also the CDR of the call as well, as shown in the middle box in Figure 7-13. If you restart ephone 1 again, you will see that the event logs are sent to the syslog server too, as shown in the top box in Figure 7-13.

Note: By default, the Kiwi Syslog service has the newest entries at the top of the log, so when looking at Figure 7-13, read the entries from the bottom of the image upward to see them in chronological order.

Figure 7-13 Syslog Messages in Kiwi Syslog Server



Note: This is the last lab configuring CUCME until troubleshooting is discussed in Chapter 15, "Troubleshooting Cisco Unified Communications Manager Express (CUCME)." You might want to skip ahead to that chapter before starting Chapter 8, "Administrative Interfaces."

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CHAPTER 8

Administrative Interfaces

This chapter explores the administrative interfaces of the Cisco Unified Communications Manager (CUCM). (The Cisco Unity Connection administrative interface will be covered in Chapter 13, "Cisco Unity Connection.")

The IP addresses of the servers for the lab setup are as follows (where *x* is your pod number):

- CUCM: 10.*x*0.0.5 /24
- CUC: 10.*x*0.0.8 /24
- CUPS: 10.*x*0.0.10 /24

If you are doing a custom lab using different addresses, write them down here for reference.

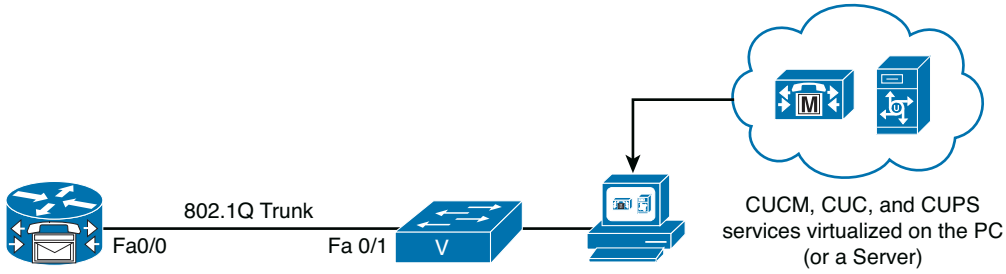
There are two sets of login credentials that will be utilized in this lab. One is known as the Application Administration username, and the other is the Platform Administration username. The usernames and passwords from the build in Appendix C are

- Application Administration username: **icomm**
- Application Administration password: **ccnavoice**
- Platform Administration username: **hwadmin**
- Platform Administration password: **thehwadmin**

If you are doing a custom lab using different usernames or passwords, write them down here for reference.

Lab 8-1: Exploring the CUCM GUI

Figure 8-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Learning Objectives

Upon completion of this lab, you will be able to

- Understand the basic elements of the CUCM GUI
- Switch between CUCM web utilities to accomplish configuration tasks

Scenario

Shiny Objects Inc. (SOI) has expanded (and so has your salary) to the point that SOI has outgrown the Cisco Unified Communications Manager Express (CUCME) system. SOI decided to move to the Cisco Unified Communications solutions servers. After setting up the CUCM server, you want to explore the new interfaces.

Task 1: CUCM Administrative Interfaces

Table 8-1 summarizes the command-line interface (CLI) and the five different web pages to administer CUCM.

Table 8-1 CUCM Web Tools and Credentials

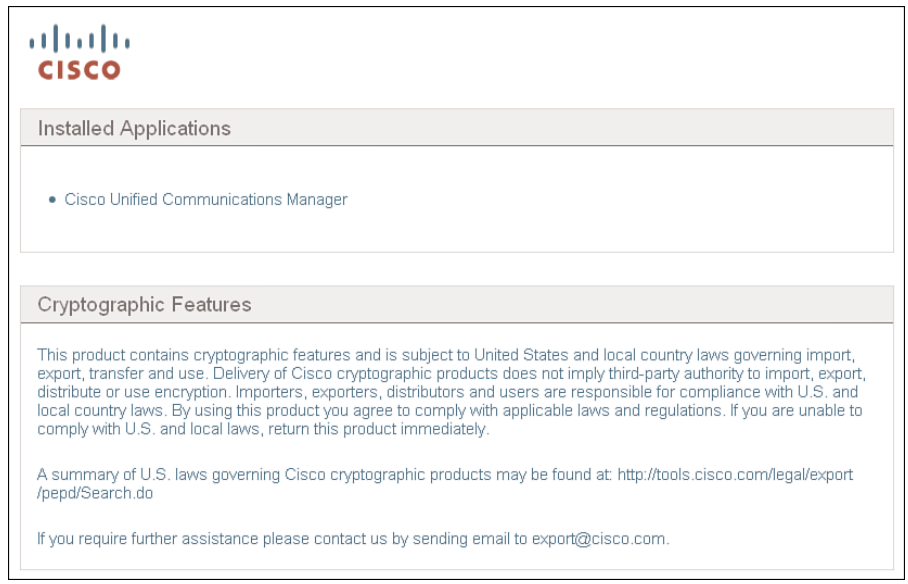
Tool Name	Purpose	Username Needed	Direct URL
Cisco Unified CM Administration	Administration and configuration	Application	https://*cucm-ip-address*:8443/ccmadmin
Cisco Unified Serviceability	Starting, stopping, and restarting of system services	Application	https://*cucm-ip-address*:8443/ccmservice
Cisco Unified Reporting	System status and report generation	Application	https://*cucm-ip-address*:8443/cucreports
Cisco Unified OS Administration	Installation of patches, upgrades, and certificates	Platform	https://*cucm-ip-address*:8443/cmplatform
Disaster Recovery System	Backup and restore of CUCM nodes	Platform	https://*cucm-ip-address*:8443/drf
CLI	Hardware settings and OS administration	Platform	Access from the console, or SSH to *cucm-ip-address*

You can access the system by using a supported web browser and entering the http://*cucm-ip-address* URL. See Figure 8-2 for an example of this page.

https://t.me/learningnets

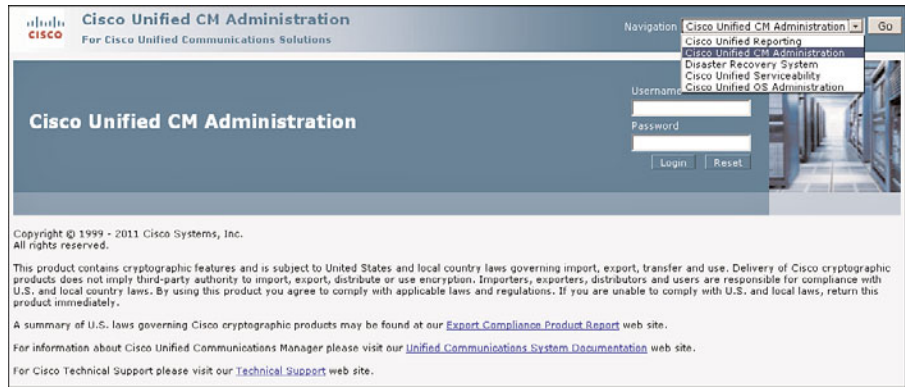
From the Library of Aliwarman Tarihoran

Figure 8-2 Initial Web Page



Click the **Cisco Unified Communications Manager** hyperlink to go to the CCMAdmin page. (Alternatively, you could enter the direct URL of https://*cucm-ip-address*:8443/ccmadmin to get to the same page.) On the login page, in the upper-right corner, there is a navigation drop-down list that also lets you change to any of the other administration web pages listed in Table 8-1. See Figure 8-3 for an example of this page.

Figure 8-3 CCMAdmin Login Page



Be aware that some pages use different usernames, as noted in Table 8-1. Given that CUCM is designed for large enterprises, CUCM configures two different administrator accounts during the install:

- The platform administrator has access to server settings, but not the telephony settings. This account is designed for staff operating the servers in the data center so that they can change IP addresses, back up the server, and so on, without being able to make changes to the phones or phone users.

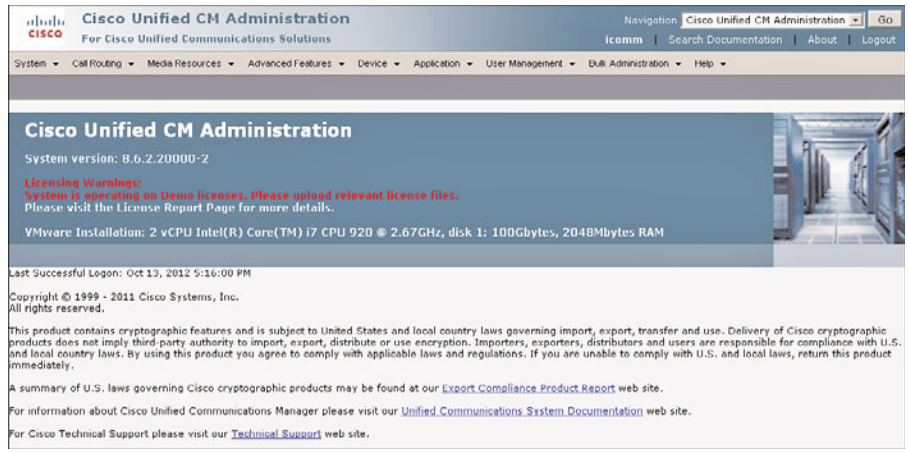
https://t.me/learningnets
From the Library of Aliwarman Tarihoran

- The application administrator can make changes to telephony settings, but not the server settings. This account is designed for staff who add phones and users to the system but are not responsible for maintaining the servers in the data center.

Task 2: The CCMAdmin Page

The Cisco Unified CM Administration (CCMAdmin) page is the primary interface utilized in configuring and maintaining the CUCM server. In fact, the Publisher server's CCMAdmin page is the primary configuration interface for the entire cluster. Use your application username to log in to the CCMAdmin page. See Figure 8-4 for an example of this page.

Figure 8-4 CCMAdmin Page



Using the menu bar across the top of the page, navigate through the various menus to become familiar with the placement and purpose of various submenus. Later chapters will go into the details of some of, but not all, the various menu items on this page, and some of the other administration pages.

Consult the *Official Cert Guide CCNA Voice 640-461* for more information about the menus, or use the Help menu to get more details.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CHAPTER 9

Managing Services, Phones, and Users

This chapter explores the methods and requirements to add or change services, phones, and users on a Cisco Unified Communications Manager (CUCM) server. Three methods will be used to add phones: autoregistration, manual configuration, and the Bulk Administration Tool (BAT). Users will be added manually, using BAT, and using Lightweight Directory Access Protocol (LDAP) synchronization (optional).

Lab 9-1: Phone Boot Process

Equipment Required

No equipment is required for this lab.

Learning Objective

Upon completion of this lab, you will better understand the boot and registration process for IP Phones.

Question 9.1

For the IP Phone registration process, write the correct letter of the steps, from startup (1) to registration (6), in the order that they occur.

Phone order

1) _____

2) _____

3) _____

4) _____

5) _____

6) _____

A) Determine the VLAN used for voice from the switch.

B) Contact the TFTP server for the SEP<*mac_address*>.cnf.xml configuration file. If the individual configuration file is not available, use the default cnf file.

C) Load firmware stored on the phone.

D) Contacts the primary CUCM server.

E) Obtains power from AC adapter or PoE.

F) Receives IP address information from DHCP, including option 150 address.

Question 9.2

List the various services and protocols used by IP Phones during startup and operation.

_____

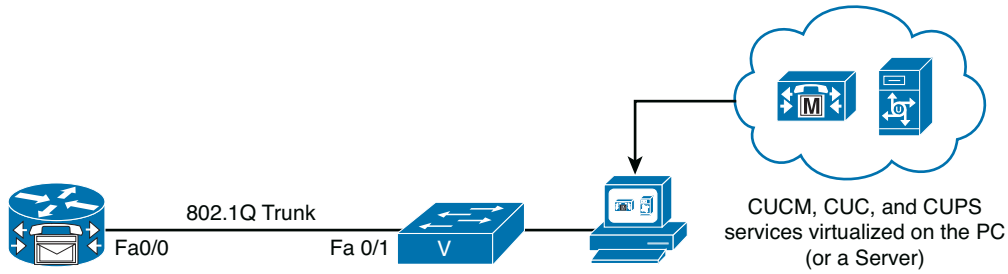
_____

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 9-2: CUCM Services

Figure 9-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- Configuration from Lab 3-2 and Lab C-1

Learning Objectives

Upon completion of this lab, you will be able to

- Remove DNS dependencies in CUCM
- View/start/stop/restart network services in CUCM
- View/start/stop/restart feature services in CUCM
- Activate or deactivate services in CUCM
- See where CUCM tracks licenses

Scenario

Shiny Objects Inc. (SOI) has installed the first CUCM server in the network and would like to prepare it for use. Each CUCM server has a number of services running automatically after installation, and a number of others that need to be activated to match the function of the server. As discussed in Chapter 2, "Understanding Cisco Unified Communication Solutions," CUCM servers are usually organized into a cluster. As a result, some of the servers in the cluster might be performing similar job functions (such as call control), while other servers are specialized to a particular job function. For example, when the number of users exceeds 1250, Cisco recommends that a server be dedicated to the TFTP role. Each CUCM server needs to have the desired services activated.

Note: Disconnect any Cisco IP Phones you have connected. They will be connected in a later lab.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Remove DNS Dependencies

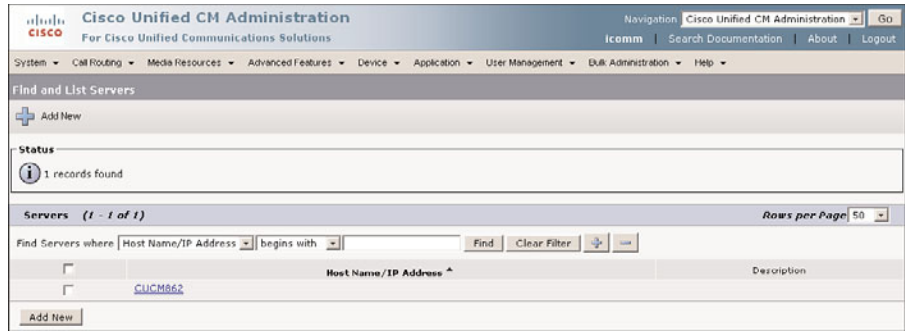
By default, the CUCM servers refer to each other, and present themselves to the phones, using Domain Name System (DNS) names. While this has the advantage of allowing the system to migrate IP addresses by changing the DNS records, it makes the phone system dependent on the DNS service to function. The recommended practice is to remove the requirement for DNS. Because there is no DNS in this lab, it is a necessity here. There are two places where the DNS name needs to be changed to an IP address for each server. The following instructions assume that there is only one CUCM in the cluster. (If there is more than one server in the cluster, there is a specific sequence to make sure that all servers are updated as each server is changed. The procedure can vary depending on the version of CUCM you are using. Search Cisco.com for "Changing the IP Address and Hostname for Cisco Unified Communications Manager" and your version of CUCM to find the process.)

Step 1-1: Change Server Host Name to IP Address

Connect to the CUCM web pages using the methods discussed in Chapter 8, "Administrative Interfaces." Log in with your application username (icomm), accept any security certificate warnings, and if the page is not on the Cisco Unified CM Administration page, use the Navigation drop-down list in the upper right to select the **Cisco Unified CM Administration** item and click **Go**.

On the **Cisco Unified CM Administration** page, navigate to **System > Server**. One of the first things you will learn with the web pages in CUCM is that to save time when displaying a page with hundreds (or even thousands) of items, you are given a search box to filter the results first. In most cases, you will find it necessary to leave the Search field empty and click the **Find** button to see whether there are any records. In this case, after clicking the **Find** button, you will see the CUCM862 server record. See Figure 9-2 for an example of this page.

Figure 9-2 Find and List Servers Page



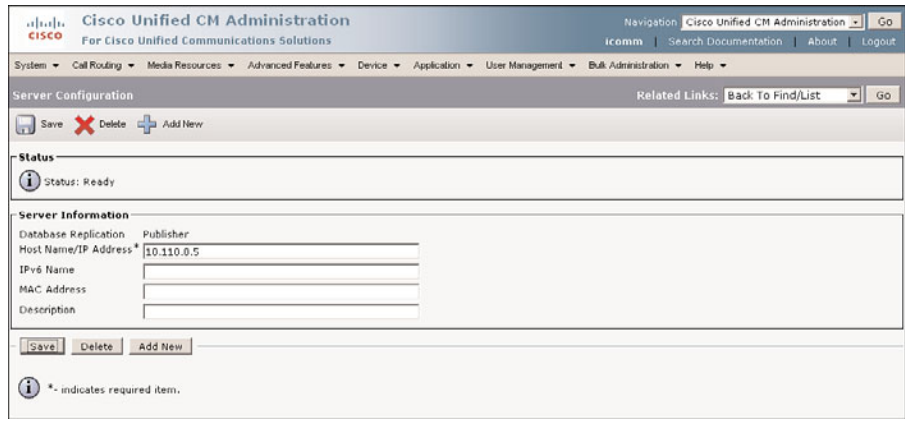
Click the hyperlinked host name of your server, and the Server Configuration details page will show. In the Host Name/IP Address field, replace the host name with the IP address of your server. See Figure 9-3 for an example of this page.

Click the **Save** button. A pop-up dialog box will appear warning you that changing the name/IP address might cause problems. Click **OK**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

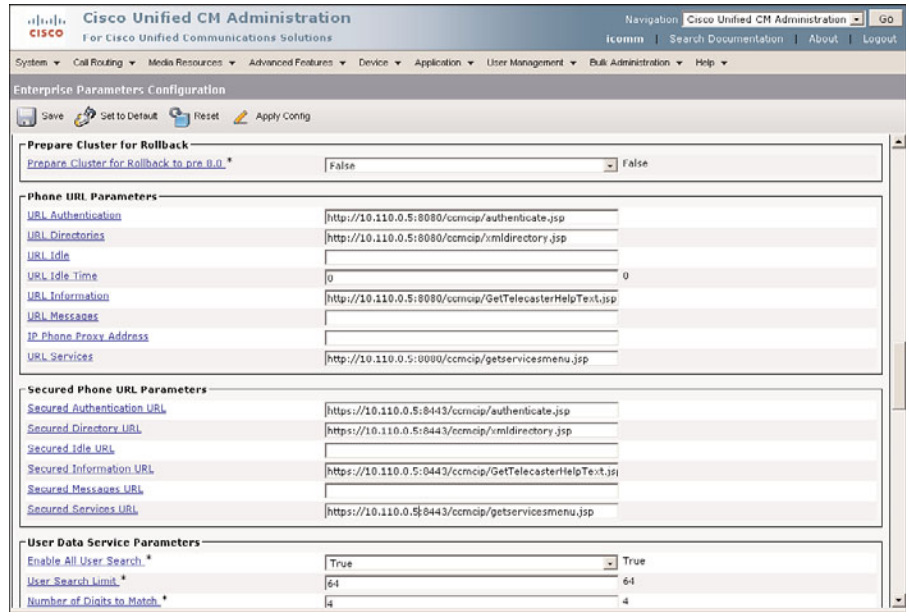
Figure 9-3 Server Configuration Page



Step 1-2: Change Phone References to IP Address

On the **Cisco Unified CM Administration** page, navigate to **System > Enterprise Parameters**. The items on this page generally impact the entire cluster of CUCM servers, and many of them never need to be changed. The second location where the host name is used is here. Scroll down to the Phone URL Parameters and the Secured Phone URL Parameters sections (scroll about midway down the page). For each section, there are four fields that reference the server host name. Replace just the host name portion of the URL with the IP address of the server for all eight items. See Figure 9-4 for an example of this page.

Figure 9-4 Enterprise Parameters Configuration Page



Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Examine Network and Feature Services

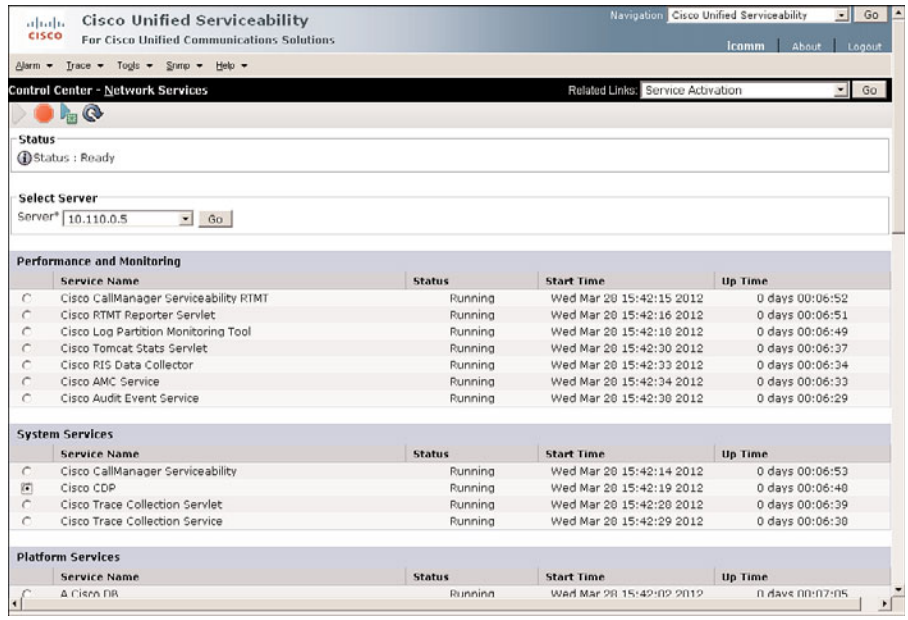
CUCM divides the services into two classes: Network Services and Feature Services. Network Services are activated during installation and are expected to be active all the time. Feature Services are items that are selected to run on the server and are deactivated by default during installation.

Step 2-1: Examine Network Services

Use the Navigation drop-down list at the upper right to select the **Cisco Unified Serviceability** item and click **Go**.

On the **Cisco Unified Serviceability** page, navigate to **Tools > Control Center – Network Services**. See Figure 9-5 for an example of this page.

Figure 9-5 Control Center – Network Services



The page shows all the network services and the status of each. By default, all the network services should have a status of Running. If you click the radio button of a service, the icons at the top (and buttons at the bottom) of the page will reflect the actions you can perform, such as Start, Stop, Restart, or Refresh. If there is more than one server in the cluster, the Server pull-down list changes the list of services to the selected server.

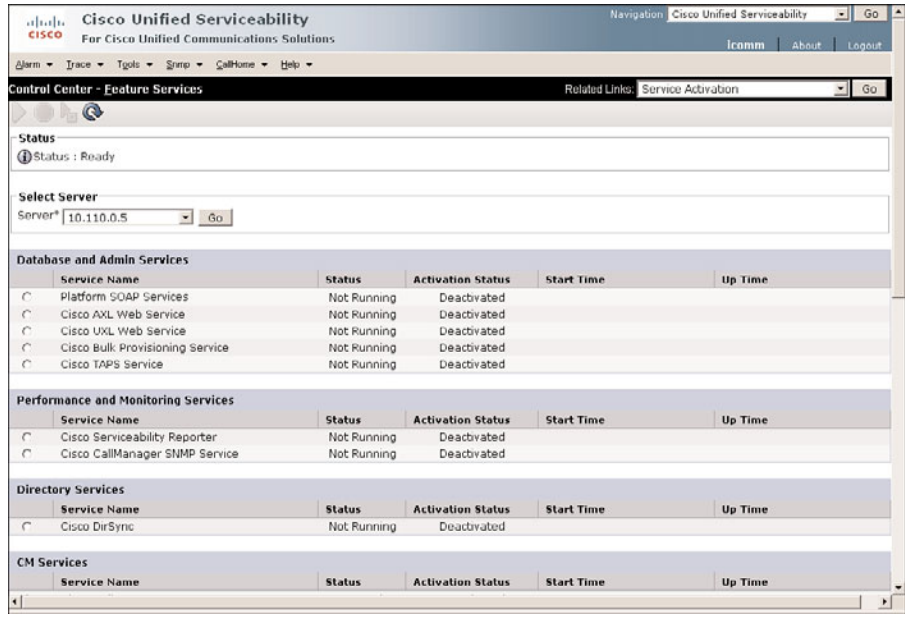
Step 2-2: Examine Feature Services

On the **Cisco Unified Serviceability** page, navigate to **Tools > Control Center – Feature Services**. The page shows all the feature services and the status of each. By default, all the feature services should have a status of Deactivated. See Figure 9-6 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-6 Control Center – Feature Services



If you click the radio button of a service that is deactivated, a dialog box will pop up notifying you that the service needs to be activated first. After the service is activated, the icons at the top (and buttons at the bottom) of the page will reflect the actions you can perform, such as Start, Stop, Restart, or Refresh. If there is more than one server in the cluster, the Server pull-down list changes the list of services to the selected server.

Task 3: Activating Feature Services and Using Help

Step 3-1: Service Activation Page

There are two ways to get to the Service Activation page to activate feature services. The first is to navigate to **Tools > Service Activation**. The other method is to use the Related Links drop-down list with the **Go** button (on the right side in the title bar) that some pages in CUCM have. The related links are necessary in some other areas to configure items, so it is worthwhile to start using them. (For example, from the Service Activation page, you can see a related link to the Control Center – Feature Services page.) See Figure 9-7 for an example of the Service Activation page.

To understand how the Service Activation page works, keep this in mind: Each service with a check mark next to it will be activated when the **Save** button is clicked, and any service without a check mark will be deactivated. Thus, if you want to add a new service to some that are already activated, leave those services selected and add a check mark to the new services before clicking **Save**.

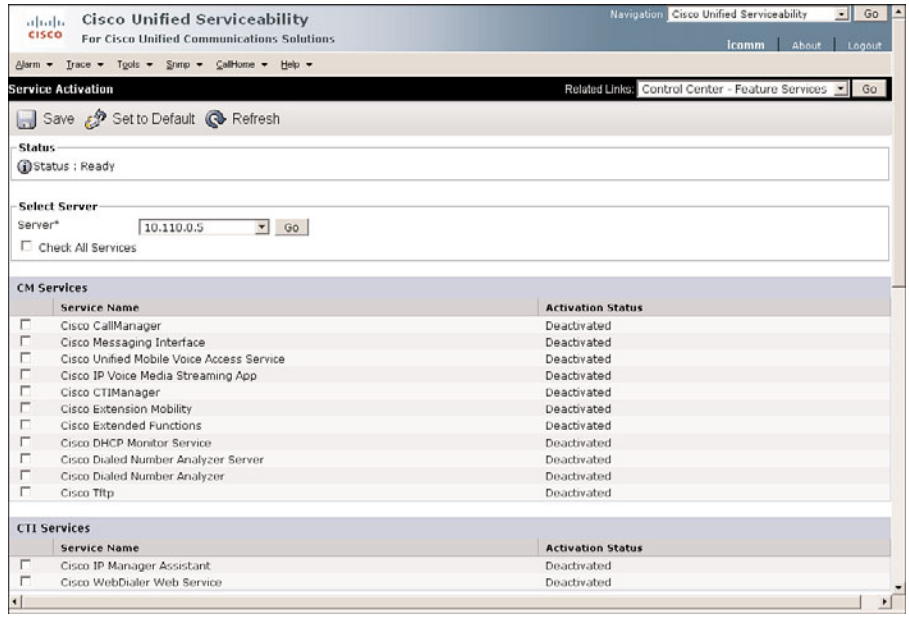
Note: It might be tempting to just select the Check All Services check box, but this is not a good idea. For one thing, not all services should be running on the same server. But there is also another reason: The more services that are running, the longer the server takes to boot and the more memory it needs. The next step will demonstrate how to get more information on the various services before activating.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

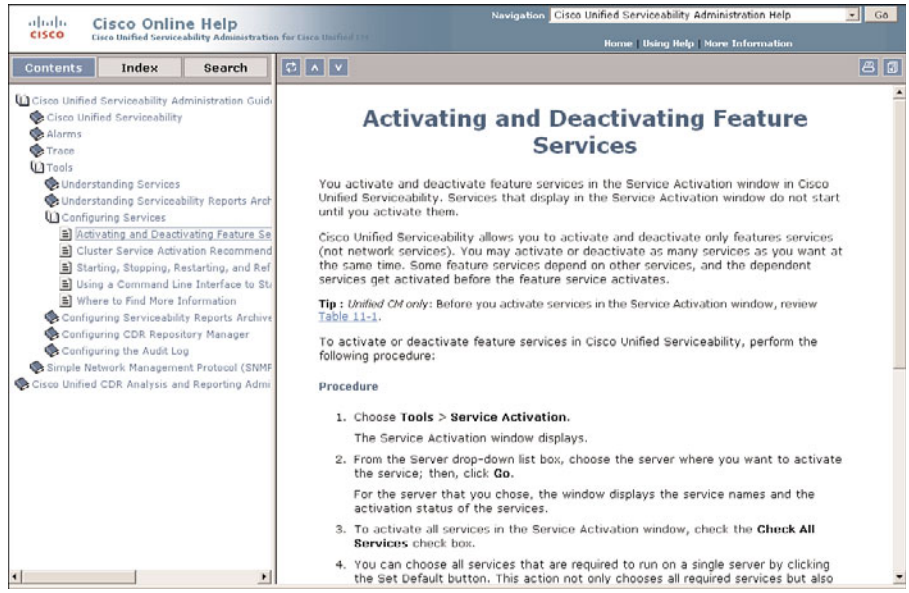
Figure 9-7 Service Activation



Step 3-2: Using the Help Menu

CUCM has a very useful Help menu built right in. In many cases, the information is the same as that listed in the product manuals. The best feature, however, is the ability to go straight to the information about the page you are working on. While you are on the Service Activation page, navigate to **Help > This Page**. A new page or tab opens in your browser. See Figure 9-8 for an example of the Help page on Service Activation.

Figure 9-8 Help on Service Activation



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

In the Help pane, you see a tip about reviewing Table 11-1 before activating feature services. Click the hyperlink to **Table 11-1** in the Help pane.

Table 11-1 in the Help pane gives more details on each of the feature services. For example, in the Cisco Messaging Interface item, it says, "Activate on only one node in the cluster. Do not activate this service if you plan to use Cisco Unity voice-messaging system." The Help menu is a handy resource if you have questions about any item on a page.

When you are done looking at the Help page, close the window or press **Tab** to return to the Service Activation page. If you have been gone for a while, you might need to log in again and navigate back to the Service Activation page.

Step 3-3: Activate Cisco CallManager and Cisco TFTP Services

While there are more services that will be used in the future, for now only the Cisco CallManager and Cisco TFTP services need to be activated. Other labs might refer back to this step to reference activating or deactivating services when they are needed.

Note: It is worth repeating that this book will not show every option of configuring CUCM. These labs should not be used verbatim as a guide on how to set up a production system. Additionally, the configurations in this lab book are designed for a test lab and should not be applied directly to a production phone system, as settings are demonstrated that could break functionality in an existing production system.

Click to select the **Cisco CallManager** and **Cisco TFTP** services check boxes, and then click the **Save** button. A pop-up dialog box opens and warns that this will take a while. See Figure 9-9 for an example of this page.

Figure 9-9 Service Activation

Click the **OK** button and wait for the page to refresh. When the page refreshes, the Cisco CallManager and Cisco TFTP services should have their status listed as Activated, while all other services are deactivated.

Task 4: Examine CUCM Licenses

As you might have noticed from Chapter 8, the home page of many CUCM navigation pages displays a license warning about operating on demo licenses. Thankfully, for people learning about CUCM, Cisco included a license with the system that allows it to boot up and connect some phones. The demo license even allows up to three servers to be in the cluster. However, to run the system in a production environment will require actual licenses. One of the things you should be aware of is how to check the status of the licenses and determine whether the system has enough to add more phones.

Step 4-1: View License Unit Report

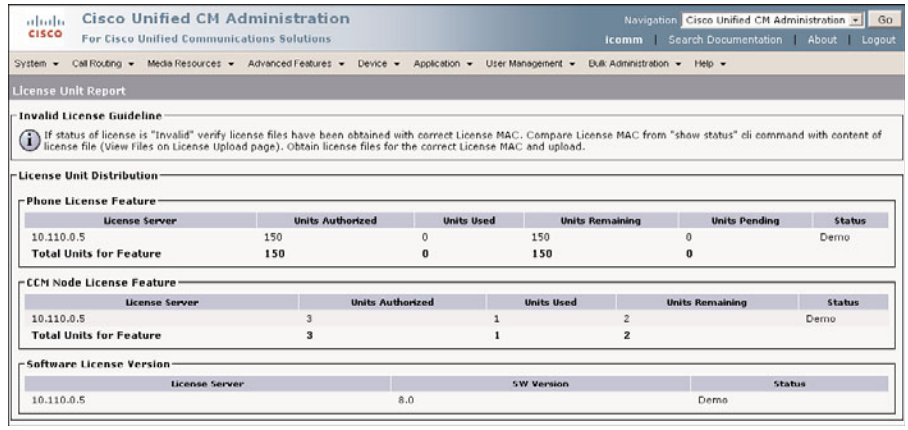
Use the Navigation drop-down list in the upper right to select the **Cisco Unified CM Administration** item and click **Go**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

On the **Cisco Unified CM Administration** page, navigate to **System > Licensing > License Unit Report**. The demo license allows 150 phone units and three CCM nodes. See Figure 9-10 for an example of this page.

Figure 9-10 License Unit Report



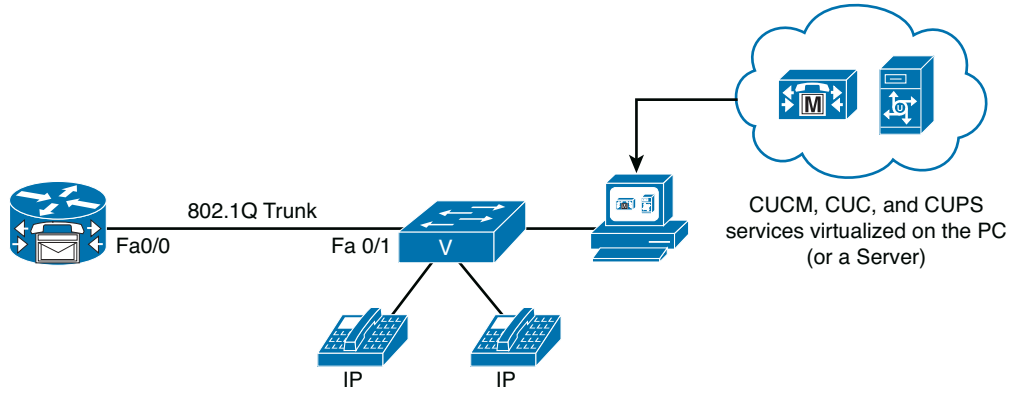
Note: The 150 units authorized does not mean that you can connect 150 phones! Each phone has a license unit count, usually between two and six units. Thus, the number of phones you can connect depends on the phone models used. If you go to the **System > Licensing > License Unit Calculator** page, a column shows the units needed for each phone model.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 9-3: Autoregistration for Phones

Figure 9-11 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- Lab configuration from Lab 9-2
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)

Learning Objective

Upon completion of this lab, you will be able to register phones automatically to CUCM.

Scenario

SOI has installed the first CUCM server in the network and would like to register a phone to test. Autoregistration is the simplest way to add phones to the CUCM system. However, autoregistration can be considered a security risk, as it allows phones to automatically register, and if not properly restricted, they can start making phone calls to the PSTN. Autoregistration should only be used when needed and deactivated otherwise. The default status of autoregistration is deactivated.

Note: *Cisco Unified Communications Manager Administration Guide Release 8.5(1)* states "Cisco recommends that you use autoregistration to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT)."

Normally, you would configure various settings to standardize and simplify phone registration before adding phones. However, it is easier to understand the settings if you use the most basic of phone registrations first—autoregistration.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Verify That Required Services Are Ready

As noted in Lab 9-1, there are many services necessary for a phone to register. Verify that the following items are functioning:

- A DHCP server is configured for the VLANs the phones will use, with option 150 set to the IP address of the CUCM server. Note: The DHCP configured in Lab 3-2 points option 150 to the router. This needs to be changed to the IP address of your CUCM server.
- The Cisco CallManager and TFTP services are activated, as detailed in Lab 9-2.
- The switch is configured with voice VLANs on the ports where desk phones will connect and data VLANs for PCs with soft phones installed.

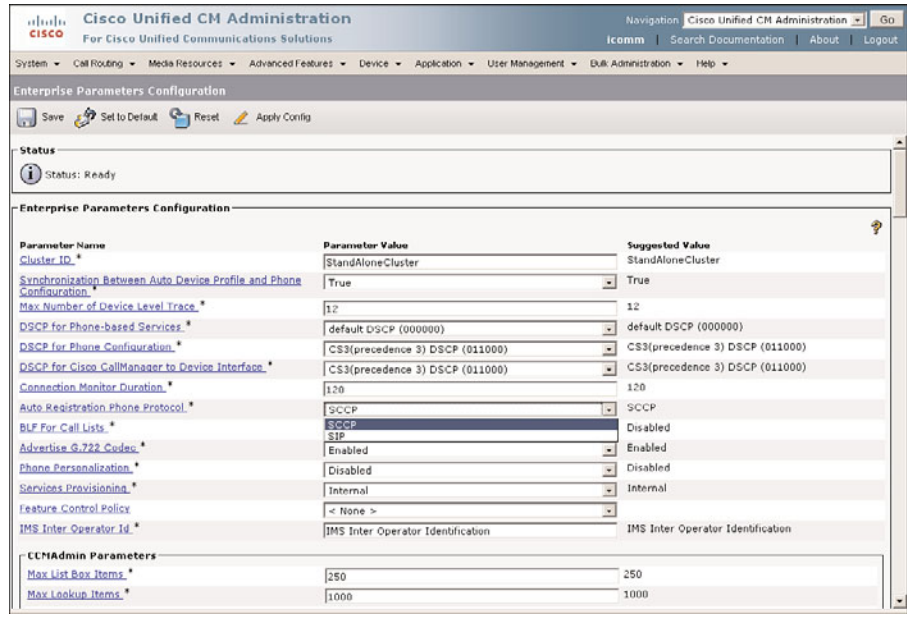
Task 2: Enable Autoregistration

Step 2-1: Verify Enterprise Settings for Autoregistration

Note: Disconnect any Cisco IP Phones you have connected. They will be connected later.

Before enabling autoregistration, it is a good idea to verify the expected registration protocol, especially if you are using phones with SIP firmware. On the **Cisco Unified CM Administration** page, navigate to **System > Enterprise Parameters**. Near the top of the list is **Auto Registration Phone Protocol**. Verify that the protocol your phone will use is selected. Unless you are using SIP phones, the default value of SCCP is fine. See Figure 9-12 for an example of this page.

Figure 9-12 Enterprise Parameters Configuration



Step 2-2: Enable Autoregistration

On the **Cisco Unified CM Administration** page, navigate to **System > Cisco Unified CM** and click the **Find** button. Click the hyperlinked name of the server (for example, CM_CUCM862). If there is more than one server, click the server where autoregistration will be enabled.

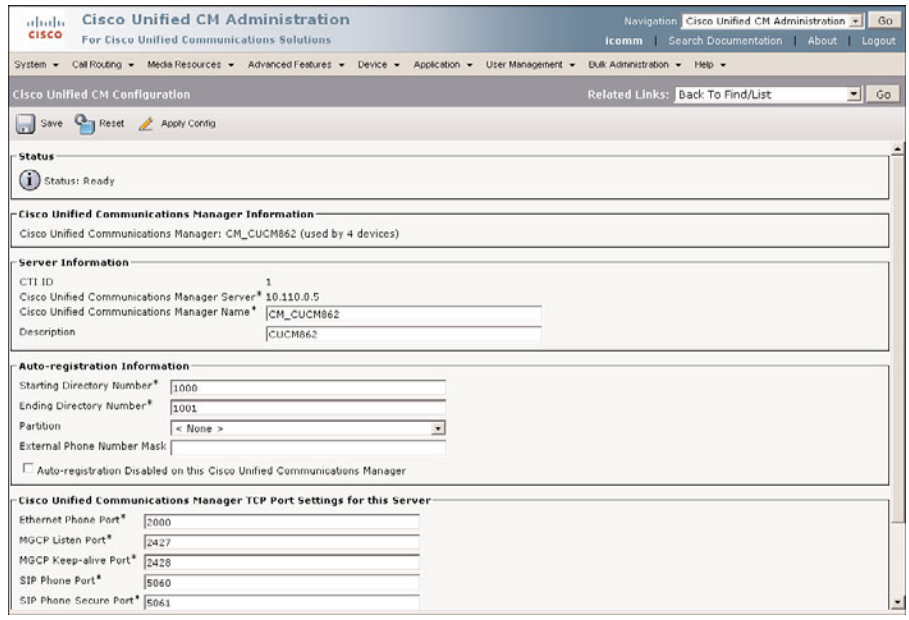
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

The Cisco Unified CM Configuration page shows various parameters related to the server. In the Auto-registration Information section are the fields that control autoregistration. By default, the extension directory numbers are assigned starting and ending at 1000.

1. To enable autoregistration, change the **Ending Directory Number** to a number higher than the **Starting Directory Number** (use 1001 for this lab). If you were using autoregistration in production, you would change both the starting and ending directory numbers to the desired extension range to be assigned to the autoregistering phones. (But for this lab, don't change the Starting Directory Number field.)
2. After you exit the Ending Directory Number field, the **Auto-registration Disabled on this Cisco Unified Communications Manager** check box is automatically deselected. (Note that if you select this box, the ending directory number is reset to the value of the starting directory number, and phones are blocked from autoregistering.)
3. Because you have not completed any advanced phone configurations, leave the **Partition** at **< None >**. See Figure 9-13 for an example of this page.
4. Click the **Save** button.

Figure 9-13 Cisco Unified CM Configuration



Task 3: Testing with Phones

Step 3-1: Connect Two Phones

Connect your desk phone or launch the soft phone on your PC.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Note: If you are using a desk phone, and this is the first time it has connected to this version of CUCM, the firmware will automatically upgrade (or downgrade). The firmware change takes a few minutes and will likely cause the phone to reboot a few times; make sure to let it finish.

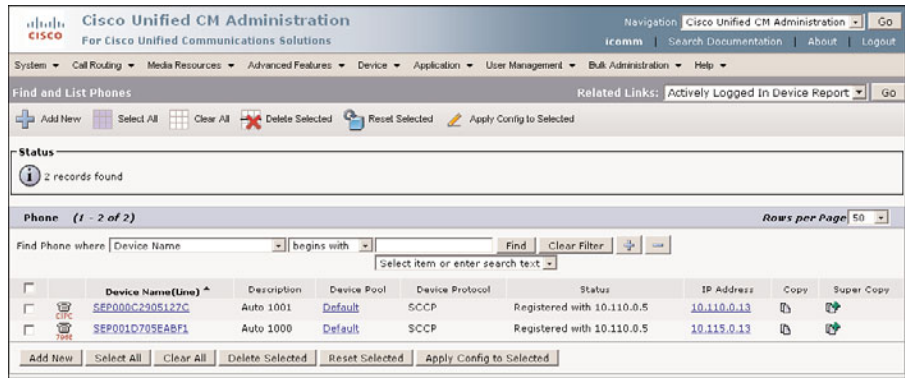
If you have problems getting the phone to register, first verify that you clicked the **Save** button in Step 2-2. If the phone was registered previously to a different CallManager, you might need to clear the settings on the phone. See the hardware section in the Introduction for more details.

After your phones have registered, you will see the assignment of extensions starting with the starting directory number (1000 by default). If you connected more than one phone, you can call from one phone to the other.

Step 3-2: Examine the Registered Phones

On the **Cisco Unified CM Administration** page, navigate to **Device > Phone** and click **Find**. Listed here are all the phones registered in the system. See Figure 9-14 for an example of this page.

Figure 9-14 Find and List Phones



Click the hyperlinked device name (SEP and the MAC address) of a phone. The Phone Configuration page opens, where you see the fields configured for phones. See Figure 9-15 for an example of this page.

On the left side are the line buttons and all the configurable options. Notice that the default profile for a phone is to assign two phone lines (but only the first is assigned a directory number), and the rest of the buttons default to user speed dials (assuming that the phone model has more than two buttons).

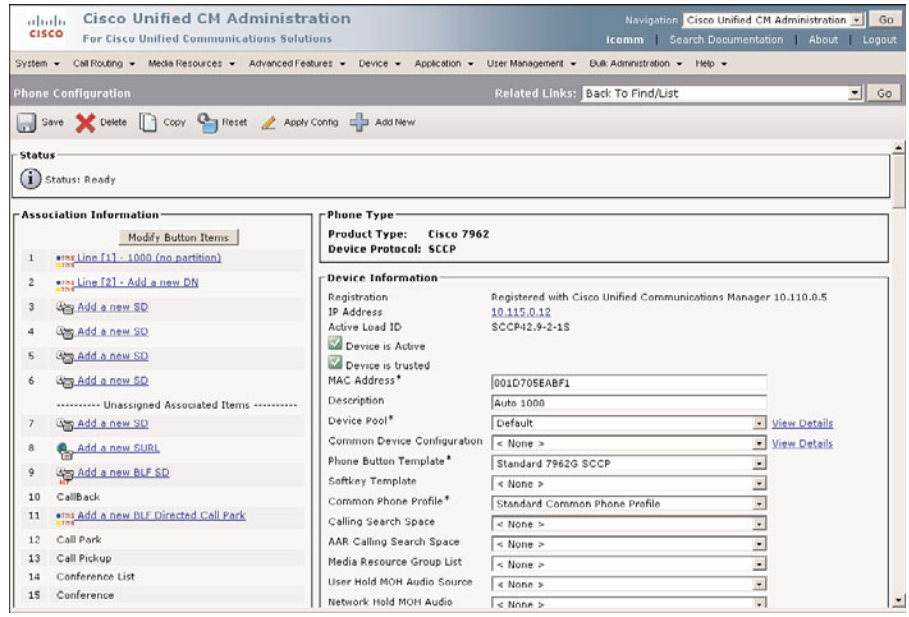
On the right side are options for the phone. As you scroll down, you see an almost-overwhelming number of options that can be configured for a phone!

If you added more than one phone, make a call from one phone to the other. Make sure to pay attention to the softkeys (at the bottom of the phone display). The options change depending on the state of the phone—if the phone is on-hook, ringing, dialing a call, and so on.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-15 Phone Configuration



Task 4: Cleanup

Step 4-1: Disable Autoregistration

On the **Cisco Unified CM Administration** page, navigate to **System > Cisco Unified CM** and click the **Find** button if no servers are listed.

1. Click the hyperlinked name of the server (**CU_CUCM862**) where autoregistration is enabled.
2. Select the **Auto-registration Disabled on this Cisco Unified Communications Manager** check box. The ending directory number will change to match the starting directory number.
3. Click the **Save** button. A pop-up dialog box will warn you that this will disable autoregistration. Click the **OK** button.
4. To be sure that autoregistration is disabled, click the **Apply Config** button, and click the **OK** button to confirm.

Step 4-2: Remove Registered Phones

Remove all autoregistered phones from the system. (However, realize that the directory numbers are not removed with the phone and are still in the system. If you later try to autoregister phones, you will need to increase the range of numbers, as CUCM will not hand out a number that is still in the system. Examining previously assigned numbers is covered in a later lab.)

There are two methods to remove phones. While on the Phone Configuration page, click the **Delete** button. If you click **OK** in the warning window, the phone is removed from CUCM.

The other option is on the Find and List Phones page. On the **Cisco Unified CM Administration** page, navigate to **Device > Phone** and click **Find**.

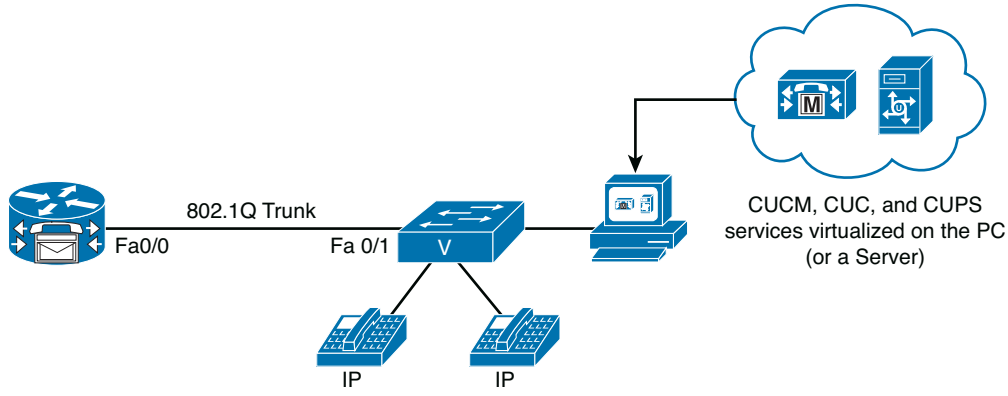
Select the check boxes in the first column for each phone that you want to delete (or use the **Select All** button) and click the **Delete Selected** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 9-4: Preparing for Phone Registration

Figure 9-16 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- CUCM Server or PC with VMware Workstation installed and a VM of CUCM
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)
- Lab configuration from Lab 9-2 or 9-3

Learning Objectives

Upon completion of this lab, you will be able to configure

- Device pools
- Communication manager groups
- Date/time groups
- Regions
- Locations
- Phone button templates
- Softkey templates
- Common phone profiles
- Device defaults

Scenario

SOI is going to add many phones in the near future. Modifying all the options that can be configured on each phone individually (as shown in Lab 9-3) can be overwhelming, time-consuming, and error-prone. To avoid having to change the settings on every phone after it is added, device pools and common device configurations can be configured to standardize some of the key options for phones.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Examine the Default Device Pool

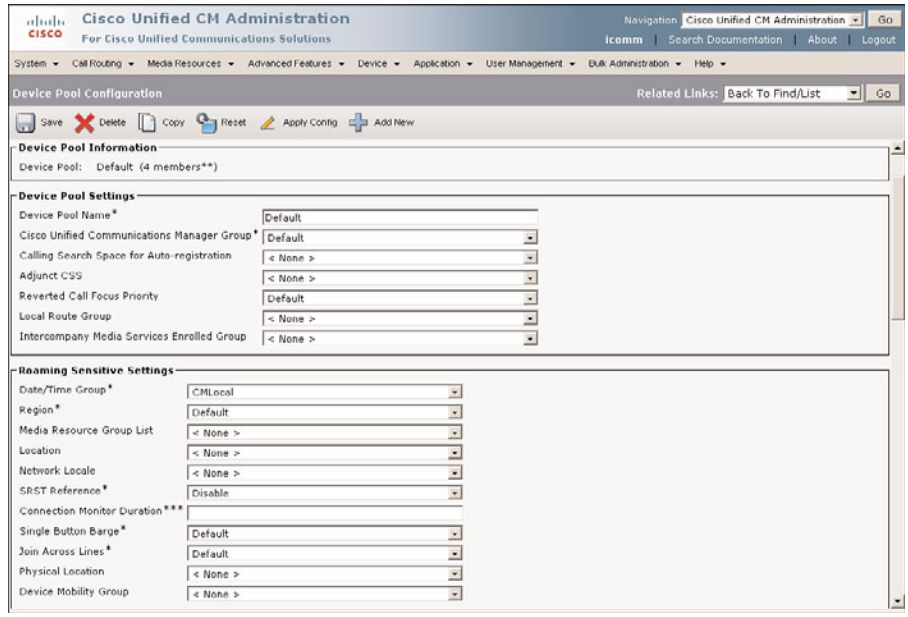
Before starting to configure various options that are commonly configured in a device pool, it helps to examine one first. CUCM has a default device pool, so you can start registering phones without too much configuration.

On the **Cisco Unified CM Administration** page, navigate to **System > Device Pool** and click the **Find** button if no pools are listed.

Click the hyperlinked name of the default pool. (Make sure that you click **Default** under the Name column, or it will take you to one of the other options, such as the CM Group.)

The device pool has settings that simplify configuring phones (and other devices, such as gateways, voicemail ports, conference bridges, and so on). Although there are many options that can be selected in a device pool, this lab will focus on the most common elements. See Figure 9-17 for an example of this page.

Figure 9-17 Default Device Pool Configuration



Before creating device pools, you need to configure some common elements used in the device pools, such as communication manager groups, date/time groups, regions, and locations.

Task 2: Communications Manager Groups

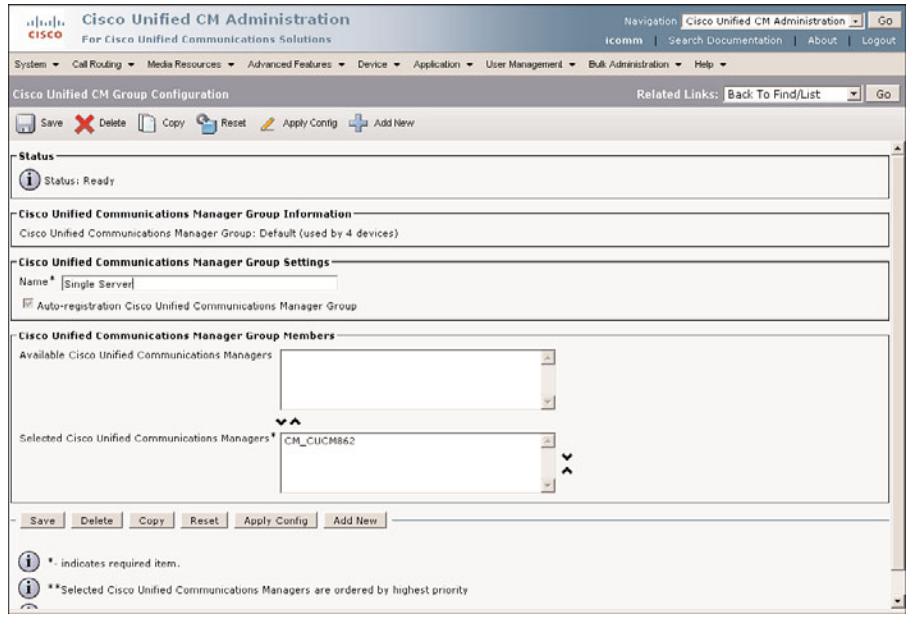
On the **Cisco Unified CM Administration** page, navigate to **System > Cisco Unified CM Group** and click the **Find** button if no pools are listed.

Click the hyperlinked name of the default group. The details of the CM Group Configuration will open. Change the Name field to **Single Server**. See Figure 9-18 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-18 Default Cisco Unified CM Configuration



Click the **Save** button. A pop-up dialog box will open, warning about the devices that will be impacted and that you might need to reset to have changes take effect. Click **OK** to close the window.

When you have a single CUCM server, there is no point in having more than one CM group. The real value in CM groups is when there is more than one server in a cluster to achieve redundancy and load balancing for phone registration.

Example of a Cluster with Three Servers

Note: You only need one CUCM server to complete these labs. The rest of Task 2 shows an example and screen captures to illustrate the concepts used if there is more than one CUCM server in a cluster, although this not required for the labs.

Adding a single subscriber to the Publisher server does not automatically change the registration default. Phones still register to the first server installed (Publisher), unless you create a CM group and prioritize the registration.

For load balancing, if there is a Publisher and two or more Subscriber servers, all the phones still register to the Publisher by default. However, by creating two CM groups, phones can be manually load-balanced between the Subscriber servers (See Figure 9-19).

For example, if there is a Publisher and two Subscriber servers (in this example called Pub, Sub1, and Sub2), create a CM group called Sub1Sub2Pub, where the Subscriber 1 server is the primary registration server, the Subscriber 2 server is the secondary registration server, and the Publisher is the tertiary server (third and last choice) for registration (See Figure 9-20). When the three servers are moved from the Available CUCM servers list to the Selected CUCM server list using the arrows between the two lists, the arrows to the right of the Selected CUCM server list are used to put them in the desired order. Notice that the phones register to the servers going down the list, starting from the top to bottom, and each CM group can only have up to three servers listed in it.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-19 CM Load Balancing

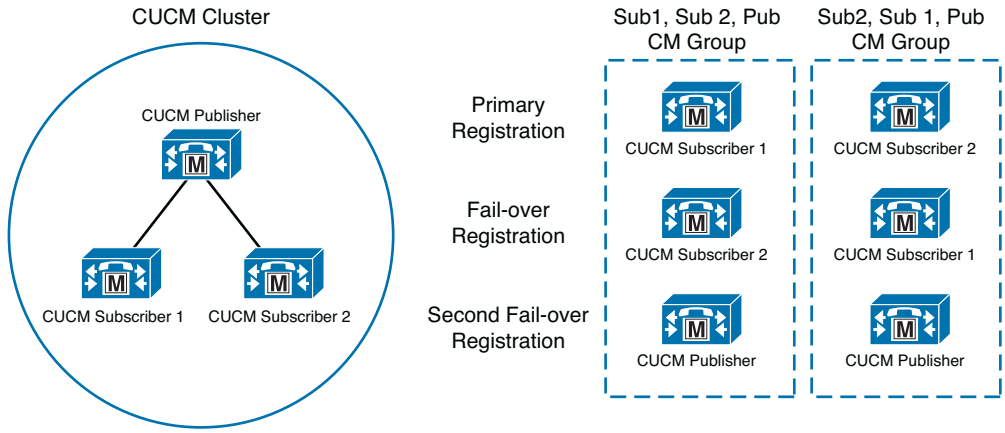
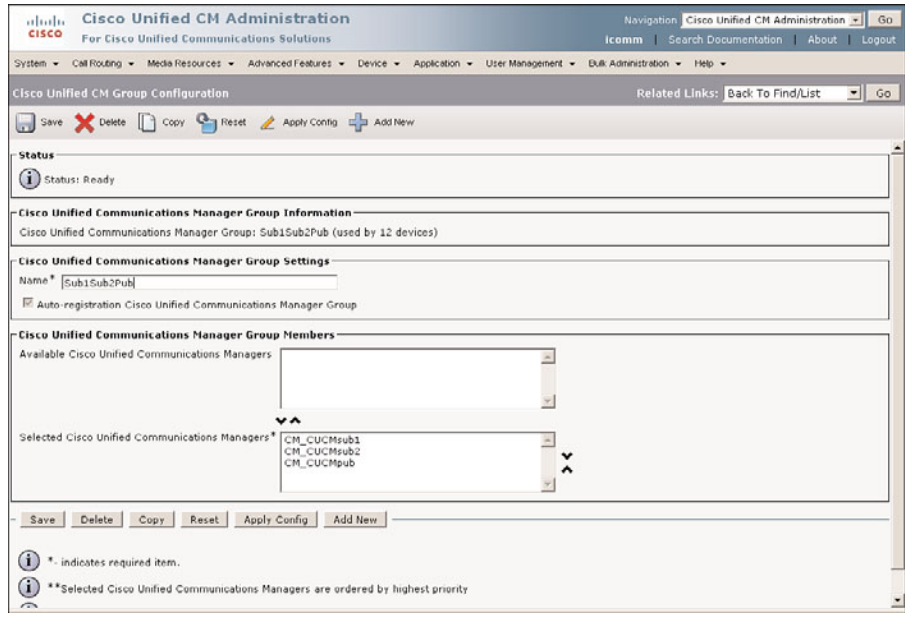


Figure 9-20 CM Group Sub1Sub2Pub



Another CM group called Sub2Sub1Pub would have the Subscriber 2 server as the primary registration server, the Subscriber 1 server as the secondary registration server, and the Publisher as the tertiary registration server (see Figure 9-21).

Later, when registering phones, the Sub1Sub2Pub CM group would be used to register some phones, and the Sub2Sub1Pub CM group is used to register other phones, providing a load balance between the Subscriber servers.

There is one warning about load balancing: It is possible to have the system run fine when everything is functioning correctly, but overload the servers when there is a failure. The maximum number of phones a single server can safely manage varies based on the hardware. For the sake of illustration, assume that your current hardware can have a maximum of 1500 phones register to a single server. If you have 2000 phones, with 1000 on Subscriber 1 and 1000 on Subscriber 2, everything is fine. However, if either subscriber fails and the other subscriber is the secondary registration server, the remaining server will suddenly have 2000 phones registered, which could overload it (see Figure 9-22).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-21 CM Group Sub2Sub1Pub

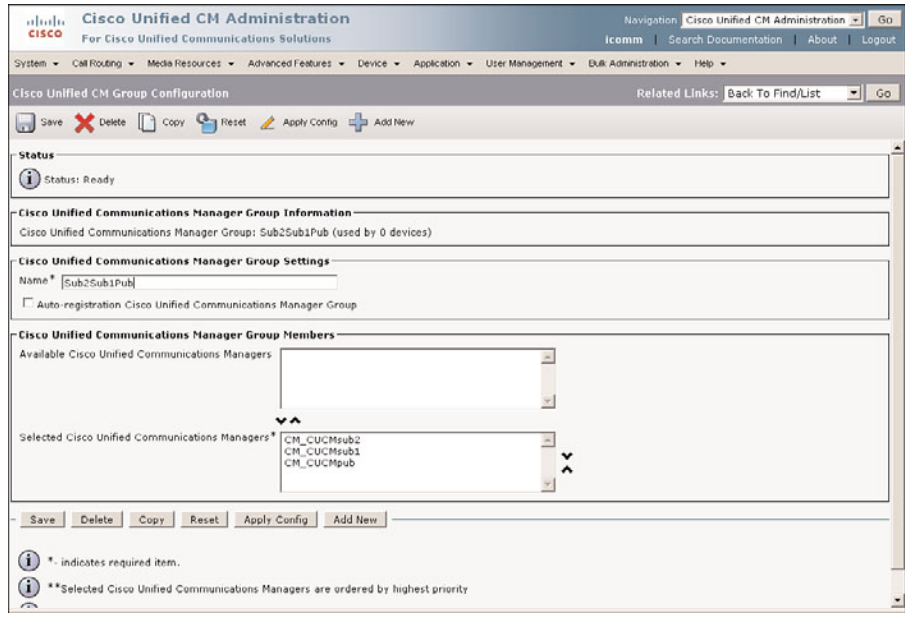
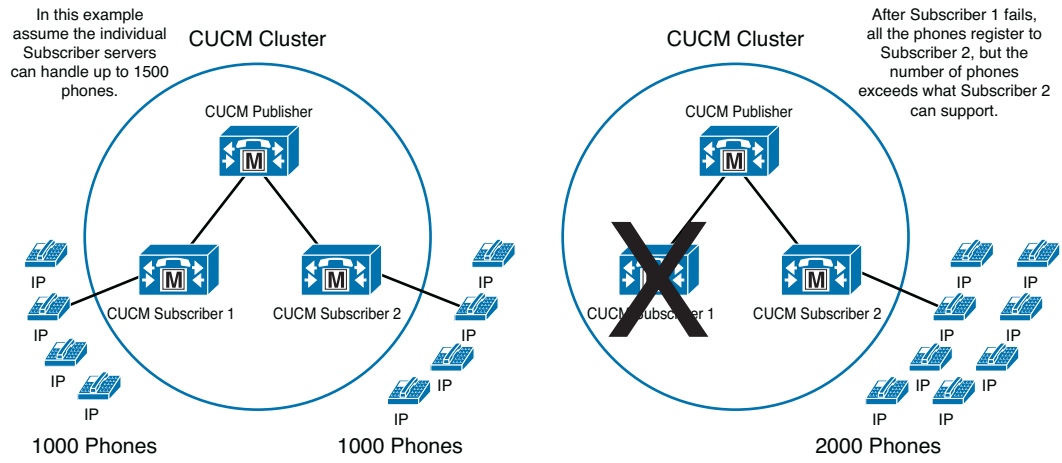


Figure 9-22 Load-Balancing Overload



To have this cluster configuration survive the failure of a server, a third CUCM Subscriber would be required. The process of creating a redundant cluster of CUCM servers is beyond the scope of the CCNA Voice exam.

Task 3: Date/Time Groups

CUCM in a centralized deployment can manage phones in different countries and time zones. Naturally, users want the display on their phones to show the correct date and time for their location. For this to work, CUCM needs to know the correct time zone for each phone, and to implement this, the time zones that CUCM supports must be defined.

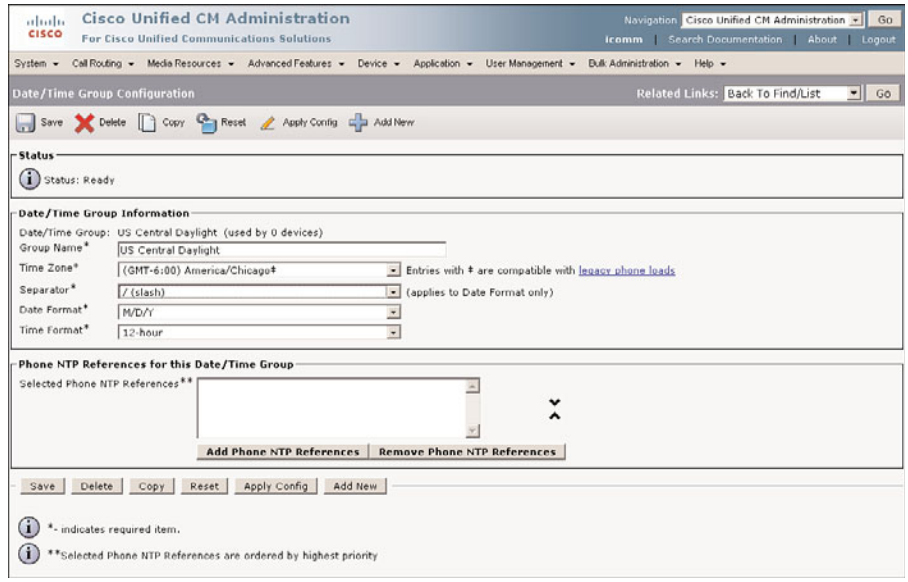
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-1: Create Central Time Zone Group

1. On the **Cisco Unified CM Administration** page, navigate to **System > Date/Time Group** and click the **Find** button if no groups are listed. You will see the **CMLocal** group, which represents the default time zone for phones. Because this is used by the system, keep the CMLocal group. Click the **Add New** button to create a new group for the actual time zone the bulk of the phone will reside in. For this lab, enter **US Central Daylight** in the Group Name field.
2. From the Time Zone drop-down list, choose **(GMT-6:00) America/Chicago**.
3. Change the Separator, Date Format, and Time Format fields to match your preferences. The Phone NTP References field for this date/time group is not needed for Skinny Client Control Protocol (SCCP)–controlled phones but is recommended for Session Initiation Protocol (SIP) phones. (Without a Network Time Protocol (NTP) server, a SIP phone has to rely on the timestamps in the SIP control messages.) See Figure 9-23 for an example of this page.
4. Click the **Save** button.

Figure 9-23 US Central Daylight Date/Time Group



Step 3-2: Create Eastern Time Zone Group

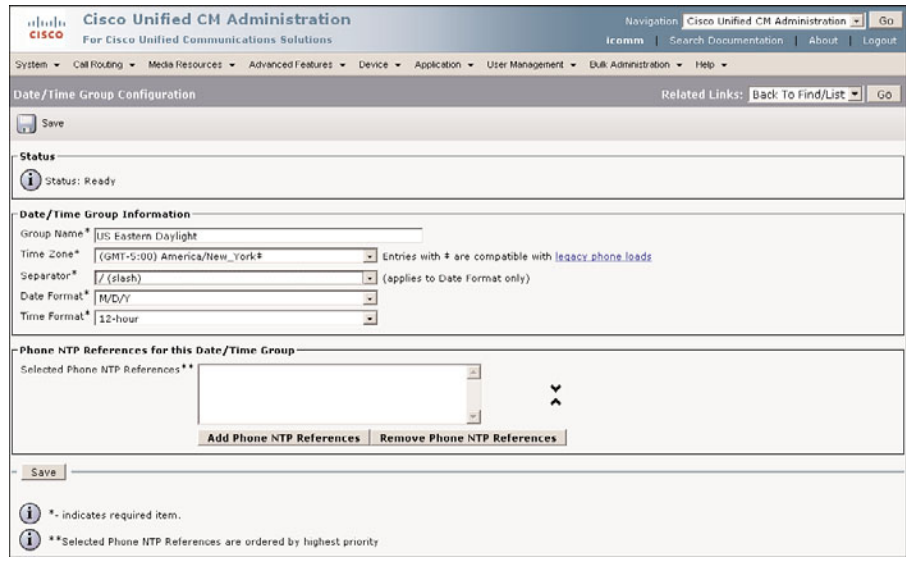
For a single-site location, one time zone would be enough, but for this lab, you will use two time zones.

1. Click the **Add New** button.
2. Enter **US Eastern Daylight** for the Group Name field.
3. From the Time Zone drop-down list, choose **(GMT-5:00) America/New_York**.
4. Change the Separator, Date Format, and Time Format fields to match your preferences. See Figure 9-24 for an example of this page.
5. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

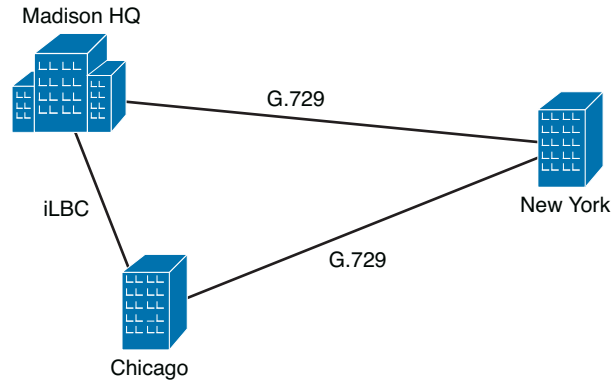
Figure 9-24 US Eastern Daylight Date/Time Group



Task 4: Regions

Regions are used in a CUCM system that has multiple locations with WAN connections between them. (For a single-location system, there is no need for regions.) The problem with WAN bandwidth is if the number of calls exceeds the assigned bandwidth for VoIP traffic, all calls suffer, not just the newest call. Regions define each LAN and the desired codec to use for each call when contacting other LANs. Using the regions to define LANs allows the CUCM system to signal the phones to use a higher-bandwidth codec when the phones are in the same LAN, but to use a less-bandwidth-intensive codec, such as G.729, when calls cross the WAN (see Figure 9-25). It is important to understand that regions will define the codec (or bandwidth) for an *individual* call. Regions do not define the total number of calls or total bandwidth that enters or exits a LAN.

Figure 9-25 SOI Offices



https://t.me/learningnets
From the Library of Aliwarman Tarihoran

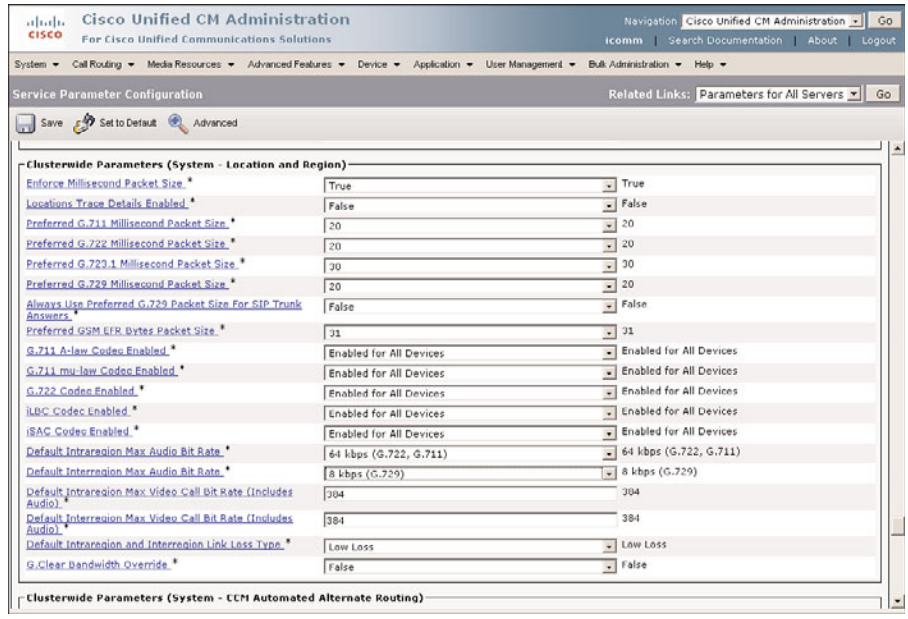
Step 4-1: Examine the Default Region Codecs

Before defining regions, it is important to understand the default codecs that CUCM uses for calls within a region (intraregion) and between regions (interregion).

On the **Cisco Unified CM Administration** page, navigate to **System > Service Parameters**.

1. Select the IP address of the server from the Server drop-down list. The Service drop-down list will appear.
2. Select **Cisco CallManager (Active)**.
3. Scroll down (way down) to the **System – Location and Region** settings.
4. Notice the values for the **Default Intraregion Max Audio Bit Rate** and the **Default Interregion Max Audio Bit Rate**. See Figure 9-26 for an example of this page.

Figure 9-26 Default Bandwidth (Codec) Values for Regions



Just by defining two or more regions, the system will signal phones to use 8 kbps (G.729 codec) for calls between phones assigned to different regions, but allow 64 kbps (G.711 or G.722 codec) between phones in the same region.

Step 4-2: Create the First Two Regions

On the **Cisco Unified CM Administration** page, navigate to **System > Region** and click the **Find** button if no regions are listed. Click the hyperlinked name of the default region.

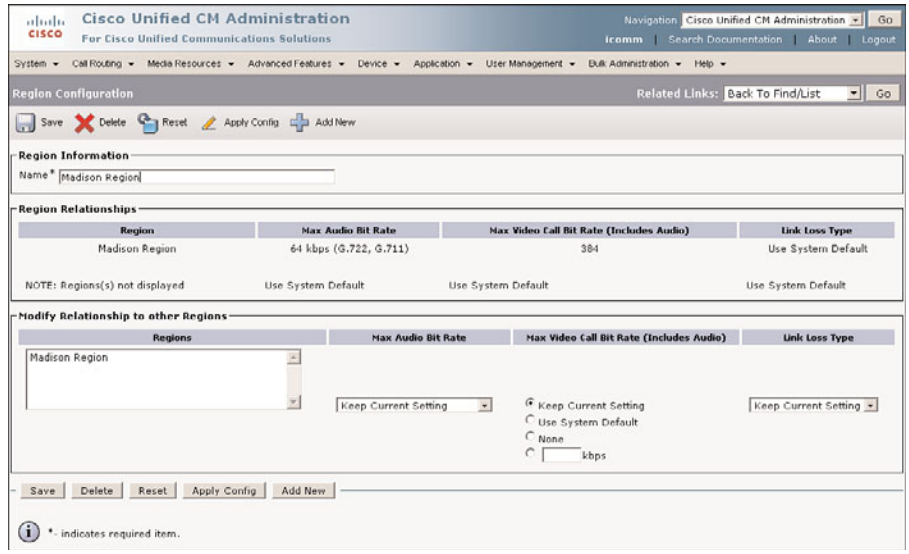
This lab will configure three regions. Changing the default region name to one of the sites will prevent devices from connecting to a region that is not assigned an actual location.

1. Replace **Default** in the Name field with **Madison Region**. The other settings will be explained after adding the second region. See Figure 9-27 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-27 Madison Region



2. Click the **Save** button. You will get a warning about impacting calls. Click **OK**.
3. Click the **Add New** button.
4. Enter **New York Region** for the Name field.
5. Click the **Save** button.

Step 4-3: Modify Region Relationships

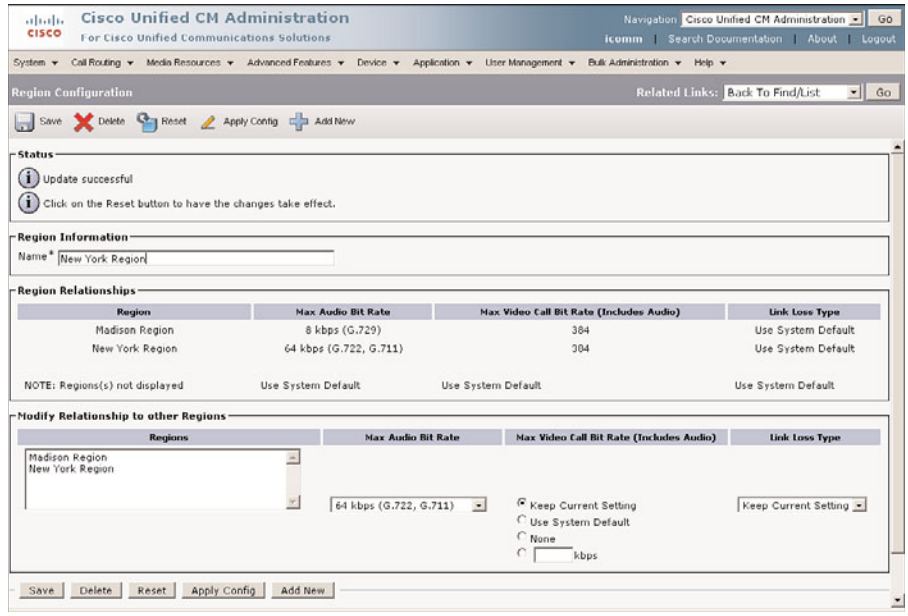
Now that there are two regions, you can change the bandwidth per call used between the regions (or even within the region).

1. In the Modify Relationship to Other Regions section of the page, click **Madison Region**.
2. From the Max Audio Bit Rate drop-down list, select **8 kbps (G.729)** and click the **Save** button. The Region Relationships section (in the middle of the page) will now show the new relationship of the New York Region to the Madison Region as 8 kbps. (Conveniently, when setting or changing the New York–to–Madison call bandwidth, the system also applies the same value to the Madison–to–New York relationship.)
3. In the Modify Relationship to Other Regions field, click **New York Region**.
4. From the Max Audio Bit Rate drop-down list, select **64 kbps (G.711, G.722)** and click the **Save** button. This defines the bandwidth used between phones within the New York region. See Figure 9-28 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-28 New York Region Relationships



Step 4-4: Create a Third Region

1. Click the **Add New** button and enter **Chicago Region** for the Name field.
2. Click the **Save** button.
3. In the Modify Relationship to Other Regions section of the page, click **Madison Region**.
4. From the Max Audio Bit Rate drop-down list, select **16 kbps (iLBC, G.728)** and then click the **Save** button.

Note: If your phones do not support the iLBC codec, change the Chicago-to-Madison bandwidth to 64 kbps (G.711, G.722).

---

5. Click **New York Region**.
6. From the Max Audio Bit Rate drop-down list, select **8 kbps (G.729)** and then click the **Save** button.
7. Click **Chicago Region** from the Max Audio Bit Rate drop-down list, select **64 kbps (G.711, G.722)**, and then click the **Save** button. See Figure 9-29 for an example of this page.

Note: Technically, the settings for all regional relationships just configured, except the Madison–Chicago relationship, are the same as the system defaults. The *Cisco Unified Communications System Release 8.x SRND* states "Changing these values for individual regions and locations from the default has an impact on server initialization and publisher upgrade times. Hence, with a total of 2,000 regions and 2,000 locations, you can modify up to 200 of them to use non-default values. With a total of 1,000 or fewer regions and locations, you can modify up to 500 of them to use non-default values."

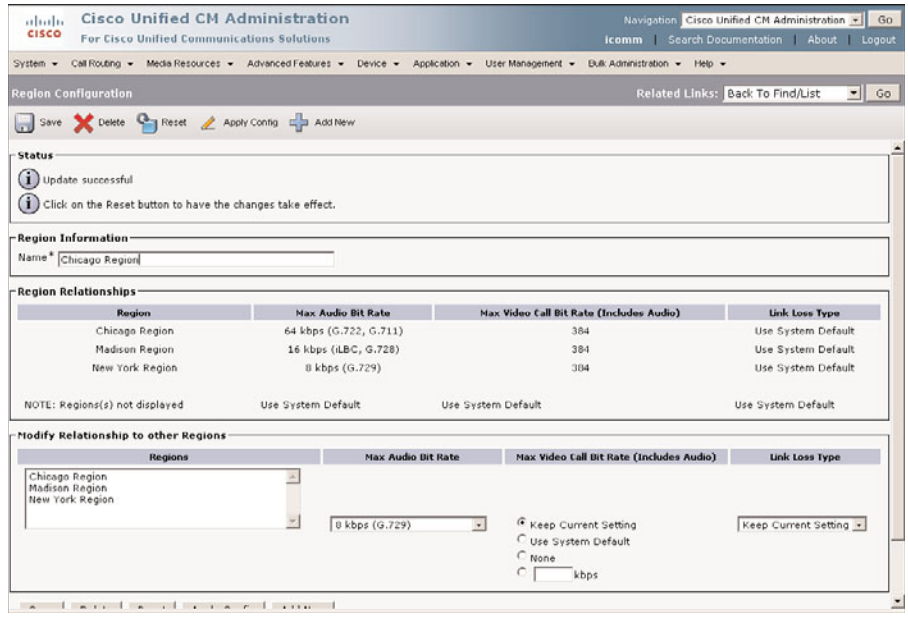
The settings were configured mainly to illustrate how the configuration works. For a production system, it would be best to just create regions and only modify relationships that differ from the defaults. Thus, only the Madison–Chicago relationships needed to be defined.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-29 Chicago Region Relationships



Task 5: Locations

While regions define the per-call bandwidth, the locations define the total WAN bandwidth a location can send or receive. The actual function of locations will be explored in Chapter 10, "CUCM Dial Plan," but for right now, you need to define a few locations.

Note: Locations work when there is one CUCM cluster that centrally controls all the devices. If you have a non-centralized system, or use gatekeepers, CUCM supports an alternate call admission control (CAC) mechanism using the Resource Reservation Protocol (RSVP).

On the **Cisco Unified CM Administration** page, navigate to **System > Location** and click the **Find** button if no locations are listed. There are two default locations called Hub_None and Phantom. Leave these default items as they are.

1. Click the **Add New** button and enter **Madison Location** for the Name field.
2. Click the **Audio Bandwidth** radio button for the empty box and enter **50** for kbps. See Figure 9-30 for an example of this page.
3. Click the **Save** button.
4. Click the **Add New** button and enter **New York Location** for the Name field.
5. Click the **Audio Bandwidth** radio button for the empty box and enter **50** for kbps.
6. Click the **Save** button.
7. Click the **Add New** button and enter **Chicago Location** for the Name field.
8. Click the **Audio Bandwidth** radio button for the empty box and enter **50** for kbps.
9. Click the **Save** button.
10. Return to the **System > Location** page and click the **Find** button if no locations are listed. See Figure 9-31 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-30 Madison Location Settings

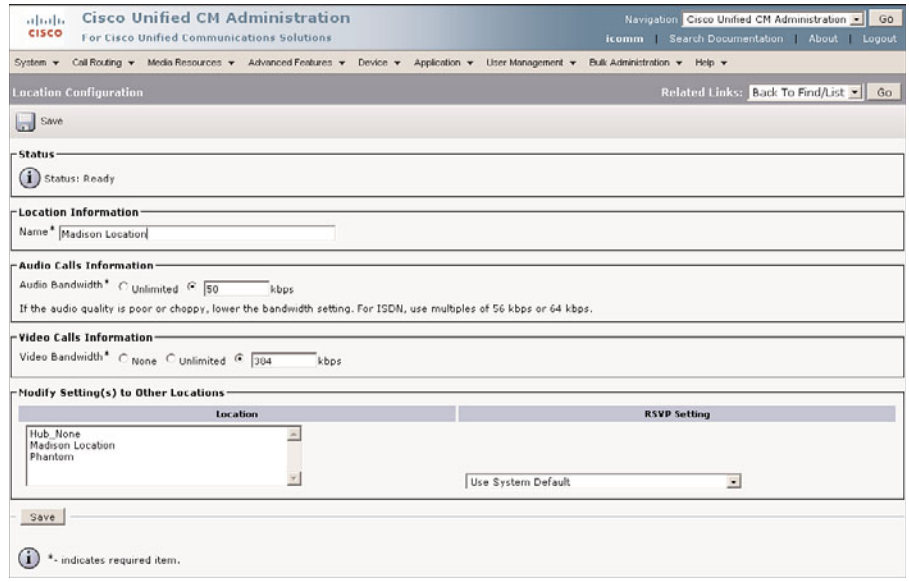
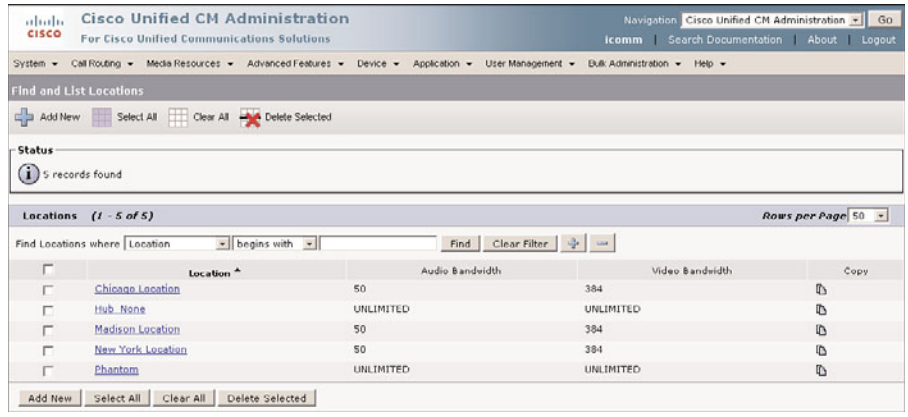


Figure 9-31 Locations



Task 6: Device Pools

With key settings configured, it is time to build some device pools! (There are many options that can be configured in device pools that are beyond the scope of the CCNA Voice exam, and other options you will configure later, such as device mobility groups.)

Before configuring device pools, a naming convention should be discussed. If there is just the default CM group, a device pool for each Region–Location combination is necessary. However, if there is more than one CM group, to achieve load balancing, the Region–Location combinations will need a device pool for each CM group. Using naming for the device pool that reflects the CM group helps when registering phones to correctly load balance. Using the previous example of a cluster with three servers, if there are two CM groups called Sub1Sub2Pub and Sub2Sub1Pub, there should be device pools named something like this:

- Madison S1S2P DG
- Madison S2S1P DG

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

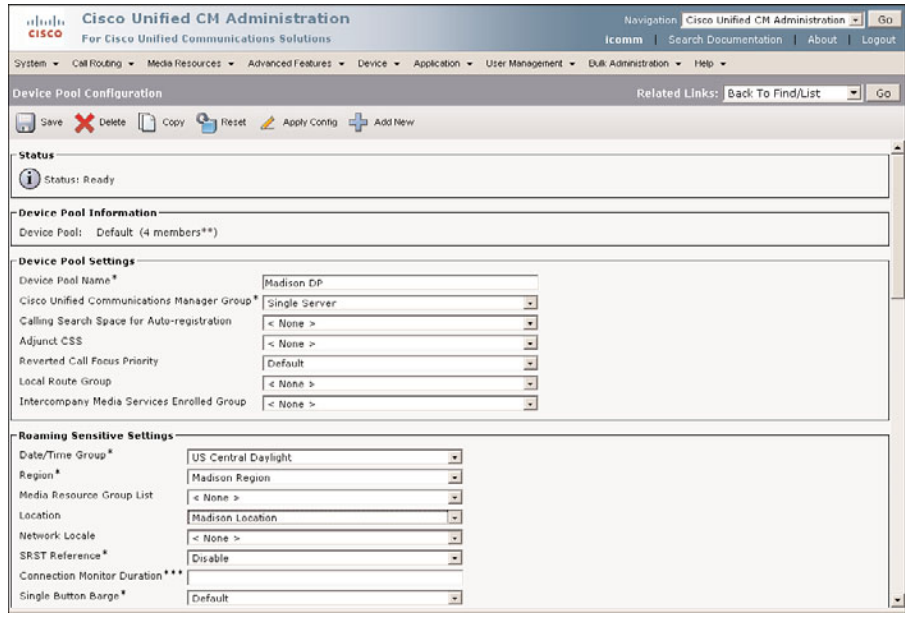
- New York S1S2P DG
- New York S2S1P DG
- Chicago S1S2P DG
- Chicago S2S1P DG

Step 6-1: Create Madison Device Pool

On the **Cisco Unified CM Administration** page, navigate to **System > Device Pool** and click the **Find** button if no pools are listed.

1. Click the hyperlinked name of the default pool.
2. Replace **Default** in the Device Pool Name field with **Madison DP**.
3. From the Date/Time Group drop-down list, select **US Central Daylight**.
4. The Region drop-down list should already be set to **Madison Region**.
5. From the Location drop-down list, choose **Madison Location.** See Figure 9-32 for an example of this page.
6. Click the **Save** button.

Figure 9-32 Madison Device Pool



Step 6-2: Create New York Device Pool

1. Click the **Add New** button and enter **New York DP** for the Device Pool Name field.
2. From the Cisco Unified Communications Manager Group drop-down list, choose **Single Server**.
3. From the Date/Time Group drop-down list, choose **US Eastern Daylight**.
4. From the Region drop-down list, choose **New York Region**.

https://t.me/learningnets

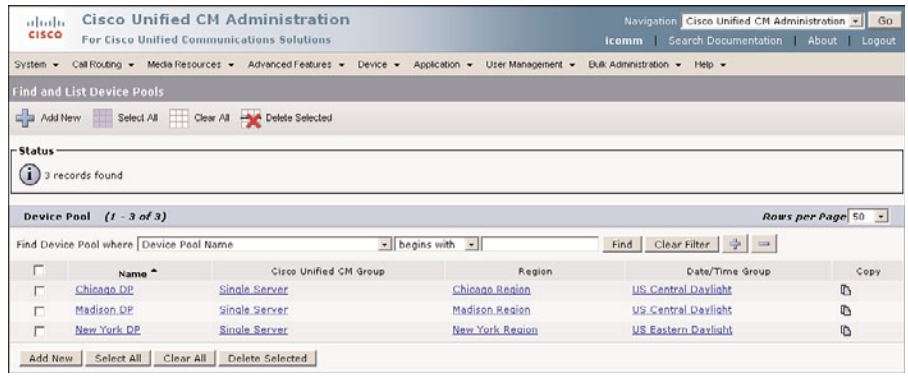
From the Library of Aliwarman Tarihoran

5. From the Location drop-down list, choose **New York Location**.
6. Click the **Save** button.

Step 6-3: Create Chicago Device Pool

1. Click the **Add New** button and enter **Chicago DP** for the Device Pool Name field.
2. From the Cisco Unified Communications Manager Group drop-down list, choose **Single Server**.
3. From the Date/Time Group drop-down list, choose **US Central Daylight**.
4. From the Region drop-down list, choose **Chicago Region**.
5. From the Location drop-down list, choose **Chicago Location**.
6. Click the **Save** button.
7. In the Related Links drop-down list, select **Back to Find/List** and click the **Go** button to see the new device pools. See Figure 9-33 for an example of this page.

Figure 9-33 Device Pools



Task 7: Phone Button Templates

The previous items for the device pools impact not just phones but also other devices such as gateways, voicemail ports, conference bridges, and so on. The next few items will only impact phones. Phone button templates help standardize the use of the line buttons on the phones. In Lab 9-2, the autoregistered phones had two line buttons, and the remaining buttons were assigned to be user speed dials. By creating a phone button template for the phone, the line buttons can be preconfigured for the necessary functions. Line buttons are not limited to just lines and speed dials. They can be programmed to do many of the same functions as the softkeys, such as call park, hold, transfer, do not disturb, and so on.

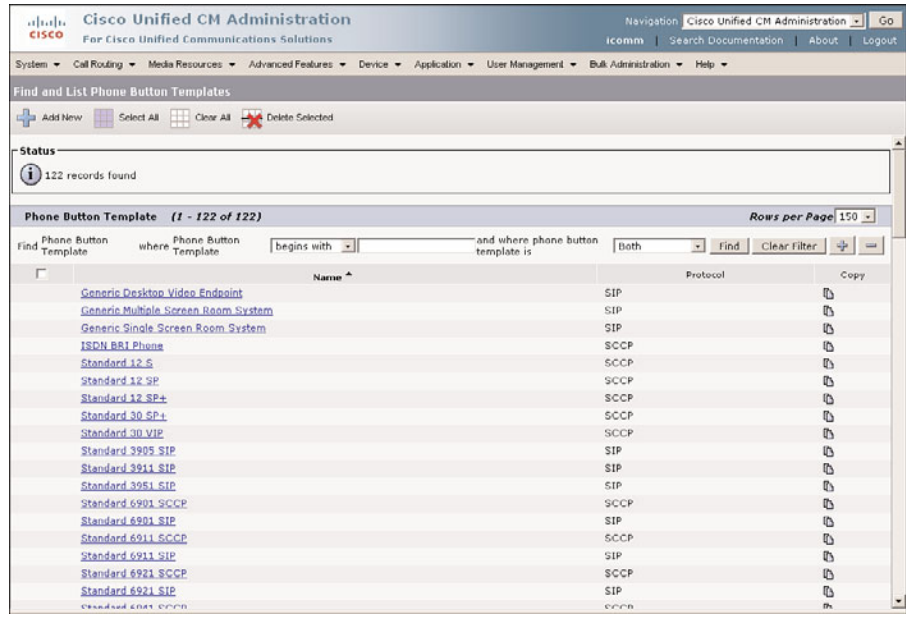
Step 7-1: Create Phone Button Template

On the **Cisco Unified CM Administration** page, navigate to **Device > Device Settings > Phone Button Template** and click the **Find** button if no templates are listed. By default, there are templates for every model of phone (and some have two per phone, one each for the SCCP and SIP signaling protocols) so that manual and autoregistration can function with minimal setup. Unlike the previous List/Find pages, this one has so many items they do not all show on the page. See Figure 9-34 for an example of this page.

https://t.me/learningnets

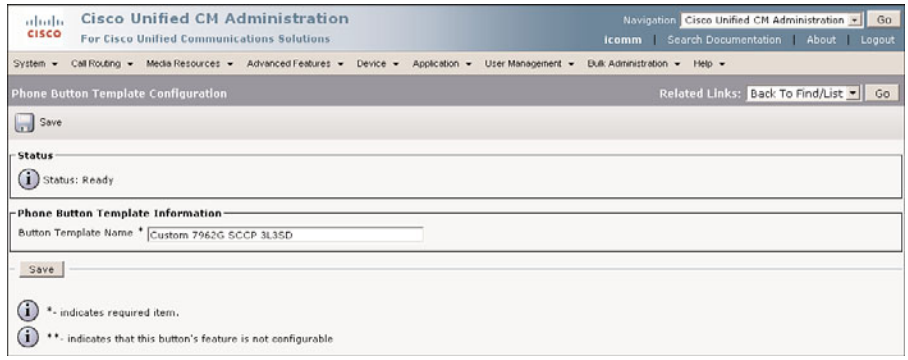
From the Library of Aliwarman Tarihoran

Figure 9-34 Find and List Phone Button Templates



1. The top of the list shows that 1 to 50 of 122 items are showing. On the right side, from the Rows Per Page drop-down list, select **150** to see all the items on one page.
2. This action will vary, depending on the phone model you have. A Cisco 7962 desk phone is demonstrated; adjust to match your model. Click the **Add New** button. Because the default templates cannot be modified, it is necessary to copy an existing template to make changes. From the Phone Button Template drop-down list, select the phone model and make sure that you get the SCCP or SIP selection correct. (Note: If using the Cisco IP Communicator, the default template is called Standard CIPC.) Click the **Copy** button.
3. Since there could be more than one custom template for this phone model, it is a good idea to indicate the unique functions in the template name. This will make it easier to select the correct template when configuring a phone later. For example, 3L3SD would indicate three lines and three speed dials, while 3L1int2SD could be three lines, one intercom, and two speed dials. For this lab, replace the button template name with **Custom *XXXX YYYY* 3L3SD**, where *XXXX* is the model number and *YYYY* is the protocol. See Figure 9-35 for an example of this page.
4. Click the **Save** button.

Figure 9-35 Phone Button Template Name



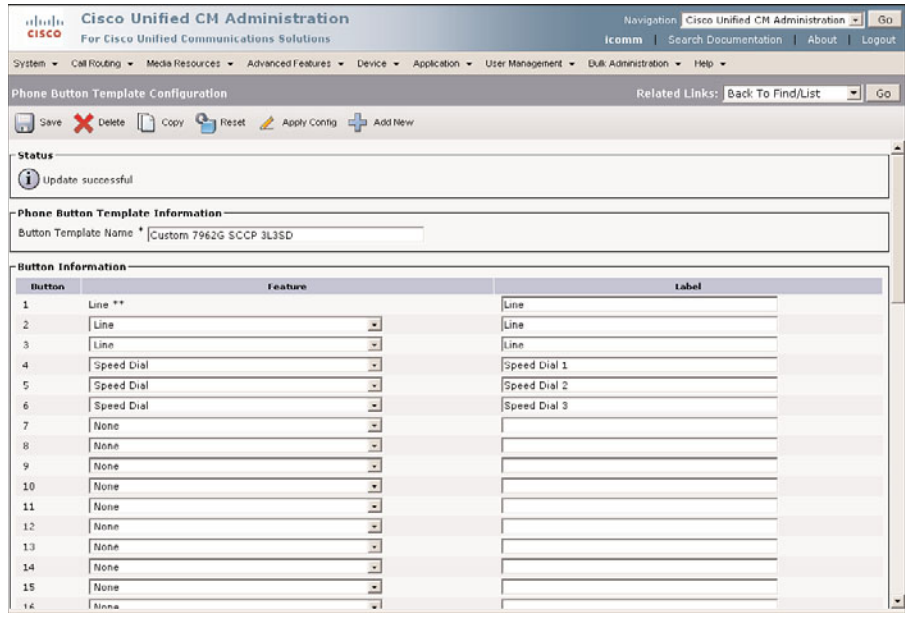
https://t.me/learningnets
From the Library of Aliwarman Tarihoran

Step 7-2: Modify Phone Button Template

The first thing you might notice is that the first line button cannot be changed, as it always needs to have a line assigned. The second thing to notice is that some models (such as the 7962) only have six buttons, but the template has 54 buttons listed! Be aware that some models support the 7914, 7915, or 7916 expansion modules, which would allow up to 48 additional buttons, which the template accommodates.

Use the Feature drop-down list for Button 3 to change from **Speed Dial** to **Line**. The label will automatically change from Speed Dial 1 to Line. You can change the numbers on the speed dial labels to reflect that speed dial 1 was just changed so that they do not start with Speed Dial 2. See Figure 9-36 for an example of this page.

Figure 9-36 Custom 7962 Phone Button Template



Click the **Save** button.

Repeat this task if you have other models of phones. For example, if you have the Cisco IP Communicator, configure four lines and four speed dials. The template should look like Figure 9-37.

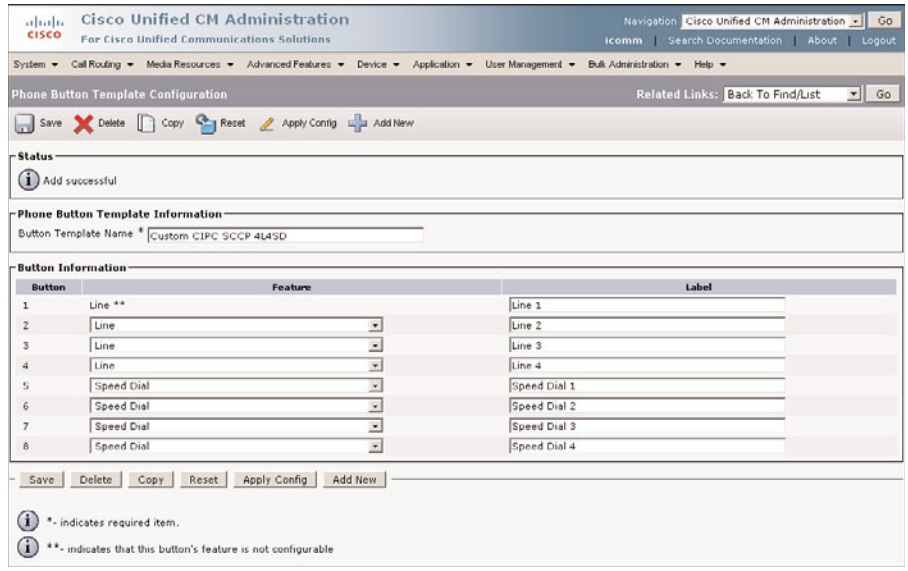
Note: In production, you might not have more than one line assigned to a phone, but for this lab, if possible, create a template for each of your phone models to support three or more line buttons. This makes it easier to test some functionality in later labs without needing as many phones. For example, you can place three calls between Phones A and B by using the first line button and placing the call on hold on both phones. Then, make another call using the second line buttons and place that on hold, while using the third line buttons for yet another call.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-37 Custom CIPC Phone Button Template



Task 8: Softkey Templates

Softkeys are the buttons below the display on phones that allow you to select common functions, such as call park, hold, transfer, do not disturb, and so on. The function of a button can vary depending on the state of the phone: on-hook, dialing, ringing, and so on. For many office users, the standard softkey functions might work just fine, but for other phones, it might be important to have a different set of functions. For example, phones at the registers in retail locations, lobby phones, and common break areas might not need to have some functions on the phones, such as Call Forward and Conference. Creating custom softkey templates allows the company to control exactly what functions a phone can perform.

Step 8-1: Create Softkey Template

On the **Cisco Unified CM Administration** page, navigate to **Device > Device Settings > Softkey Template** and click the **Find** button if no templates are listed. By default, there are seven templates for various job classifications. The default templates cannot be changed or deleted, so a new template based on one of the defaults needs to be created. See Figure 9-38 for an example of this page.

1. To create a phone that can be used in a common area, SOI wants a template that does not have all the functions available. To set up a new template, click the **Add New** button.
2. From the Create a Softkey Template Based On drop-down list, select **Standard User** and click the **Copy** button.
3. Enter **Restricted User** in the Name field.
4. Change the Description field to **Restricted Softkey Template**. Click the **Save** button. See Figure 9-39 for an example of this page.
5. This is one of the points in CUCM where the Related Links drop-down list is necessary, as it is the way to get to the layout options for the new template. With the Related Links set to **Configure Softkey Layout**, click the **Go** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-38 Softkey Templates

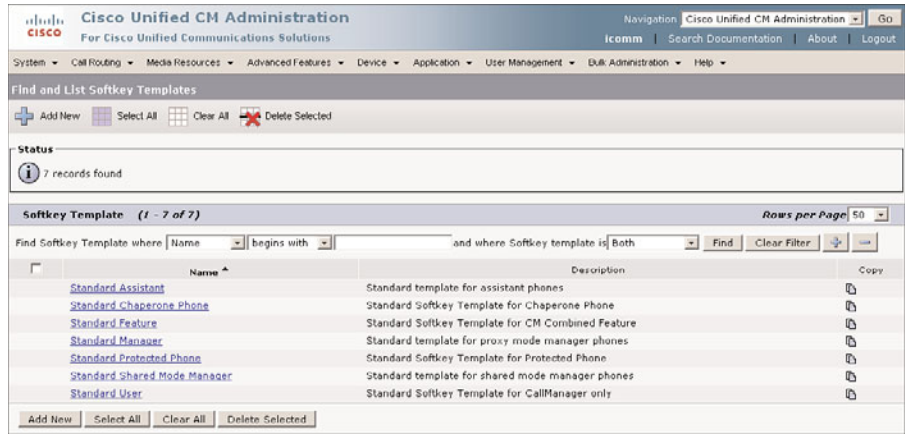
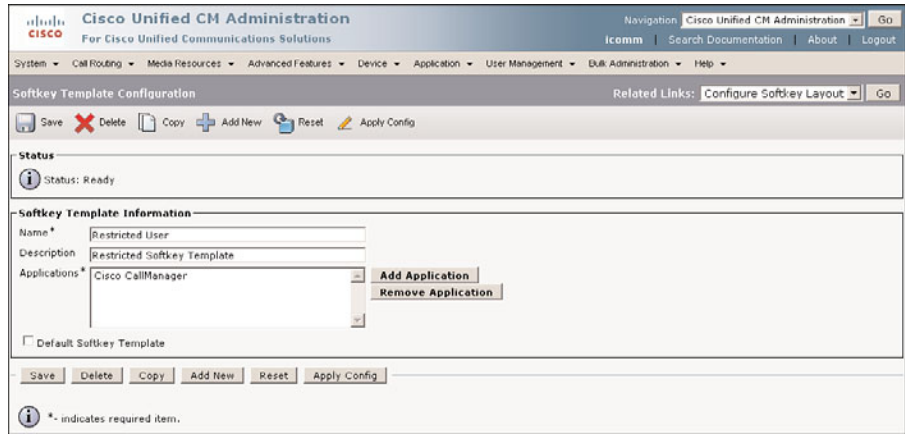


Figure 9-39 Restricted User Softkey Template



Step 8-2: Modify Softkey Template

In the middle of the page is the Select a Call State to Configure drop-down list, which shows every possible call state. Below this are the Unselected Softkeys and Selected Softkeys boxes with the functions available for the selected call state.

Note: The Undefined softkey will create a blank space to position softkeys on the phone display. It is helpful for phone users to have a function (for example, End Call) on the same softkey in all the call states. The Undefined softkey is used for exactly this purpose in the Connected Transfer call state to make the End Call function show on the second softkey, to be compatible with all the other states that use the End Call softkey, such as Connected, Off Hook, and Ring Out.

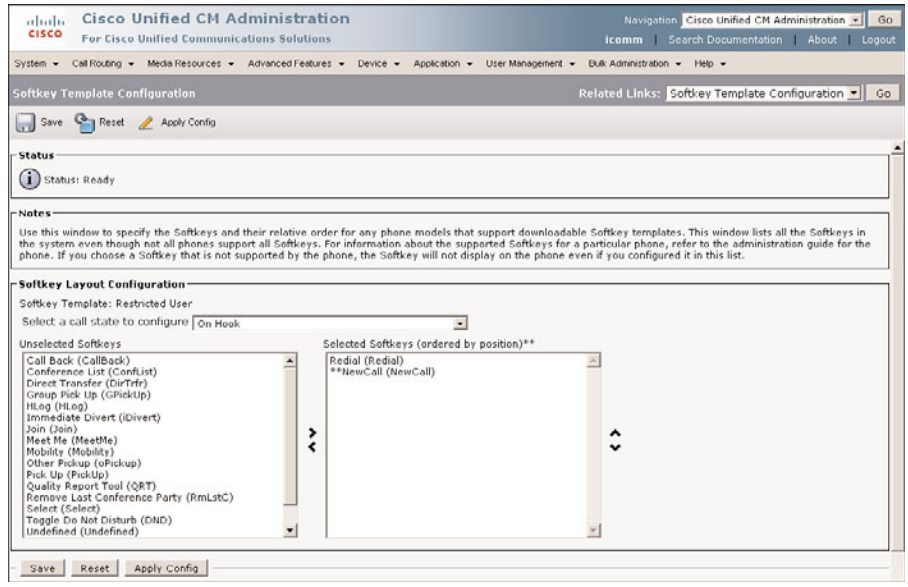
1. With the Select a Call State to Configure drop-down list set to **On Hook**, click the **Forward All (CFwdAll)** item in the Selected Softkeys box, and then click the left-facing arrow between the two lists to move the item to the Unselected Softkeys list. This leaves just the **Redial**

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

(Redial) and **NewCall (NewCall)** functions when the phone is on-hook. See Figure 9-40 for an example of this page.

Figure 9-40 Restricted User On-Hook Softkeys



2. Click the **Save** button.

Note: It is necessary to click **Save** before changing to a different call state, or any changes made to the current call state will be lost.

---

3. From the Select a Call State to Configure drop-down list, select **Connected**. Use the same process to move the **Transfer (Trnsfer)**, **Conference (Confrn)**, **Conference List (ConfList), Select (Select), Join (Join)**, **Direct Transfer (DirTrfr)**, and **Video Mode Command (VidMode)** softkeys by clicking the left-facing arrow between the two lists to move the items to the Unselected Softkeys list. (Note that the Ctrl key can be used to select more than one item at a time.) The only items remaining in the Connected call state should be **Hold (Hold)**, **End Call (EndCall)**, and **Park (Park)**. Click the **Save** button.

4. Use the Select a Call State to Configure drop-down list to select **On Hold**. Move the **Direct Transfer (DirTrfr)**, **Select (Select)**, and **Join (Join)** softkeys to the Unselected Softkeys list. The only items remaining in the On Hold call state should be **Resume (Resume)** and **New Call (NewCall)**. Click the **Save** button.

5. Use the Select a Call State to Configure drop-down list to select **Off Hook**. Move the **Forward All (CFwdAll)**, **Pick Up (Pickup)**, **Group Pick Up (GPickup)**, and **Meet Me (MeetMe)** softkeys to the Unselected Softkeys list. The only items remaining in the Off Hook call state should be **Redial (Redial)** and **End Call (NewCall)**. Click the **Save** button.

6. Use the Select a Call State to Configure drop-down list to select **Remote In Use**. Move all the softkeys to the Unselected Softkeys list. There should be no items remaining in the Selected Softkeys box. Click the **Save** button.

https://t.me/learningnets

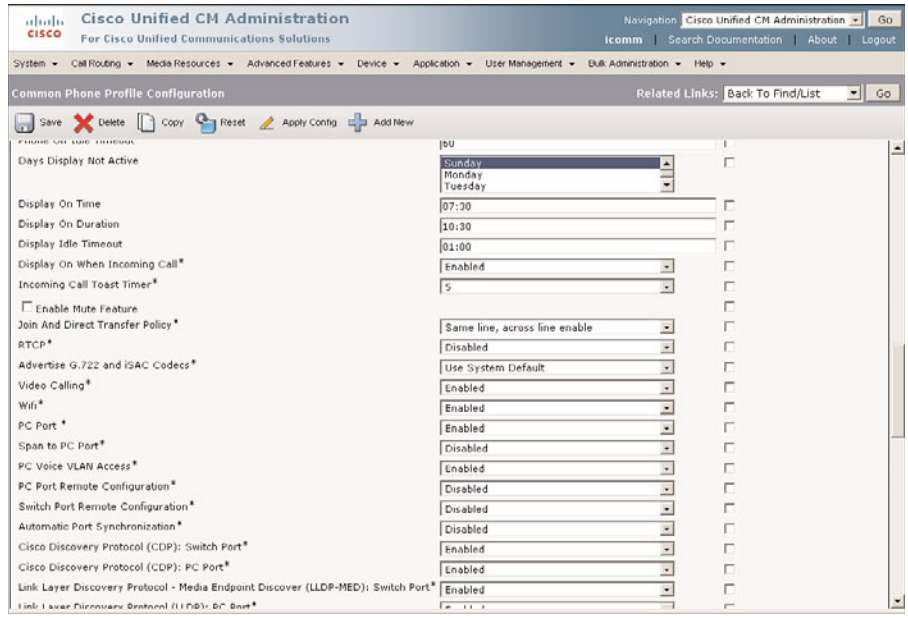
From the Library of Aliwarman Tarihoran

Task 9: Common Phone Profile

Common phone profiles are mainly concerned with the hardware settings on the phone. For example, phones with color displays have backlighting that uses power to light up the display. To reduce energy consumption, the phones turn off the backlighting if they are inactive for a period of time, after hours, or on the weekend. This power-saving behavior can be configured as part of the standard common phone profile (or a custom profile).

On the **Cisco Unified CM Administration** page, navigate to **Device > Device Settings > Common Phone Profile** and click the **Find** button if no templates are listed. By default, there is a standard template, and it can be modified but cannot be deleted. Click the **Standard Common Phone Profile** to see the details. For this task, just look at the various settings, as there will be no changes made. To see the display power settings (for phones with backlit screens), scroll down to the Product Specific Configuration Layout and the Display On Time. Notice that the system will keep the display on from 7:30 a.m. for 10-1/2 hours (until 6 p.m.). See Figure 9-41 for an example of this page.

Figure 9-41 Common Phone Profile Configuration



Task 10: Device Defaults

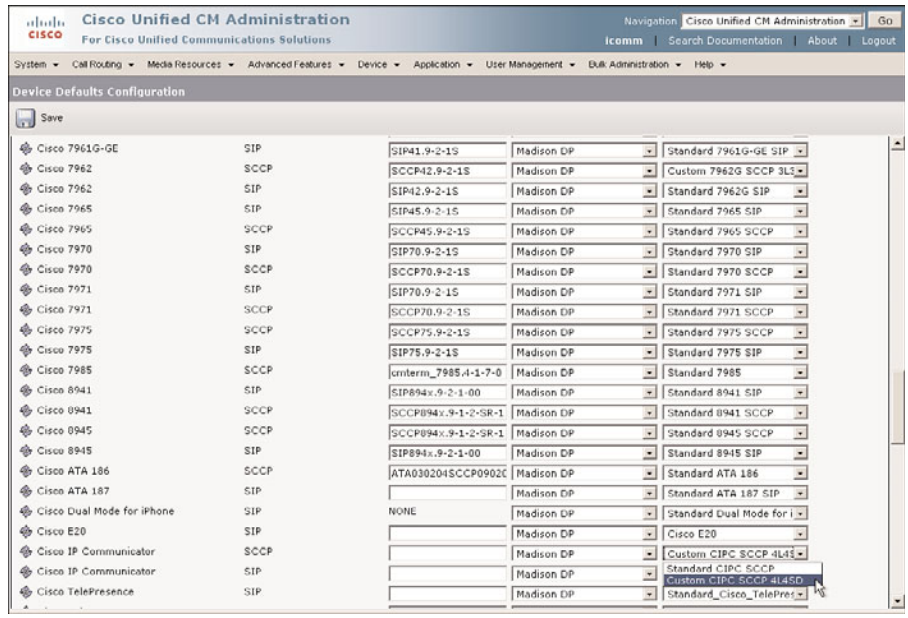
Device defaults impact the settings used for phones that are autoimported. The device defaults determine the firmware the phones get, the device pool they will register to, and the phone button template to use. The settings are customizable by phone model and protocol, so it is possible for a 7962 phone using SIP to register to a different device pool than a 7962 phone using SCCP.

On the **Cisco Unified CM Administration** page, navigate to **Device > Device Settings > Device Defaults**. (This is one of the few pages where you do not need to click a **Find** button to see the entries!) Scroll down to find the phone models for which you created custom phone button templates, and from the Phone Template column, use the drop-down list to select the custom template for that phone. Make sure that you get the desired protocol (SCCP or SIP) for the phone model! Figure 9-42 shows an example of a 7962 using SCCP and a Cisco IP Communicator using SCCP, with custom phone templates.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-42 Device Defaults Configuration



Notice that by renaming the default device pool to **Madison DP**, all phones will autoregister to the Madison DP by default and get the various settings configured.

Click the **Save** button.

Task 11: Testing

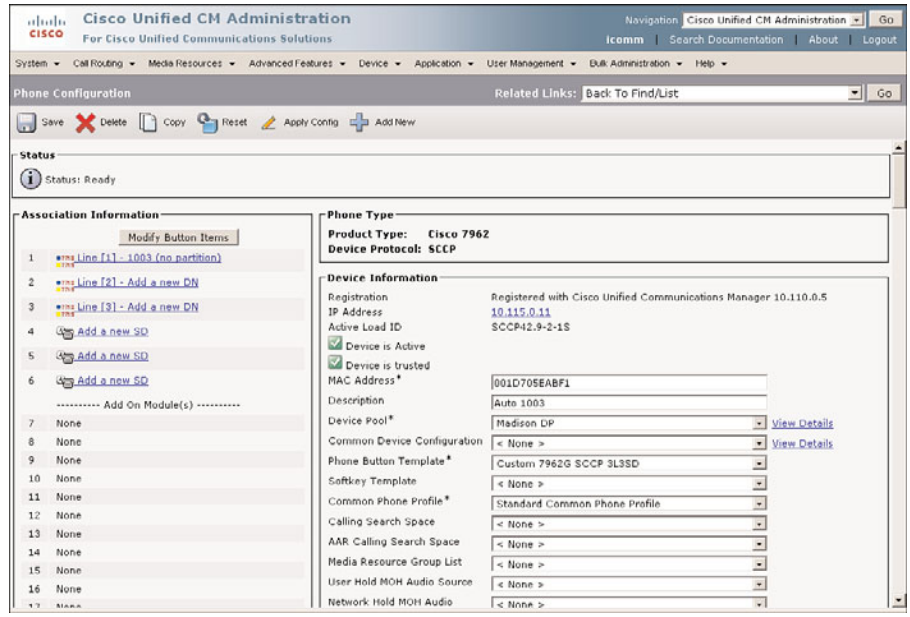
1. Use the instructions in Lab 9-3, Step 2-2 to reenable autoregistration. (As noted in Lab 9-3, Step 4-1, the previous phone numbers are still in the system and will not be handed out again, so increase the ending directory number to a higher number than previously used in Lab 9-3.)
2. Connect two phones that have the custom phone button templates configured and let them autoregister. (It might be necessary to reset the network settings on the phones to get them to clear the previous setting and register. See the hardware section of the Introduction for more information.) From the phones, there will be no obvious changes, other than the new directory numbers. Each phone will still have only one directory number assigned. However, if you examine the details of the phone, you will see the number of line buttons correctly assigned, as designated in the template, but only one of them has a directory number.
3. On the **Cisco Unified CM Administration** page, navigate to **Device > Phone** and click **Find**. Listed here are all the phones registered in the system.
4. Click the hyperlinked device name (SEP and the MAC address) of a phone. The Phone Configuration page opens, where you see the fields configured for phones. On the left side, the increased number of line buttons will be assigned. See Figure 9-43 for an example of this page.

Note: If you scroll down to the Location item under the Device Information section on the right side of the page, you will notice it is showing Hub_None, instead of the Madison Location that was set in the device pool. The location is a required parameter, so the Hub_None location is assigned by default, but the Device Pool location setting will override Hub_None on the phone; thus the Madison Location is active for the phone. However, if any other location is assigned directly on this phone, it will override the Device Pool setting.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-43 Phone Configuration After Device Pool and Phone Button Template



Task 12: Cleanup

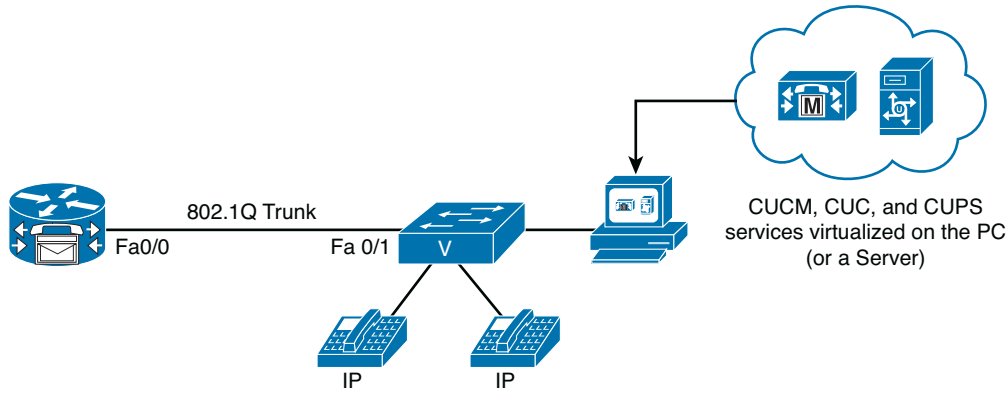
Use the instructions in Lab 9-3, Steps 4-1 and 4-2 to disable autoregistration and remove all phones.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 9-5: Registering Phones Manually

Figure 9-44 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- CUCM Server or PC with VMware Workstation installed and a VM of CUCM
- Two or more IP Phones (desk phone or soft phone on PC or Windows VM)
- Lab configuration from Lab 9-4

Learning Objective

Upon completion of this lab, you will be able to register phones manually.

Scenario

SOI is adding two phones, each with three directory numbers. While using autoregistration, as shown in Labs 9-3 and 9-4, would import the phones, there are enough other options to configure after the autoregistration that manually registering a phone can be faster. If SOI needed more than a dozen or so phones registered at a time, the Bulk Automation Tool (BAT) (covered in Lab 9-6) is the best solution.

Task 1: Manually Register a Phone

Step 1-1: Manually Add a Phone

On the **Cisco Unified CM Administration** page, navigate to **Device > Phone** and click **Find**. There should be no phones listed at this time.

1. Click the **Add New** button and the Add a New Phone page opens. From the Phone Type drop-down list, select the model of your phone and click the **Next** button. A Cisco 7962 desk phone is demonstrated; adjust to match your model.
2. From the Select the Device Protocol drop-down list, select either **SCCP** or **SIP** to match the protocol used on your phone and click the **Next** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. The Phone Configuration page now shows the items to register the phone. The MAC address is one of the required fields. There are three main ways to get the MAC address of a phone:
   - **From the box of the IP Phone:** The outside of the box has both the printed MAC address and a bar code. The bar code makes it easier to scan and enter related information (such as extension and username) for bulk importing.
   - **From the back of the IP Phone:** (Soft phones use "SEP" in front of the MAC address of the PC.) Turn the phone over and find the bar code with 12 hex digits. This method also benefits from using a bar-code scanner to capture the MAC address for bulk import.
   - **From the screen of the IP Phone:** Press the Settings button and then navigate to Model Information to show the MAC address. (The disadvantage of this option is that it requires the phone to be powered on.)
4. Enter the MAC address of the phone into the MAC Address field. (For Cisco IP Communicator phones, instead of the MAC Address field, the field is called Device Name.) The MAC address is entered without any separators such as periods or hyphens. (The Cisco IP Communicator needs to have "SEP" in front of the MAC address before it will register. Thus, a soft phone on a PC with a MAC address of AAA.BBBB.CCCC would have a device name of SEPAAAABBBBCCCC.)
5. After the MAC address is entered, the Description field will automatically show SEP plus the MAC address. In a smaller business, this might be fine, but when you have hundreds of phones, finding the phone for an individual user could prove tedious. However, a suggestion to enter the user's last name, first name, and main extension on the phone in the Description field[1] makes it far easier to locate the phone, as the Find/List search box can be used to locate the phone associated with any user.
6. From the Device Pool drop-down list, select **Madison DP**.
7. Select the **Custom Phone Button Template** from the Phone Button Template drop-down list (custom templates should be near the top of the list).
8. For right now, leave the softkey template set to **< None >** and the Location set to **Hub_None**.

Note: The location is a required parameter, so the Hub_None location is assigned by default, but the Device Pool location setting will override Hub_None on the phone. However, if any other location is assigned directly on this phone, it will override the Device Pool setting.

---

9. Scroll down to the Protocol Specific Information section, and under the device security profile, select the **Standard Non-Secure Profile** for the phone model. (If you are using a phone with the SIP protocol, you will also need to select the **Standard SIP Profile** from the SIP Profile drop-down list.) See Figure 9-45 for an example of this page.
10. Click the **Save** button. A pop-up window will remind you to use the **Apply Config** button. Click **OK**.
11. The full phone configuration window will open showing the line buttons on the left side and the device information on the right side. See Figure 9-46 for an example of this page.

[1] Credit for the suggestion for the description field goes to Cisco Press author David Bateman from *Configuring Cisco Unified Communications Manager and Unity Connection*

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-45 Manual Phone Configuration

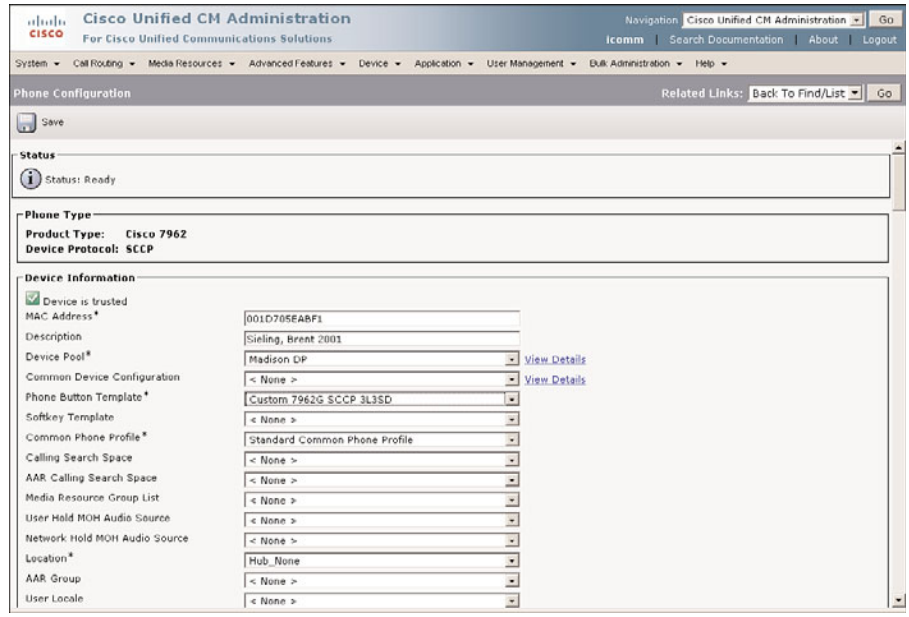
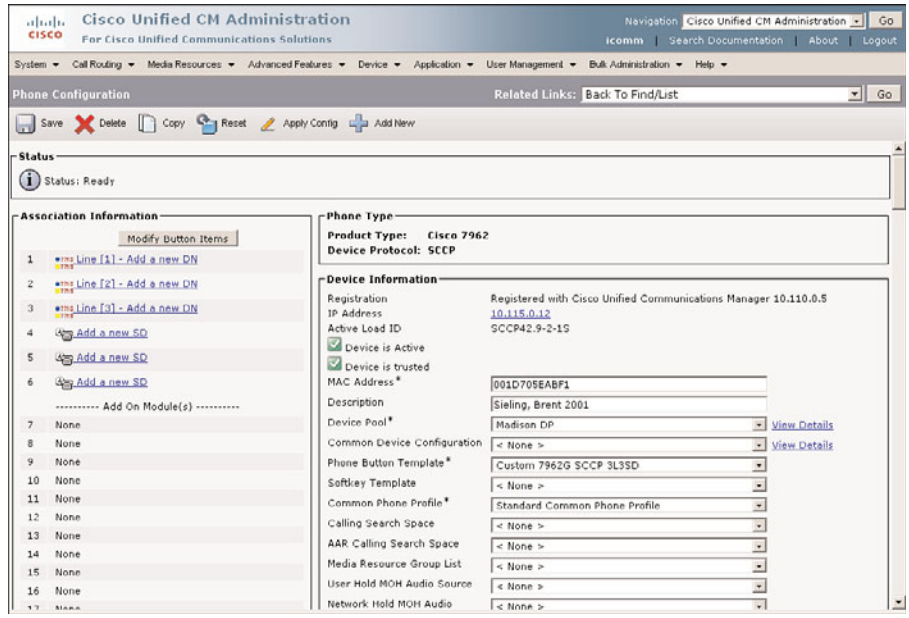


Figure 9-46 Manual Phone Configuration with Line Buttons



Step 1-2: Manually Add a Directory Number

Note: The design of a company's directory numbers involves many aspects, such as the use of Direct Inward Dialing (DID), the number of extensions needed now and expected in the future, the number of locations, and so on. For this lab, the goal is to just use four-digit extensions for directory numbers to keep it simple. CUCM also has many ways to manipulate both the calling party number and the number dialed by the user. Some of these digit manipulations will be covered in later labs.

https://t.me/learningnets

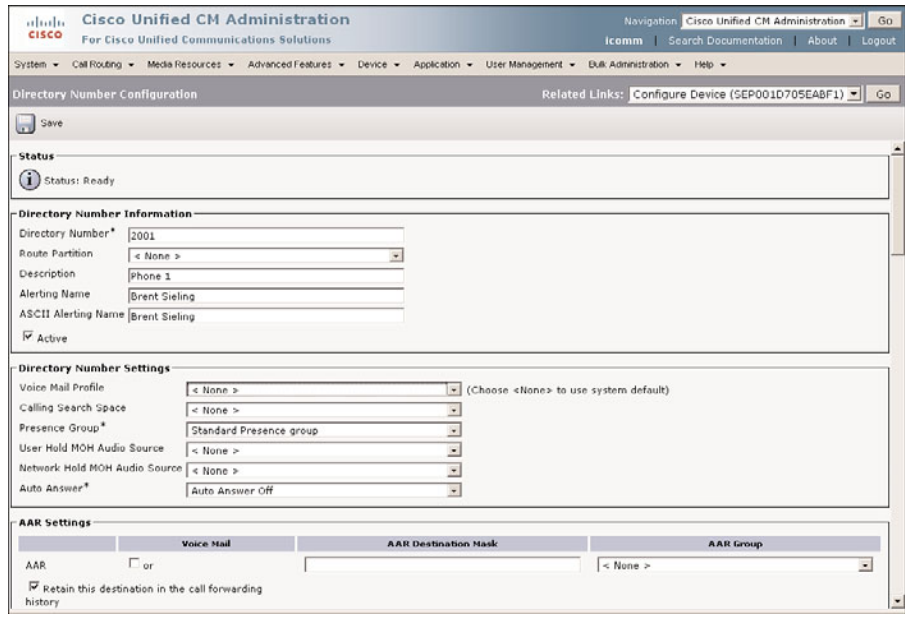
From the Library of Aliwarman Tarihoran

1. To assign directory numbers on the Phone Configuration page, click the **Line [*x*] – Add a New DN** hyperlink on the left, where *x* is the line number. The Directory Number Configuration page will open.
2. Use the CUCM Pod Phone Number Table in Appendix B to determine the correct extension number range to use. For the first HQ phone, pick the second extension in the range. (For example, the instructor range is 2000 to 2099, so 2001 is the first extension used.) Enter the extension in the Directory Number field.

Note: When you press **Tab** or click out of the Directory Number field, the page will refresh, and you will not be on the next field. You will need to click on the next field to select it.

3. Enter a description, such as **Phone 1**.
4. Enter the username of the line from the CUCM Pod Phone Number Table in Appendix B in the Alerting Name field. (For the first phone, use your own name.) The alerting name is what a phone that calls you displays while your phone is ringing. After you complete the Alerting Name field, the entry will automatically be copied to the ASCII Alerting Name field. See Figure 9-47 for an example of the top of this page.

Figure 9-47 Directory Number Configuration Part 1



Note: There are several options in the Directory Number Configuration window that will covered in later labs. For this lab, the goal is to get a simple configuration working.

5. Now scroll down to the Line *x* on Device *SEPmac_address* section, where *x* is the line number.
6. Enter the username of the line in the Display (Internal Caller ID) field. The Display field is what other phones see on their display when you call them (Caller ID for internal calls). After you complete the Display field, the entry will automatically be copied to the ASCII Display field.

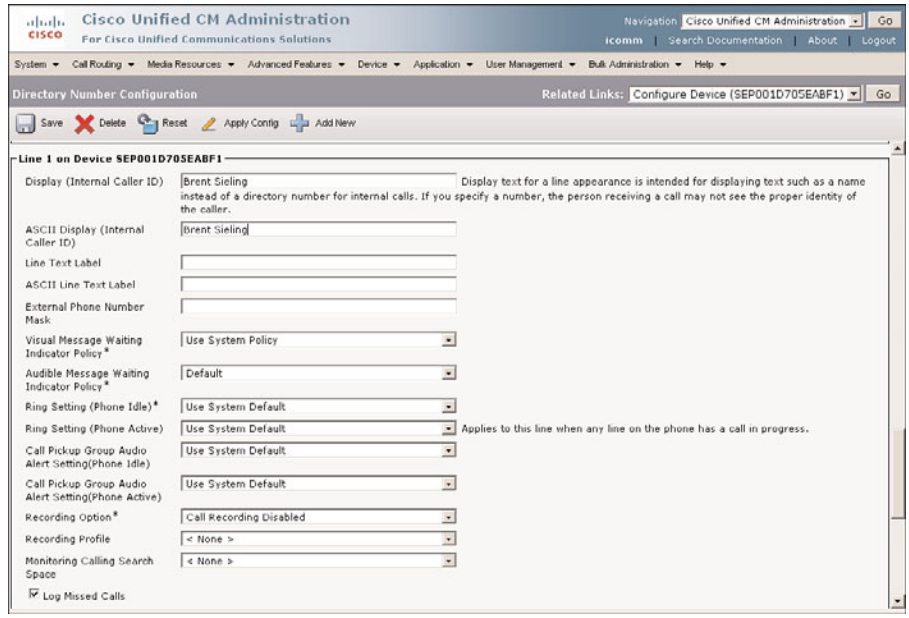
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

7. Leave the Line Text Label field blank for now. Any text entered here shows up next to the line button on the phone (same function as the Label command in CallManager Express).

8. Leave the External Phone Number Mask field blank for now. This field allows your internal extensions to be translated (for example to change the four-digit extension into full numbers the PSTN use), and it modifies the number that will show on the header bar of the phone display. Be aware that the mask values can be overridden in the CUCM call-routing steps configured in Chapter 10. See Figure 9-48 for an example of the second part of this page.

Figure 9-48 Directory Number Configuration Part 2



9. Click the **Save** button.

10. The Directory Number Configuration page will refresh, and now the Associated Devices box will show the MAC address of the phone or phones the directory number is assigned to.

11. In the Related Links drop-down list, with **Configure Device (SEP*mac_address*)** selected, click the **Go** button to return to the phone configuration page. The Line [*x*] should have the directory number assigned. If your phone has already registered, it should show the new number.

Step 1-3: Manually Add More Directory Numbers

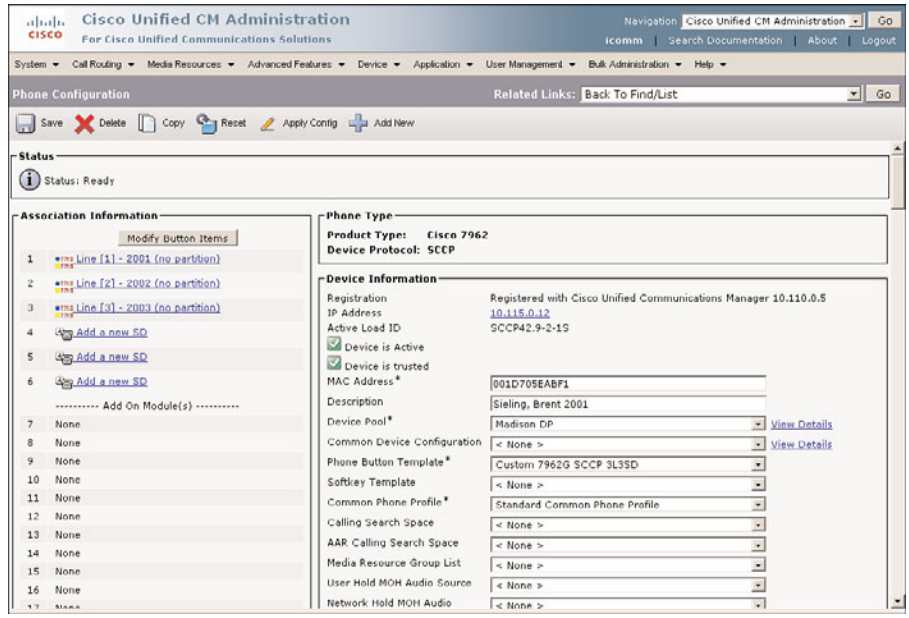
Repeat Step 1-2 to configure the remaining line buttons for this phone, incrementing the directory number by 1 for each, but use the same description and name for each of the lines on the phone. See Figure 9-49 for an example of this page after three directory numbers are added.

Note: For Cisco IP Communicator phones, instead of the MAC Address field, the field is called Device Name.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-49 Phone Configuration with All Directory Numbers Assigned



Task 2: Manually Register More Phones

1. Repeat Task 1 to add the rest of your phones manually. (These will be used in future labs.) Use the next available directory numbers for your pod to register all the phones you have. Ideally, you should have three or more phones each with three unique directory numbers (for a total of nine directory numbers used) configured at the end of this task.
2. To experiment with the difference between the Alerting Name and the Display fields, on the second phone's Line 2, leave the Alerting Name field (and the ASCII Alerting Name field) blank, and on the second phone's Line 3, leave the Display field (and the ASCII Display field) blank.
3. Then make phone calls from phone 1 to the extensions of all three lines on phone 2, and make calls from the extensions of all three lines on phone 2 to phone 1, to see the difference. You should notice the call from phone 1 to phone 2's line 2 does not show the name on phone 1's display. Likewise, when you call from phone 2's line 3 to phone 1, phone 1's display does not show the calling party name.
4. After you understand the difference between the Alerting Name and the Display fields, go back to the phones and add the missing name.
5. Make additional calls between phones. Pay special attention to the softkeys in the various states of making and receiving a call.

Task 3: Test Custom Softkey Templates

1. Back in Lab 9-4, Task 8, you created a restricted softkey template. Select one of your phones in the **Device > Phone** list and from the Phone Configuration page.
2. Change the softkey template to **Restricted User** and click the **Save** button.
3. Click **Apply Config** to make sure that the phone accepts the change.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. The first thing you should notice is that the CFwdAll button is no longer on the phone with the Restricted User template when on-hook. Place a call from another phone to the phone with the Restricted User template and notice the difference in the softkeys. Figure 9-50 shows an example (on the left) of a Cisco IP Communicator with the Standard User softkey template and (on the right) a Cisco IP Communicator with the Restricted User softkey template, while both are on a call. Notice that the Restricted User softkey template has fewer options. Also notice that the Park softkey has moved from the fourth softkey from the left to the third softkey.

Figure 9-50a Standard User Softkey Template

Figure 9-50b Restricted User Softkey Template

5. If the Park option was consistently expected on the fourth softkey spot, what softkey could be used to position it back where it was previously, while leaving the third softkey spot blank?

_____

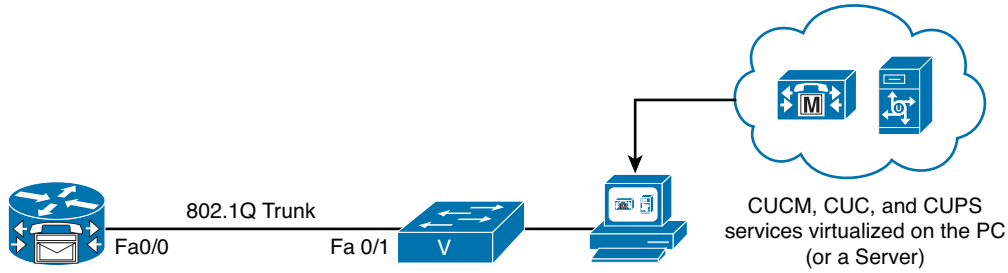
6. When you are done examining the differences in the Restricted User softkey template, go back to the phone page and change the Softkey Template field to **Standard User**. Make sure to click the **Save** and **Apply Config** buttons.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 9-6: Registering and Updating Phones Using the Bulk Administration Tool (BAT)

Figure 9-51 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- CUCM Server or PC with VMware Workstation installed and a VM of CUCM
- PC with Microsoft Excel installed
- (Optional) One or more IP Phones (desk phone or soft phone on PC or Windows VM)
- Configuration from Lab 9-4 completed, and preferably at least one phone still registered as shown in Lab 9-5

Learning Objectives

Upon completion of this lab, you will be able to

- Export phones using the Bulk Administration Tool (BAT)
- Add phones using BAT
- Modify existing phones using BAT

Scenario

SOI is going to add a large number of phones in the near future. The staff wants a more efficient way than auto or manual registration to add the phones. Additionally, they would like a way to modify the information for large numbers of previously registered phones. BAT is the answer!

Note: For this lab, you will import information for phones that don't actually exist using "dummy MAC addresses," so there is no need to delete the manually registered phones. You can import any model of phone (even one that you don't have), but you should select a model that you have created a custom button template for, as shown in Lab 9-4, Task 7.

When importing/updating phones using BAT, there are two components: the CSV (comma-separated value) data in a text file and a matching template in CUCM. The template takes each line of the data file and adds/updates each phone in much the same way that an assembly line die (the template) stamps out finished products from the material coming off a conveyer belt (the data).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Activate the BAT Service

From the Navigation drop-down list at the top of the page, choose **Cisco Unified Serviceability** and click the **Go** button.

1. On the **Cisco Unified Serviceability** page, navigate to **Tools > Service Activation**.
2. Select the check box for the **Cisco Bulk Provisioning Service** (leave the other check boxes as they are).
3. Click the **Save** button.
4. A window will inform you that activating the service will take a while. Click **OK** and wait for the page to refresh.
5. Verify that the service is now listed as Activated.

From the Navigation drop-down list at the top of the page, choose **Cisco Unified CM Administration** and click the **Go** button.

Task 2: Examine a Phone Export File

One of the main reasons to export phone data is to make changes and then reimport the changes into CUCM. However, for this task, you want to export already-registered phones (from Lab 9-5) to examine the output in order to better understand the BAT export process.

Step 2-1: Export Phone Configurations

On the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Phones > Export Phones > All Details**.

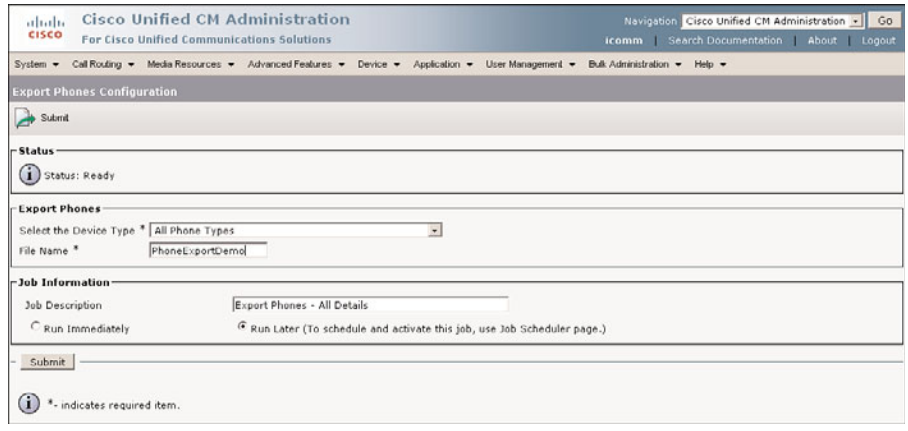
1. Enter **PhoneExportDemo** for the File Name field.
2. If the job is a large process that might impact the system, it is better to use the Run Later option and schedule the job to run during off-peak hours. To demonstrate how to schedule jobs, leave it set at **Run Later**. See Figure 9-52 for an example of this page.

Note: The filename cannot have spaces or special characters. Only alphanumeric, dash, underscore, and dot characters are allowed.

---

3. Click the **Submit** button to send the job to the job scheduler.

Figure 9-52 Export Phones Configuration



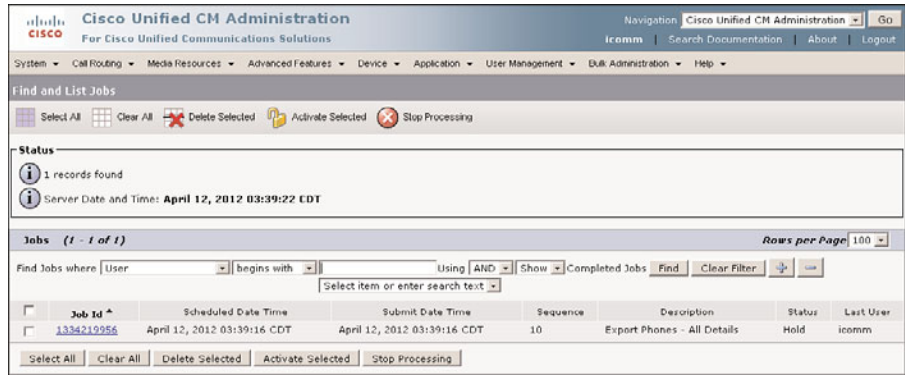
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-2: Job Scheduler

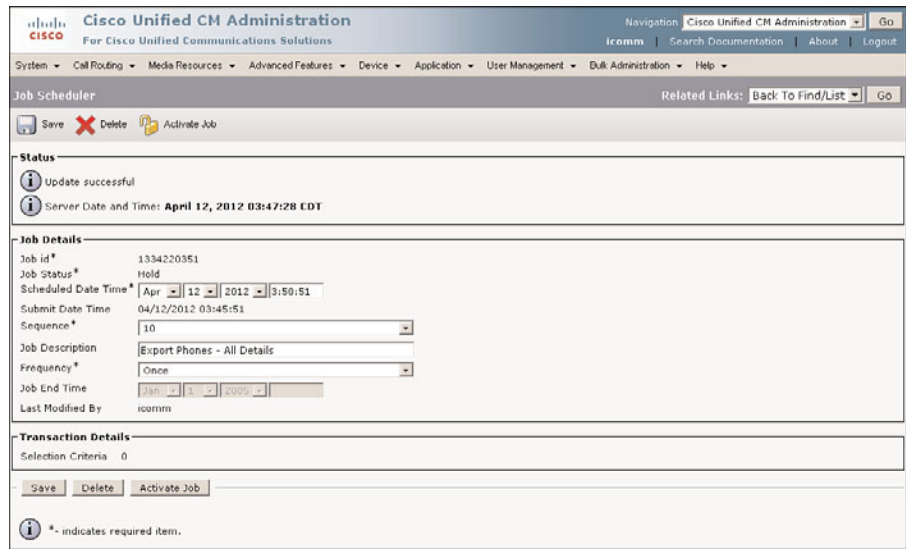
To schedule a job, or see the progress of it, on the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Job Scheduler** and click the **Find** button if your job does not show. See Figure 9-53 for an example of this page.

Figure 9-53 Find and List Jobs



1. The job will show a status of Hold, as it has not been scheduled.
2. Click the hyperlinked job ID name for your job.
3. The Job Scheduler page lists the job details. Change the Scheduled Date Time field so that it is a minute or two after the current time (see the Status section at the top) and click the **Save** button. See Figure 9-54 for an example of this page.

Figure 9-54 Job Scheduler



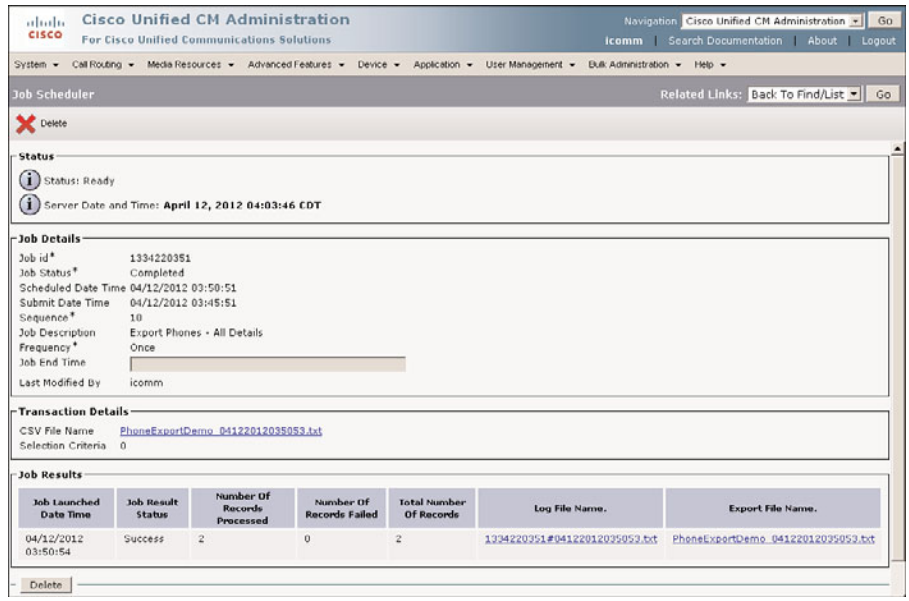
4. Click the **Activate Job** button and the page will return to the Find and List Jobs window, but the status should now be listed as Pending or Processing.
5. Click the **Find** button until the status changes from Pending or Processing to Completed.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

6. To verify that the job completed without any errors, check the job status by clicking the hyperlinked job ID number for your job. The Job Result Status should be Success. See Figure 9-55 for an example of this page.

Figure 9-55 Job Status



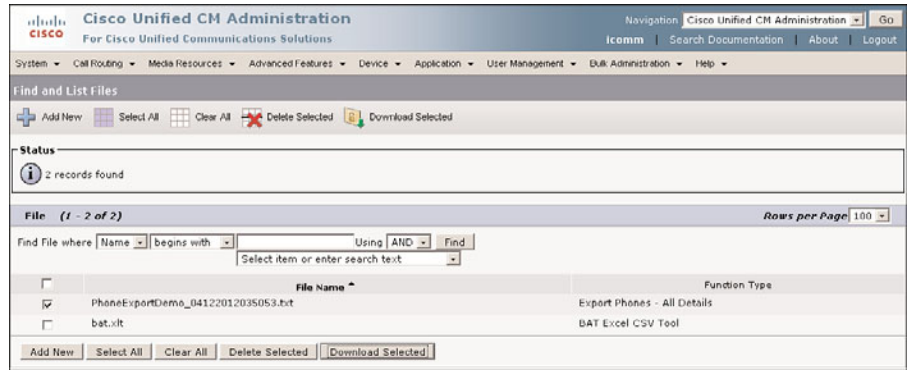
7. Click the hyperlinked log file name at the bottom to see the job processing details. The results should show that no errors were found.

Step 2-3: Download Files

To download the processed job, on the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Upload/Download Files** and click the **Find** button if no files show.

1. You should see the **PhoneExportDemo** file (which includes a date and time code).
2. Select the check box in front of the row with your job. See Figure 9-56 for an example of this page.

Figure 9-56 Find and List Files



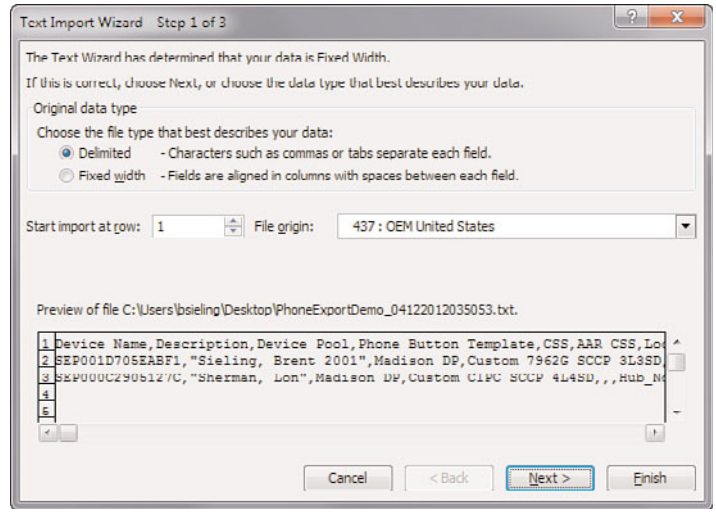
https://t.me/learningnets
From the Library of Aliwarman Tarihoran

3. Click the **Download Selected** button and the Open File dialog box opens.
4. Choose **Save File** and click **OK**.

Step 2-4: Open the Phone Export File in Microsoft Excel

1. Open Microsoft Excel.
2. Use the Open File command on the file that you downloaded. (Make sure to change the file list to see **All Files (*.*)** or you will not find the .txt file.)
3. The Text Import Wizard dialog box will open. Click the **Delimited** radio button. See Figure 9-57 for an example of this page.

Figure 9-57 Excel Text Import Wizard

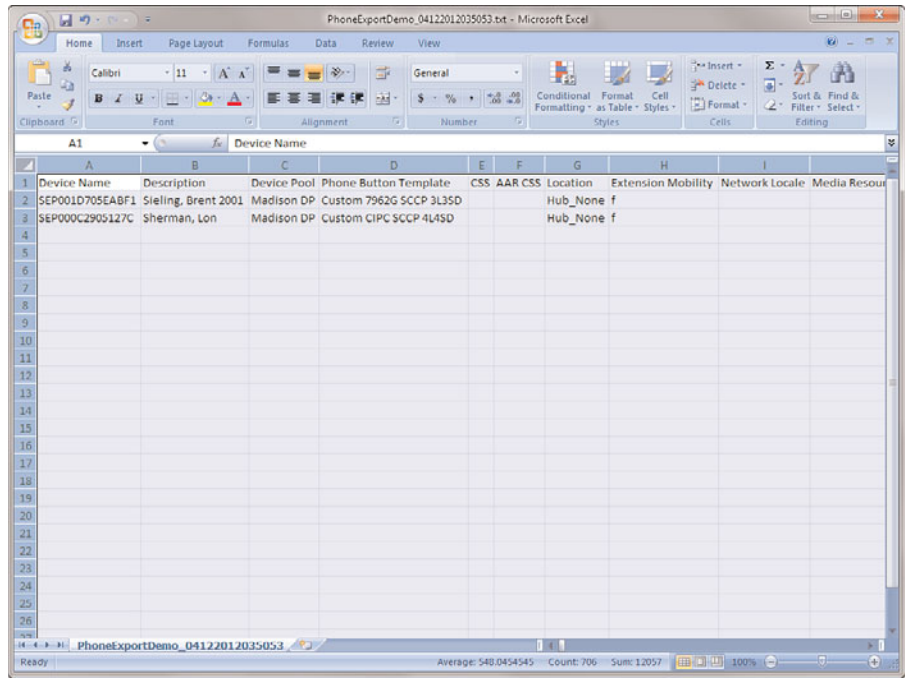


4. Click **Next**.
5. In Step 2 of the wizard, deselect the **Tab** check box and select the box for **Comma**; then click **Next**.
6. Click **Finish** to see the results.
7. Press **Ctrl+A** to select all cells, and on the ribbon Home tab, under Cells, click the **Format** item to select the **AutoFit Column Width** item from the pull-down menu. See Figure 9-58 for an example of this page.
8. Each row in the spreadsheet is associated with a phone. Each column holds a unique setting for the phones. As you scroll through all the columns, you see that there are a large number of them (with Excel, when the columns reach X, Y, and then Z, they continue with AA, AB, AC, and so on). The phone fields continue until at least column NL, which is a total of 376 columns! Clearly, if you had to fill out all this information before importing a phone, it would be a long, tedious process. However, CUCM includes a handy spreadsheet with macros to simplify the process of creating phones.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-58 Excel Phone Export



Task 3: Download BAT File to Import Phones

The bat.xlt file from CUCM will allow you to easily and quickly create a standardized data file that pairs with a template later on. It is important to understand that a separate data file/template pair is needed for each element: phone model, device pool, phone button template, and so on. For example, if you have two locations, with two models of phones at each, and one of the phone models needs half of the phones to be two-line button phones, and the other half to be three-line buttons, this will result in six different data file/template pairs (one pair for the two-line phones, one for the three-line phones, one for the other phone model, equals three pairs times two locations, so six different pairs). This might seem like more work than it is worth to set up, and for a small number of phones, that might be true, but when a job requires rolling out hundreds, if not thousands, of phones, BAT is the only practical method.

For this lab, you will be importing a single phone model into the Madison device pool, so only a single data file/template pair is needed.

Step 3-1: Using the BAT File

To download the bat.xlt file, on the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Upload/Download Files** and click the **Find** button if no files show.

1. Select the check box in the row with the bat.xlt file.
2. Click the **Download Selected** button and the Open File dialog box opens. Choose **Save File** and click **OK**.
3. Open Microsoft Excel and open the bat file you downloaded.

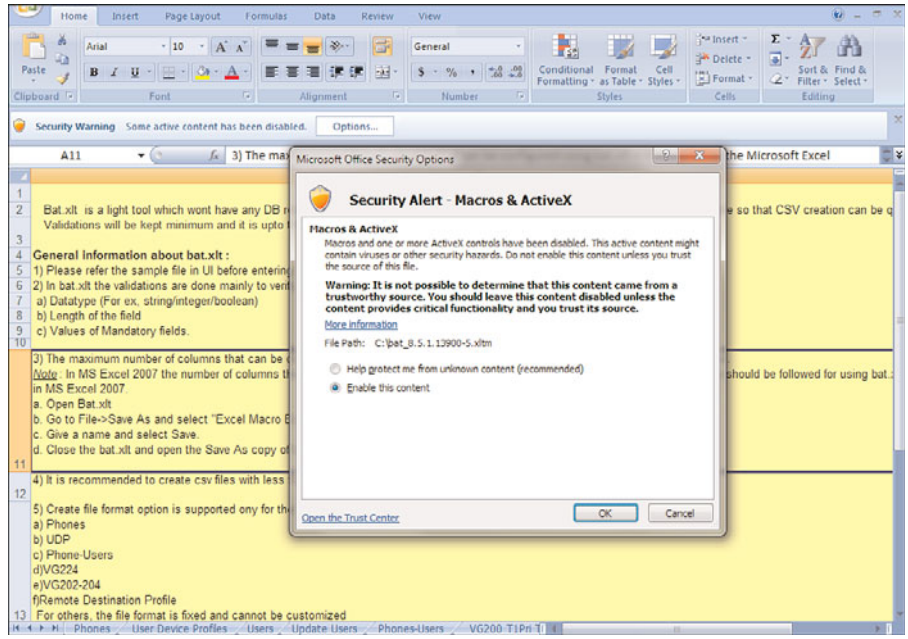
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. There are many different workbook tabs along the bottom of the spreadsheet. The first tab that opens displays the guidelines to use the bat file. Row 11 has directions if you are using Excel 2007.

5. Follow the directions if needed. After the file is saved as a macro-enabled workbook and reopened, a security warning will show under the ribbon regarding the macros included in the spreadsheet. Click the **Options** button and a pop-up window will open. Click the **Enable this content** radio button and click **OK**. See Figure 9-59 for an example of this page.

Figure 9-59 Excel Security Warning



6. It will be necessary to use the small tab navigation arrow in the lower-left corner of the window to scroll to the Phones worksheet tab.

7. Click the **Phones** worksheet tab at the bottom of the page. At first, it looks like there are only two fields for phones: MAC Address/Device Name and Description. This is where the macros come in.

8. Click the **Create File Format** button in the first row of the spreadsheet and a Field Selection window will open. The fields are divided into three categories: Device Fields, Line Fields, and Intercom Fields. This window allows you to modify the spreadsheet to include any of the various fields listed, thus customizing the file to only the information you need to import.

9. In the Line Fields section, scroll down to the **Directory Number** and click the double arrow (**>>**) button to move the field to the Selected Line Fields box. See Figure 9-60 for an example of this page.

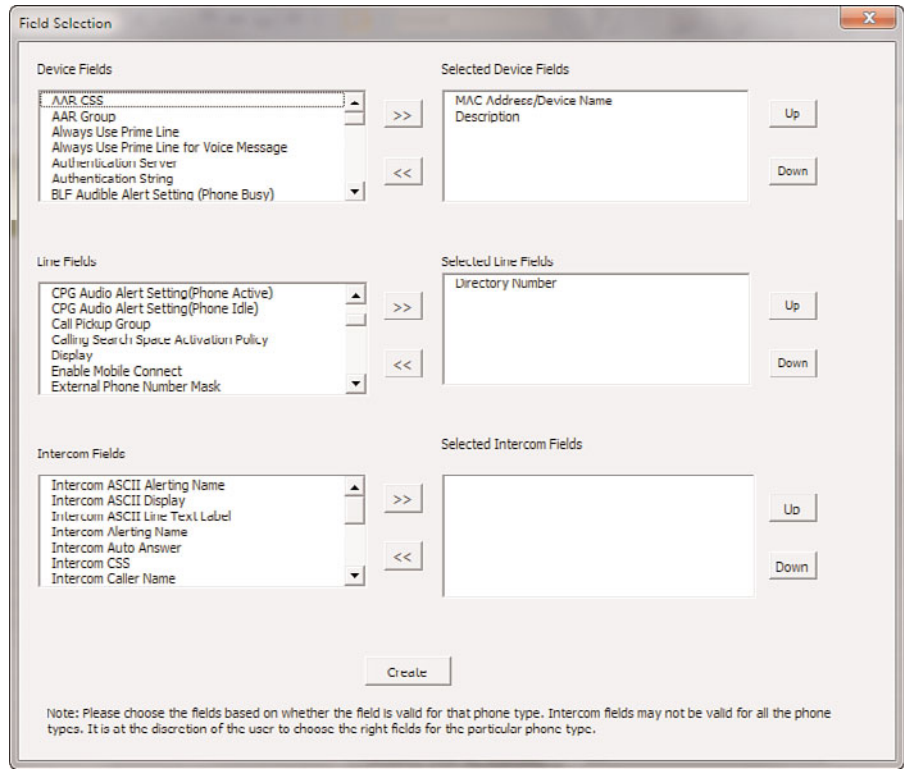
10. Click the **Create** button near the bottom of the window. An information dialog box will open asking whether you want to override the existing CSV format. Click **Yes**.

11. The spreadsheet will now have a new column for Directory Number 1. What if you want to assign more than one directory number? To the right is a column with a **Maximum Number of Phone Lines** box.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-60 Excel Field Selection



Note: Lab 9-4, Task 7 demonstrated creating a phone button template that supports three directory numbers. This lab will demonstrate using that custom button template, so if your template has fewer buttons (or more), adjust the number of directory numbers selected to match your custom phone template.

12. Enter **3** in the **Maximum Number of Phone Lines** box and then click outside of that column. The spreadsheet will automatically add extra columns to create the requested number of lines!

13. As mentioned at the start of the lab, you will be importing phones that don't actually exist, and you might think this is something you would never do outside a lab. However, importing phones with unknown MAC addresses is used in production systems in two cases: when the MAC address will be updated later manually or when using the Auto Register Phone Tool (TAPS), where the temporary MAC address is replaced with the correct one after the users follow the prompts of an Interactive Voice Response (IVR) server. As a result, leave the MAC Address/Device Name column empty, but select the **Dummy MAC Address** check box (right above the Maximum Number of Phone Lines box). This check box does not enter MAC addresses into the spreadsheet (the dummy addresses will be created on import to CUCM). Rather it tells the error-checking script to ignore the blank MAC address fields.

14. In the first row under the Description column, enter **BAT_Phone_Test1**. Excel has a handy feature: Grab and drag the little black box in the lower-right corner of the selected cell, and it will copy down and autoincrement the values for the selection. Click and hold before dragging down the first description cell to create four phone descriptions.

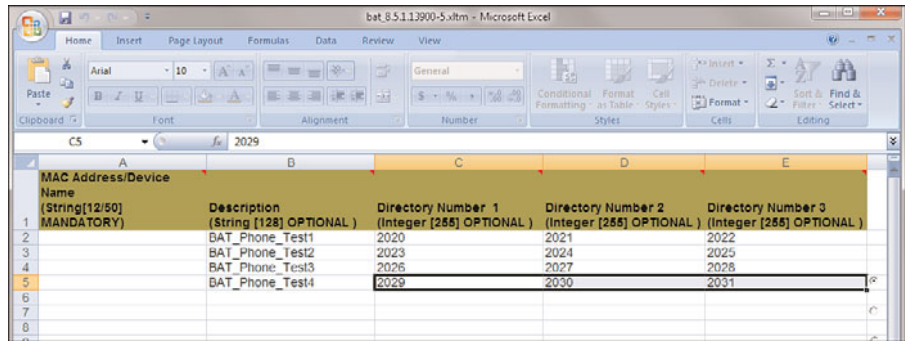
15. Use the CUCM Pod Phone Number Table in Appendix B and the last manually assigned directory in Lab 9-5 to determine the next directory numbers to use for the phones. The same Excel feature can also be used to autoincrement numbers when dragged to the right. Enter the next

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

available directory number in the first phone row, under Directory Number 1, and then drag the little black box to the right to have it automatically fill in numbers for the other columns. Repeat this step for the other three dummy phones. See Figure 9-61 for an example of this window.

Figure 9-61 Four-Phone Data Import Example



16. After all the data is entered, click the **Export to BAT Format** button (right above the Dummy MAC Address check box).

17. A dialog box will open to allow you to specify the path and to change the filename to **PhoneImport1** to save the new file. Click **OK**.

Note: The filename cannot have spaces or special characters. Only alphanumeric, dash, underscore, and dot characters are allowed.

Step 3-2: Upload the BAT Import File

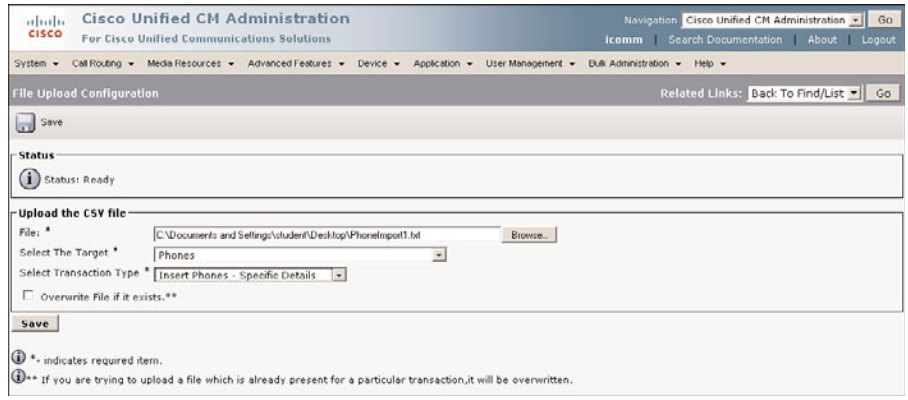
To upload the PhoneImport1.txt file, on the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Upload/Download Files** and click the **Find** button if no files show.

1. Click the **Add New** button and the File Upload Configuration window will show.
2. Click the **Browse** button at the end of the File field and the Open File dialog box opens.
3. Navigate to the location that you saved the PhoneImport1.txt file and click **OK**.
4. From the Select The Target drop-down list, select **Phones**.
5. From the Select Transaction Type drop-down list, select **Insert Phones – Specific Details**. See Figure 9-62 for an example of this page.
6. Click **Save** to have the file uploaded into the CUCM system.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-62 File Upload Configuration



Task 4: Create BAT Template

Now that the data file is created, it is time to create the matching template that will correctly parse the data file for importing.

Step 4-1: Create BAT Phone Template

On the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Phones > Phone Template**.

1. Click the **Add New** button to create a template. From this point, using the template is similar to manually creating a phone.
2. First the phone model needs to be selected. (You don't need to have the actual phone model for this step, but you do need to have a custom phone line button template to match the number of phone lines per phone created in the data file.) From the Phone Type drop-down list, select a model you created a custom phone button template for. This example will use the 7962 three-line phone template created in the Lab 9-4, Task 7 demonstration. Click **Next**.
3. From the Select the Device Protocol drop-down list, select the protocol for the selected phone (either **SCCP** or **SIP**). Click **Next**.
4. Give the Template Name field a useful entry that will help distinguish this template from other templates created in the future. For example, a template for a 7962 phone, using the Madison Device pool with a custom three-line, three-speed-dial button template could be called **Madison 7962 3L3SD**.
5. From the Device Pool drop-down list, select **Madison DP**.
6. Select the **Custom Phone Button Template** from the Phone Button Template drop-down list (custom templates should be near the top of the list).
7. From the Softkey Template drop-down list, select **Standard User**.
8. Leave the Location set to **Hub_None**.

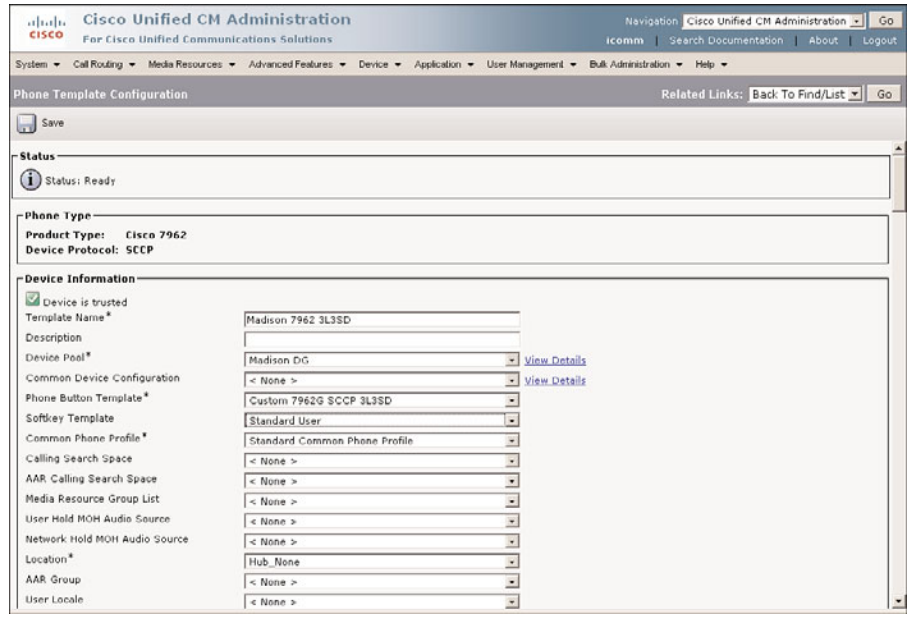
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Note: The location is a required parameter, so the Hub_None location is assigned by default, but the Device Pool location setting will override Hub_None on the phone. If any other location is assigned directly on the phone, however, it will override the Device Pool setting.

9. Scroll down to the Protocol Specific Information section, and under the Device Security Profile, select the **Standard Non-Secure Profile** for the phone model. See Figure 9-63 for an example of this page.

Figure 9-63 BAT Phone Template Configuration



10. Click **Save** to get to the next page.

Step 4-2: Add Lines to the BAT Phone Template

After the template is created, another step is needed before it can be used. Although the custom phone button template used in this example specified three lines, the BAT template still needs to be told that three lines will be found in the data file.

1. Click the **Line [1] – Add a New DN** link in the template. This will open the Line Template Configuration window.
2. Enter a name such as **Line 1** in the Line Template Name field. (At this point, there are no other settings you will be changing.) Press **Tab** to exit the field and the page will refresh. See Figure 9-64 for an example of this page.
3. Click **Save** to finalize the line template.
4. Click **Go** in the Related Links menu to return to the Template Configuration page.
5. Back on the Phone Template page, you can see that line 1 now has an assignment. Repeat this step to add line templates for **Line 2** and **Line 3** (assuming that you are using a three-line custom button template). See Figure 9-65 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-64 BAT Line Template Configuration

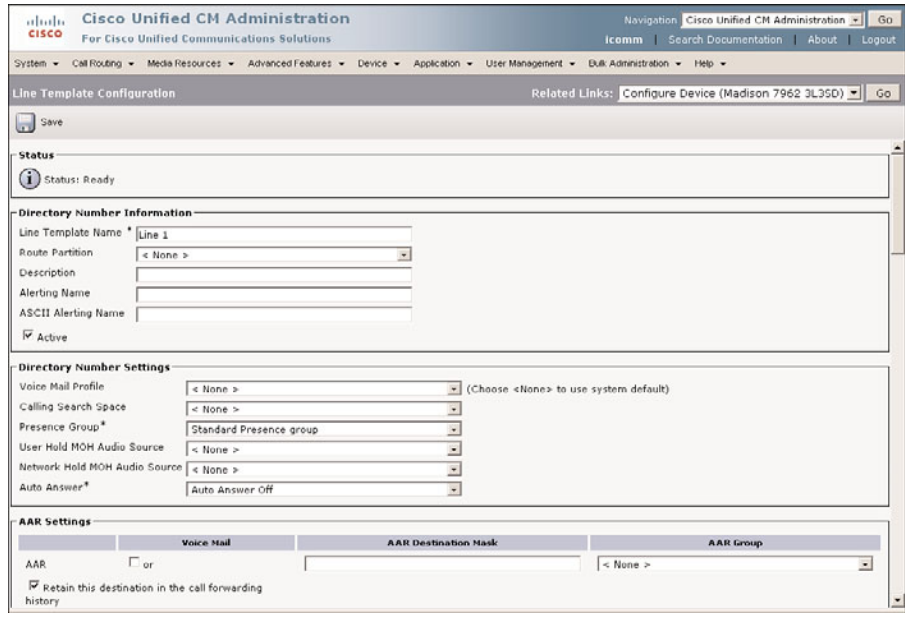
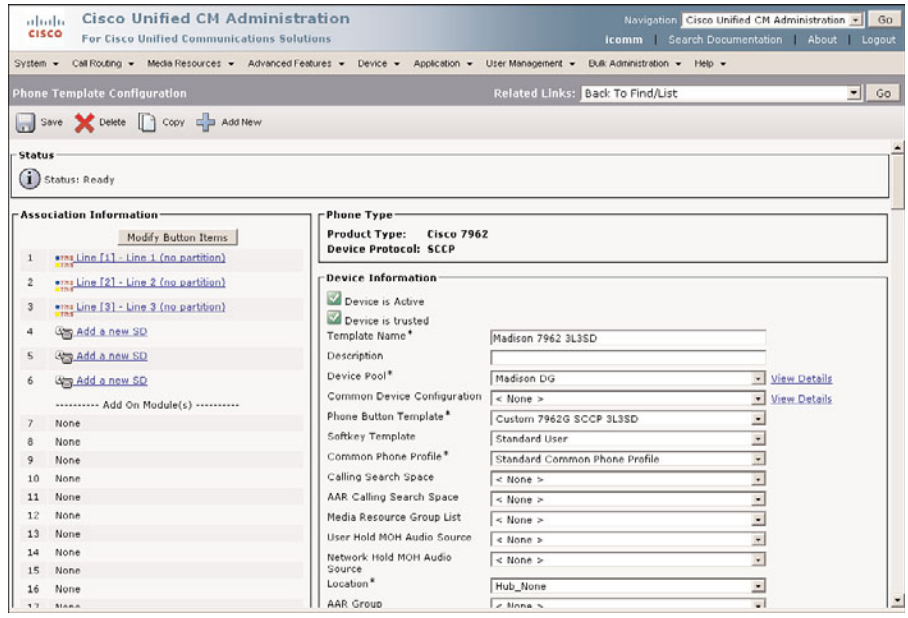


Figure 9-65 BAT Phone Template Configuration Complete



6. Click **Save**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

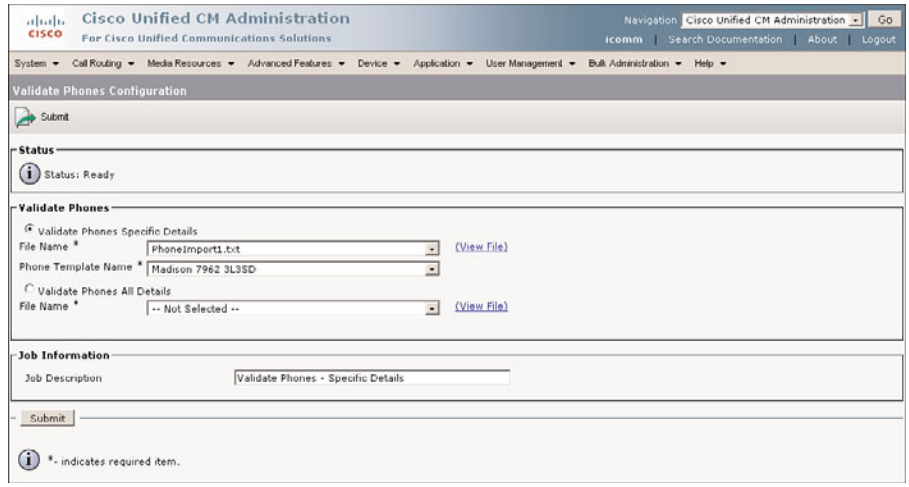
Task 5: Validate Data Import

CUCM includes a process to test for errors in the template and data file before they are actually imported. This is extremely useful. The last thing you would want in a system with thousands of phones is to have another few thousand phones imported when the import fails midway because of bad data, forcing you to sort out how far the import completed and fixing the file before you resubmit the part of the data file that did not complete.

On the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Phones > Validate Phones**.

1. Because you are only importing some details, leave the radio button selected on **Validate Phones Specific Details**.
2. From the File Name drop-down list, select the **PhoneImport1.txt** file.
3. From the Phone Template Name drop-down list, select the name of the template (**Madison 7962 3L3SD**, in this example). See Figure 9-66 for an example of this page.

Figure 9-66 BAT Validate Phones Configuration

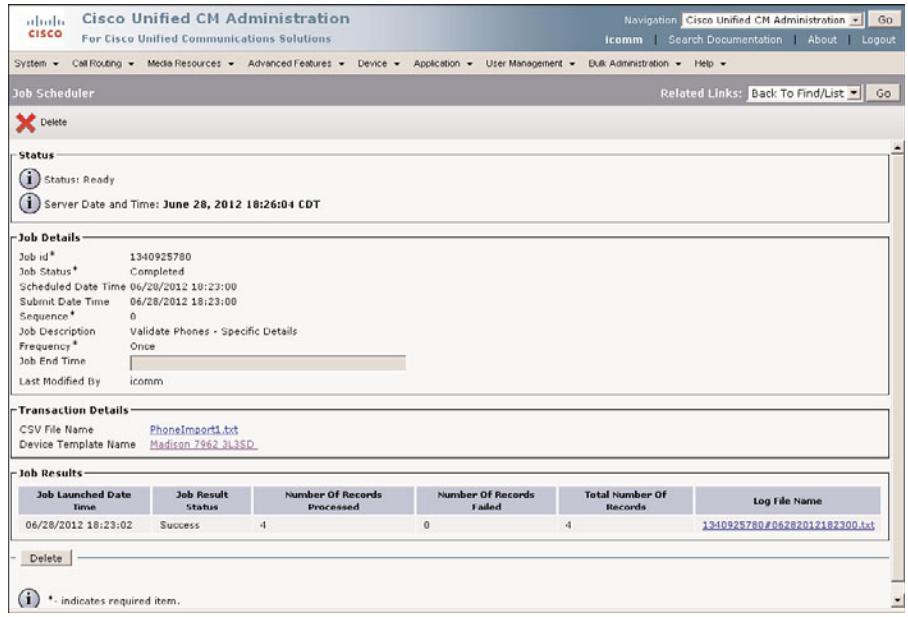


4. Click **Submit** to process the job. The page will refresh to show that the job request was submitted.
5. To see the progress of a job, on the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Job Scheduler** and click the **Find** button if your job does not show.
6. To verify that the job completed without any errors, check the job status by clicking the hyperlinked job ID number for your job. The Job Result Status should be Success. (If not, click the hyperlink for the Log File Name to see details on what went wrong so that you can fix it.) See Figure 9-67 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-67 BAT Validate Phones Job Status



Task 6: Complete Importing Phones

After verifying that the template and data file are correct, it is now time to import the new phones.

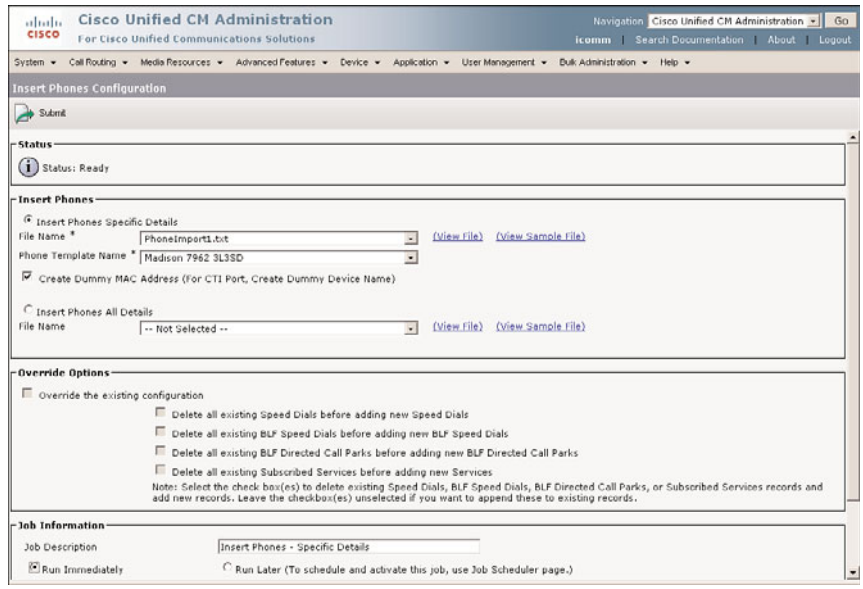
On the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Phones > Insert Phones**.

1. Because you are only importing some details, leave the radio button selected on **Insert Phones Specific Details**.
2. From the File Name drop-down list, select the **PhoneImport1.txt** file.
3. From the Phone Template Name drop-down list, select the name of the template (**Madison 7962 3L3SD**, in this example).
4. Select the **Create Dummy MAC Address** check box.
5. Because you are importing only four phones, and this small job will not impact the system, in the Job Information section, click the **Run Immediately** radio button. See Figure 9-68 for an example of this page.
6. Click **Submit** to process the job. The page will refresh to show that the job request was submitted.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-68 BAT Insert Phones Configuration



Task 7: Verify Phone Import

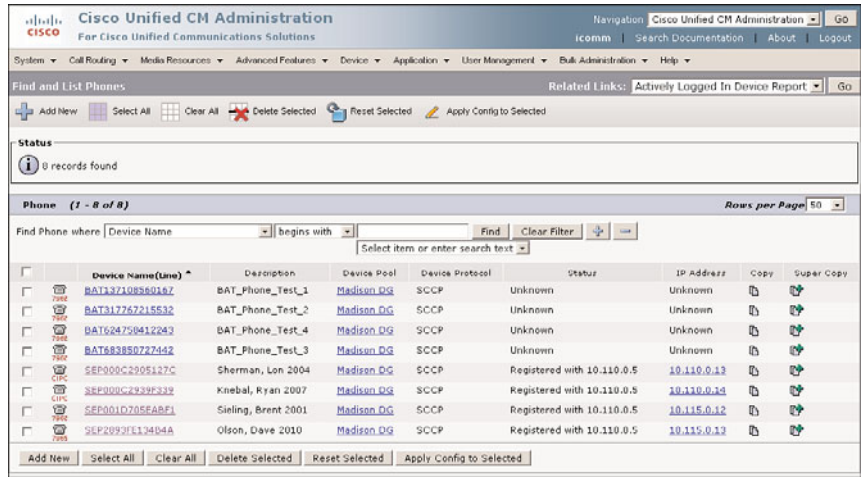
To verify that the phones imported, on the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Job Scheduler** and click the **Find** button if your job does not show. To verify that the job completed without any errors, check the job status by clicking the hyperlinked job ID number for your job. The Job Result Status should be Success.

The other method is to examine the phones to see whether the new entries are there. On the **Cisco Unified CM Administration** page, navigate to **Device > Phone** and click the **Find** button to see the phones. You should see the new phones. Not only will they have the BAT_Phone_Test description, but the dummy MAC addresses also start with BAT.

Note: Insert joke about how Commissioner Gordon can't call you on the BAT phone here.

See Figure 9-69 for an example of this page.

Figure 9-69 Phones with BAT Imports



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 8: Modifying Existing Phones

BAT is useful for more than just exporting and importing phones. BAT can be used to modify existing phones with a few quick steps.

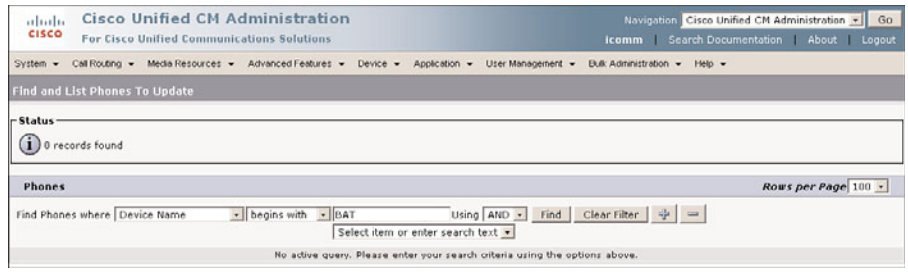
For example, if the phones you just imported should have been in the Chicago device pool, you can select them in BAT and change just the device pool setting in a batch job.

Step 8-1: Find the Phones to Update

To find the phones, on the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Phones > Update Phones > Query**.

1. Because the phones that you want to change start with BAT in the device name, now is the time to use the search function. Leave the drop-down lists set to **Device Name** and **begins with**, and enter **BAT** in the text box. See Figure 9-70 for an example of this page.

Figure 9-70 Find and List Phones to Update



2. Click **Find** to list the phones that match the criteria. (You also could have searched by any of the other criteria, such as Description, Directory Number, and so on).
3. The list should show the four phones you imported. Click **Next** to get the Update Phones page.

Step 8-2: Update Phone Parameters

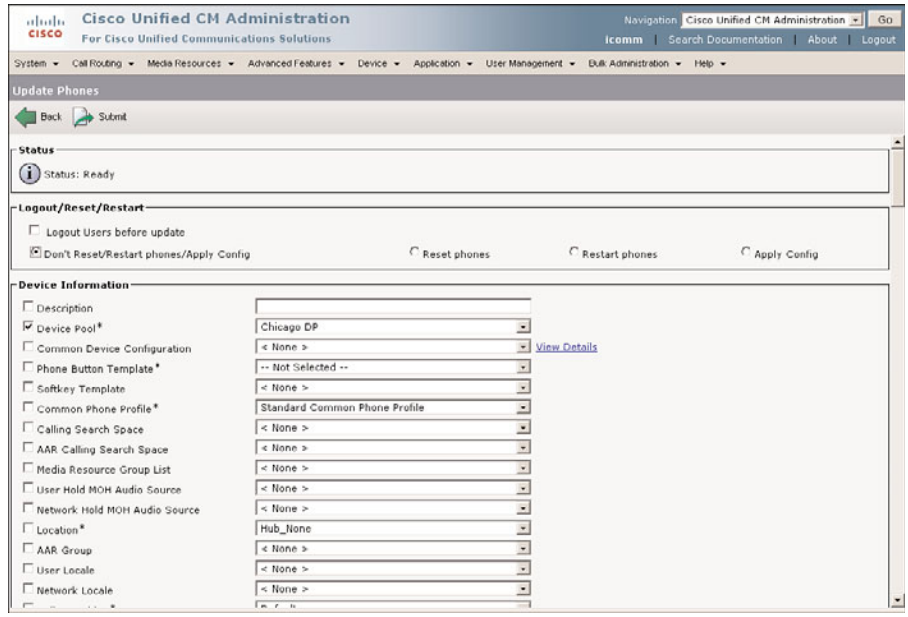
1. In this lab, the imported phones don't exist, so the Logout/Reset/Restart section option does not matter. Leave the radio button selected on **Don't Reset/Restart phones/Apply Config**. With real phones, you should select the best option to implement the changes.
2. Under Device Information, select the **Device Pool** check box, and from the drop-down list, select **Chicago DP**. See Figure 9-71 for an example of this page.
3. Scroll down to the bottom. Because this small job will not impact the system, under Job Information, click the **Run Immediately** radio button.
4. Click **Submit** to commit the change.
5. Navigate to **Bulk Administration > Job Scheduler** and click the **Find** button if your job does not show. To verify that the job completed without any errors, check the job status by clicking the hyperlinked job ID number for your job. The Job Result Status should be Success.
6. On the **Cisco Unified CM Administration** page, navigate to **Device > Phone** and click the **Find** button to see the phones. You should see that the BAT phones are now using the Chicago DP device pool.

Because the phones don't exist, leave them in the system to use as future endpoints.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-71 Update Phones

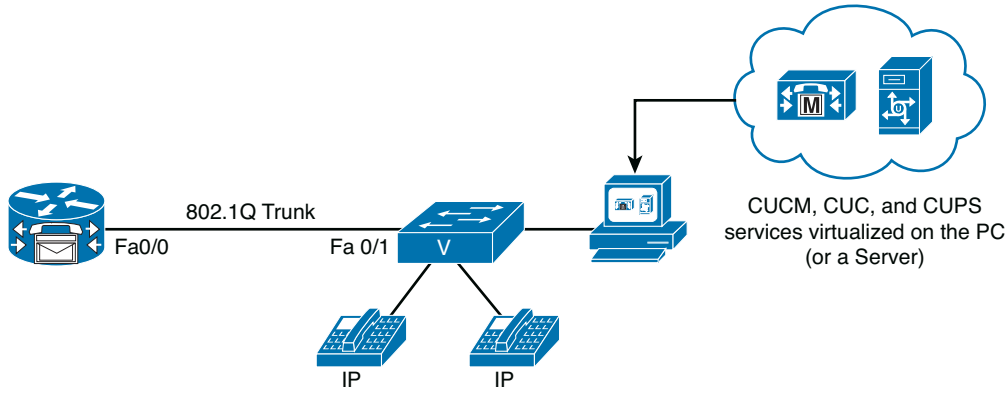


https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 9-7: Adding End Users Manually

Figure 9-72 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- CUCM Server or PC with VMware Workstation installed and a VM of CUCM
- One or more IP Phones (desk phone or soft phone on PC or Windows VM)
- Configuration from Lab 9-5 or 9-6 completed, and at least one phone registered as shown in Lab 9-5

Learning Objectives

Upon completion of this lab, you will be able to

- Add both applications and end users to the CUCM system
- Create and modify user groups
- View end-user web pages

Scenario

SOI wants to add users to the phone system. While creating users is not necessary to make phones ring or display the caller ID information, there are benefits to having users in the system. For features such as extension mobility, having a user account is essential to log in to a phone (more on this in Lab 11-1), and user accounts also allow users to change features on their phone (such as call forwarding, covered in Lab 11-2) without administrator intervention.

Before creating users, it is important to understand that CUCM has two categories of users: Application Users (the icomm user account is one of them) and End Users (which is where all the phone users will be located). For the most part, the Application Users are for system functions and application-to-application communication, while the End Users are for people wanting to access features of the system. Both of these users get their rights from groups and roles.

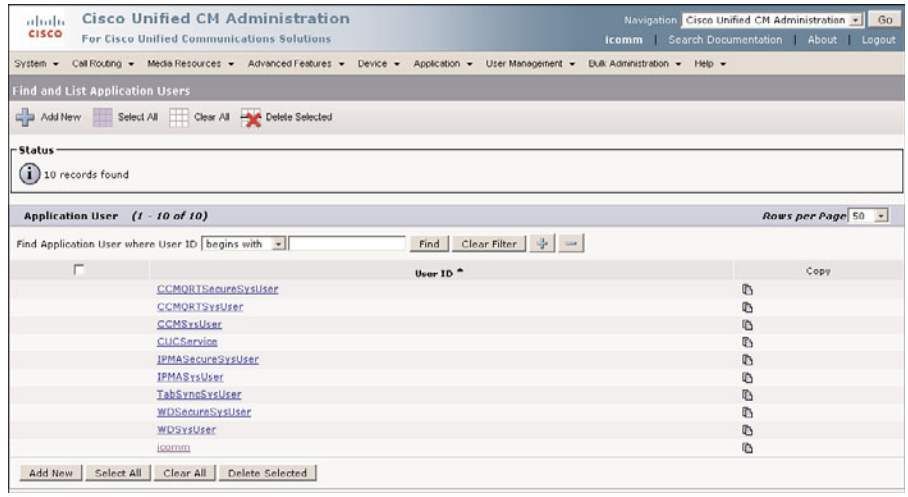
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Examine Administrative Users

On the **Cisco Unified CM Administration** page, navigate to **User Management > Application User** and click the **Find** button to see the preexisting users. See Figure 9-73 for an example of this page.

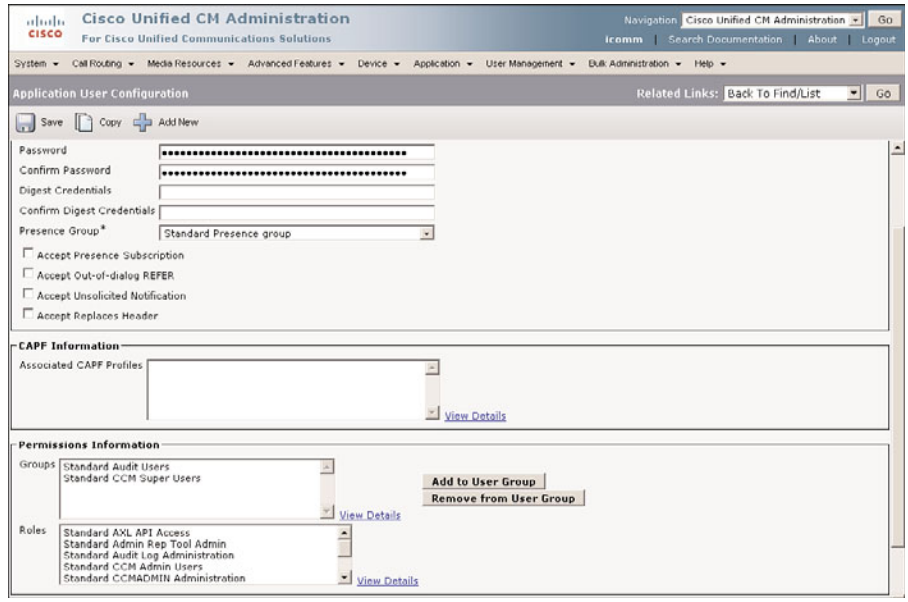
Figure 9-73 Default Application Users



Click the **icomm** username to see the details. For example, this is one of the places you could change the password for the icomm user.

Scroll down (if necessary) to see the Permissions Information section. Notice that the icomm user is a member of two groups: Standard Audit Users and Standard CCM Super Users. The groups are assigned various roles in the system, and you can see the roles the icomm user has inherited from the two groups (such as Standard CCM Admin Users, Standard SERVICABILITY Administration, and so on). It is the roles that grant the icomm user account all the rights it has to run the system. See Figure 9-74 for an example of this page.

Figure 9-74 Icomm Application User Configuration



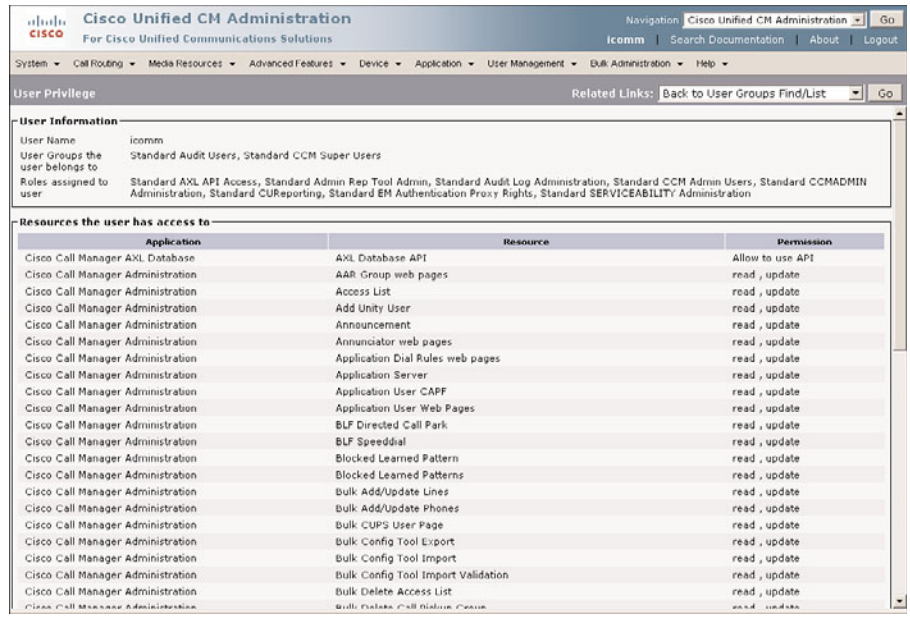
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

To see these rights in more detail, from the Related Links drop-down list, select **User Privilege Report** and click the **Go** button.

The User Privilege page for the icomm user shows all the applications, resources, and permissions granted from the roles (which are inherited from the groups assigned to the icomm user). See Figure 9-75 for an example of this page.

Figure 9-75 Icomm User Privilege



Note: If you scroll to the bottom of the page, you see by default that the listing is only showing 50 items per page, but there are eight pages of items! (Even if you change the Rows per Page field to the maximum of 250, you will still have two pages of items.)

Task 2: Examine User Groups

To understand user groups better, on the **Cisco Unified CM Administration** page, navigate to **User Management > User Group** and click the **Find** button to see the preexisting groups. See Figure 9-76 for an example of this page.

Click the "i in a circle" under Roles (See Figure 9-76) for the **Standard CCM Super Users** group to get more information about the roles assigned to that group. The User Group Configuration page shows the roles for this group (which is where the icomm user gets most of the rights). See Figure 9-77 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-76 Default User Groups

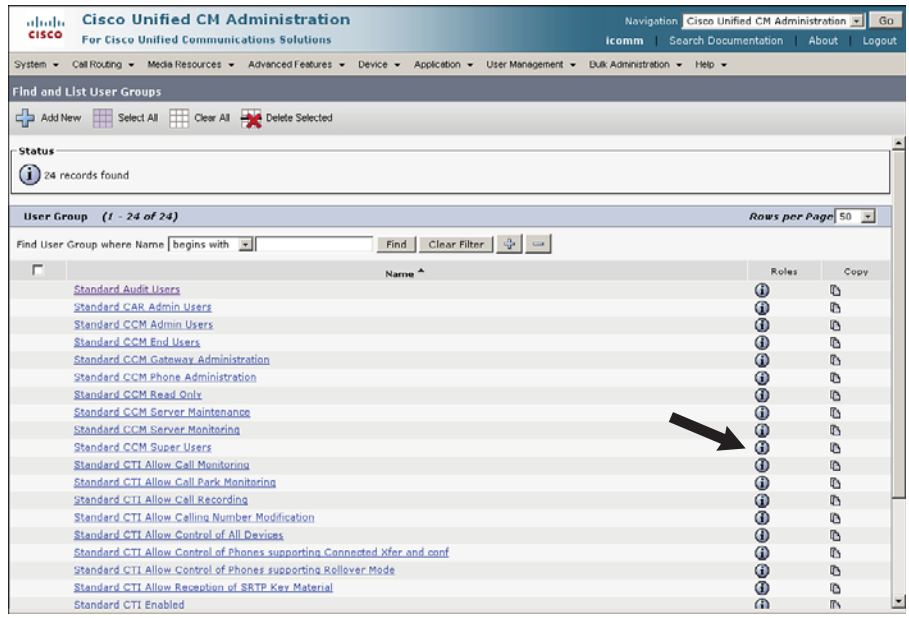
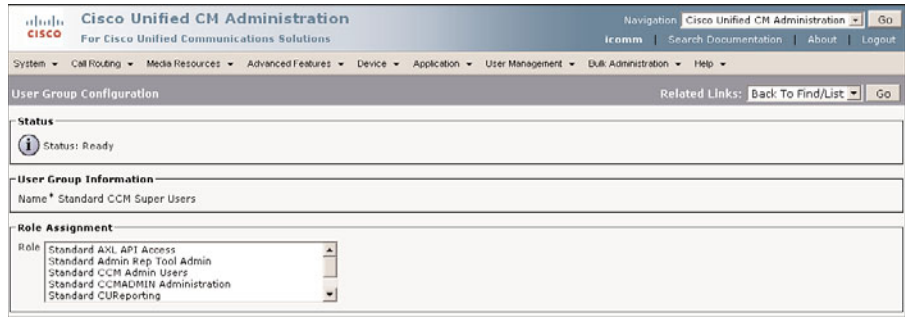


Figure 9-77 User Group Configuration



Task 3: Examine Roles

To understand roles better, on the **Cisco Unified CM Administration** page, navigate to **User Management > Role** and click the **Find** button to see the roles. See Figure 9-78 for an example of this page.

Click the hyperlinked name of the first **Standard CCMADMIN Administration** role (the one that lists Cisco Call Manager Administration in the Application column). Here you see the various resources that this role has access to and the privileges assigned (read and/or update). See Figure 9-79 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-78 Find and List Roles

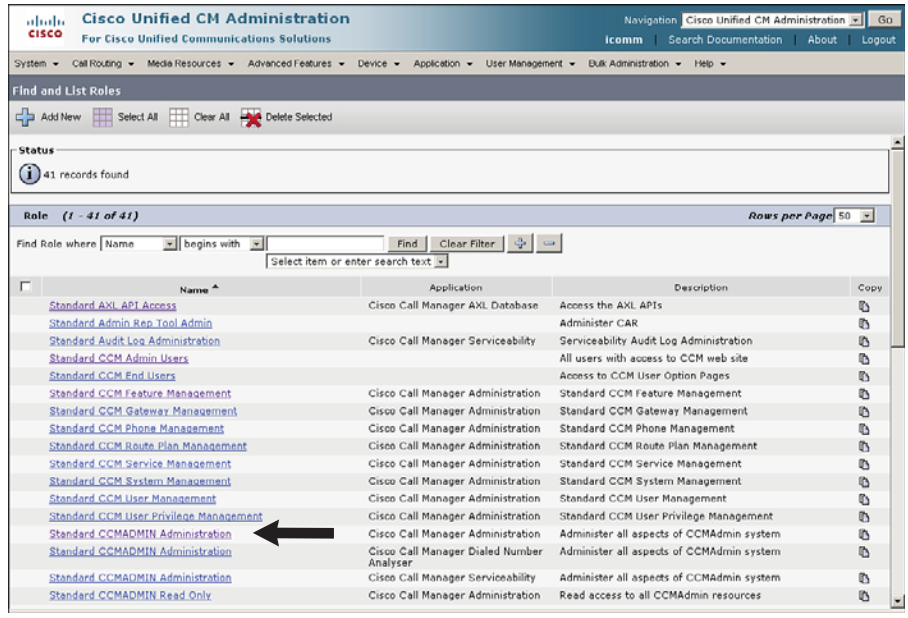
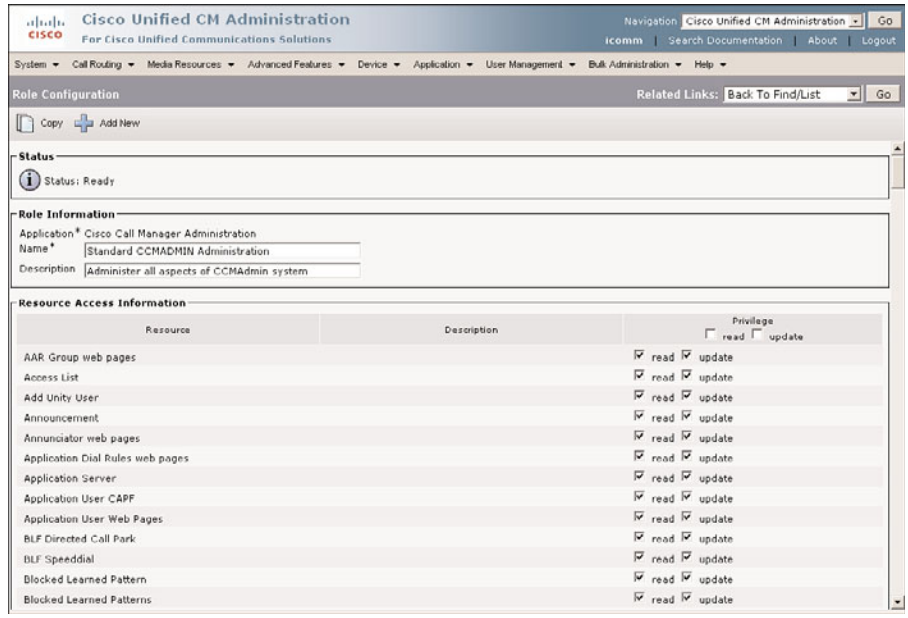


Figure 9-79 Role Configuration



To summarize: Users are assigned groups, which in turn have roles assigned to them, and roles in turn have resources assigned to them.

Note: What happens if a user is assigned groups that have roles with different privileges for the same resource? The setting "Effective Access Privileges For Overlapping User Groups and Roles" under the System > Enterprise Parameters menu determines whether the higher privileges or the more restrictive privileges prevail. The default value is Maximum, which allows the higher privileges of the conflicting settings to be active for the user. If you want the more restrictive privileges to be enforced, change the setting to Minimum.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

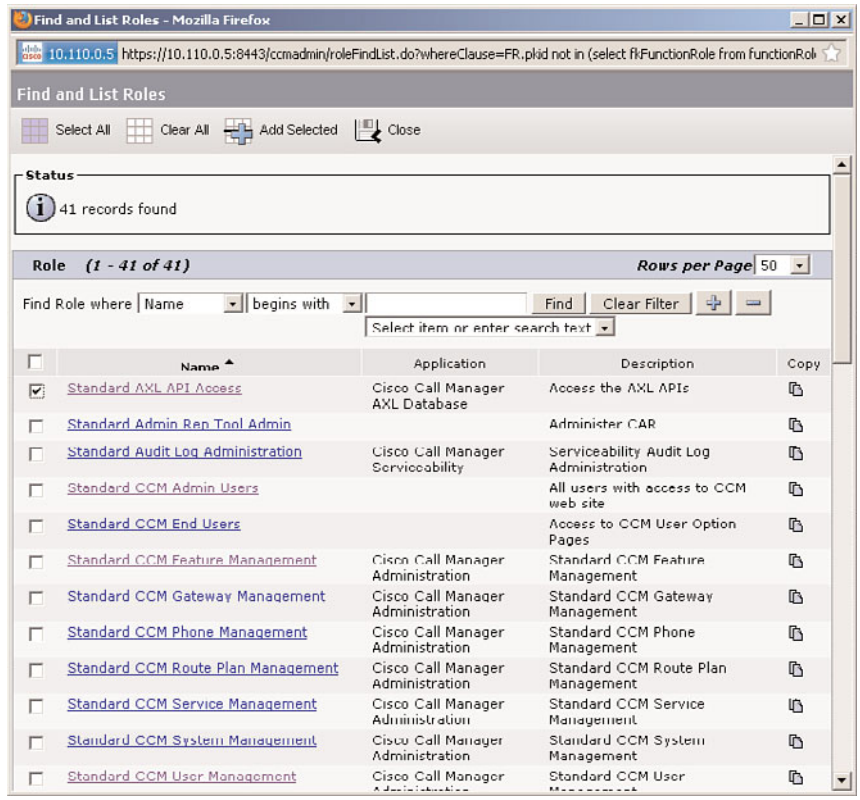
Task 4: Create New AXL Group

AXL stands for Administrative XML (where XML stands for eXtensible Markup Language). It is a protocol used to exchange data between applications. In later labs, other applications will need access to the CUCM AXL service (for example, in Lab 13-3, the Unity Connection Voicemail will use AXL to exchange information with CUCM). While the icomm user would have all the necessary rights, using the icomm user for the login would be a bad choice for two reasons: The icomm user has far more rights than needed, so it is a security risk, and if the icomm user password is changed in the future, any applications that use that account could fail until they are updated with the new password. For those reasons, it is better to create another application user that has just the necessary rights. However, there is no predefined group that contains only the Standard AXL API Access role, so you need to create a new user group.

To create a new user group, on the **Cisco Unified CM Administration** page, navigate to **User Management > User Group** and click the **Find** button to see the preexisting groups.

1. Click the **Add New** button to create a group.
2. Enter **AXL Users** for the Name field, and click the **Save** button.
3. From the Related Links drop-down list, select **Assign Role to User Group** and click **Go**.
4. In the Role Assignment area, click the **Assign Role to Group** button to open the Find and List Roles window. Click the **Find** button in the roles if none show.
5. Select the check box in front of the **Standard AXL API Access** name. See Figure 9-80 for an example of this page.

Figure 9-80 AXL—Find and List Roles



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

6. Click the **Add Selected** button.
7. The User Group Configuration window shows the Standard AXL API Access role. Click **Save**.

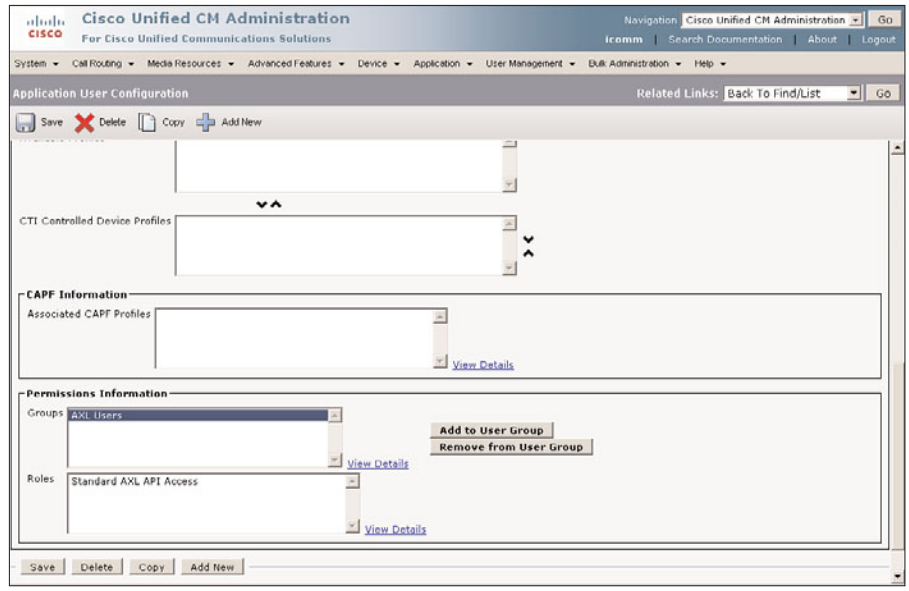
Now that the AXL Users group is created and has the role assigned, you can create an AXL_Admin and assign the group to the user.

Task 5: Create the New AXL User

On the **Cisco Unified CM Administration** page, navigate to **User Management > Application User** and click the **Find** button to see the users.

1. Click the **Add New** button and the Application User Configuration window opens.
2. For the User ID, enter **AXL_Admin** (note the underscore in the name).
3. Enter **cisco** for both the Password and Confirm Password fields.
4. Scroll down to the Permissions Information section and click the **Add to User Group** button to open the Find and List User Groups window.
5. Select the **AXL Users** check box to choose that group. Click the **Add Selected** button to save the group.
6. The Groups box now shows the AXL Users group. (Notice that the Roles box is still empty at this point.) Click the **Save** button. Now that the user is saved, the Roles box will show the assigned role. See Figure 9-81 for an example of this page.

Figure 9-81 AXL_Admin Configuration



Task 6: Examine the Default Login Credential Policy

Before creating end users, it is useful to examine the default login security credentials. On the **Cisco Unified CM Administration** page, navigate to **User Management > Credential Policy** (not Credential Policy Default) to see the existing default policy.

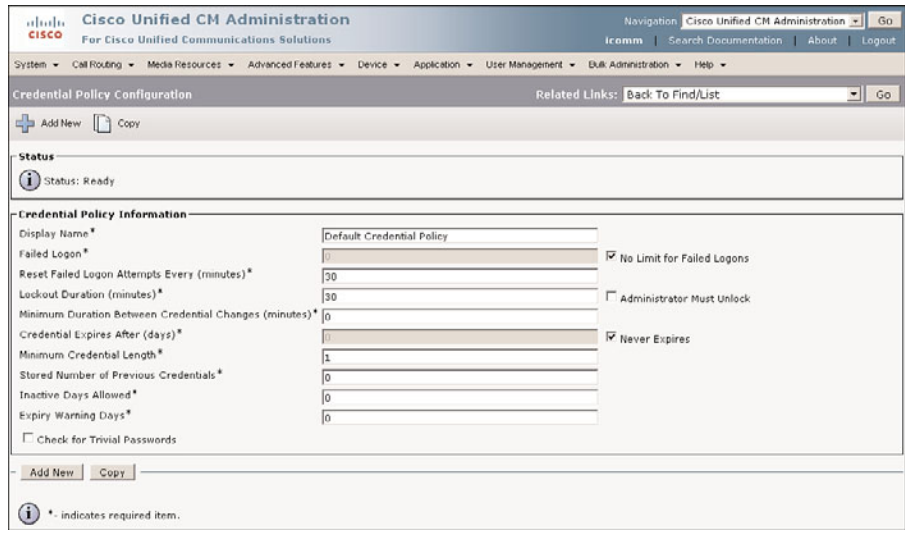
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Click the hyperlinked default credential policy to see the details.

The Credential Policy Configuration page shows the various security settings for user logins that can be configured. For this lab, leave the settings as they are. However, if a company's security policy dictates certain things, such as passwords being changed at regular intervals, this is where the policy can be set to force a change every *x* number of days, and so on. See Figure 9-82 for an example of this page.

Figure 9-82 Default Credential Policy Configuration



Task 7: Manually Create an End User

The bulk of users created will be end users. End users are created in two stages: First, the basic required and optional entries are collected, and then, after those items are saved, the ability to add phones (and other devices) and groups is enabled.

On the **Cisco Unified CM Administration** page, navigate to **User Management > End User** and click the **Find** button to see any existing users. Click the **Add New** button and the End User Configuration window opens.

Note: The User ID field must be unique for the entire system. It is also what users will be required to enter using a phone keypad for services like Extension Mobility. If services like Extension Mobility are planned, using a numeric ID (such as an employee's ID number) will make logging in on a phone keypad easier.

---

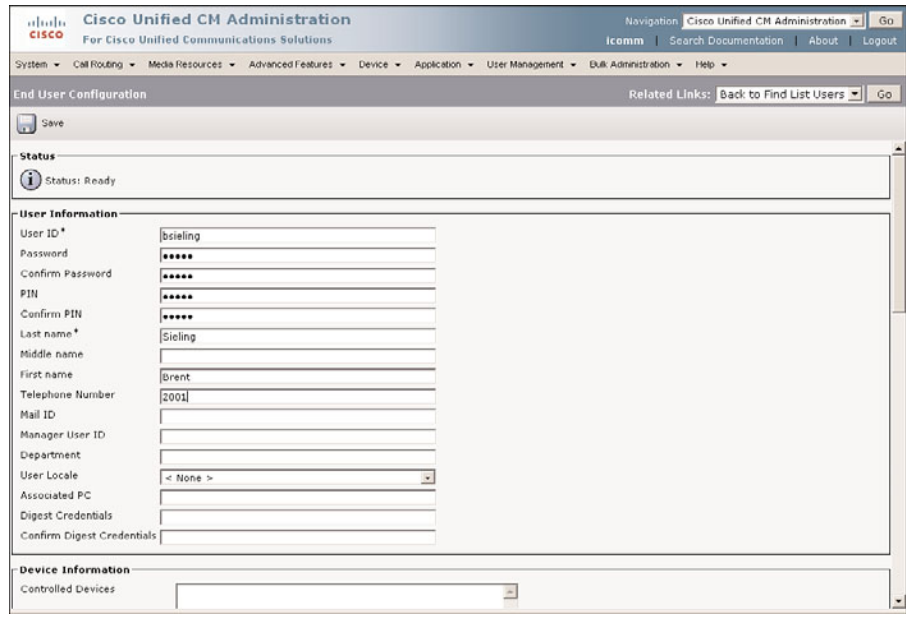
1. SOI uses the first initial and last name of the user as its naming convention (with the middle initial after the first initial to avoid duplicates and a number added as a final tiebreaker). For the first end user, enter your own username in the User ID field (**bsieling** in my case).
2. Enter **cisco** for both the Password and Confirm Password fields.
3. The PIN field is used for the login password on keypad-only systems. Enter **12345** for both the PIN and Confirm PIN fields.
4. The Last Name field is required but does not have to be unique. For the first end user, enter your own last name the Last Name field (**Sieling** in my case).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

5. The First Name field is optional, but because you have to enter the last name, you might as well use this field too. For the first end user, enter your own first name in the First Name field (**Brent** in my case).
6. Enter the primary extension for the user in the Telephone Number field (**2001** in my case).
7. The other fields are not needed at this time. Notice that you are unable to add any phones to the user in the Device Information section at this time, and the Permissions Information section is not even displayed. See Figure 9-83 for an example of this page.

Figure 9-83 End User Initial Configuration



8. Click **Save** to move past the initial user creation stage. The page will refresh, and the Password and PIN fields are replaced with a long line of black dots, thus hiding the length of the original items. (Note: The Edit Credential button allows you to change the credential policy applied to the user or to override some of the policy settings.)
9. Now that the initial user information has been entered, devices can be associated, primary extension selected, and user groups assigned. Under the Device Information section, click the now-visible **Device Association** button and the User Device Association window will open.
10. Because no devices have been associated yet, click the **Find** button. Instead of phone devices showing up, you instead see the individual directory numbers for all phones. Select the check boxes for the phone lines on the actual phone you have registered for yourself (this is where using the name in the phone description is handy), and for a future example, select the boxes for one of the BAT-registered phones. See Figure 9-84 for an example of this page.
11. Click the **Save Selected/Changes** button. The page will refresh to show the items you selected at the top of the list.
12. With the Related Links set at Back to User, click the **Go** button to return to the end user.
13. The End User Configuration page now shows the controlled devices for the user. See Figure 9-85 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-84 User Device Association

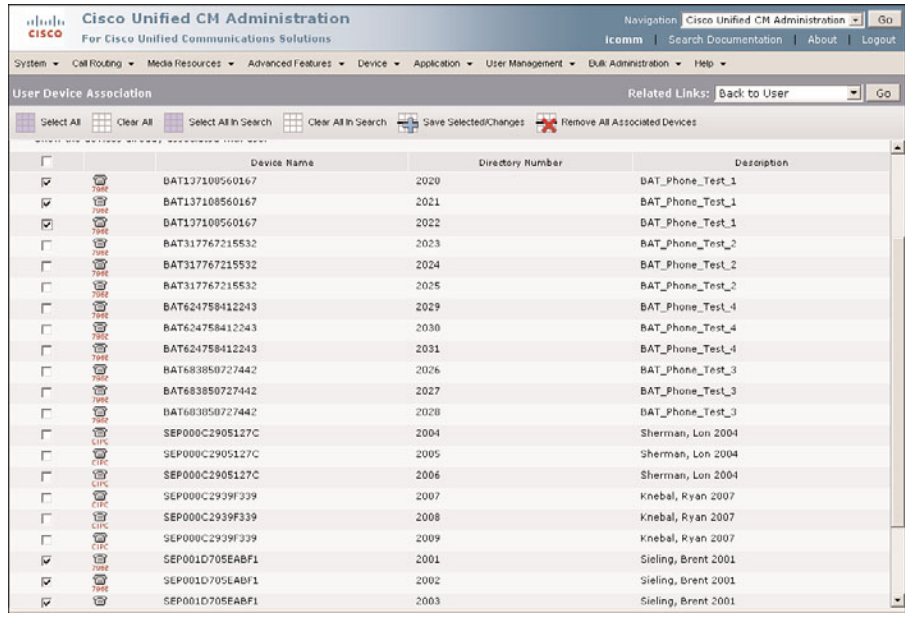
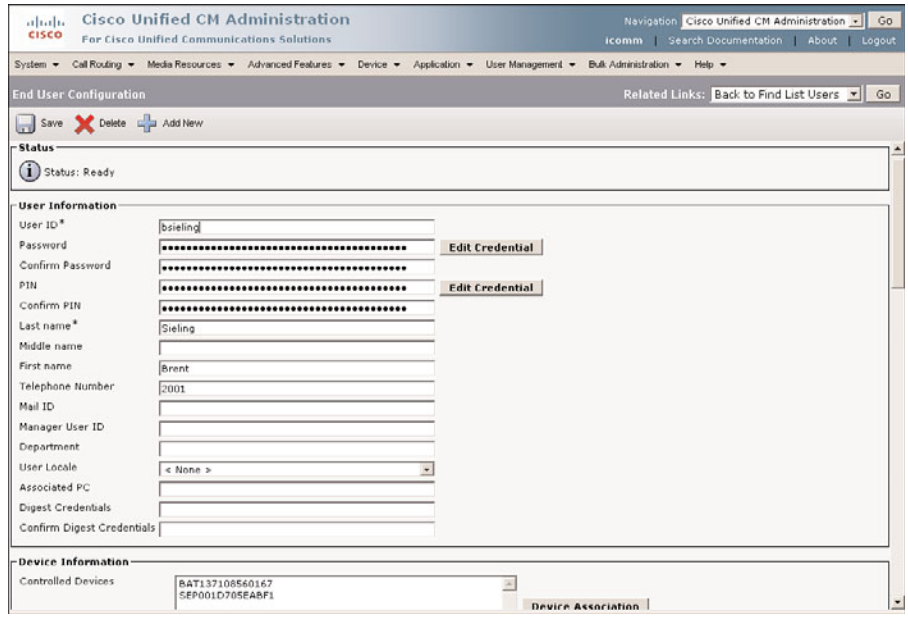


Figure 9-85 Updated End User Configuration with Devices



14. After a phone or phones have been associated with an end user, you can then select the primary line for the user. Scroll down to the Directory Number Associations section, and from the Primary Extension drop-down list, choose the first extension for the actual phone. (**2001** in my example).

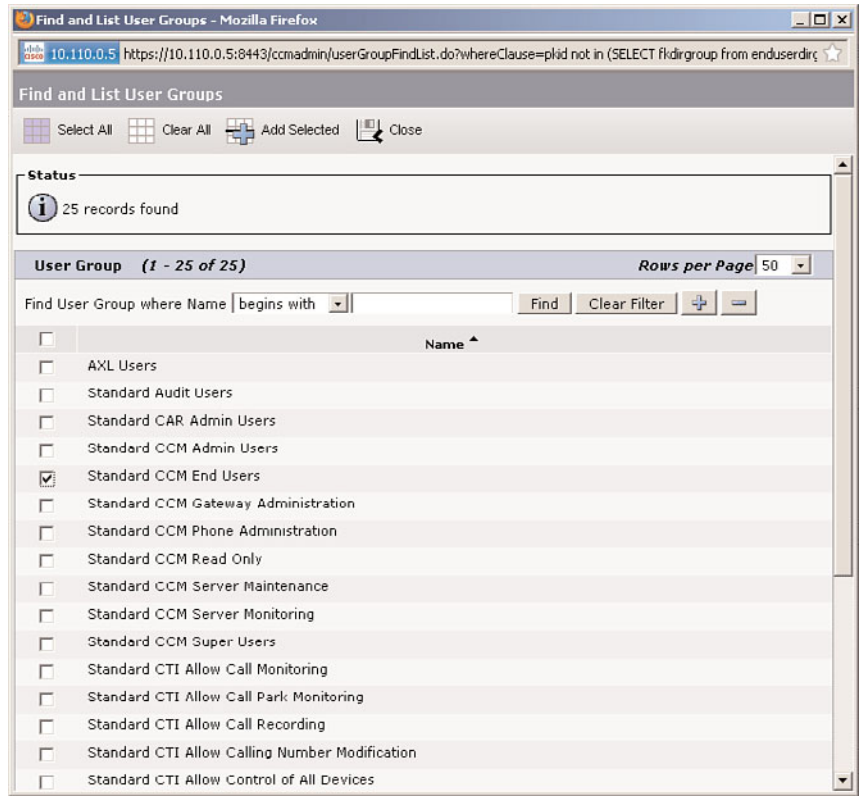
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

15. By default, end users have almost no rights to information in the CUCM system. To be able to log in with Extension Mobility or access the web page to manage user features, they need the appropriate group (and resulting roles) assigned to them. Scroll down to the Permissions Information section. Click the **Add to User Group** button, and when the Find and List User Groups window opens, click the **Find** button.

16. Select the check box for the **Standard CCM End Users** group. See Figure 9-86 for an example of this page.

Figure 9-86 Selecting Standard CCM End User Group



17. Click the **Add Selected** button to add the user to the group and return to the End User Configuration page.

18. While the group shows up, the user is not actually added until the End User page is saved, and then the roles will show up. Click the **Save** button. Now the user is added to the Standard CCM End User group, and the Standard CCM End Users and Standard CCMUSER Administration roles are showing. (Note that the Standard CCMUSER Administration does not mean that the user can administer other end users; it just gives the user permission to modify his own user settings.)

Task 8: Explore End User Web Pages

One of the benefits of creating end users is the ability for the end user to administer some of his own settings without administrator intervention.

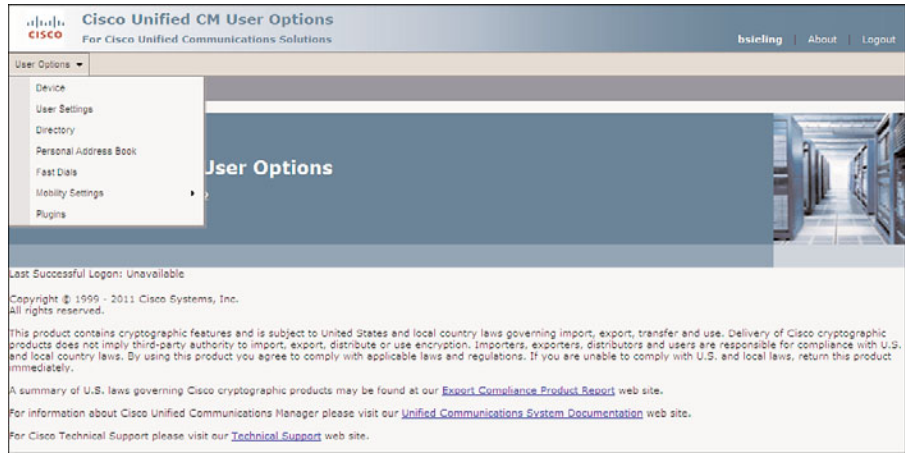
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Note: The access rights to the CUCM pages are preserved across all pages of a browser. So, to experiment with an end-user web page, while still maintaining your icomm user login, it is necessary to use a completely different web browser. Opening a new window in the same web browser will *not* work to separate the rights, and you will have to log out as icomm first, or you will have permission problems.

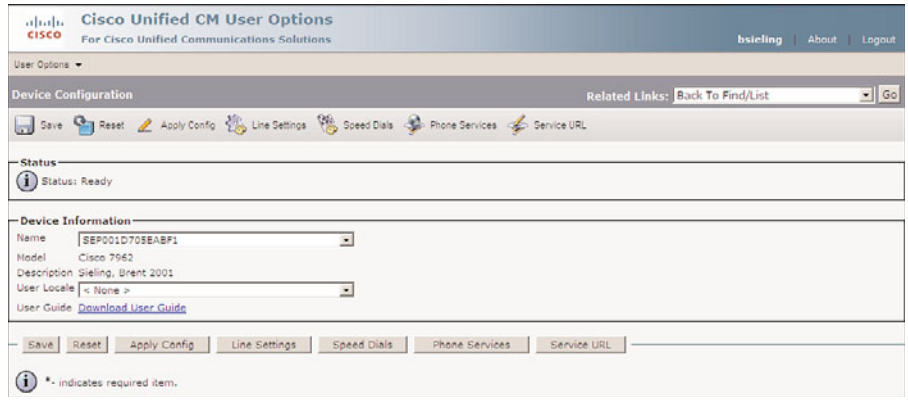
Open a different web browser and enter **https://**<*ip_address_of_your_server*>**/ccmuser** (make sure that you enter **ccmuser** at the end) and accept any security certificate warnings. You should be at the Cisco Unified CM User Options page. (Unlike the Administrative pages, this does not have a Navigation drop-down list.) Enter the username just created in Task 7 and the password **cisco** to log in. (If you have problems with the login, verify that you are on the correct web page and that the end user account has the correct roles associated.) On the left side is the User Options drop-down list. See Figure 9-87 for an example of this page.

Figure 9-87 End-User Options Menu



Select **Device** from the User Options drop-down list. Because you assigned two phones to the user, the Name drop-down list allows the user to select which device to change settings on. (There are buttons for items like Line Settings and Speed Dials that will be discussed in later labs.) See Figure 9-88 for an example of this page.

Figure 9-88 End-User Device Configuration

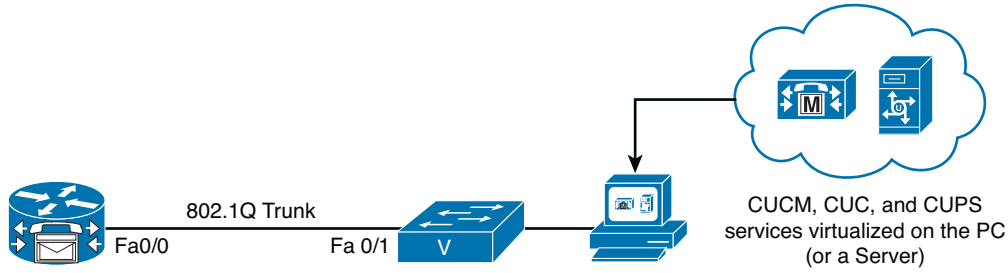


After you are done looking around, click the **Logout** button.

https://t.me/learningnets
From the Library of Aliwarman Tarihoran

Lab 9-8: Adding End Users with the Bulk Administration Tool (BAT)

Figure 9-89 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- CUCM Server or PC with VMware Workstation installed and a VM of CUCM
- PC with Microsoft Excel installed
- (Optional) One or more IP Phones (desk phone or soft phone on PC or Windows VM)
- Configuration from Lab 9-6 completed, and preferably at least one phone still registered, as shown in Lab 9-5

Learning Objective

Upon completion of this lab, you will be able to import end users using Bulk Administration Tool (BAT).

Scenario

SOI is going to add a large number of users in the near future. The staff wants a more efficient way than manual registration to add them. Additionally, they would like a way to modify the information for large numbers of previously created users. BAT is still the answer!

Task 1: Use BAT to Import End Users

Step 1-1: Use BAT Template

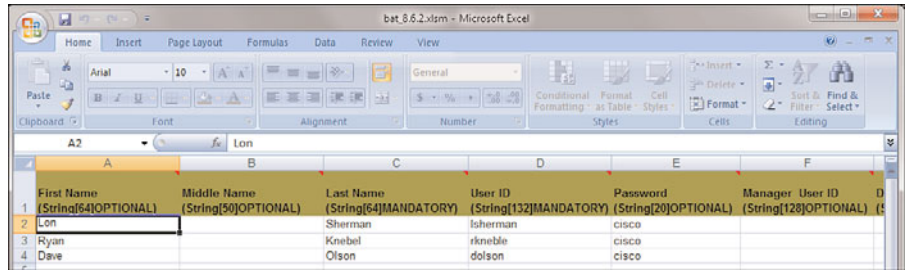
1. Open Microsoft Excel, and then use the **Open** command on the bat.xlsm macro-enabled workbook (downloaded in Lab 9-6, Task 3).
2. When the security warning shows under the ribbon regarding the macros included in the spreadsheet, click the **Options** button and a pop-up window will open. Click the **Enable This Content** radio button and click **OK**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. Change to the **Users** worksheet tab at the bottom of the file. There are more columns for users than when importing phones, but notice that only two of them are mandatory: Last Name and User ID, just like when creating a user manually.
4. Use the CUCM Pod Phone Number Table in Appendix B to find the first names and last names to enter for your pod.
5. Use the SOI naming convention (SOI uses the first initial and last name of the user as its naming convention with the middle initial after the first initial to avoid duplicates, and a number added as a final tiebreaker) to create user IDs for each.
6. Enter **cisco** for the Password field and **12345** for the PIN field.
7. Use the CUCM Pod Phone Number Table in Appendix B to find the telephone number. However, leave the Primary Extension blank. (To get the Primary Extension to import requires some effort; search the web if you want more details.) See Figure 9-90 for an example of this page.

Figure 9-90 Excel BAT Users Tab



Note: If you were doing this in production, you might want to change the Number Of Controlled Devices macro box (after the last column) to 1 and then enter the device name of the associated phone for each user in the new column. However, to simplify the lab, leave it set to 0.

8. Scroll over to the last column, where you see the macro boxes that can change the worksheet, and click the **Export to BAT Format** button.
9. A dialog box will open to allow you to specify the path and to change the filename to **UserImport1** to save the new file. Click **OK**.

Note: The filename cannot have spaces or special characters. Only alphanumeric, dash, underscore, and dot characters are allowed.

Step 1-2: Upload the BAT Import File

To upload the UserImport1.txt file, on the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Upload/Download Files** and click the **Find** button if no files show.

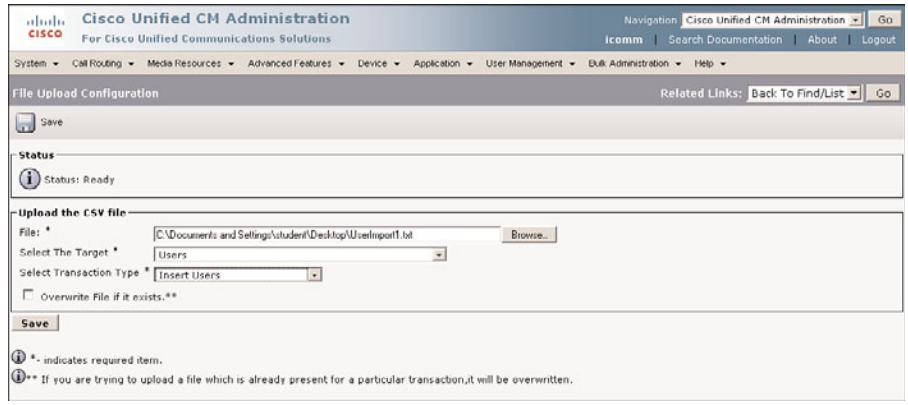
1. Click the **Add New** button and the File Upload Configuration window will show.
2. Click the **Browse** button at the end of the File field and the Open File dialog box opens.
3. Navigate to the location you saved the UserImport1.txt file and click **OK**.
4. From the Select The Target drop-down list, select **Users**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

5. From the Select Transaction Type drop-down list, select **Insert Users**. (Note: This does not actually insert the users; it just tells CUCM what you plan to do with the data.) See Figure 9-91 for an example of this page.
6. Click **Save** to have the file uploaded into the CUCM system.

Figure 9-91 BAT User Data Upload

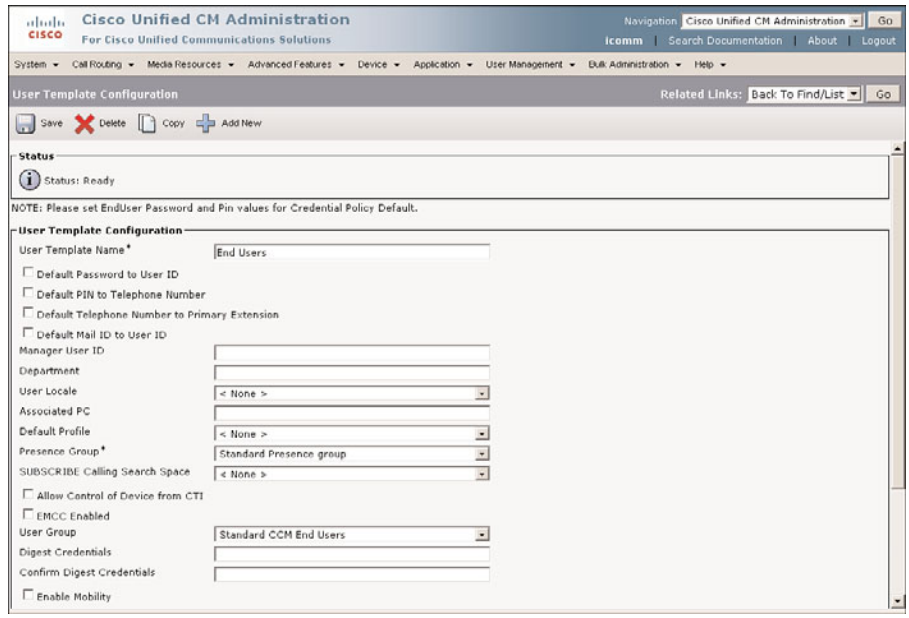


Step 1-3: Create BAT User Template

On the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Users > User Template**.

1. Click the **Add New** button to create a template.
2. Enter **End Users** for the User Template Name.
3. From the User Group drop-down list, select **Standard CCM End Users**. See Figure 9-92 for an example of this page.

Figure 9-92 BAT User Template Configuration



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

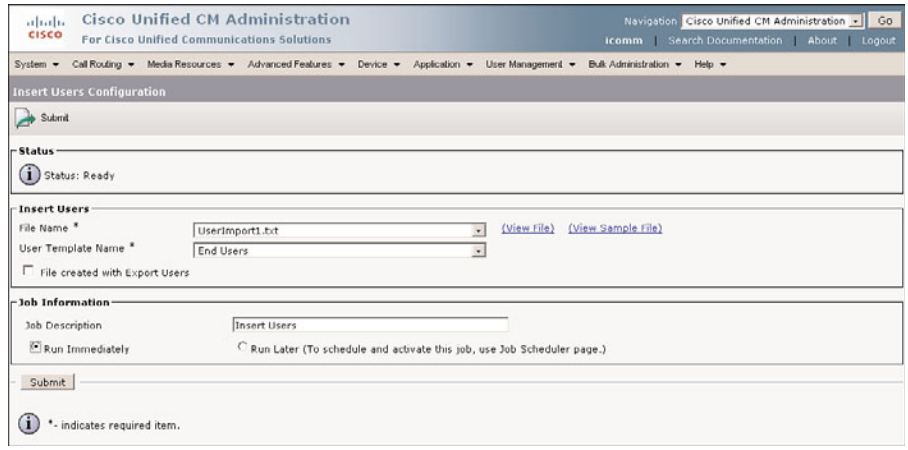
4. Click **Save** to finish the template.

Step 1-4: Insert New Users

Interestingly enough, there is no validate function for User Import. On the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Users > Insert Users**.

1. From the File Name drop-down list, select the **UserImport1.txt** file.
2. From the User Template Name drop-down list, select **End Users**.
3. Because you are importing only a few users and this small job will not impact the system, in the Job Information section, click the **Run Immediately** radio button. See Figure 9-93 for an example of this page.
4. Click **Submit** to create the users.

Figure 9-93 BAT Insert Users Configuration



Step 1-5: Verify User Import

To verify that the users imported, on the **Cisco Unified CM Administration** page, navigate to **Bulk Administration > Job Scheduler** and click the **Find** button if your job does not show. To verify that the job completed without any errors, check the job status by clicking the hyperlinked job ID number for your job. The Job Result Status should be Success.

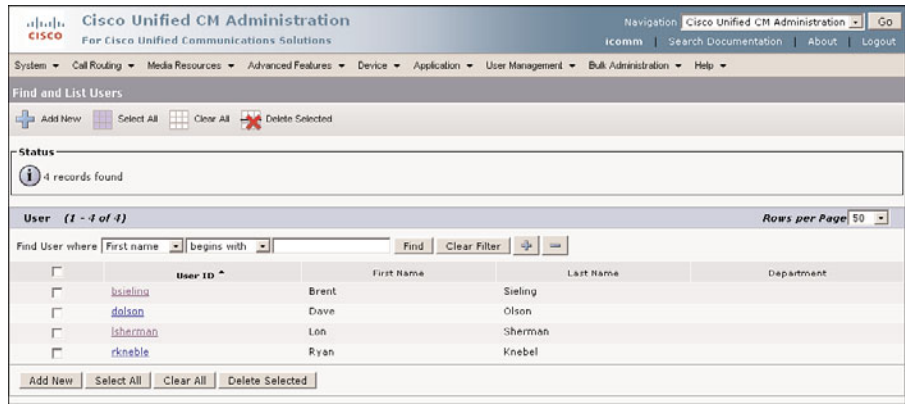
The other method is to examine the end users to see whether the new entries are there. On the **Cisco Unified CM Administration** page, navigate to **User Management > End User** and click the **Find** button to see the existing users. You should see the new users. See Figure 9-94 for an example of this page.

Click the hyperlinked user ID with your name to see the details. Then click one of the newly imported users. The only difference between the two is that the newly imported users do not have any device associations or primary extensions identified. Do not bother associating them with phones or granting them rights at this point.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-94 End Users After Import

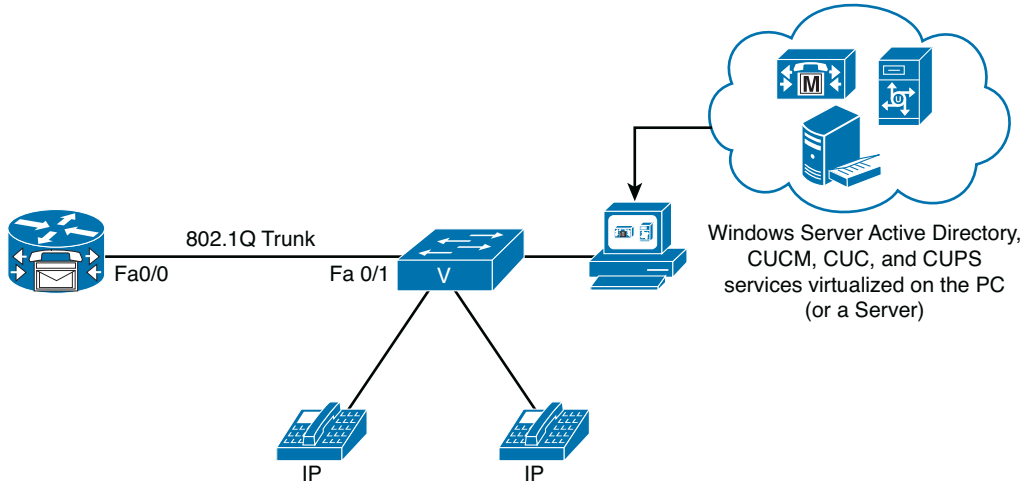


https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 9-9: Adding End Users with LDAP Synchronization

Figure 9-95 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router.
- Switch that supports voice VLANs.
- CUCM Server or PC with VMware Workstation installed and a VM of CUCM.
- Microsoft Windows Server with Active Directory installed. (This lab will demonstrate Windows Server 2008 running in a VM.) See the notes in the lab about the version used.
- (Optional) One or more IP Phones (desk phone or soft phone on PC or Windows VM).
- Configuration from Lab 9-8 completed, and preferably at least one phone still registered as shown in Lab 9-5.

Learning Objectives

Upon completion of this lab, you will be able to

- Implement LDAP synchronization
- Implement LDAP authentication

Scenario

SOI already has an Active Directory domain of users, and it wants to integrate that system of usernames and passwords into the CUCM system. The Lightweight Directory Access Protocol (LDAP) allows systems to exchange directory information.

CUCM has two methods of integrating LDAP:

- **LDAP synchronization:** Here user accounts are replicated to the CUCM system. After this is done, all end-user accounts are created or deleted in the LDAP system, not CUCM.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

(Applications users are always maintained in CUCM.) Additionally, several fields in user accounts can no longer be modified in CUCM. Not all fields are populated with information from LDAP, so there are always some fields in the end-user accounts that can be managed within CUCM. With just LDAP synchronization, the passwords still reside in CUCM and must be managed in CUCM. This means that if an end user changes her Active Directory login, the password for CUCM is not changed to match.

- **LDAP authentication:** Here any password request to CUCM is redirected to the LDAP system. The password is not stored in CUCM, as all passwords are kept only in the LDAP system. With LDAP authentication, if an end user changes her Active Directory login, the password for CUCM is the same, thus allowing a single sign-on. (However, some items, such as the user PIN, still exist in CUCM, as they don't have a counterpart in the LDAP system.)

LADP synchronization and authentication are usually combined to maximize the advantages of using the LDAP database system.

Warning: The steps in this lab will make changes to the CUCM system that are difficult to undo. Before proceeding, consider these three options:

- Continue to use the Windows server for managing user accounts for all labs from this point forward.
- Wait to complete this lab later.
- Make a copy of the CUCM server to complete this lab. (If you are using VMware Workstation, you can make a snapshot to revert back to later.)

This lab will demonstrate configuring a standard Windows 2008 32-bit server (running in a VM) that has Active Directory Domain Services installed.

Note: These concepts should also apply to a Windows 2003 AD Server, but the steps might not be the exactly the same. According to the *Cisco Unified Communications System 8.x SRND* section on LDAP Directory Integration, Windows 2000 is not supported by CUCM 8.x, and only the 32-bit versions of Windows 2003 and 2008 are supported. Verify that your server version is on the supported list in the SRND document.

Task 1: Set Up Windows Server

The domain name was configured as SOI.local when Active Directory was installed on the Windows Server, so if your server is set up with a different domain, just substitute the names in the lab.

Step 1-1: Verify Server IP Address

Before proceeding, make sure that your server has a valid IP address and connectivity with the CUCM system. Set the IP address to the one listed in the CUCM Pod Phone Number Table in Appendix B. Ping from the Windows server to the CUCM server to verify connectivity.

Step 1-2: Configure Active Directory Sync Admin Account

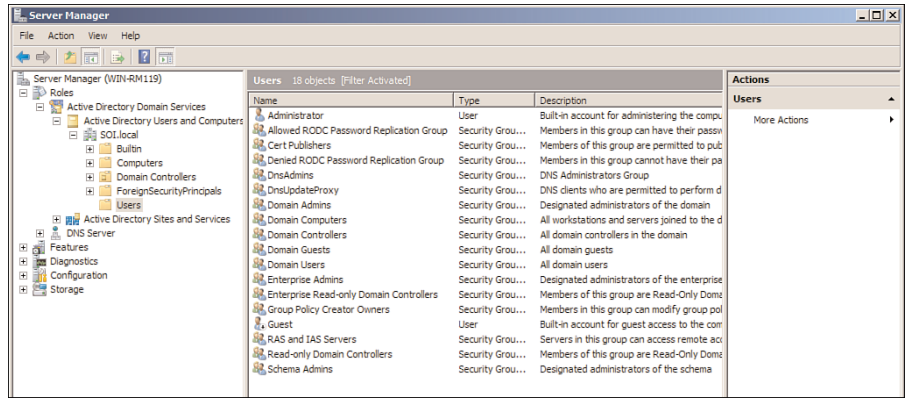
The CUCM system needs an account to log in to the LDAP server to get the records. Rather than use the Windows Administrator account, you will create another account for the LDAP synchronization.

1. On the Windows server, open the Server Manager application.
2. Navigate to the **Roles > Active Directory Domain Services > Active Directory Users and Computers > SOI.local > Users** organizational unit (OU). See Figure 9-96 for an example of this page.

https://t.me/learningnets

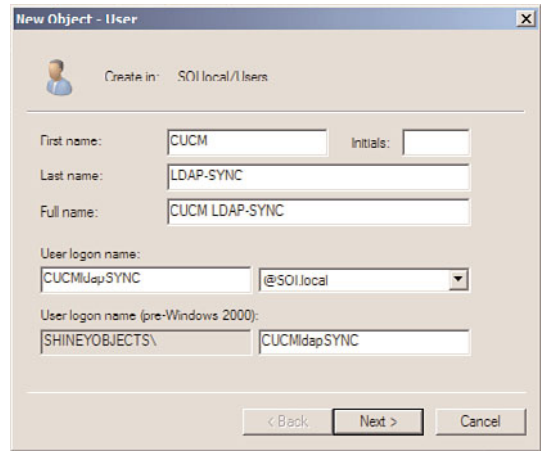
From the Library of Aliwarman Tarihoran

Figure 9-96 SOI Users OU



3. Right-click the Users OU and select **New > User** from the menu to open the New Object – User window.
4. Enter **CUCM** in the First Name field.
5. Enter **LDAP-SYNC** in the Last Name field.
6. Enter **CUCMldapSYNC** in the User Logon Name field. See Figure 9-97 for an example of this page.

Figure 9-97 LDAP Admin Creation

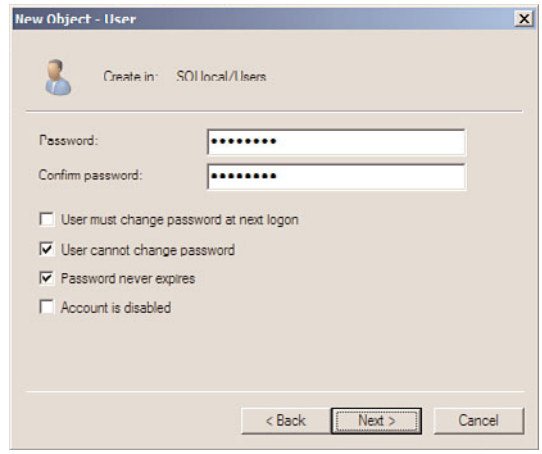


7. Click the **Next** button.
8. Enter **P@$$W0rd** (note the zero after the uppercase W) for the Password and Confirm Password fields.
9. Deselect the **User must change password at next logon** check box.
10. Select the **User cannot change password** and the **Password never expires** check boxes. See Figure 9-98 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 9-98 LDAP Admin Password

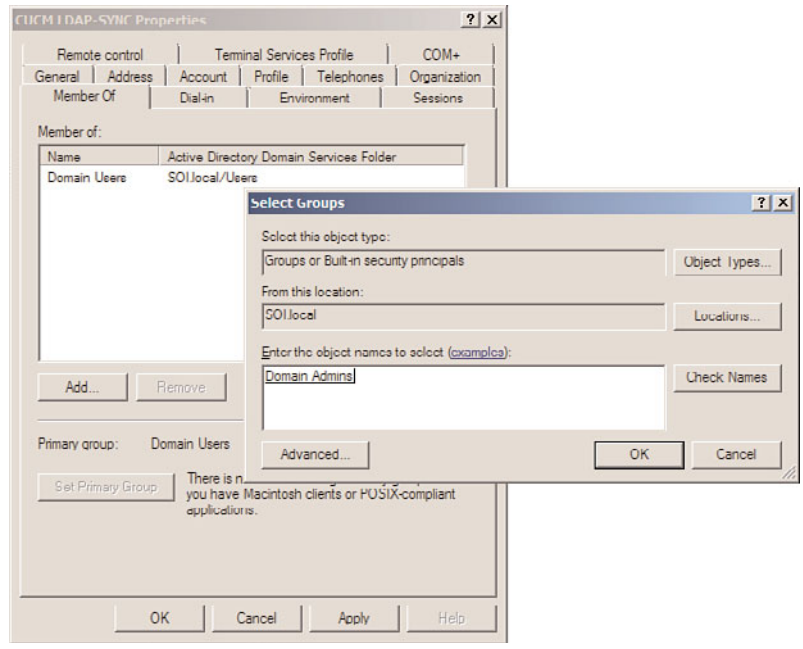


11. Click the **Next** button and then the **Finish** button to create the user.

12. The user will need the correct rights to be able to read the Active Directory domain. Right-click the CUCM LDAP SYNC user and select **Properties** from the menu. In the Properties window, click to change to the **Member Of** tab.

13. Click the **Add** button. In the Select Groups window, enter **Domain Admins** in the Enter the Object Names to Select text box. Click the **Check Names** button to verify. See Figure 9-99 for an example of this page.

Figure 9-99 Adding Domain Admins Group



14. Click **OK** to add the group.

15. Click **OK** to complete the changes to the CUCM LDAP SYNC user.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 1-3: Create New Organizational Unit in Windows

LDAP could be set up to access the Users.SOI.local OU. However, the *Cisco Unified Communications System 8.x SRND* recommends that to optimize the LDAP synchronization, you should include only users that will be using CUCM resources. Importing users that will not be using CUCM resources can increase LDAP sync times, slow CUCM searches and database performance, and in some cases, exceed the recommended number of users in the CUCM database. (Cisco recommends limiting the users to the maximum allowed number of phones for the cluster.) To demonstrate how to narrow the scope of the LDAP synchronization, you will create a new OU and only the users in that OU (and any OUs below that) will be added to CUCM.

In the Server Manager application, right-click the **SOI.local** OU and select **New > Organizational Unit** from the menu.

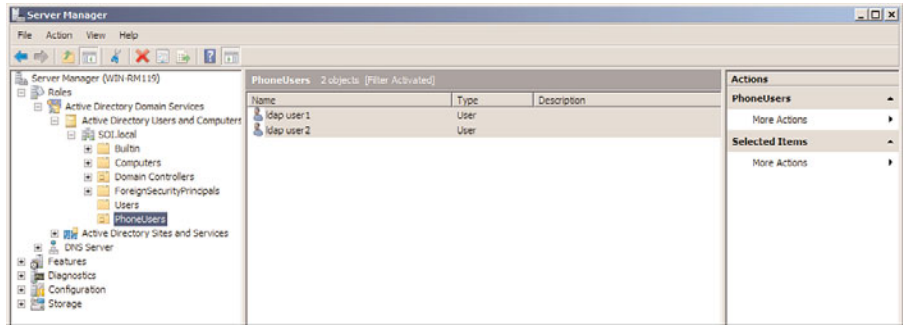
In the New Object – Organizational Unit window, enter **PhoneUsers** in the Name field. Click the **OK** button to create the OU.

Step 1-4: Create End Users in Windows

In the Server Manager application, right-click the **PhoneUsers** OU and select **New > User** from the menu.

1. Enter **ldap** for the First Name.
2. Enter **user1** for the Last Name.
3. Enter **user1** for the User Login Name.
4. Click the **Next** button.
5. Enter **P@$$W0rd** (note the 0 after the uppercase W) for the Password and Confirm Password fields.
6. Deselect the **User must change password at next logon** check box.
7. Select the **Password never expires** check box.
8. Click the **Next** button and then the **Finish** button to create the user.
9. Repeat this step to create a **user2** account. See Figure 9-100 for an example of this page.

Figure 9-100 Two Phone End Users



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Activate DirSync Service in CUCM

From the Navigation drop-down list at the top of the page, choose **Cisco Unified Serviceability** and click the **Go** button.

On the **Cisco Unified Serviceability** page, navigate to **Tools > Service Activation**. Select the check box for **DirSync** (leave the other check boxes as they are) and click the **Save** button. A window will inform you that activating the service will take a while. Click **OK** and wait for the page to refresh. Verify that the service is now listed as Activated.

From the Navigation drop-down list at the top of the page, choose **Cisco Unified CM Administration** and click the **Go** button.

Task 3: Configure CUCM LDAP Synchronization

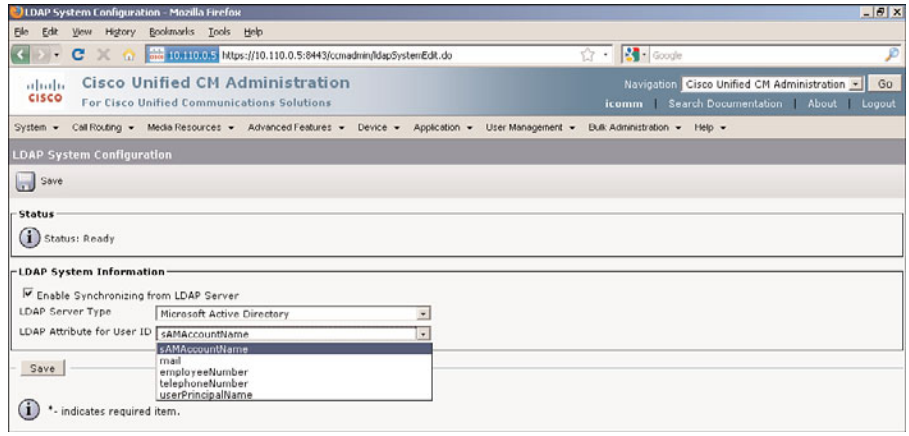
Note: After you set up LDAP synchronization, the users already created in CUCM that do not match an entry in the LDAP system will be marked Inactive. After any account has been inactive for 24 hours, it will be removed from the CUCM system by the Garbage Collection process, which happens at the fixed time of 3:15 a.m. If an account is added to the LDAP system that matches an inactive account and is synchronized before the Garbage Collection routine, it will be kept.

Step 3-1: Configure LDAP System

On the **Cisco Unified CM Administration** page, navigate to **System > LDAP > LDAP System**.

Select the **Enable Synchronizing from LDAP Server** check box. The LDAP Attribute for User ID determines the CUCM user ID and must be unique for the entire system. The **sAMAccountName** item will use the Active Directory login ID as the CUCM user ID, which will be used for this lab. If your company was using employeeNumber for computer logins, that would also be a good candidate. See Figure 9-101 for an example of this page.

Figure 9-101 LDAP System Configuration



Click the **Save** button.

https://t.me/learningnets

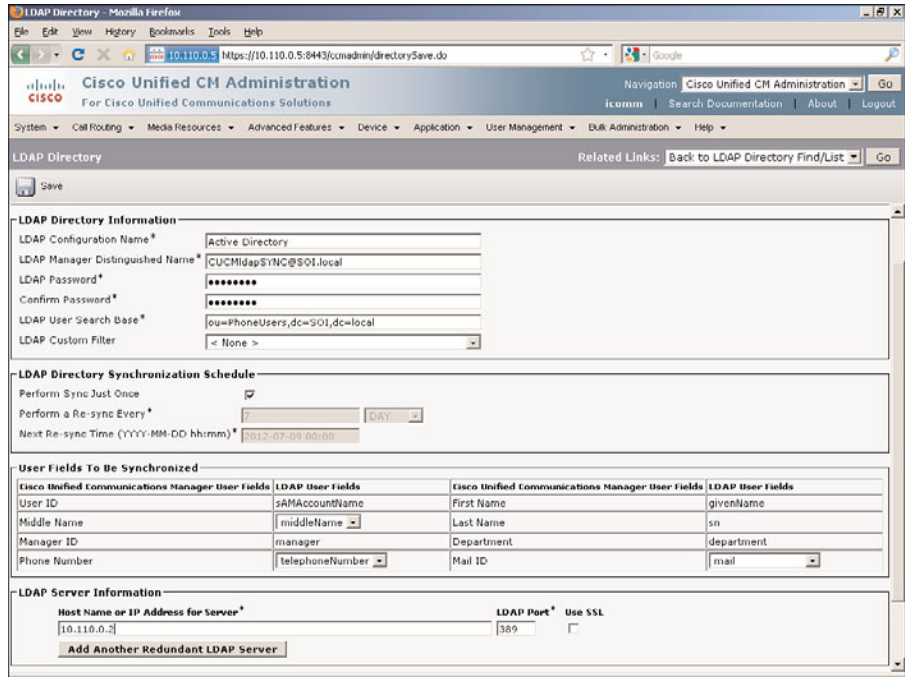
From the Library of Aliwarman Tarihoran

Step 3-2: Configure LDAP Directory

On the **Cisco Unified CM Administration** page, navigate to **System > LDAP > LDAP Directory**.

1. Click the **Add New** button. A warning box will inform you that "Existing end users not found in the corporate directory will be deleted." Click the **OK** button. Another warning box will inform you that the User ID attribute must be unique for LDAP users. Click the **OK** button.
2. In the LDAP Directory Information section, enter **Active Directory** for the LDAP Configuration Name.
3. Enter **CUCMldapSYNC@SOI.local** for the LDAP Manager Distinguished Name.
4. Enter **P@$$W0rd** for the LDAP Password and Confirm Password.
5. Enter **ou=PhoneUsers,dc=SOI,dc=local** for the LDAP User Search Base.
6. In the LDAP Directory Synchronization Schedule section, select the **Perform Sync Just Once** check box. (In production, you should set this on a schedule so that when a new user is added, he will get put into the CUCM system. For this lab, you will manually run the job.)
7. In the LDAP Server Information section, enter the IP address of the Windows server (**10.110.0.2** in this example). See Figure 9-102 for an example of this page.

Figure 9-102 LDAP Directory



8. Click the **Save** button to create the LDAP Directory configuration. If you get an error message, verify the previous actions and make sure to check the case of the letters you entered.
9. To run the LDAP synchronization, click the **Perform Full Sync Now** button. Click **OK** at the warning that you are about to perform a complete sync from the LDAP server.

https://t.me/learningnets

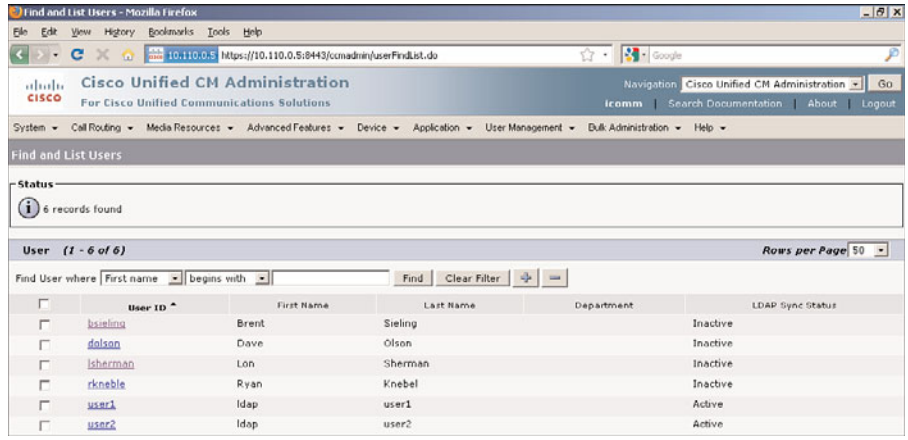
From the Library of Aliwarman Tarihoran

Step 3-3: Verify New Users

To see the results, on the **Cisco Unified CM Administration** page, navigate to **User Management** > **End User** and click the **Find** button to see any existing users.

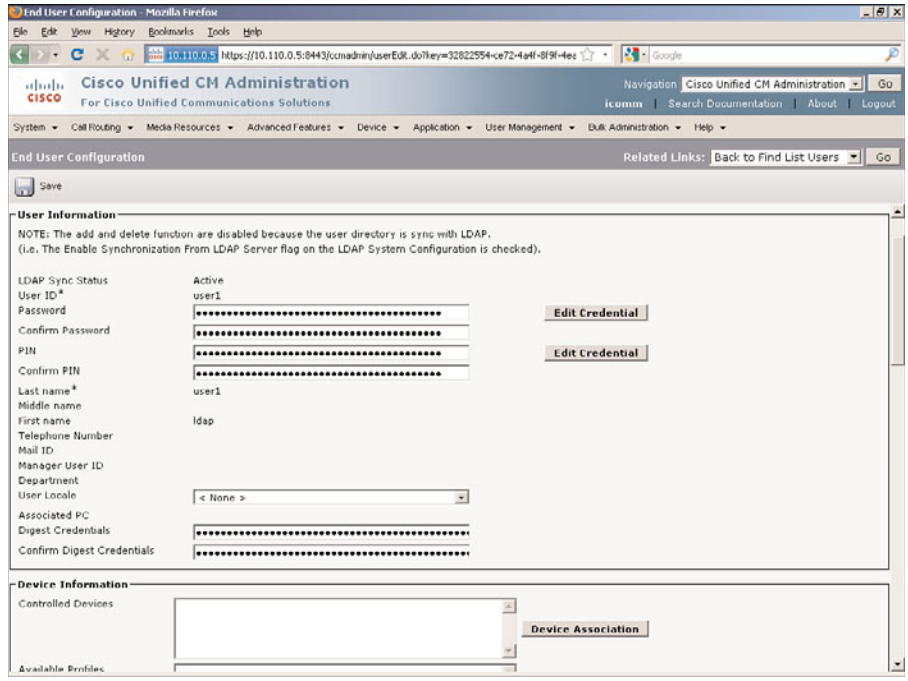
1. You should notice that all the manually and BAT-created users show in the LDAP Sync Status column as Inactive, while there are the two new users that show as Active. See Figure 9-103 for an example of this page.

Figure 9-103 End Users After LDAP Synchronization



2. Click the hyperlinked **user1** name to view the details of the user. (The same is also true for the other users.) You will see that some of the fields, such as User ID, Last Name, First Name, and so on are no longer editable in CUCM, while other fields such as PIN and Controlled Devices are still managed in CUCM. See Figure 9-104 for an example of this page. (Compare this to Figure 9-85 to see the difference.)

Figure 9-104 End-User Details After LDAP Synchronization



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. Before user1 can access the User web pages, she needs to have the user group assigned. Scroll down to the Permissions Information section and click the **Add to User Group** button, and when the Find and List User Groups window opens, click the **Find** button.
4. Select the check box for the **Standard CCM End Users** group.
5. Click the **Add Selected** button to add the user to the group and return to the End User Configuration page.
6. Click the **Save** button.
7. Open a completely different web browser and enter **https://**<*ip_address_of_your_server*>**/ccmuser** (make sure that you enter **ccmuser** at the end), and accept any security certificate warnings. You should be at the Cisco Unified CM User Options page. Enter the user1 just created in Step 1-4 and the password **P@$$W0rd** to attempt to log in. You will not be able to log in, as LDAP synchronization only imports the user details, but their login credentials never leave the LDAP system.
8. Back in the CUCM system in the user1 configuration, enter **cisco** for the Password and Confirm Password fields, and then click the **Save** button.
9. At this point, you can log in to the CUCM User Web Page with **user1** and **cisco**. However, to log in to the Active Directory domain, user1 has to use P@$$W**0**rd.

Step 3-4: Add CUCM User to Active Directory

If you try to log in to the user web pages with the CUCM user account you created manually in Lab 9-7, you will find that you cannot, because the account is inactive. After 24 hours, this account will be removed if not added into Active Directory and the LDAP synchronization run again.

1. In the Windows 2008 Server, with the Server Manager application, right-click the **PhoneUsers** OU and select **New > User** from the menu.
2. Enter your first name for the First Name field.
3. Enter your last name for the Last Name field.
4. Enter your username (the same one used in CUCM) for the User Login Name field.
5. Click the **Next** button.
6. Enter **P@$$W0rd** (note the 0 after the uppercase W) for the Password and Confirm Password.
7. Deselect the **User must change password at next logon** check box.
8. Select the **Password never expires** check box.
9. Click the **Next** button and then the **Finish** button to create the user.

Note: If you plan to continue using LDAP to manage user accounts from this point on, repeat this step for each of the other users in the CUCM that are not in the LDAP directory.

Step 3-5: Resync LDAP

On the **Cisco Unified CM Administration** page, navigate to **System > LDAP > LDAP Directory**.

1. Click the **Find** button if you do not see the Active Directory name.
2. Click the hyperlinked Active Directory name.
3. To run the LDAP synchronization, click the **Perform Full Sync Now** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. Click **OK** at the warning that you are about to perform a complete resync from the LDAP server.

5. To see the results, on the **Cisco Unified CM Administration** page, navigate to **User Management > End User** and click the **Find** button to see any existing users. You should notice that the YourName account shows as Active. You should also be able to log in to the user web page using the **cisco** password (which is still managed in CUCM with only LDAP synchronization).

Task 4: Configure CUCM LDAP Authentication

LDAP authentication redirects all end-user login and password requests to the LDAP system for verification or rejection. (However, all application users are still maintained in CUCM. The End User PIN field is also still maintained in CUCM, as it does not match any field in the LDAP system.)

Step 4-1: Configure LDAP Authentication

On the **Cisco Unified CM Administration** page, navigate to **System > LDAP > LDAP Authentication**.

1. In the LDAP Authentication For End Users section, select the **Use LDAP Authentication for End Users** check box.

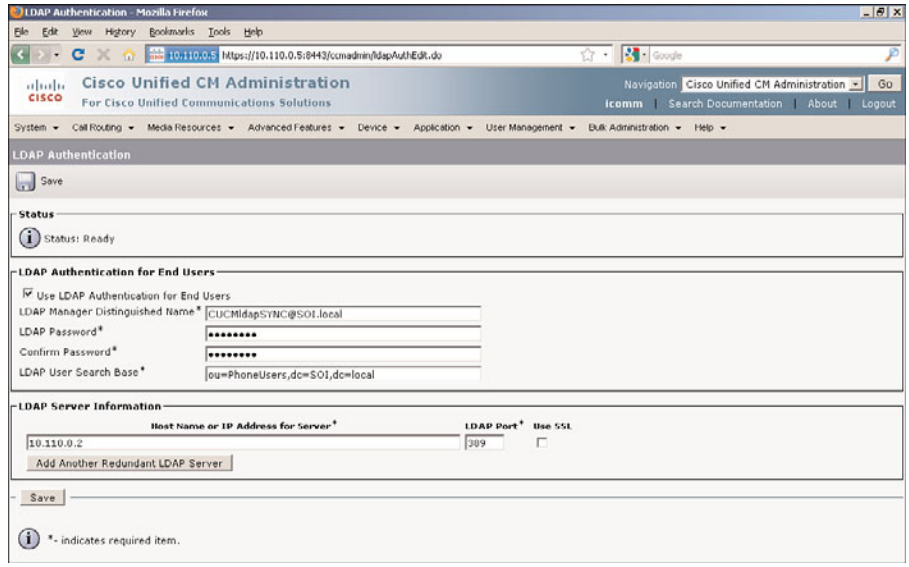
2. Enter **CUCMldapSYNC@SOI.local** for the LDAP Manager Distinguished Name.

3. Enter **P@$$W0rd** for the LDAP Password and Confirm Password.

4. Enter **ou=PhoneUsers,dc=SOI,dc=local** for the LDAP User Search Base.

5. In the LDAP Server Information section, enter the IP address of the Windows server (**10.110.0.2** in this example). See Figure 9-105 for an example of this page.

Figure 9-105 LDAP Authentication



6. Click the **Save** button to implement.

https://t.me/learningnets

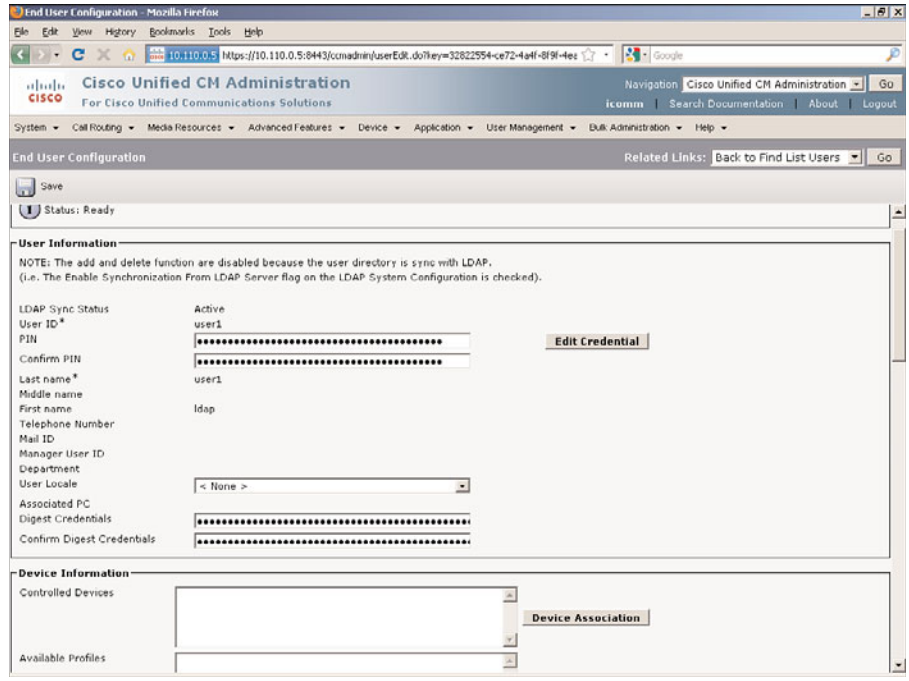
From the Library of Aliwarman Tarihoran

Step 4-2: Verification of End-User Passwords

To see the results, on the **Cisco Unified CM Administration** page, navigate to **User Management** > **End User** and click the **Find** button to see any existing users.

Click the hyperlinked **user1** name to view the details of the user. Notice that the Password field is no longer visible (but the PIN field can be changed). See Figure 9-106 for an example of this page. (Compare this to Figures 9-104 and 9-85 to see the differences.)

Figure 9-106 End Users After LDAP Authentication



You should also be able to log in to the user web page, but now using the **P@$$W0rd** password (which is managed only in LDAP).

Task 5: Clean Up

When you are done experimenting with LDAP, either make sure that all the end users show as Active and plan to have the Windows server up from now on, or revert to your previous copy or VMware snapshot.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

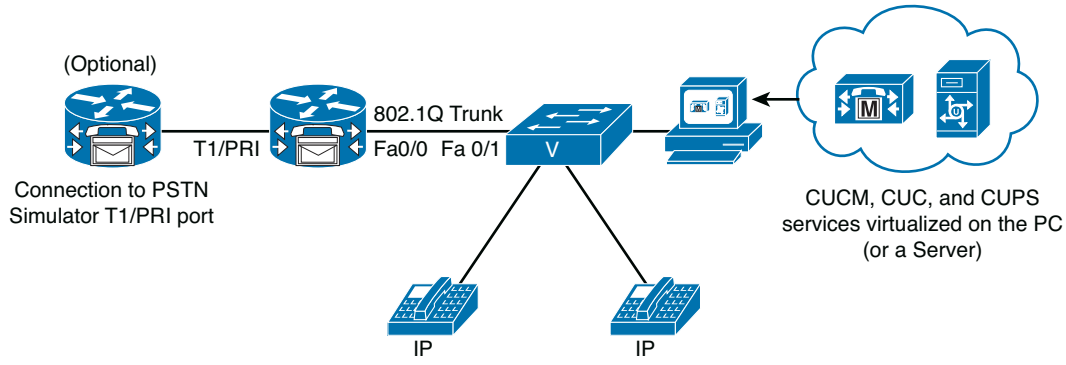
CHAPTER 10

CUCM Dial Plan

This chapter explores the connection of a Cisco Unified Communications Manager (CUCM) system to the public switched telephone network (PSTN) and branch offices. Configuring CUCM to route calls can be a complex endeavor, with many components involved. With the requirements to cover failover in the event of overloaded WAN links or hardware failure added to the design, the complexity increases even more. The labs in this chapter demonstrate the basics of call routing, failover, and call control.

Lab 10-1: Call Routing

Figure 10-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- Configuration from Lab 9-5, 9-6, 9-7, 9-8, or 9-9
- Two or more IP Phones registered (desk phone or soft phone on PC or Windows VM)

Optional hardware components (see Scenario for details):

- Cisco router configured as a PSTN Simulator
- T1/E1/PRI Multiflex Trunk Voice/WAN Interface Cards (VWIC) or network modules
- Digital signal processor (DSP) resources in the routers (Packet Voice Digital Signal Module [PVDM] chips) to enable the Multiflex Trunks

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Learning Objectives

Upon completion of this lab, you will be able to

- Add devices to CUCM
- Configure route groups in CUCM
- Configure route lists in CUCM
- Configure route patterns in CUCM
- Understand call routing in CUCM

Scenario

Shiny Objects Inc. (SOI) has calls working between phones at headquarters. It now wants a connection to make and receive calls from the PSTN.

Note: Having T1/PRI interfaces and a PSTN Simulator is not necessary to complete the lab. However, without those items, you will not be able to test your configuration.

This lab is based on the configuration from Lab 9-5, 9-6, 9-7, 9-8, or 9-9. Verify that you can call between the VoIP phones. Troubleshoot if necessary.

Task 1: Examine CUCM Call-Routing Logic

Before configuring call routing in CUCM, a basic understanding of the wildcards, call logic, and how external route patterns are configured is necessary.

Step 1-1: Understanding CUCM Wildcards

Note: The patterns in this lab are built using the North American Numbering Plan (NANP). Be aware that outside of the NANP, different patterns might apply. For example, in the NANP, the emergency services number is 911, but in European Union countries, users dial 112 for emergency services.

CUCM does not use exactly the same wildcards as Cisco Unified Communications Manager Express (CUCME). Although some items are the same, there are some differences to be aware of. Table 10-1 list the most common wildcards used in CUCM.

Table 10-1 Common Wildcards Used in CUCM Patterns

Wildcard	Description
X	Matches any *single* digit from 0 to 9. (The *X* must be uppercase. In some areas, CUCM will change a lowercase *x* to uppercase for you, but in other areas, it will not, so get into the habit of using the uppercase *X*.) A pattern of 30XX would match digits from 3000 to 3099. A pattern of 30X0 would only match 3000, 3010, 3020, 3030, 3040, 3050, 3060, 3070, 3080, or 3090.
Period (.) (also called dot)	Used to indicate which digits are to be stripped. Unlike CUCME, CUCM does not automatically strip digits, so items like outside-line access digits need to be marked to be stripped. For example, if a 9 is the outside-line access digit, a pattern such as 9.XXXXXXX indicates that the digits before the dot (the 9) should be stripped off before being sent to the PSTN.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Wildcard	Description
Square brackets ([])	Match a set or range of numbers for any *single* digit. Individual numbers can be listed or separated by commas. The hyphen (-) is used for a consecutive range. Thus, [5-8], [5,6,7,8], or [5678] would select numbers from 5 to 8 for a single digit. A pattern of 300[0-3] would match 3000 to 3003. Note: The brackets only match a single digit, so it is not possible to match a range of numbers that spans more than a single digit. Thus, 5523 to 5546 *cannot* be matched as 55[23-46], as that pattern would only cover 552, 553, 554, and 556. Likewise, using two brackets to match 5523 to 5546 *cannot* be done as such: 55[2-4][3-6]. That pattern will only match 5523 to 5526, 5533 to 5536, and 5543 to 5546. Each bracket works independently. The only way to match a range, such as 5523 to 5546, is to use three separate patterns such as this: 552[3-9], 553X, and 554[0-6].
Caret (^)	The caret (sometimes also called a circumflex), when used inside brackets, designates a number or range to *exclude*. A pattern of 300[^0-6] would match 3007 to 3009, while a pattern of 300[^0^2] would match 3001 and 3003 to 3009. Note that if not in front of a range, the caret should appear in front of every digit to be excluded.
Exclamation point (!)	Matches one *or more* digits in the range of 0 to 9. This is very useful when constructing patterns for international calls, as the number of digits used by a foreign PSTN can vary. However, unlike in CUCME, the pound digit (#) does not automatically signify the end of the dialed string. As a result, the "end of dialing" behavior of the pound digit must be included in the patterns created. Note: This is typically used with the international access digits before the !. (In the NANP, a pattern of 011! would work.)
Pound (#)	This is a valid dialed digit in CUCM, and it does not automatically signal the end of dialed digits. However, the # is usually added to route patterns with unknown length to signal the end of dialed digits, matching the same behavior as CUCME.
At sign (@)	A macro that represents patterns that cover the selected national dial plan. The *Cisco Unified Communications System 8.x SRND* recommends not using this wildcard for the following reasons: ■ Configures a large number of dial plan entries in the database. A single 9.@ macro for the NANP really adds 166 individual route patterns. ■ The actual patterns used are unknown. ■ Problematic when trying to override patterns to block numbers, such as 1-900 numbers. ■ Complicates troubleshooting, because the patterns used are unknown.

With an understanding of how wildcards are used, it is time to examine the call-routing logic.

Step 1-2: Understanding CUCM Call-Routing Logic

CUCM uses the best match when comparing dialed digits to route patterns. However, it does not stop when it finds a match, because there might be other patterns that match when more digits are dialed. This is in contrast to CUCME, which stops matching when a match has been found. If you recall from Chapter 6, "Cisco Unified Communications Manager Express (CUCME) Dial Plans and QoS,"

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CUCME considers the largest number of nonwildcard digits matching as the best match, and in the case of a tie, randomly selects one of the matching patterns. CUCM, however, evaluates the lowest number of possible matches to each pattern, as shown in the "Call-Routing Behavior" section of the *CCNA-Voice 640-461 Official Cert Guide*.

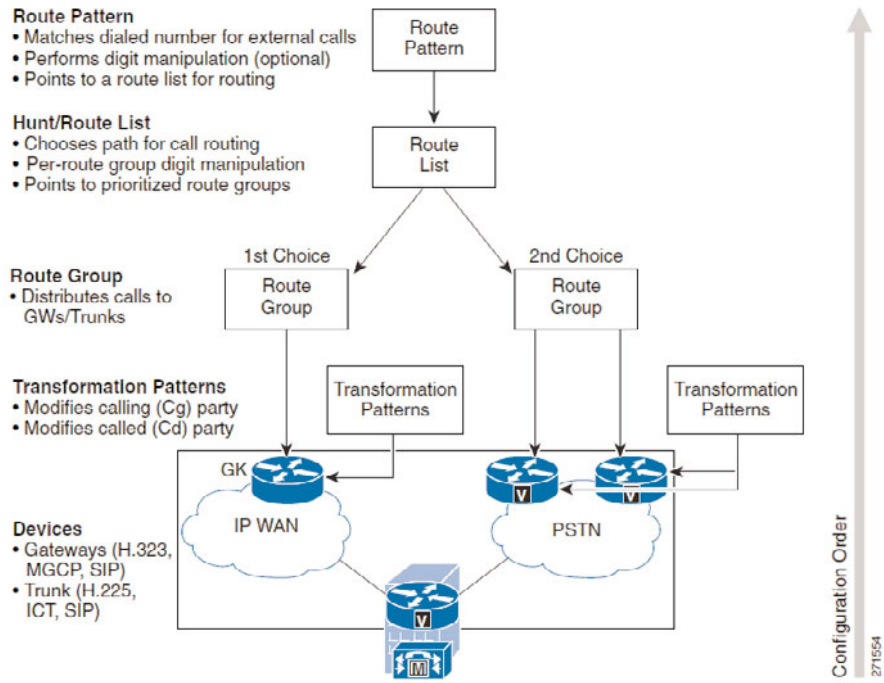
You might ask, "If CUCM waits for more digits, does it have to wait on a pattern such as 911 if there is another pattern for a local, seven-digit call, such as 9XXXXXXX?" By default, the answer is yes. The exception to waiting for more digits is that a route pattern can be marked as urgent in CUCM. This causes the urgent pattern to be selected as soon as it matches. This allows the 911 pattern (marked as urgent) to match and be used as soon as the digits are dialed, just as in CUCME.

Step 1-3: Understanding CUCM Call-Routing Architecture

Before configuring call routing in CUCM, the architecture of the call-routing components and services needs to be examined. Using Figure 10-2, examine the path from dialing digits to the PSTN (or WAN) connection. Moving down the diagram, these steps are followed:

1. The dialed digits need to match a route pattern, as discussed in Steps 1-1 and 1-2. The route pattern is connected to a route list.
2. The route list chooses the path the call will take by pointing to route groups. For example, the desired path to a branch office is to use the WAN, but if the WAN is down, the call uses the PSTN.
3. The route group is a collection of devices that connect to the destination. More than one device can be in a route group for failover or for increasing capacity and load balancing.
4. The call is sent from the device to the connected network.

Figure 10-2 External Route Pattern Architecture



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

While the call flow goes in the order described in Figure 10-2, the configuration order is the exact opposite. (Thus, the devices need to be configured before route groups can be created, and so on.) To help remember the order in which the items are configured, just remember that they are configured in alphabetical order: *d*evices, route *g*roup, route *l*ist, and route *p*attern. It also helps that CUCM has them listed in the menu in the order that they are created as well.

Note: Although this lab book strives to introduce the basics of CUCM call routing, there are many different ways to implement it. Designing a dial plan for an enterprise is one of the few tasks that cannot be easily corrected if done wrong. (Try telling everyone in the company that he or she has new telephone numbers!) For more information about advanced dial plan and call routing, read the *Cisco Unified Communications System 8.x SRND* section "Unified Communications Call Routing" > "Dial Plan" > "Design Considerations," especially the section "Globalized Design Approach Using Local Route Groups."

Task 2: Create Devices in CUCM

Connect to the CUCM web pages using the methods discussed in Chapter 8, "Administrative Interfaces." Log in with your application user (icomm), accept any security certificate warnings, and if the page is not on the Cisco Unified CM Administration page, use the Navigation drop-down list at the upper right to select the **Cisco Unified CM Administration** item and click **Go**.

There are multiple types of devices that can be created in CUCM. Creating gateways is a topic for the CVOICE exam, so this lab only shows two types that you can create. If you do not have access to a router with T1/PRI interfaces or a PSTN Simulator, complete Step 2-1 to create a dummy H.323 gateway. (Without at least a single gateway, you cannot create a route group.) If you have access to a router with T1/PRI interfaces and a PSTN Simulator, skip ahead to Step 2-2.

Step 2-1: (Optional) Create a Dummy H.323 Gateway

This step is only necessary if you do not have access to a router with T1/PRI interfaces and the PSTN Simulator. It will allow you to create the route gateway, route list, and route patterns, but you will not be able to test them.

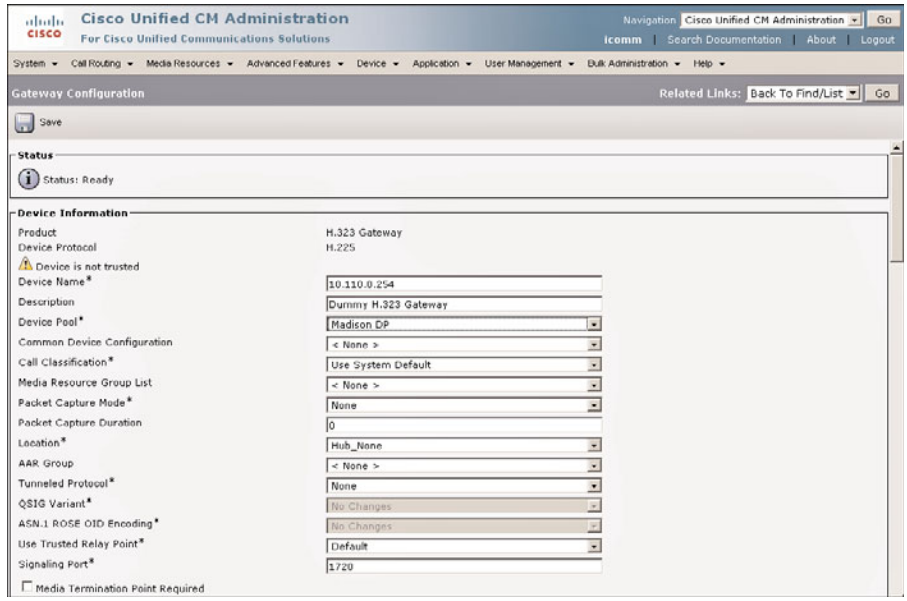
On the Cisco Unified CM Administration page**,** navigate to **Device > Gateway**.

1. Click the **Add New** button.
2. From the Gateway Type drop-down list, select **H.323 Gateway** and click the **Next** button.
3. Because the gateway does not actually exist, enter the last usable IP address for your data network in the Device Name field.
4. Enter **Dummy H.323 Gateway** in the Description field.
5. From the Device Pool drop-down list, select **Madison DP**. See Figure 10-3 for an example of this page.
6. Click the **Save** button to create the gateway.
7. You should see a pop-up window telling you to click the **Apply Config** button, but the button is not active at this time.
8. Click **OK** to close the pop-up window.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-3 Creating a Dummy H.323 Gateway



Step 2-2: Prep the Router to Become an MGCP Gateway

Media Gateway Control Protocol (MGCP) is one of the easiest gateways to configure on the router, as the CUCM system will do most of the configuration of the router for you. The flip side of this is that you will need to give CUCM more information about the router hardware so that CUCM can send the right commands.

It is best to configure the domain name on the router now, as CUCM will prepare the configuration for the router using the router host name and domain name. The host name is added in front of the domain name assigned to the router to make a Fully Qualified Domain Name (FQDN). If the router does not have a domain name now, realize that this would change if other functions, such as Secure Shell (SSH), were implemented later, and then the CUCM configuration would break. Because the router is part of SOI, establish soi.local as the domain name. The domain name is case sensitive and must match on both router and CUCM configuration.

```
RtrPodx(config)# ip domain-name soi.local
```

When the router is later told to contact CUCM to get the MGCP configuration, CUCM will identify the router by the full FQDN (host name plus domain name). For example, the Pod 1 router would have RtrPod1.SOI.local for the FQDN.

The router needs to have the basics of the T1/PRI configured for MGCP to work. Follow the steps from Lab 6-2, Step 2-1 up through Step 3-2. Here is a short version of the commands, assuming that the T1/PRI interface is in 0/2/0. (Note: the **card type** command is only needed for combined T1/E1 cards.)

```
RtrPodx(config)# card type t1 0 2
RtrPodx(config)# isdn switch-type primary-ni
RtrPodx(config)# network-clock-participate wic 2
```

https://t.me/learningnets

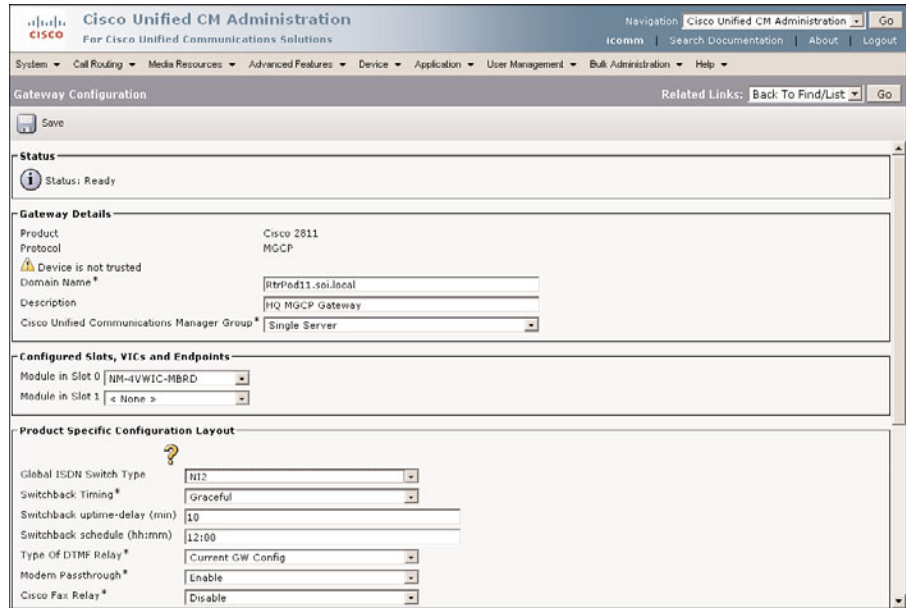
From the Library of Aliwarman Tarihoran

Step 2-3: Create the MGCP Gateway in CUCM

On the **Cisco Unified CM Administration page,** navigate to **Device > Gateway**.

1. Click the **Add New** button.
2. From the Gateway Type drop-down list, select your router model and click the **Next** button.
3. From the Protocol drop-down list, select **MGCP** and click the **Next** button.
4. Enter the FQDN of the router (as noted in Step 2-2) in the Domain Name field. (Make sure that the case of the letters matches the entries on the router exactly.)
5. Enter **HQ MGCP Gateway** in the Description field.
6. From the Cisco Unified Communications Manager Group drop-down list, select **Single Server**.
7. In the Configured Slots, VICs and Endpoints section, select the hardware where the T1/PRI interface is located. The selection can seem a bit strange at first. For example, if you have a 2811 router with a T1/PRI on VWIC card, the 2811 has four onboard slots, so from the **Module in Slot 0** drop-down list, select **NM-4VWIC-MBRD** (which says there are four VWIC slots on the motherboard, even though you will not see the individual VWIC slots until after you save the gateway configuration). If your router has a T1/PRI on a network module, select the module from the **Module in Slot 1** drop-down list.
8. To match the PSTN Simulator, in the Product Specific Configuration Layout section, from the Global ISDN Switch Type drop-down list, select **NI2**. See Figure 10-4 for an example of this page.

Figure 10-4 Creating an MGCP Gateway



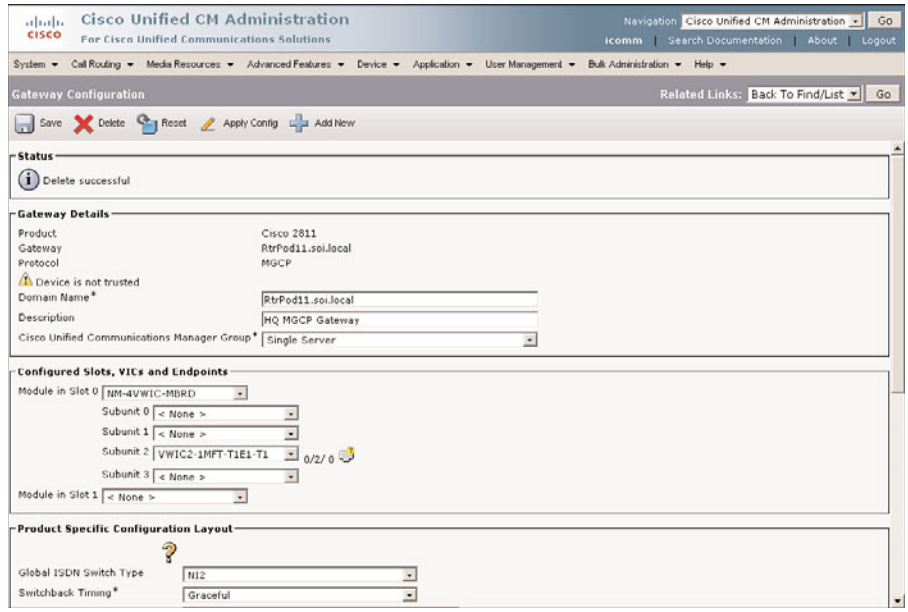
9. Click the **Save** button to create the gateway. You should see a pop-up window telling you to click the **Apply Config** button, but the button is not active at this time.
10. Click **OK** to close the pop-up window.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

11. With the gateway configuration saved, if you are using a VWIC, the subunits under the Module in Slot 0 field are now present. From the correct subunit (where the VWIC is installed) drop-down list, select your VWIC type and, if necessary, the mode (for cards that operate as a T1 or E1). In Figure 10-5, a 2811 router with a VWIC2-1MFT-T1/E1 card in HWIC slot 2 needs to be selected as VWIC2-1MFT-T1E1-T1 to operate in T1 mode instead of E1.
12. Click the **Save** button to create the gateway. You should see a pop-up window telling you to click the **Apply Config** button.
13. Click **OK** to close the pop-up window.
14. After the configuration is saved, an icon of a telephone jack with a yellow question mark will show next to the subunit or module. See Figure 10-5 for an example of this page.

Figure 10-5 MGCP Gateway Configuration

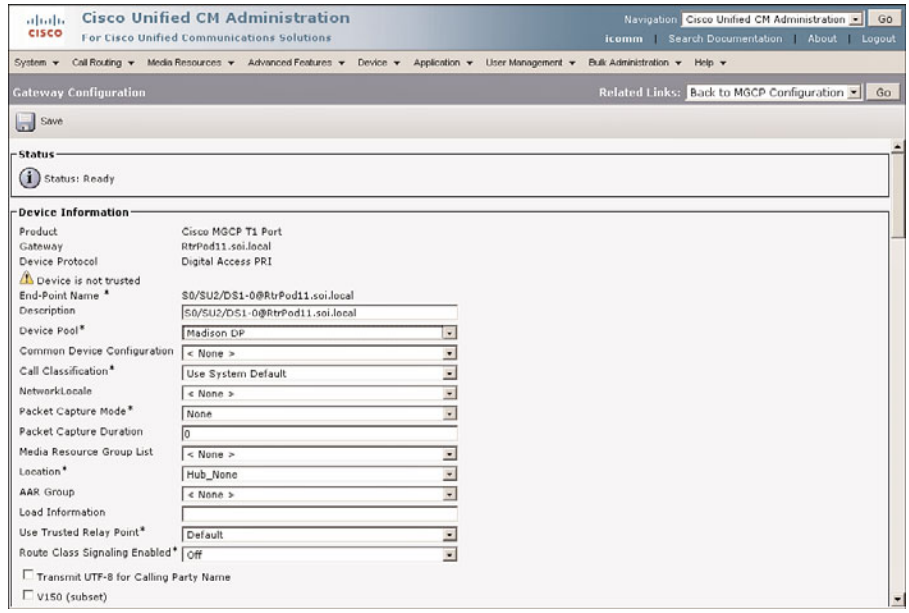


15. Click the icon of a telephone jack with a yellow question mark to configure the interface.
16. The Find and List Gateway page will open. From the Device Protocol drop-down list, choose **Digital Access PRI** and click the **Next** button.
17. The Gateway Configuration page will open to show the details for the interface. Notice that the End-Point Name field shows the port name and the FQDN of this interface (for example, S0/SU2/DS1-0@RtrPod11.soi.local, as shown in Figure 10-6).
18. From the Device Pool drop-down list, select **Madison DP**. See Figure 10-6 for an example of the top of this page.
19. Scroll down to the Interface Information section. If your PSTN Simulator is using fractional PRI (not all 23 channels active—which is likely, because of DSP resources), change the Channel Selection Order drop-down list to **Top Down** (or see the note regarding fractional PRIs).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-6 Gateway Configuration – Part 1



Note: CUCM assumes that you are using full PRI circuits (all 23 voice channels), rather than fractional PRIs. By changing the Channel Selection Order field to Top Down, the PRI will start with the lowest channel number. Another option is to limit the voice channels to the number configured by the PSTN by signaling that the unused channels are busy. The Cisco document "Busy-Out ISDN B-Channels in Cisco CallManager Configuration Example" shows how to configure this method. However, this is more of a troubleshooting solution, as only five devices in the system can be configured with this process.

20. Select the **Enable status poll** check box.
21. Under the Call Routing Information – Inbound Calls section, from the Significant Digits drop-down list, select **4**.
22. In the Call Routing Information – Outbound Calls section, from the Calling Party Presentation drop-down list, select **Allowed** (to allow caller ID information). See Figure 10-7 for an example of the middle of this page.
23. In the PRI Protocol Type Specific Information section, select the **Display IE Delivery** check box (to allow the ISDN PRI caller ID info).
24. Select the **Redirecting Number IE Delivery – Outbound** check box. See Figure 10-8 for an example of the lower-middle portion of this page.
25. Click the **Save** button to commit the changes.
26. Click **OK** to close the pop-up window.
27. With the Related Links drop-down list set to **Back to MGCP Configuration**, click the **Go** button.

The icon of a telephone jack next to the port should not have a yellow question mark anymore; instead there should be "T1PRI" under the jack icon in tiny, red letters. This indicates that the jack for the router has been correctly configured.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-7 Gateway Configuration – Part 2

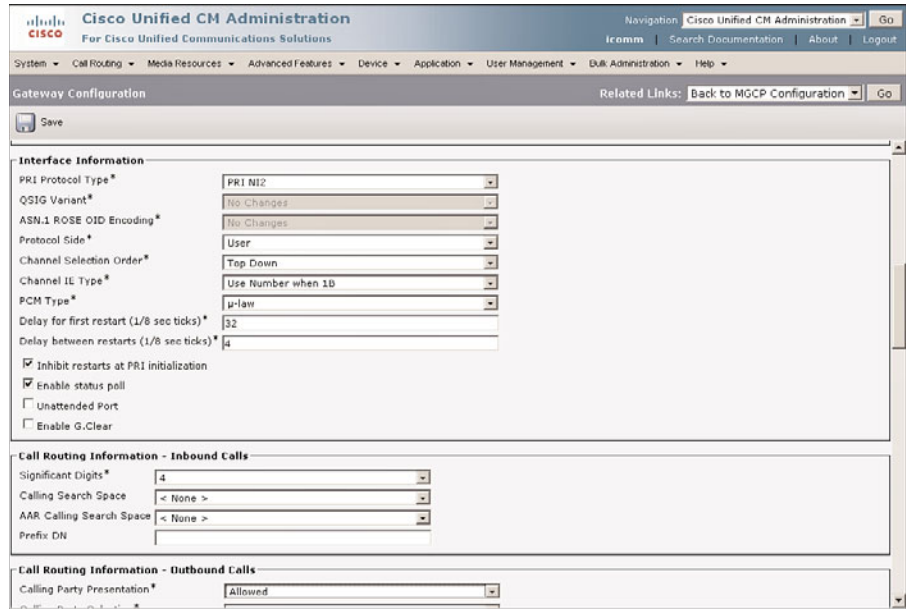
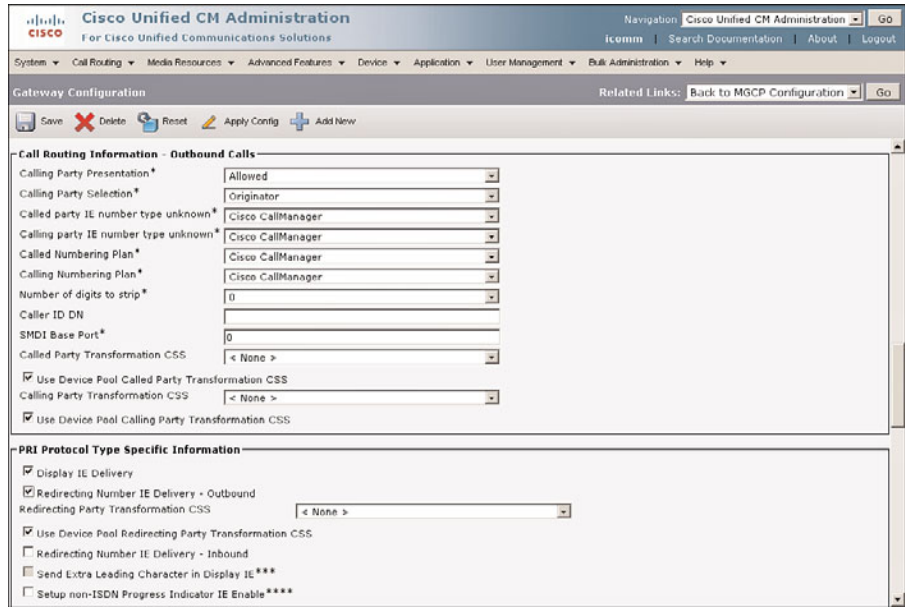


Figure 10-8 Gateway Configuration – Part 3



Step 2-4: Activating the MGCP Gateway on the Router

The router needs to be told how to reach the CUCM that will send the configuration and commands to control the calls. The **ccm-manager** command informs the router of the IP address of the TFTP server where the configuration is stored and tells it to use the TFTP server to get the configuration (the same way that phones get their configuration). Because the CUCM server is the TFTP server in this lab, use the IP address of your server.

```
RtrPodx(config)# ccm-manager config server <CUCM_IP_Address>
RtrPodx(config)# ccm-manager config
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

After the commands are entered, the CLI of the router should show that the router is being configured from the CUCM server, as shown in Example 10-1. If you do not see any changes to the router, verify that the host name and domain name are entered into the CUCM correctly. (They are case sensitive.)

Example 10-1 Output from MGCP Configuration

```
RtrPod11(config)#
Loading RtrPod11.soi.local.cnf.xml from 10.110.0.5 (via FastEthernet0/0.110): !
[OK - 4844 bytes]


This package type is not the default package type.


Sep  5 04:33:48.755: %CONTROLLER-5-UPDOWN: Controller T1 0/2/0, changed state to
  administratively down
RtrPod11(config)#



Sep  5 04:33:54.748: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:0,
  changed state to down
Sep  5 04:33:54.748: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:1,
  changed state to down
Sep  5 04:33:54.748: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:2,
  changed state to down
Sep  5 04:33:54.748: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:3,
  changed state to down
Sep  5 04:33:54.752: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:4,
  changed state to down
Sep  5 04:33:54.752: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:5,
  changed state to down
Sep  5 04:33:54.752: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:6,
  changed state to down
Sep  5 04:33:54.756: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:7,
  changed state to down
Sep  5 04:33:54.756: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0:8,
  changed state to down
Sep  5 04:33:54.756: %LINEPROT
RtrPod11(confi
O-5-UPDOWN: Line protocol on Interface Serial0/2/0:9, changed state to downg)#
RtrPod11(config)#


The MGCP process is currently active.
It must be disabled with 'no mgcp' before restarting.
Building configuration...


[OK]
Sep  5 04:33:58.460: %CMAPP-6-CONFIG_DONE: Configuration by CCM is done


Sep  5 04:33:58.848: %CONTROLLER-5-UPDOWN: Controller T1 0/2/0, changed state to up
RtrPod11(config)#
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
Sep  5 04:34:00.848: %LINK-3-UPDOWN: Interface Serial0/2/0:23, changed state to up
RtrPod11(config)#
Sep  5 04:34:01.212: %ISDN-6-LAYER2UP: Layer 2 for Interface Se0/2/0:23, TEI 0
  changed to up
RtrPod11(config)#
Loading RtrPod11.soi.local.cnf.xml from 10.110.0.5 (via FastEthernet0/0.110): !
[OK - 4844 bytes]
```

The **show ccm-manager** command can verify that CUCM is configuring the router (or provide information if there are problems). In the following output from Pod 11, the router has registered to the CUCM server, two configurations were downloaded, and one configuration was installed.

```
RtrPod11(config)# exit
RtrPod11# show ccm-manager
MGCP Domain Name: RtrPod11.soi.local
Priority        Status                  Host
============================================================
Primary         Registered              10.110.0.5
First Backup    None
Second Backup   None

Current active Call Manager:    10.110.0.5
Backhaul/Redundant link port:   2428
Failover Interval:              30 seconds
Keepalive Interval:             15 seconds
Last keepalive sent:            23:37:16 cdt Sep 4 2012 (elapsed time: 00:00:02)
Last MGCP traffic time:         23:37:16 cdt Sep 4 2012 (elapsed time: 00:00:02)
Last failover time:             None
Last switchback time:           None
Switchback mode:                Graceful
MGCP Fallback mode:             Not Selected
Last MGCP Fallback start time:  None
Last MGCP Fallback end time:    None
MGCP Download Tones:            Disabled
TFTP retry count to shut Ports: 2

Backhaul Link info:
    Link Protocol:      TCP
    Remote Port Number: 2428
    Remote IP Address:  10.110.0.5
    Current Link State: OPEN
    Statistics:
        Packets recvd:   5
        Recv failures:   0
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
        Packets xmitted: 6
        Xmit failures:   0
    PRI Ports being backhauled:
        Slot 0, VIC 2, port 0
Configuration Auto-Download Information
=======================================
Current version-id: 1346819500-bd944016-062a-4d9f-8cb6-c5cb2dfa0a27
Last config-downloaded:00:00:00
Current state: Waiting for commands
Configuration Download statistics:
        Download Attempted              : 2
          Download Successful           : 2
          Download Failed               : 0
          TFTP Download Failed          : 0
        Configuration Attempted         : 1
          Configuration Successful      : 1
          Configuration Failed(Parsing): 0
          Configuration Failed(config) : 0
Last config download command: New Registration
FAX mode: disable
Configuration Error History:
```

Task 3: Create Route Group in CUCM

Now that a device is created, the next item, moving up the chain, is the route group.

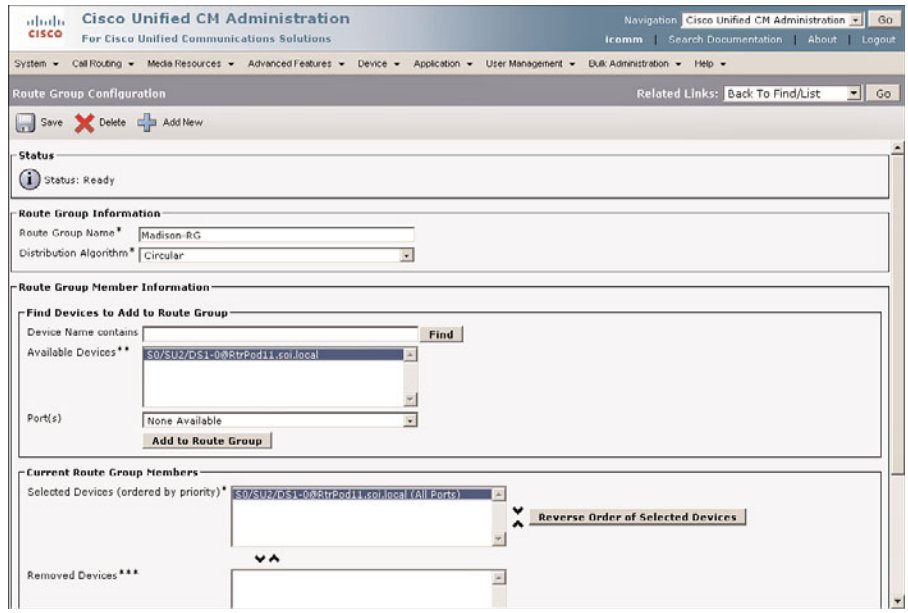
On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Group**.

1. Click the **Add New** button.
2. In the Route Group Name field, enter **Madison-RG**.
3. In the Find Devices to Add to Route Group section, the interface/gateway device you just created should be listed in the Available Devices box. (Use the H.323 gateway from Step 2-1 if you do not have a T1/PRI connection to the PSTN Simulator.) Click the **Add to Route Group** button.
4. The interface/gateway device should now be listed in the Current Route Group Members section in the Selected Devices (Ordered by Priority) box. See Figure 10-9 for an example of this page.
5. Click the **Save** button to create the route group.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-9 Route Group Configuration



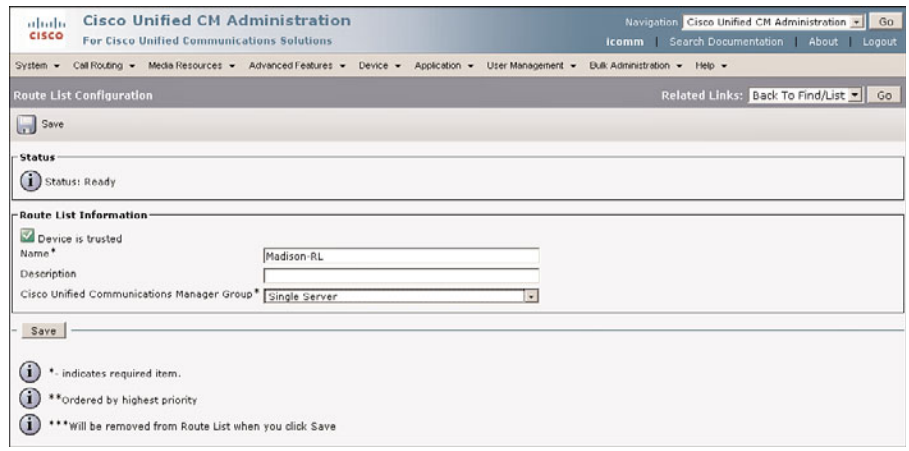
Task 4: Create Route Lists in CUCM

With a route group created, the next item, moving up the chain, is the route list.

On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route List**.

1. Click the **Add New** button.
2. In the Name field, enter **Madison-RL**.
3. In the Cisco Unified Communications Manager Group drop-down list, select **Single Server**. See Figure 10-10 for an example of this page.

Figure 10-10 Route List Configuration

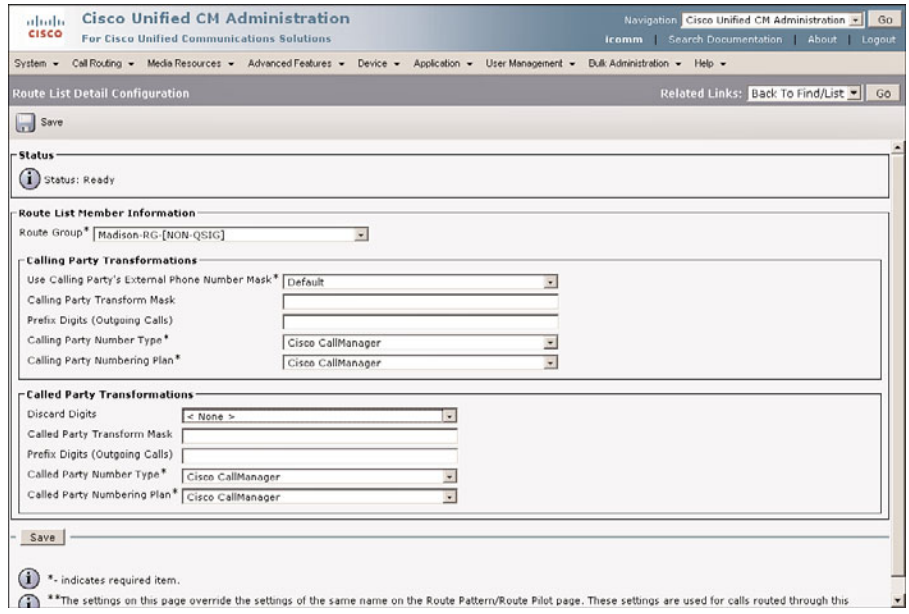


https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. Click the **Save** button to create the route list.
5. After the route list is saved, the Route List Member section shows. Click the **Add Route Group** button.
6. The Route List Detail Configuration page will open. From the Route Group drop-down list, select **Madison-RG-[NON-QSIG]**. Note that there are various options to transform the calling party's and called party's numbering plan. For example, these options could be used when four-digit calls to extensions over the WAN need to be redirected to the PSTN because of a WAN failure. Four-digit numbers will not work on the PSTN, so they need to be expanded into local, long-distance, or even international numbers. The Transformations sections can modify the digits for the calls that go over the PSTN without modifying the WAN calls. Leave the transformations at the current defaults. See Figure 10-11 for an example of this page.

Figure 10-11 Route List Detail Configuration



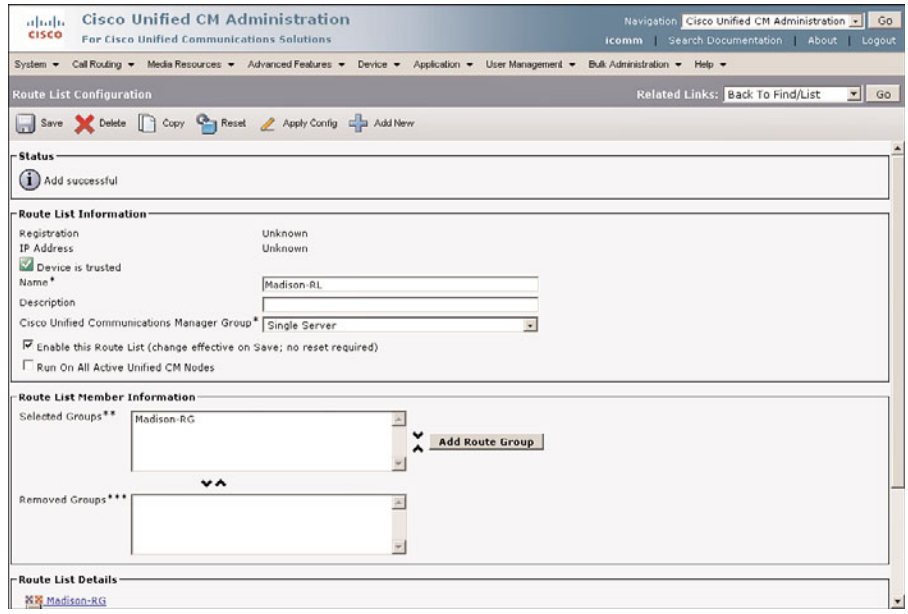
7. Click the **Save** button to create the route list details. You should see a pop-up window telling you that you need to reset the route list for the changes to take effect.
8. Click **OK** to close the pop-up window.
9. The Route List Configuration page will open and show Madison-RG in the Selected Groups area under the Route List Member Information section. See Figure 10-12 for an example of this page.
10. To make sure that the route list details changes take effect, click the **Save** button and then the **Reset** button.
11. The Route List Information section will update and show the registration status as Registered with Cisco Unified Communications Manger.

Note: If you scroll down in the route list, at the bottom are icons for the route list details. Click the icon if you ever need to change the route list details in the future.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-12 Updated Route List Configuration



Task 5: Create Route Patterns in CUCM to Build a Dial Plan to Match the North American Numbering Plan (NANP)

The final element to configure in call routing is the route pattern. Route patterns are what CUCM needs to match calls that will leave the system. If no pattern exists (and the digits do not match internal extensions), the phones just display "Enter number," no matter how many digits you dial. Typically, there are several patterns created to match various call categories, such as local calls, emergency services, long-distance, toll-free, and so on. Refer back to Lab 6-4, Task 4, Step 4-1 to review details about the NANP.

Step 5-1: Creating a Seven-Digit Local Calls Route Pattern

In this route pattern, you will create a match for seven-digit local calls. (Local numbers using ten digits will be covered in the next step.) A 9 will be used to access an outside line. As noted in Table 10-1, the period (.) is used to indicate leading digits to be stripped off (such as the outside-line access digit). Lab 6-4, Task 4 explains the NANP, including the fact that the first digit of the area code and central office code (exchange) cannot start with a 0 or a 1, as those are reserved. To avoid incorrect calls being routed to the PSTN, the pattern will limit the first digit (after the outside access digit) to 2 through 9.

On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Pattern**.

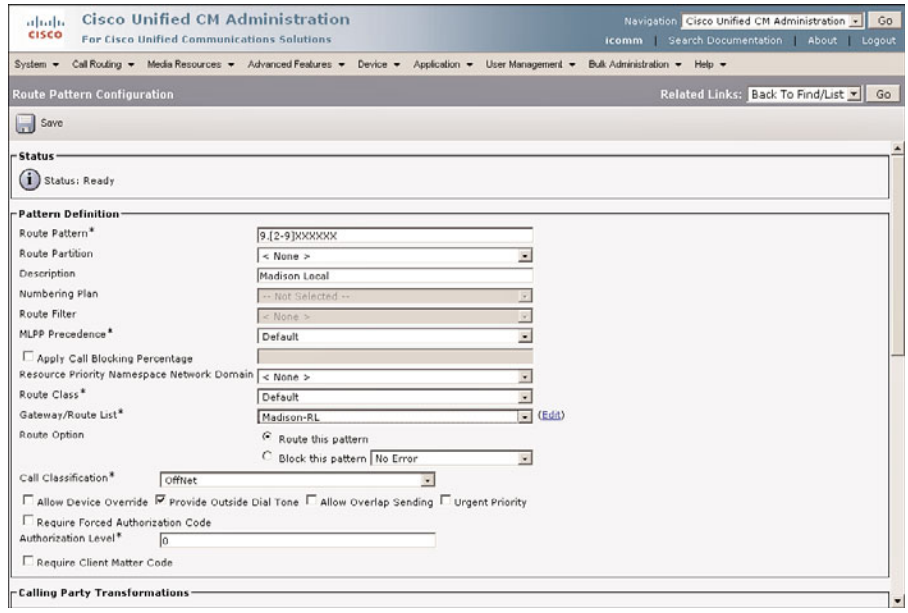
1. Click the **Add New** button.
2. In the Route Pattern field, enter **9.[2-9]XXXXXX**.
3. In the Description field, enter **Madison Local**.
4. From the Gateway/Route List drop-down list, select **Madison-RL**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

5. Notice that the Provide Outside Dial Tone check box is already selected. This provides the expected secondary dial tone after the 9 is dialed to get an outside line. See Figure 10-13 for an example of this page.

Figure 10-13 Local Calls Route Pattern Configuration – Part 1



If we place a call to the PSTN, the calling party number will be just the four-digit extension. The PSTN provider might reject the call or people receiving the call will not be able to return it from their caller ID. One solution is to transform the calling party number to expand it to match the requirements of the PSTN provider. In this case, you will expand the four-digit extension to a ten-digit number. As mentioned previously, there are many places the number can be transformed:

a. In the line settings (when a directory number is assigned to a phone). The External Phone Number Mask (EPNM) can use wildcards to determine the caller ID information sent. For example, a mask of 510555XXXX uses the wildcards to create a ten-digit number using the extension number.

b. In the route pattern. If the **Use Calling Party's External Phone Number Mask** check box is selected, the EPNM on the line is used. However, if the **Calling Party Transform Mask** field is filled in, it overrides the EPNM on the line.

c. In the route list details (as just discussed in Task 4). The **Use Calling Party's External Phone Number Mask** drop-down list defaults to using the EPNM from the line (or the route pattern). If the **Calling Party Transform Mask** field is filled in on the route list, it overrides the EPNM assigned on either the line or the route pattern.

This lab will use the **Calling Party Transform Mask** in the route pattern to transform the extension to a PSTN-routable number. For more details on this topic, see the "Calling and Called Party Transformation" section in the *Cisco Unified Communications Manager System Guide*.

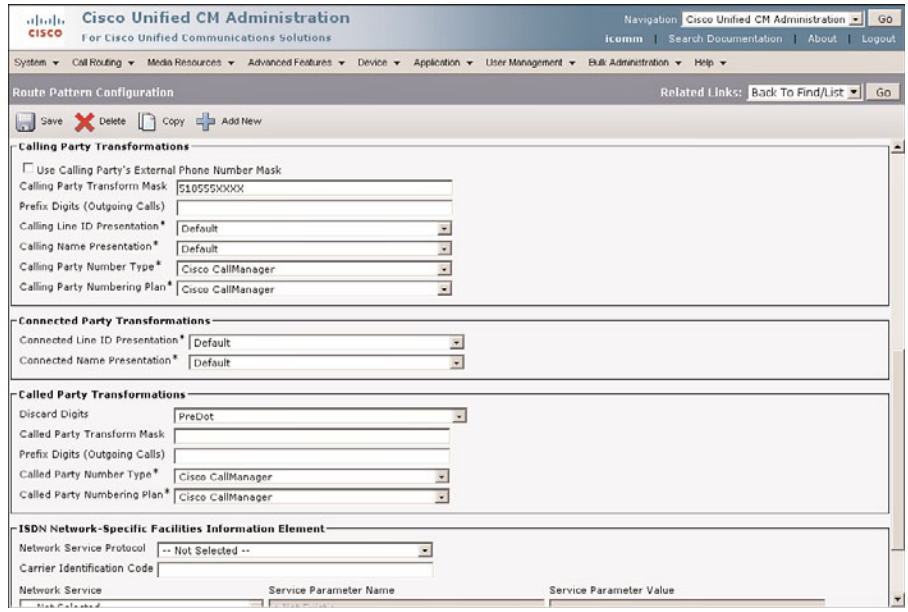
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

6. In the **Calling Party Transform Mask** field, enter **510555XXXX**. This will add the area code and exchange to the extension to make a complete long-distance phone number.

7. To indicate that the outside-line access digit needs to be stripped, in the Called Party Transformations section, from the Discard Digits drop-down list, select **PreDot**. See Figure 10-14 for an example of this page.

Figure 10-14 Local Calls Route Pattern Configuration – Part 2



8. Click the **Save** button. A pop-up window will inform you that an authorization code was not activated.

9. Click the **OK** button to close the pop-up window. Another pop-up window will inform you that any change to the route pattern will automatically reset the associated gateway or route list.

10. Click the **OK** button to close the pop-up window.

With the route pattern saved, if you have the PSTN Simulator connected to the MGCP gateway, call a local number, such as 98675309. Notice that after the 9 is dialed, the dial tone changes to indicate the outside-line access. The PSTN Simulator will answer and play the local call audio file if you are successful.

To further verify the operation of the PRI, on the router, use the **debug isdn q931** command and then place the call again. In the following output, you can see how extension 2001 (now expanded to 5105552001) is calling local number 8675309 (the 9 has been stripped off). You will see the ISDN signaling messages to connect and acknowledge the connection (CONNECT_ACK) when the call starts. They are followed by disconnect, release, and completion of the release (RELEASE_COMP) status messages when the call ends.

```
RtrPodx# debug isdn q931
debug isdn q931 is              ON.
RtrPod11#
Sep  6 08:18:36.292: ISDN Se0/2/0:23 Q931: TX -> SETUP pd = 8  callref = 0x0004
        Bearer Capability i = 0x8090A2
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
                Standard = CCITT
                Transfer Capability = Speech
                Transfer Mode = Circuit
                Transfer Rate = 64 kbit/s
        Channel ID i = 0xA98381
                Exclusive, Channel 1
        Display i = 'Brent Sieling'
        Calling Party Number i = 0x0081, '5105552001'
                Plan:Unknown, Type:Unknown
        Called Party Number i = 0x80, '8675309'
                Plan:Unknown, Type:Unknown
Sep  6 08:18:36.320: ISDN Se0/2/0:23 Q931: RX <- CALL_PROC pd = 8  callref = 0x8004
        Channel ID i = 0xA98381
                Exclusive, Channel 1
Sep  6 08:18:36.324: ISDN Se0/2/0:23 Q931: RX <- CONNECT pd = 8  callref = 0x8004
RtrPod11#
Sep  6 08:18:36.328: ISDN Se0/2/0:23 Q931: TX -> CONNECT_ACK pd = 8  callref = 0x0004
RtrPod11#
Sep  6 08:18:41.380: ISDN Se0/2/0:23 Q931: RX <- DISCONNECT pd = 8  callref = 0x8004
        Cause i = 0x8290 - Normal call clearing
Sep  6 08:18:41.424: ISDN Se0/2/0:23 Q931: TX -> RELEASE pd = 8  callref = 0x0004
Sep  6 08:18:41.432: ISDN Se0/2/0:23 Q931: RX <- RELEASE_COMP pd = 8  callref =
  0x8004
```

Step 5-2: Creating a Ten-Digit Local Calls Route Pattern

As the note in Lab 6-4, Task 4, Step 4-1 points out, not all parts of the NANP can dial seven-digit local calls, especially if they have an overlay of area codes. However, adding a ten-digit route pattern, while having seven-digit route patterns, would cause all the seven-digit route patterns to wait the T302 timer to see whether more digits are dialed. As part of the NANP, the central office code cannot be the same as the area code. (Thus, you cannot have a number like 510-510-XXXX.) This allows us to create a specific ten-digit route pattern for the area code that avoids any seven-digit numbers, and because the seven-digit numbers no longer match, they do not wait to be dialed.

Note: The PSTN Simulator configuration in Appendix E does accept numbers where the area code and central office code are the same (such as 510510XXXX), but this would not be valid on the PSTN in the NANP.

On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Pattern**.

1. Click the **Add New** button.
2. In the Route Pattern field, enter **9.510[2-9]XXXXXX**.
3. In the Description field, enter **Madison 10 Digit Local**.
4. From the Gateway/Route List drop-down list, select **Madison-RL**.
5. In the Calling Party Transform Mask field, enter **510555XXXX**. This will add the area code and exchange to the extension to make a complete long-distance phone number.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

6. To indicate that the outside line access digit needs to be stripped, in the Called Party Transformations section, from the Discard Digits drop-down list, select **PreDot**.
7. Click the **Save** button.
8. Click **OK** for both of the pop-up windows.

With the route pattern saved, if you have the PSTN Simulator connected to the MGCP gateway, call a local number, such as 95108675309. Notice that after the 9 is dialed, the dial tone changes to indicated the outside-line access. The PSTN Simulator will answer and play the local call audio file if you are successful.

Step 5-3: Creating an Emergency Services Calls Route Pattern

In this step, you will create two route patterns for emergency services calls (911 in the NANP). The first will use a 9 to access an outside line. As noted in Table 10-1, the period (.) is used to indicate leading digits to be stripped off (such as the outside-line access digit).

Note: From a legal and regulatory standpoint, access to emergency service numbers is one of the most critical functions of the phone system. This can cause design issues with your dial plan. To avoid accidental calls (and people hanging up on emergency operators), the approach you take can vary. See the note just before Task 3 in Lab 6-4 for details.

On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Pattern**.

1. Click the **Add New** button.
2. In the Route Pattern field, enter **9.911**.
3. In the Description field, enter **Madison Emergency**.
4. From the Gateway/Route List drop-down list, select **Madison-RL**.
5. For now, leave the **Urgent Priority** check box deselected.
6. In the Calling Party Transform Mask field, enter **510555XXXX**. This will add the area code and exchange to the extension to make a complete long-distance phone number. See Figure 10-15 for an example of this page.
7. To indicate that the outside-line access digit needs to be stripped, in the Called Party Transformations section, from the Discard Digits drop-down list, select **PreDot**.
8. Click the **Save** button.
9. Click **OK** for both of the pop-up windows.

   With the route pattern saved, if you have the PSTN Simulator connected to the MGCP gateway, call 9911. Notice that after the 9 is dialed, the dial tone changes to indicate the outside-line access. However, the call will not connect right away. The call has to wait for the T302 interdigit timeout value to expire (15 seconds by default). Local calls are not impacted, as they require more digits. This is where the Urgent Priority check box comes into play.

10. Select the **Urgent Priority** check box, and save the route pattern again.

    The 9911 calls should now route immediately.

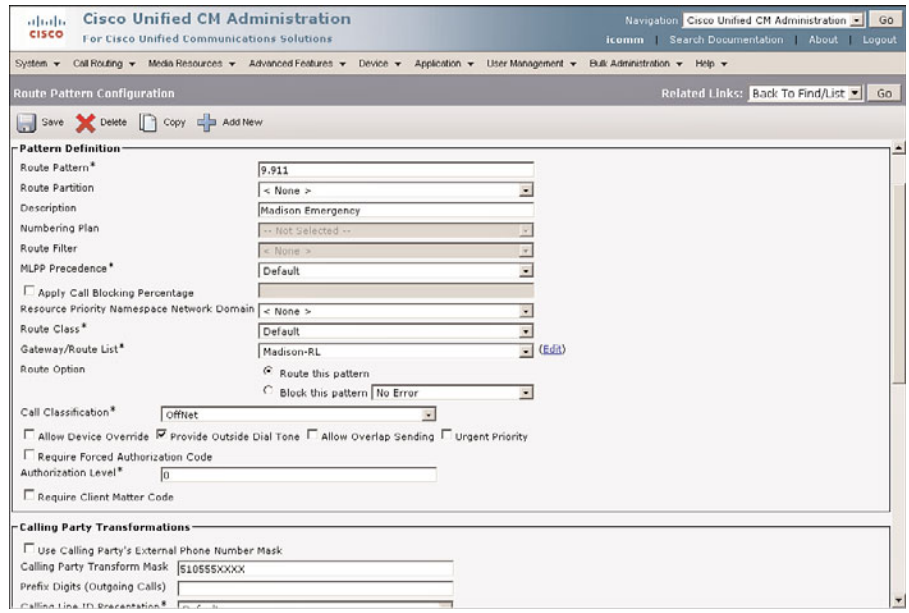
    You also need to deal with the dialing of 911 without the outside-line access digit.

11. While on the 9.911 route pattern, click the **Copy** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-15 Emergency Services Route Pattern Configuration – Part 1

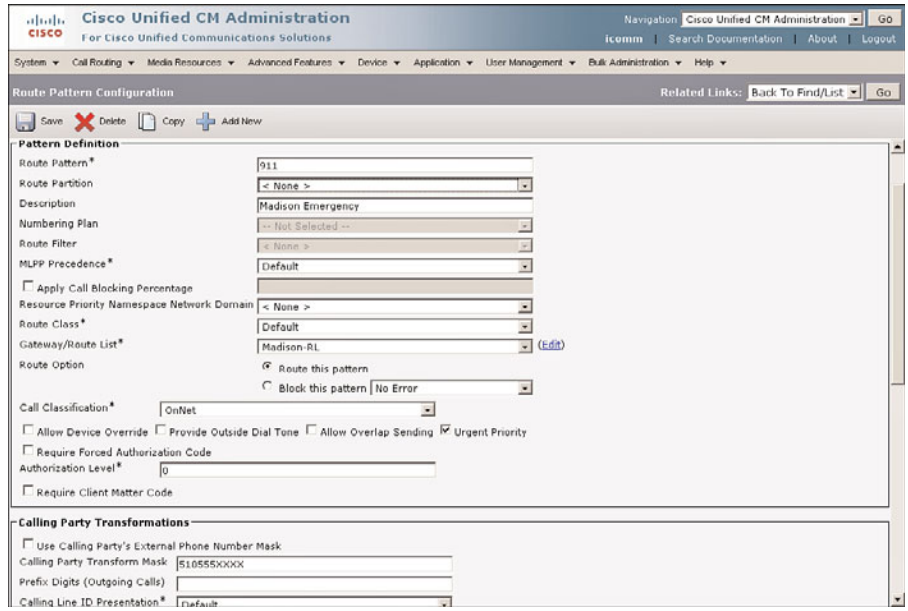


12. Enter **911** to change the Route Pattern field.

13. Because we might not want the outside access line dial tone to play when the 9 is dialed, deselect the **Provide Outside Dial Tone** check box.

14. When the **Provide Outside Dial Tone** check box is deselected, the Call Classification field automatically changes to **OnNet**. From the Call Classification drop-down list, change the selection back to **OffNet**. See Figure 10-16 for an example of this page.

Figure 10-16 Emergency Services Route Pattern Configuration – Part 2



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

15. Note that because there is no outside access line digit or dot, in the Called Party Transformations section, the Discard Digits drop-down list is grayed out and cannot be changed.

16. Click the **Save** button.

17. Click **OK** for both of the pop-up windows.

    With the route pattern saved, if you have the PSTN Simulator connected to the MGCP gateway, call 911. The call should succeed. However, if you call a local number, such as 98675309, the outside access dial tone will not play until after the 9 and 8 digits are dialed. (The same is true for the 9.911 number, where the dial tone does not change until after the second 9 is dialed.)

    This is because the first 9 initially matches all three route patterns, and the 911 pattern does not allow the outside dial tone.

    a. 911 (does not allow outside dial tone) (might match)

    b. 9911 (allows outside dial tone) (might match)

    c. 9[2-9]XXXXXX (allows outside dial tone) (might match)

    As a result, until CUCM determines that the dialed digit after the 9 is not a 1, the outside access dial tone will not play, resulting in the other patterns waiting an extra digit before playing the outside access dial tone. It is important to realize that one route pattern can indirectly impact other route patterns.

18. Select the **Provide Outside Dial Tone** check box, and save the route pattern again.

All three of the route patterns should now provide the expected call behavior, although the 911 will play an outside-line access tone when the 9 is dialed.

Step 5-4: Creating a Long-Distance Calls Route Pattern

In this step, you will create a route pattern for long-distance calls. A 9 will be used to access an outside line. As noted in Table 10-1, the period (.) is used to indicate leading digits to be stripped off (such as the outside-line access digit). Lab 6-4, Task 4 explains the NANP, including the fact that the first digit of the area code and central office code (exchange) cannot start with a 0 or a 1, as those are reserved. In the NANP, if the first digit is a 1, the system expects to route the call outside the local central office, and ten digits should follow. To avoid incorrect calls being routed to the PSTN, the pattern will limit the first digit of the area code and central office code to 2 through 9.

On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Pattern**.

1. Click the **Add New** button.

2. In the Route Pattern field, enter **9.1[2-9]XX[2-9]XXXXXX**.

3. In the Description field, enter **Long Distance**.

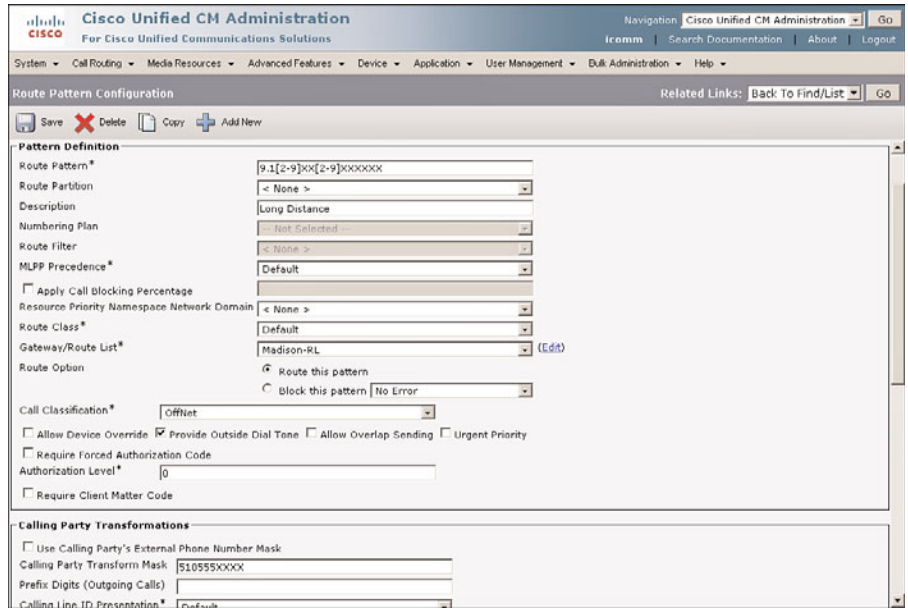
4. From the Gateway/Route List drop-down list, select **Madison-RL**.

5. In the Calling Party Transform Mask field, enter **510555XXXX**. This will add the area code and exchange to the extension to make a complete long-distance phone number. See Figure 10-17 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-17 Long-Distance Calls Route Pattern Configuration



6. To indicate that the outside-line access digit needs to be stripped, in the Called Party Transformations section, from the Discard Digits drop-down list, select **PreDot**.
7. Click the **Save** button.
8. Click **OK** for both of the pop-up windows.

With the route pattern saved, if you have the PSTN Simulator connected to the MGCP gateway, call a long-distance number, such as 912223334444. Notice that after the 9 is dialed, the dial tone changes to indicate the outside-line access. The PSTN Simulator will answer and play the long-distance audio file if you are successful.

Step 5-5: Creating a Premium Services Blocked Calls Route Pattern

In the previous step, you created a route pattern for long-distance calls. That pattern will also allow calls to premium rate numbers (1-900), and the company wants to restrict these calls. (If you have the PSTN connected, test this by calling 919003334444, and the PSTN Simulator will answer and play the 1-900 audio file.) A 9 will be used to access an outside line. As noted in Table 10-1, the period (.) is used to indicate leading digits to be stripped off (such as the outside-line access digit).

On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Pattern**.

1. Click the **Add New** button.
2. In the Route Pattern field, enter **9.1900[2-9]XXXXXX**.
3. In the Description field, enter **Block 1-900 calls**.
4. From the Gateway/Route List drop-down list, select **Madison-RL**.
5. In the Route Option field, click the **Block this pattern** radio button.

https://t.me/learningnets

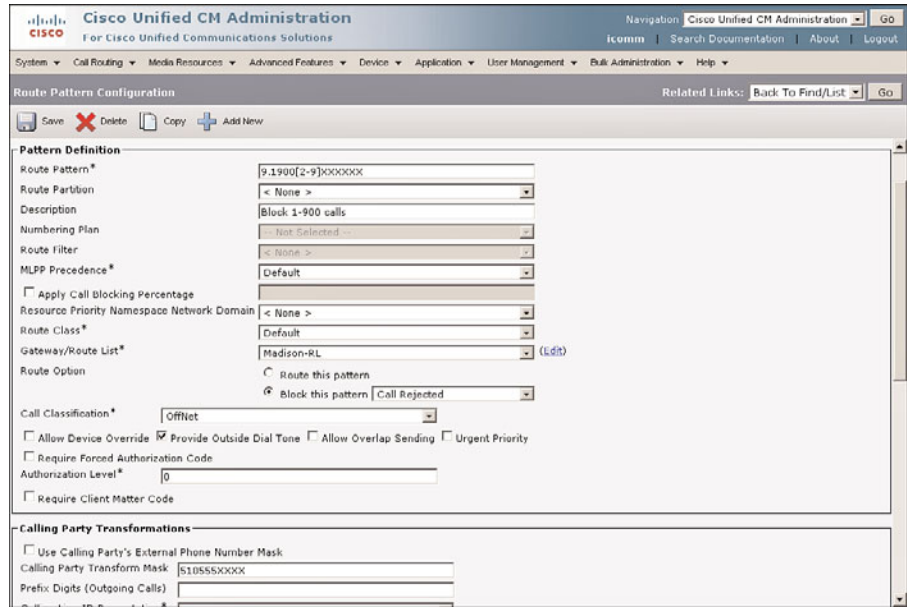
From the Library of Aliwarman Tarihoran

6. The Block This Pattern drop-down list shows **No Error** by default, which just drops the call. A better option in this case would be to select **Call Rejected** from the drop-down list, which will play a busy signal.

Note: Technically, transformations are ignored (items 6, 7, and 8) after the **Block this pattern** radio button is chosen. However, I like to set them the same as a normal pattern, just so they are present if the Route Option field is later changed.

7. In the Calling Party Transform Mask field, enter **510555XXXX**. This will add the area code and exchange to the extension to make a complete long-distance phone number. See Figure 10-18 for an example of this page.

Figure 10-18 Blocked Calls Route Pattern Configuration



8. To indicate that the outside-line access digit needs to be stripped, in the Called Party Transformations section, from the Discard Digits drop-down list, select **PreDot**.
9. Click the **Save** button.
10. Click **OK** for both of the pop-up windows.

With the route pattern saved, if you have the PSTN Simulator connected to the MGCP gateway, call a premium number such as 919003334444. The call should now give you a busy signal.

Step 5-6: Creating a Toll-Free Calls Route Pattern

In this step, you will create a route pattern for toll-free calls. While toll-free calls match the long-distance route pattern, when you create restrictions in a later lab to allow a user access to only emergency, local, and toll-free calls, a separate route pattern is needed. A 9 will be used to access an outside line. As noted in Table 10-1, the period (.) is used to indicate leading digits to be stripped off (such as the outside-line access digit).

On the Cisco Unified CM Administration page, navigate to **Call Routing** > **Route/Hunt** > **Route Pattern**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

1. Click the **Add New** button.
2. In the Route Pattern field, enter **9.1800[2-9]XXXXXX**.
3. In the Description field, enter **Toll-Free 1-800**.
4. From the Gateway/Route List drop-down list, select **Madison-RL**.
5. In the Calling Party Transform Mask field, enter **510555XXXX**. This will add the area code and exchange to the extension to make a complete long-distance phone number.
6. To indicate that the outside-line access digit needs to be stripped, in the Called Party Transformations section, from the Discard Digits drop-down list, select **PreDot**.
7. Click the **Save** button.
8. Click **OK** for both of the pop-up windows.

   With the route pattern saved, if you have the PSTN Simulator connected to the MGCP gateway, call a toll-free number such as 918003334444. Notice that after the 9 is dialed, the dial tone changes to indicate the outside-line access. The PSTN Simulator will answer and play the 1-800 audio file if you are successful.

   There are currently five area codes that are toll-free: 800, 888, 877, 866, and 855. (See www.fcc.gov/guides/toll-free-numbers-and-how-they-work for details.) A single route pattern like 9.18[05678][05678]XXXXXXX would allow calls to toll numbers in area codes such as 850, 805, 876, and so on that should not be allowed in a toll-free-only restriction. The only way to cover just the toll-free numbers (without using the 9@ pattern and route filters) is to create five separate route patterns. The easiest way to do this is to use the **Copy** button while on a toll-free pattern.
9. Click the **Copy** button.
10. Change the Route Pattern and Description fields to the next toll-free area code.
11. Click the **Save** button.
12. Click **OK** for both of the pop-up windows.

Repeat Steps 9 through 12 to create route patterns for the remaining toll-free area codes.

Step 5-7: Creating a Service Codes Calls Route Pattern

In this step, you will create a route pattern for service code calls (N11). Lab 6-4, Task 4 explains the use of service codes (such as 211, 311, 411, and so on) in the NANP. Emergency service (911) is also part of the service codes, but it should *never* be blocked. Other service codes, such as information, might incur charges for features and might be restricted to selected users, so they should be a separate route pattern. A 9 will be used to access an outside line. As noted in Table 10-1, the period (.) is used to indicate leading digits to be stripped off (such as the outside-line access digit).

On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Pattern**.

1. Click the **Add New** button.
2. In the Route Pattern field, enter **9.[2-8]11**.
3. In the Description field, enter **Madison Service Codes**.
4. From the Gateway/Route List drop-down list, select **Madison-RL**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

5. Select the **Urgent Priority** check box.
6. In the Calling Party Transform Mask field, enter **510555XXXX**. This will add the area code and exchange to the extension to make a complete long-distance phone number.
7. To indicate that the outside-line access digit needs to be stripped, in the Called Party Transformations section, from the Discard Digits drop-down list, select **PreDot**.
8. Click the **Save** button.
9. Click **OK** for both of the pop-up windows.

With the route pattern saved, if you have the PSTN Simulator connected to the MGCP gateway, call from a phone to a service code number such as 9311. Notice that after the 9 is dialed, the dial tone changes to indicate the outside-line access. The PSTN Simulator will answer and play the info audio file if you are successful.

Step 5-8: Creating an International Calls Route Pattern

In this step, you will create two route patterns for international calls (calls that start with 011 in the NANP). As noted in Table 10-1, the pound (#) does not automatically signal the end of dialed digits, so there needs to be two route patterns. One pattern will explicitly include the # for users who know to use it to signal the end of dialed digits. Another pattern will not include the # for users who do not know to use it, but they will need to wait for the T302 timer (15 seconds by default) before the call will complete. The period (.) is used to indicate leading digits to be stripped off (such as the outside-line access digit).

Note: The T302 interdigit timer can be changed from the default of 15 seconds to a lower value, but it is not recommended to select a number less than 4 to avoid premature call-dialing attempts.

On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Pattern**.

1. Click the **Add New** button.
2. In the Route Pattern field, enter **9.011!**.
3. In the Description field, enter **International**.
4. From the Gateway/Route List drop-down list, select **Madison-RL**.
5. In the Calling Party Transform Mask field, enter **510555XXXX**. This will add the area code and exchange to the extension to make a complete long-distance phone number.
6. To indicate that the outside-line access digit needs to be stripped, in the Called Party Transformations section, from the Discard Digits drop-down list, select **PreDot**.
7. Click the **Save** button.
8. Click **OK** for both of the pop-up windows.

   With the route pattern saved, if you have the PSTN Simulator connected to the MGCP gateway, call an international number, such as 9011223334444. Notice that after the 9 is dialed, the dial tone changes to indicate the outside-line access. However, the call will not connect right away, as it has to wait for the T302 interdigit timeout value to expire after the last digit is dialed (15 seconds by default).

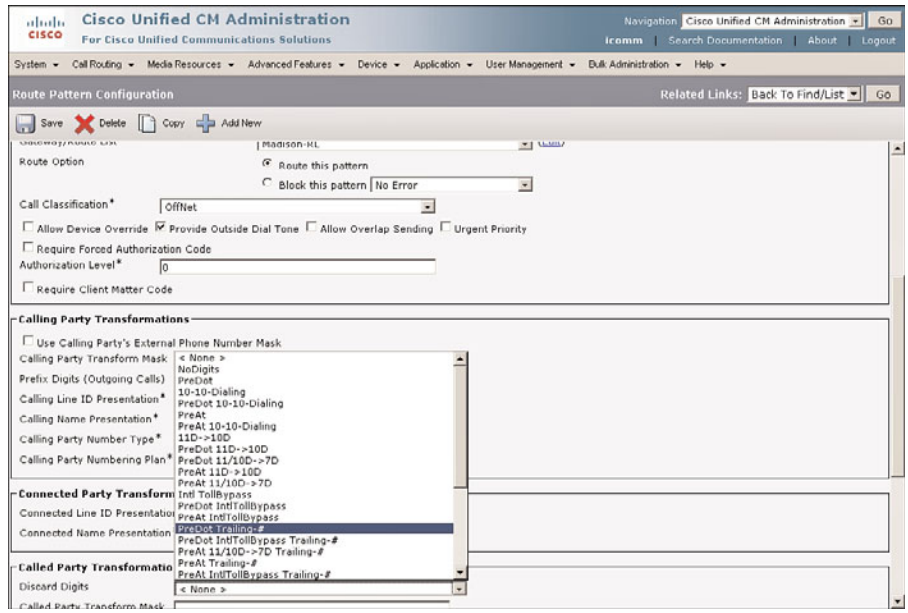
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Create the route pattern that will utilize the #. Be aware that the Calling Party Transform Mask field will be different from all the previous route patterns, as both the predot and ending # need to be stripped.

9. While on the 9.011! route pattern, click the **Copy** button.
10. Enter **9.011!#** to change the Route Pattern field.
11. Change the Description field to **International #**.
12. In the Called Party Transformations section, from the Discard Digits drop-down list, change to **PreDot Trailing-#**. See Figure 10-19 for an example of this page.

Figure 10-19 International Calls with # Route Pattern Configuration



13. Click the **Save** button.
14. Click **OK** for both of the pop-up windows.

With the route pattern saved, if you have the PSTN Simulator connected to the MGCP gateway, call an international number, such as 9011223334444#. The call should succeed right away.

Step 5-9: Examine the NANP Route Patterns

To examine all the route patterns created, do either of the following:

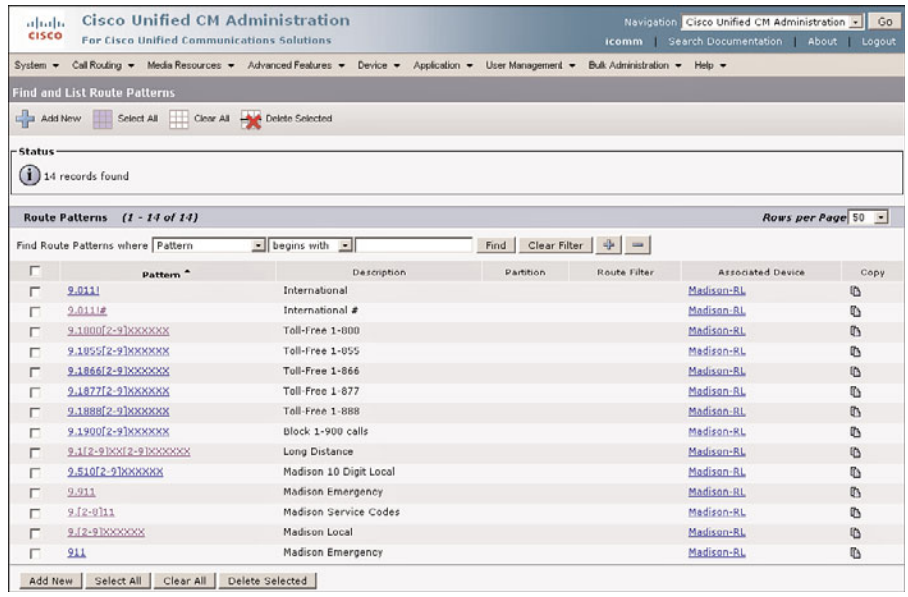
- From any Route Pattern Configuration page, with the Related Links set to **Back To Find/List**, click the **Go** button.
- On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Pattern**. Click **Find** to see the route patterns.

See Figure 10-20 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-20 Find and List Route Patterns

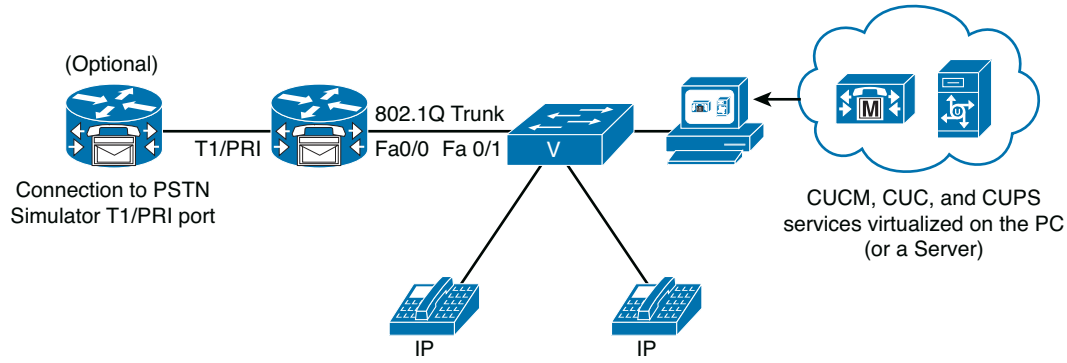


https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 10-2: Class of Control—Partitions and Calling Search Spaces (CSS)

Figure 10-21 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- Configuration from Lab 10-1
- Two or more IP Phones registered (desk phone or soft phone on PC or Windows VM)

Optional hardware components (see Scenario for details):

- Cisco router configured as a PSTN Simulator
- T1/E1/PRI Multiflex Trunk VWICs or network modules
- Digital signal processor (DSP) resources in the routers (PVDM chips) to enable the Multiflex Trunks

Learning Objectives

Upon completion of this lab, you will be able to

- Understand Class of Control
- Understand and configure partitions
- Understand and configure Calling Search Spaces (CSS)

Scenario

Shiny Objects Inc. (SOI) has calls working between phones at headquarters and to the PSTN. However, the company is concerned that people might incur large phone bills on premium-rate (1-900) and international calls, especially on restricted-usage phones in places such as the lobby and cafeteria.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Class of Control is the answer to this problem. (Class of Control is similar to Class of Restriction [CoR] in the Cisco Unified Communications Manager Express environment.) Class of Control has two primary functions:

- **Restricting who can call what numbers:** Many companies want to restrict access to expensive calls, such as premium-rate and international numbers. Class of Control can restrict which users are allowed access to any route pattern. Additionally, Class of Control can be used to restrict calls within the company. For example, in a large company, only a select number of people might be able call the CEO's extension directly. Most calls to the CEO need to be transferred by the executive assistant.
- **Location routing:** This is a critical function for calls to emergency services (911). When a user at a branch office calls 911 and the call is directed out the HQ gateway, the emergency responders will show up at the wrong location. Class of Control can force 911 calls to use the gateway at the branch office, sending the emergency responders to the correct location.

Task 1: Examine Partitions and Calling Search Spaces (CSS)

Class of Control can be one of the most difficult topics to understand in CUCM. It starts out pretty simple, but after it is implemented, it can get quite complicated. There are two main elements of Class of Control: partitions and Calling Search Spaces (CSS).

Step 1-1: Examine Partitions

Partitions can be thought of as "locks." By applying a partition, you effectively restrict access to only those users who have the "key." Partitions can be applied to a variety of constructs, such as

- **Directory numbers (extensions):** This is how you can restrict who can call an executive.
- **Route patterns:** This is how you can restrict what number a user can call on the PSTN.
- **Translation patterns:** Modify (or block) a calling or called number before it reaches the route patterns.
- **Transformation patterns:** Can modify a calling or called number. As shown in Lab 10-1, the route patterns modified the outgoing calling party four-digit extension to be a ten-digit number.

By default, unless assigned a partition, all the items previously listed are assigned to the null partition (which shows as <none> in CUCM). The null partition does not have a "lock," and as a result, everything can reach directory numbers and route patterns that do not have a partition assigned. However, using the null partition is not recommended, as it is complex to change after the system is in production.

Note: I have heard that changing away from the null partition after a system is in production can be done, but it is a lot more work than if the correct setup was implemented from the beginning.

Step 1-2: Examine Calling Search Spaces

If partitions act like "locks," Calling Search Spaces act like "key rings." A calling search space is a list of partitions that can be accessed by a construct, such as

- Directory numbers (extensions)
- Devices (including phones)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- Gateways
- Translation patterns

The CSS becomes the list of partitions that a construct can search to dial. If the dialed number is not among the partitions listed in the construct's CSS (or the null partition), the call will not be completed.

As shown in the previous list of constructs that can be assigned a CSS, both a directory number (line) and a phone can have a CSS assigned. What happens when both the directory number and the phone have a CSS assigned? They are combined, with the line CSS searched before the phone CSS. If a line CSS contains the target number (even if it blocks the call), that CSS is selected before the phone CSS. However, if the target cannot be found in the line CSS, but is in the phone CSS, the phone CSS will be used.

The order that the partitions are assigned in a CSS does matter in the event that more than one target matches exactly. In this case, the order of the partitions determines which target gets the call. It is recommended to avoid having overlapping numbers that are reachable in the same CSS. (This might not be possible when branches in different area codes or exchanges have the same last four digits from the PSTN, or when another company is acquired.)

Step 1-3: Examine Partitions and CSS Together

Before looking at an example, review the following points:

- A construct with the default null partition can be reached from any other construct (because it has no partition "lock").
- A construct with the default null CSS can only contact constructs in the null partition (because it has no "keys" on the CSS "key ring").
- When both the directory number (line) and the phone have a CSS assigned, they are combined, with the directory number CSS taking priority.
- If multiple exact matches are found in the CSS (in different partitions), the ordering of the partitions determines the match selected.
- Just because two constructs have the same partition does not automatically mean that they can contact each other. The CSS assigned to both must include the partition they are assigned to.

Looking at Table 10-2, there are four partitions with the rather nondescript names of A, B, C, and D. There are five CSSs, with the following partition assignments:

- CSS1 has partition A
- CSS2 has partition B and C
- CSS3 has partition A and C
- CSS4 has partition A, B, and C
- CSS5 has partition B, A, C, and D

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Table 10-2 Example of Partition and CSS Assignments

Phone	Directory Number	Assigned Partition	Assigned CSS
Phone 1	Line 1500	A	<none>
	Line 1501	A	CSS2
Phone CSS		Not applicable	<none>
Phone 2	Line 1505	B	CSS3
	Line 1509	C	CSS2
	Line 1501	B	CSS2
Phone CSS		Not applicable	CSS1
Phone 3	Line 1652	C	CSS4
	Line 1681	D	CSS5
	Line 1690	Null	<none>
Phone CSS		Not applicable	<none>
Local route pattern: 9.[2-9]XXXXXX		B	Not applicable
Long-distance route pattern: 9.1[2-9]XX[2-9]XXXXXX		D	Not applicable

The first thing you might assume by looking at Table 10-2 is that because directory numbers 1500 and 1501 (on phone 1) are both in partition A, they should be able to call each other. As noted, the partitions act as "locks," so just because they have the same "locks" does not mean they have the same "keys." In this case, 1500 has only the default CSS assigned (and there is no CSS on the phone), so the only number 1500 can call is 1690, as 1690 does not have a partition assigned.

Using the information in Table 10-2, you can chart out what number each directory number can call, and what numbers have the correct CSS to contact the directory number and route pattern, as shown in Table 10-3.

In Table 10-2, directory number 1501 (on phone 1) has CSS2 assigned, which allows calls to partitions B and C (and there is no CSS on the phone). Interestingly enough, because 1501 (on phone 1) is in partition A (which is not part of CSS2), 1501 (on phone 1) cannot call itself. However, it can call the duplicate number 1501 on phone 2, because that directory number is in partition B (which is part of CSS2). As a result, 1501 (on phone 1) can call 1505, 1509, 1501 (on phone 2), 1652, 1690, and any local numbers on the PSTN (using the local route partition).

In Table 10-2, directory number 1505 (on phone 2) has CSS3 assigned, which allows calls to partitions A and C. (The phone also has CSS1 assigned, which allows calls to partition A, but 1505 already has access to that.) As a result, 1505 can call 1500, 1501 (on phone 1 only), 1509, 1652, and 1690.

In Table 10-2, directory number 1509 (on phone 2) has CSS2 assigned, which allows calls to partitions B and C. The phone also has CSS1 assigned, which allows calls to partition A. As a result, 1509 can access partitions B, C, and A. Because there is a 1501 in both partitions A (phone 1) and B (phone 2), can 1509 call both? Because the line CSS (partition B) has priority over the phone CSS (partition A), only the 1501 on phone 2 is accessible. As a result, 1509 can call 1500, 1505, itself, 1501 (on phone 2), 1652, 1690, and any local number on the PSTN (using the local route partition).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

In Table 10-2, directory number 1501 (on phone 2) has CSS2 assigned, which allows calls to partitions B and C. The phone also has CSS1 assigned, which allows calls to partition A. As a result, 1501 (on phone 2) can access partitions B, C, and A. Because there is a 1501 in both partitions A (phone 1) and B (phone 2), what happens when you call 1501 from 1501 (on phone 2)? Because the line CSS (partition B) has priority over the phone CSS (partition A), only the 1501 on phone 2 is accessible. As a result, 1501 (on phone 2) can call 1500, 1505, 1509, itself, 1652, 1690, and any local numbers on the PSTN (using the local route partition).

In Table 10-2, directory number 1652 (on phone 3) has CSS4 assigned, which allows calls to partitions A, B, and C (and there is no CSS on the phone). At this point, based on the results of the two previous directory numbers, you might assume that 1652 will only be able to contact 1501 (on phone 2). However, this is where the priority of the partitions in a CSS comes into play. Because partition A is listed before B in this CSS, 1501 (on phone 1) will be the directory number that 1652 can call. As a result, 1652 can call 1500, 1501 (on phone 1), 1505, 1509, itself, 1690, and any local numbers on the PSTN (using the local route partition).

In Table 10-2, directory number 1681 (on phone 3) has CSS5 assigned, which allows calls to partitions B, A, C, and D (and there is no CSS on the phone). Again, the priority of the partitions in a CSS comes into play. Because partition B is listed before A in this CSS, 1501 (on phone 2) will be the directory number 1681 can call. As a result, 1681 can call any of the numbers in the system (excluding 1501 on phone 1, because of the match with 1501 on phone 2). As it currently stands, no other number can call 1681 or the long-distance route pattern.

Finally, in Table 10-2, when directory number 1690 was created, no partition or CSS was added (and there is no CSS on the phone). As a result, all directory numbers can call 1690, but 1690 can only call itself, as it has no CSS with "keys" to reach other partitions.

Table 10-3 Partition and CSS Results

Phone	Directory Number	Numbers This DN Can Call	Numbers That Can Call This DN
Phone 1	Line 1500	1690	1505, 1509, 1501 (phone 2), 1652, 1681
	Line 1501	1505, 1509, 1501 (phone 2), 1652, 1690, local calls	1505, 1652 (*See note: 1509, 1501 on phone 2, 1681)
Phone 2	Line 1505	1500, 1501 (phone 1), 1509, 1652, 1690	1501 (phone 1), 1509, 1501 (phone 2), 1652, 1681
	Line 1509	1500, 1505, itself, 1501 (phone 2), 1652, 1690, local calls (*See note: 1501 on phone 1)	1501 (phone 1), 1505, itself, 1501 (phone 2), 1652, 1681
	Line 1501	1500, 1505, 1509, itself, 1652, 1690, local calls (*See note: 1501 on phone 1)	1501 (phone 1), 1509, itself, 1681 (*See note: 1652)
Phone 3	Line 1652	1500, 1501 (phone 1), 1505, 1509, itself, 1690, local calls (*See note: 1501 on phone 2)	1501 (phone 1), 1505, 1509, 1501 (phone 2), itself, 1681

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Table 10-3 Partition and CSS Results *continued*

Phone	Directory Number	Numbers This DN Can Call	Numbers That Can Call This DN
	Line 1681	1500, 1505, 1509, 1501 (phone 2), 1652, itself, 1690, local calls, long-distance calls (*See note: 1501 on phone 1)	Itself
	Line 1690	Only itself	Everyone
Local route pattern: 9.[2-9]XXXXXX		Not applicable	1501 (phone 1), 1509, 1501 (phone 2), 1652, 1681
Long-distance route pattern: 9.1[2-9]XX[2-9]XXXXXX		Not applicable	1681

* While a call might match the partition of a number, if a match is found in a higher-priority partition (listed first), the call will not be completed.

Step 1-4: Calculate Partitions and CSS Interactions

To improve your understanding of the behavior of partitions and CSSs, examine the information for Table 10-4 and fill in the answers in Table 10-5.

Looking at Table 10-4, there are four partitions with the rather nondescript names of PT1, PT2, PT3, and PT4. There are four CSSs, with the following partition assignments:

- CSS1 has partition PT1
- CSS2 has partition PT2 and PT3
- CSS3 has partition PT4
- CSS4 has partition PT1, PT2, and PT4

Table 10-4 Sample Partition and CSS Assignments

Phone	Directory Number	Assigned Partition	Assigned CSS
Phone 1	Line 1700	PT1	CSS4
	Line 1701	PT2	CSS1
	Line 1664	PT3	CSS3
	Phone CSS	Not Applicable	<none>
Phone 2	Line 1703	PT4	CSS3
	Line 1709	PT4	<none>
	Line 1657	Null	CSS1
	Phone CSS	Not Applicable	CSS2
Phone 3	Line 1702	PT2	CSS1
	Line 1717	Null	<none>
	Line 1701	PT1	CSS4
	Phone CSS	Not Applicable	<none>

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Phone	Directory Number	Assigned Partition	Assigned CSS
Local route pattern: 9.[2-9]XXXXXX		PT1	Not applicable
Long-distance route pattern: 9.1[2-9]XX[2-9]XXXXXX		PT3	Not applicable

Using Table 10-4, fill in what number each directory number can call, and what numbers have the correct CSS to contact the directory number and route pattern.

Table 10-5 Partition and CSS Results

Phone	Directory Number	Numbers This DN Can Call	Numbers That Can Call This DN
Phone 1	Line 1700	Itself, 1703, 1709, 1657, 1702, 1717, 1701 (phone 3), local calls (*See note: 1701 on phone 1)	Itself, 1701 (phone 1), 1657, 1702, 1701 (phone 3)
	Line 1701		
	Line 1664		
Phone 2	Line 1703		
	Line 1709		
	Line 1657		
Phone 3	Line 1702		
	Line 1717		
	Line 1701		
Local Route Pattern: 9.[2-9]XXXXXX		Not applicable	
Long-Distance Route Pattern: 9.1[2-9]XX[2-9]XXXXXX		Not applicable	

* While a call might match the partition of a number, if a match is found in a higher-priority partition (listed first), the call will not be completed.

Step 1-5: Partitions and CSS for SOI

The type of partitions implemented depends on a company's objectives. For this lab, assume that SOI has four categories of users, with the numbers that each category should be able to reach, as shown in Table 10-6.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Table 10-6 User Categories and Numbers Reachable

User Categories	Numbers Reachable
Restricted (common-area phones, such as the lobby, break room, elevator, and so on)	Internal extensions, emergency services
Guest (includes contractors and limited-term employees)	Internal extensions, emergency services, local, toll-free (1-800)
Employee	Internal extensions, emergency services, local, toll-free (1-800), info services (N11), long-distance (excluding premium-rate (1-900)
Unrestricted (senior executives and department heads)	All numbers, including premium rate (1-900) and international

If you think of each of the names in the Numbers Reachable column in Table 10-6 as a "lock" on a route pattern, you can see what sort of partitions might be needed.

Before creating the partitions, there is one other aspect that needs to be considered, and that is the locations. As mentioned previously, one of the key functions of Class of Control is location routing, especially with regard to emergency services, to make sure that the right gateway is used. The requirements to select the right gateway result in creating partitions for each location. For example, creating partitions for the New York location will prevent those employees from accessing the Madison emergency route patterns, and Madison users from getting the emergency services patterns for other gateways. Additionally, at a branch office, local calls are usually less expensive than routing the calls as long-distance from the headquarters site. Creating partitions for each location results in separate route patterns for each location, with each route pattern pointing to a different gateway. You can see that if you had dozens or hundreds of remote sites, this could be a lot of work.

While local calls and emergency services are best done on the local gateway, having long-distance, toll-free, and international calls from branch offices go across the WAN and exit at the headquarters, where discounted rates might have been negotiated, is often better. Those calls do not need to be localized.

Note: There is a way to simplify the localized route patterns and partitions using local route groups. See the "Local Route Group" section of the *Cisco Unified Communications Manager Features and Services Guide* (http://bit.ly/WisVix) for your version of CUCM. Local route groups are a more advanced topic than this lab book covers.

There is an advantage to creating an internal partition and assigning it to directory numbers. This allows future control of what internal numbers users can access, as well as control calls coming into the system from the gateways.

To properly control the outside-line access, a partition should be configured and applied to every route pattern. Examine the patterns and partitions for SOI in Table 10-7.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Table 10-7 Partition Assignments for SOI

Patterns	SOI Partition
All SOI directory numbers	Internal_PT
911 9.911	Mad_911_PT
9.[2-9]XXXXXX 9.510[2-9]XXXXXX	Mad_Local_PT
9.[2-8]11	Mad_Services_PT
9.1[2-9]XX[2-9]XXXXX	LD_PT
9.1800[2-9]XXXXXX 9.1855[2-9]XXXXXX 9.1866[2-9]XXXXXX 9.1877[2-9]XXXXXX 9.1888[2-9]XXXXXX	TF_PT
9.1900[2-9]XXXXXX	Block900_PT
9.011! 9.011!#	International_PT

Note: Regarding the SOI partition names, Madison, Wisconsin is sometimes called "Mad City," which is shortened to Mad for this lab.

With the partitions defined, examine the CSSs needed for SOI at the Madison location in Table 10-8.

Table 10-8 CSSs and Partitions for SOI

CSS	SOI Partitions
Mad_Restricted_CSS	Internal_PT Mad_911_PT
Mad_Guest_CSS	Internal_PT Mad_911_PT Mad_Local_PT TF_PT
Mad_Employee_CSS	Internal_PT Mad_911_PT Mad_Local_PT TF_PT Mad_Services_PT LD_PT Block900_PT

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Table 10-8 CSSs and Partitions for SOI *continued*

CSS	SOI Partitions
Mad_Unrestricted_CSS	Internal_PT Mad_911_PT Mad_Local_PT TF_PT Mad_Services_PT LD_PT International_PT

Task 2: Create and Assign Partitions

Use Table 10-7 to create partitions for SOI.

Step 2-1: Create Partitions

Up to 75 partitions (with descriptions) can be created at the same time. By using a comma (,) after a partition name, a description can be created. (Otherwise the description is the same as the name.)

On the Cisco Unified CM Administration page, navigate to **Call Routing > Class of Control > Partition**.

1. Click the **Add New** button.
2. In the Name box, enter each of the following items on a separate line:

   Internal_PT
   Mad_911_PT
   Mad_Local_PT
   TF_PT, Toll-Free
   Mad_Services_PT
   LD_PT, Long-Distance
   Block900_PT
   International_PT

   See Figure 10-22 for an example of this page.
3. Click the **Save** button to create the partitions.

Step 2-2: Assign a Partition

If you were to assign all the directory numbers and route patterns a partition right now, it would be like locking all the doors when no one has keys! To prove this point, configure one directory number with the Internal_PT partition.

On the Cisco Unified CM Administration page**,** navigate to **Device > Phone** and click **Find**.

1. Click the device name of an active phone to see the details.
2. In the Association Information section, click **Line [1]** to open the Directory Number Configuration page.
3. In the Directory Number Information section, select **Internal_PT** from the Route Partition drop-down list. See Figure 10-23 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-22 Partition Configuration

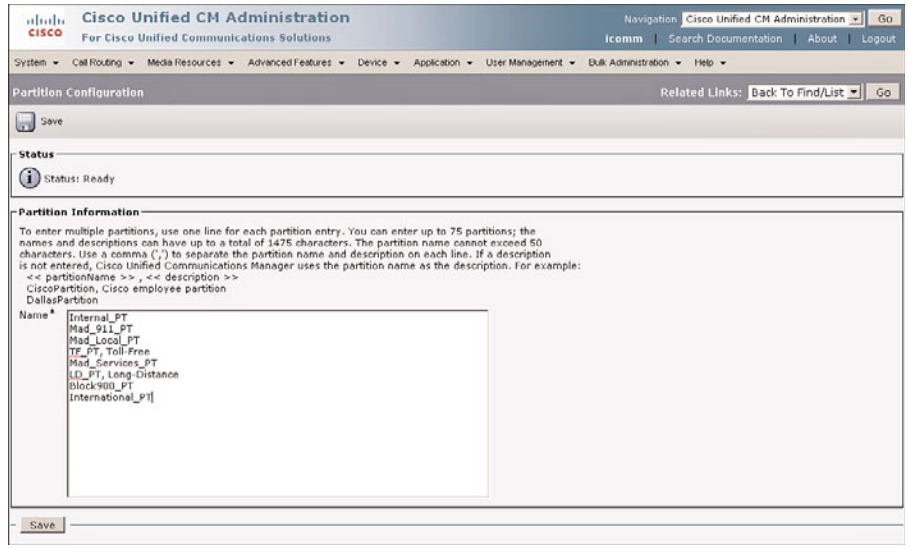
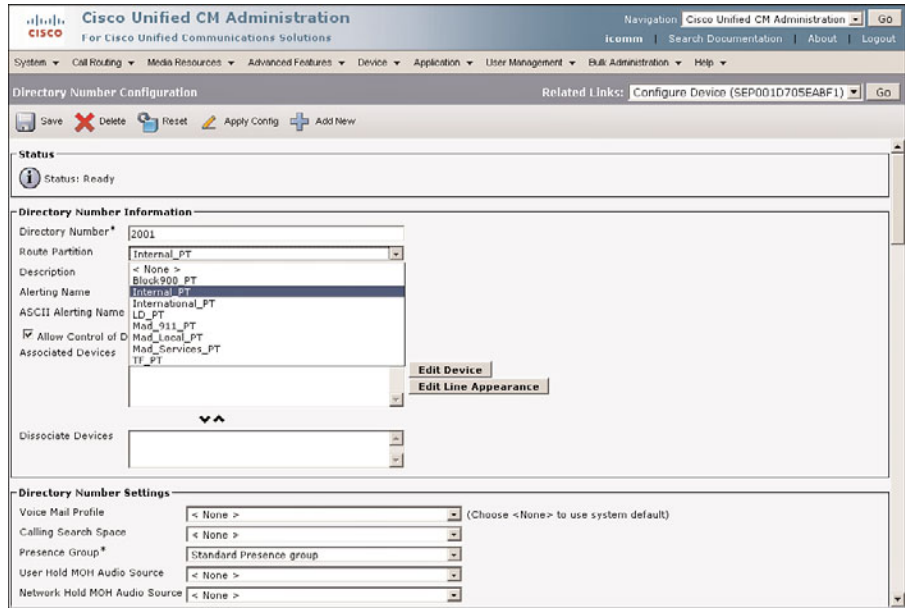


Figure 10-23 Partition Assignment on a Directory Number



4. Click the **Save** button. The display on the phone should refresh.
5. From another phone (or another extension on the same phone), call that number. As soon as you dial the last digit, you will get a busy signal.
6. From the changed extension, can you call any of the other extensions? Why or why not?

_____

7. With the Related Links drop-down list on **Configure Device**, click the **Go** button.

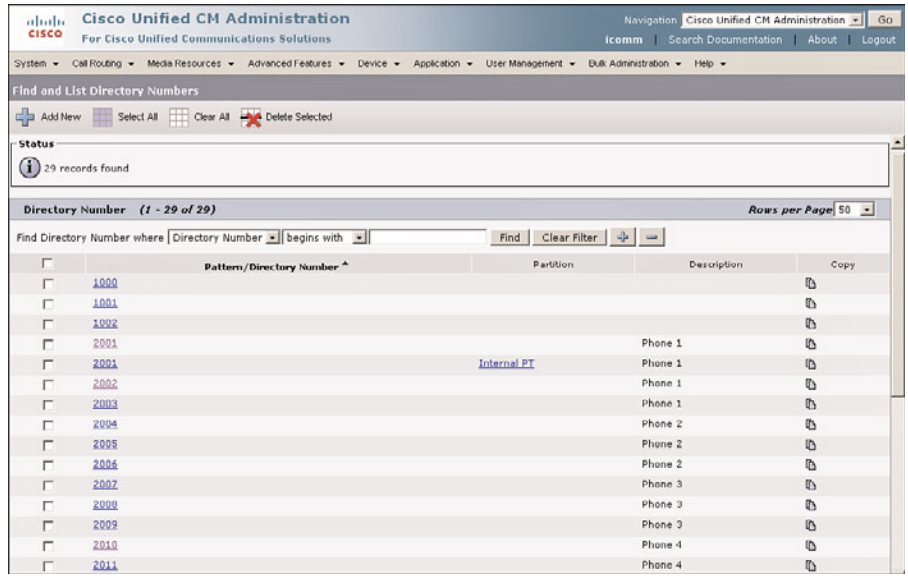
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

8. When you look at Line [1], you will see that (no partition) has been replaced with the Internal_PT name.

9. On the Cisco Unified CM Administration page, navigate to **Call Routing > Directory Number** and click **Find**. See Figure 10-24 for an example of this page.

Figure 10-24 Find and List Directory Numbers



10. You will see the number you just changed twice, once in the Internal_PT partition and once without any partition.

Note: When you change the partition of a directory number from **Device > Phone**, CUCM creates a copy of the number with the new partition. The Find and List Directory Numbers page shows some of the directory numbers you might have forgotten about, like the numbers in the 10XX range, which were created when autoregistering phones in Lab 9-3. While you can delete directory numbers here, the safer option is to run **Call Routing > Route Plan Report**, and from the Find pull-down list, select **Unassigned DN** and click **Find**. This will show only the directory numbers that are not assigned.

---

11. If you change the partition of a directory number from the Directory Number list, it updates the entry and does not copy it. Click the next directory number after the one in the Internal_PT.

12. In the Directory Number Information section, select **Internal_PT** from the Route Partition drop-down list.

13. Click the **Save** button. The phone should refresh the display.

14. With the Related Links drop-down list on **Back To Find/List**, click the **Go** button.

15. The Find and List Directory Numbers page shows that the number was not duplicated.

16. From the newly changed extension, can you call the previously changed extension? Why or why not?

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Note: There is a third way to change the partition assigned to directory numbers that will be discussed in Task 4.

Task 3: Create Calling Search Spaces

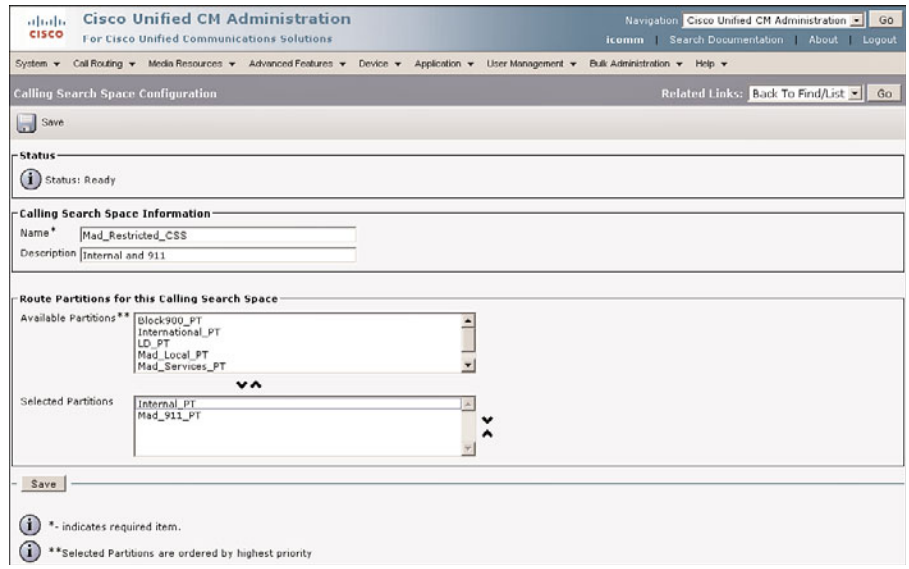
Use Table 10-8 to create the CSSs for SOI.

Step 3-1: Create the Mad_Restricted_CSS Calling Search Space

On the Cisco Unified CM Administration page, navigate to **Call Routing > Class of Control > Calling Search Space**.

1. Click the **Add New** button.
2. In the Name field, enter **Mad_Restricted_CSS**.
3. In the Description field, enter **Internal and 911**.
4. From the Route Partitions for this Calling Search Space section, hold the **Ctrl** key while clicking to highlight both **Internal_PT** and **Mad_911_PT** in the Available Partitions box.
5. Click the **down arrow** (between the Available Partitions and the Selected Partitions boxes) to move the highlighted partitions to the Selected Partitions box. The arrows to the right of the Selected Partitions box can be used to prioritize the partitions, as discussed previously. See Figure 10-25 for an example of this page.
6. Click the **Save** button.

Figure 10-25 Calling Search Space Configuration



Step 3-2: Create the Mad_Guest_CSS Calling Search Space

If you are still on the previous CSS page, click the **Add New** button. If not, on the Cisco Unified CM Administration page, navigate to **Call Routing > Class of Control > Calling Search Space** and click the **Add New** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

1. In the Name field, enter **Mad_Guest_CSS**.
2. In the Description field, enter **Internal, 911, Local, and Toll-Free**.
3. From the Route Partitions for this Calling Search Space section, hold the **Ctrl** key while clicking to highlight **Internal_PT**, **Mad_911_PT**, **Mad_Local_PT**, and **TF_PT** in the Available Partitions box.
4. Click the **down arrow** (between the Available Partitions and the Selected Partitions boxes) to move the selections to the Selected Partitions box. The arrows to the right of the Selected Partitions box can be used to prioritize the partitions, as discussed previously.
5. Click the **Save** button.

Step 3-3: Create the Mad_Employee_CSS Calling Search Space

If you are still on the previous CSS page, click the **Add New** button. If not, on the Cisco Unified CM Administration page, navigate to **Call Routing > Class of Control > Calling Search Space** and click the **Add New** button.

1. In the Name field, enter **Mad_Employee_CSS**.
2. In the Description field, enter **All except 900 and International**.
3. From the Route Partitions for this Calling Search Space section, hold the **Ctrl** key while clicking to highlight **Internal_PT**, **Mad_911_PT**, **Mad_Local_PT**, **TF_PT**, **Mad_Service_PT**, **LD_PT**, and **Block900_PT** in the Available Partitions box.
4. Click the **down arrow** to move the selections to the Selected Partitions box. (Only the **International_PT** should be left in the Available Partitions box.)
5. Click the **Save** button.

Step 3-4: Create the Mad_Unrestricted_CSS Calling Search Space

If you are still on the previous CSS page, click the **Add New** button. If not, on the Cisco Unified CM Administration page, navigate to **Call Routing > Class of Control > Calling Search Space** and click the **Add New** button.

1. In the Name field, enter **Mad_Unrestricted_CSS**.
2. In the Description field, enter **All numbers**.
3. From the Route Partitions for this Calling Search Space section, hold the **Ctrl** key while clicking to highlight **Internal_PT**, **Mad_911_PT**, **Mad_Local_PT**, **TF_PT**, **Mad_Service_PT**, **LD_PT**, and **International_PT** in the Available Partitions box.
4. Click the **down arrow** to move the selections to the Selected Partitions box. (Only the **Block900_PT** should be left in the Available Partitions box.)
5. Click the **Save** button.

Task 4: Assign Calling Search Spaces and Partitions

Now that both CSSs and partitions are created, you are ready to assign them. In a production environment, because of the chance of blocking calls, this naturally would be a procedure best done after hours. Assigning the CSSs to directory numbers first (handing out "keys") before assigning the partitions to the route patterns (putting on "locks") is the safest method.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

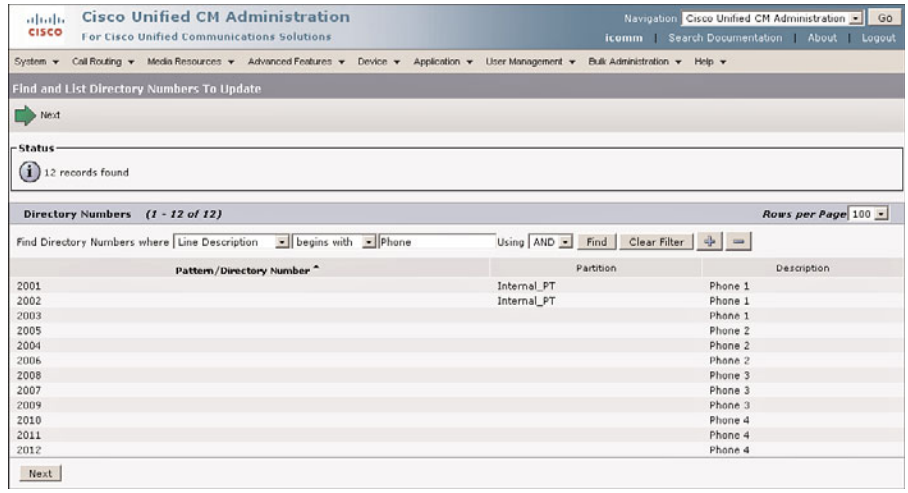
Step 4-1: Assign a CSS and Partition to the Directory Numbers

You might be thinking it will take forever to go to each directory number and assign a CSS and partition. But, do not forget that you can use the Bulk Administration Tool (BAT)! (You do not even have to export and import files to use BAT for this.)

To find the lines, on the Cisco Unified CM Administration page, navigate to **Bulk Administration > Phones > Add/Update Lines > Update Lines**.

1. Click the **Find** button or use drop-down lists to filter the results. In Figure 10-26, the line description that begins with Phone was used to select just those lines. See Figure 10-26 for an example of this page.

Figure 10-26 Find and List Directory Numbers to Update

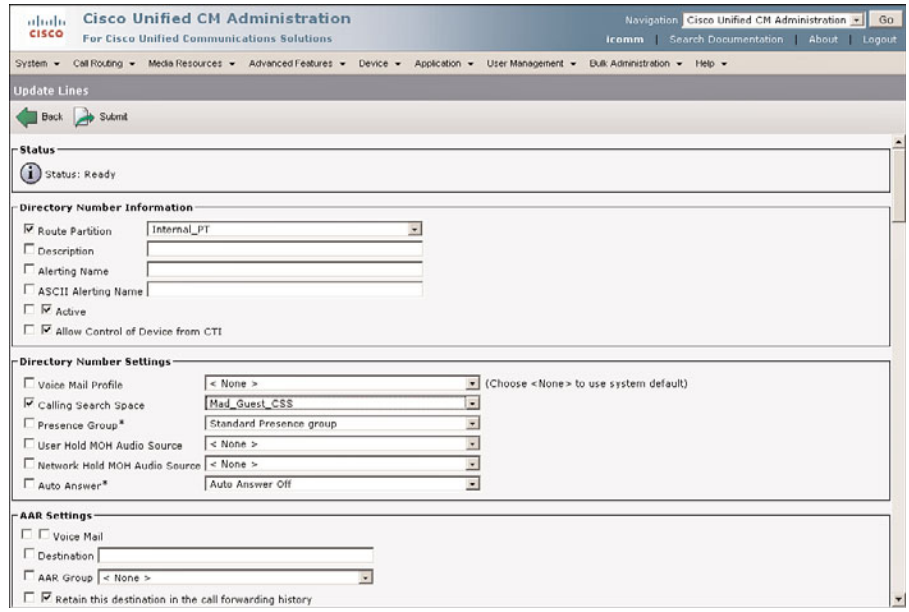


2. Click the **Next** button.
3. In the Directory Number Information section, select the **Route Partition** check box, and from the drop-down list, select **Internal_PT**.
4. In the Directory Number Settings section, select the **Calling Search Space** check box, and from the drop-down list, select **Mad_Guest_CSS**. See Figure 10-27 for an example of this page.
5. By default, the job is set to **Run Later**. Scroll down to the bottom of the page and click the **Run Immediately** radio button.
6. Click the **Submit** button and the job will be sent to the Job Scheduler.
7. To view the status of the job, on the Cisco Unified CM Administration page, navigate to **Bulk Administration > Job Scheduler** and click the **Find** button if your job does not show. Keep clicking **Find** until the Status shows as completed.
8. Click the hyperlinked **Job Id** to view the results. The Job Result Status field should show Success.
9. On the Cisco Unified CM Administration page, navigate to **Call Routing > Directory Number** and click **Find**. You should see that all the directory numbers on phones show the Internal_PT partition.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-27 Update Lines



10. From any of the extensions, can you call to a long-distance number? Why or why not?

_____

_____

_____

11. From the newly changed extension, can you call the previously changed extension? Why or why not?

_____

_____

_____

Step 4-2: Assign a Partition to a Route Pattern

To enforce the Class of Control for external calls, a partition needs to be assigned to each of the route patterns. Start by verifying that phones can call to an international number, such as 9011223334444#.

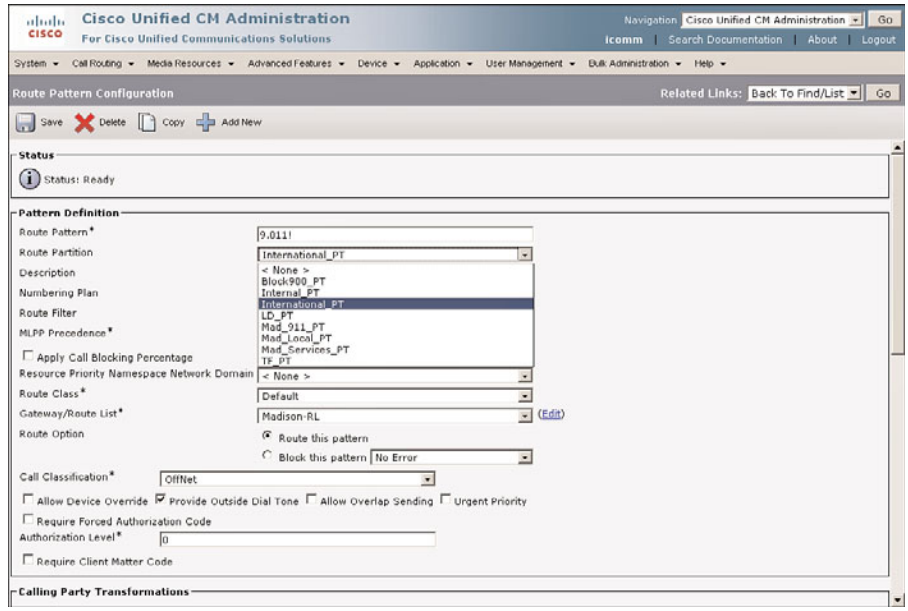
On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Pattern**. Click **Find** if no patterns are showing.

1. Click the **9.011!** pattern.
2. In the Pattern Definition section, select **International_PT** from the Route Partition drop-down list. See Figure 10-28 for an example of this page.
3. Click the **Save** button.
4. Click **OK** for both of the pop-up windows.
5. With the Related Links set to **Back To Find/List**, click the **Go** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-28 Partition Assignment to Route Pattern Configuration



Step 4-3: Assign Partitions to All the Route Patterns

Now that you know how to assign partitions to a route pattern, it is necessary to complete assignments for the other route patterns.

1. Repeat Step 4-2 for the 9.011!# route pattern.

   Now, if you place a call to an international number, you should get a busy signal right after you dial the 90, as the International_PT partition is not part of the Mad_Guest_CSS Calling Search Space the directory number has access to.

2. Repeat Step 4-2 for each of the route patterns, using Table 10-7 to determine the correct partition to apply. When you are done, go back to the Find/List page. See Figure 10-29 for an example of this page.

Note: Normally, the partitions are created before the route patterns, so they can be applied when the patterns are created. This lab book introduced Class of Control later to avoid too much complexity and troubleshooting when first encountering route patterns.

---

3. When all the partitions are assigned, what number categories should any extension be able to call? _____

4. Verify that you can call all those number categories before proceeding. Troubleshoot if you cannot make all the calls expected.

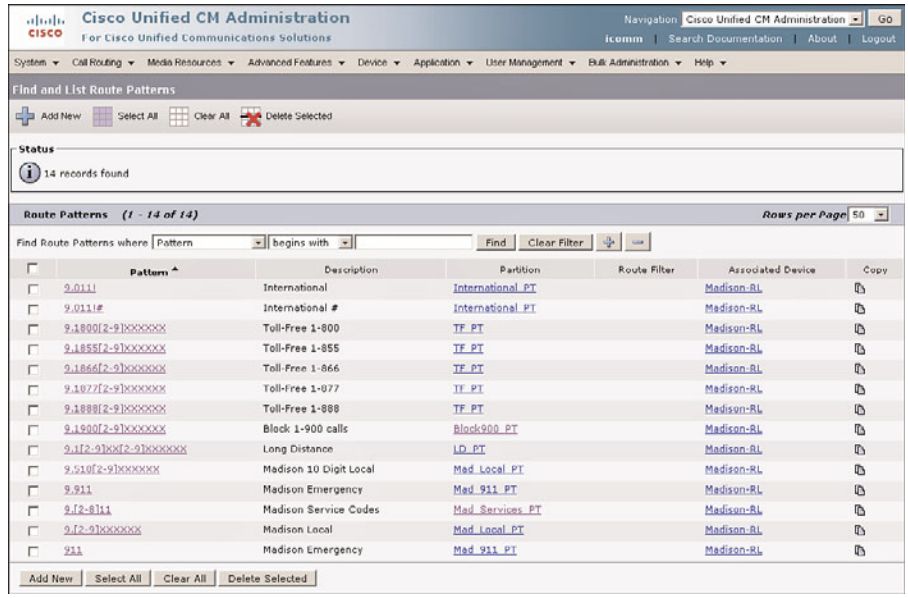
Note: You *need* to test *every* call category, as users will almost never open a ticket to complain if they can make international calls when they should not be able to. Without adequate testing, the misconfiguration is only discovered when a much larger-than-expected bill from the telephony provider arrives.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-29 Route Patterns with Partition Assignments



Step 4-4: Assign a CSS to a Gateway

Call from one extension to another, but place the call as a local call over the PSTN. (For example, if you were calling extension 2010, use 95552010.) This call is in a route pattern you should have access to, but the call will not complete. The reason the call fails is that the gateway is also a device, and it needs a CSS to route calls *into* your system.

Note: The absence of a CSS impacts *all* calls in from the PSTN. Calling your own extensions over the PSTN is simply the easiest way to run a test. If there is another pod connected to the PSTN, you can verify that its system cannot call you either.

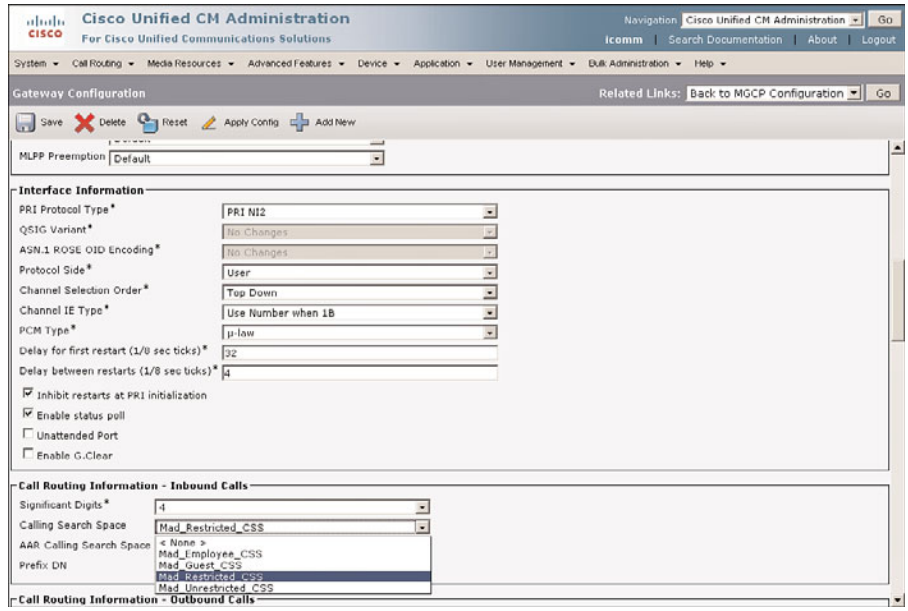
On the Cisco Unified CM Administration page, navigate to **Device > Gateway**. Click **Find** if no gateways are showing.

1. Click the FQDN of the router.
2. For MGCP gateways, the CSS is applied to the interfaces. Click the icon for the PRI interface.
3. Scroll down to the Call Routing Information – Inbound Calls section and select **Mad_Restricted_CSS** from the Calling Search Space drop-down list. The router only needs to be able to connect to internal extensions, so this CSS should be adequate. See Figure 10-30 for an example of this page.
4. Click the **Save** button. Click **OK** to close the pop-up window informing you about applying the configuration.
5. Click the **Apply Config** button. Click **OK** to close the Apply the Configuration pop-up window.
6. All inbound calls from the PSTN should now connect. If not, make sure that there are no calls using the gateway at this time; then wait one minute and try again. If necessary, use the **Save** and **Apply Config** buttons a second time, and then wait one minute for the gateway to complete the configuration before trying the call again.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-30 Inbound CSS Assignment on a Gateway



Step 4-5: Assign a CSS to a Phone

Each directory number should have the Mad_Guest_CSS Calling Search Space assigned. We know that phones can also be assigned a CSS, and they are merged with the CSS on the line (directory number), with the line CSS having priority in the event of a duplicate match. Test this concept by assigning the phone the Mad_Unrestricted_CSS Calling Search Space.

On the Cisco Unified CM Administration page, navigate to **Device > Phone**. Click **Find** if no phones are showing.

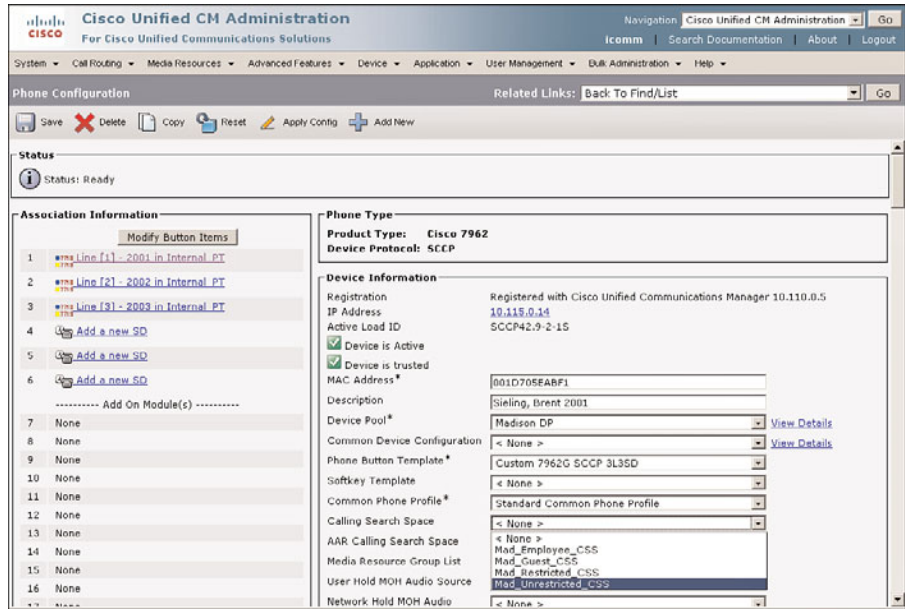
1. Click the device name of the first phone.
2. In the Device Information section, select **Mad_Unrestricted_CSS** from the Calling Search Space drop-down list. See Figure 10-31 for an example of this page.
3. Click the **Save** button. Click **OK** to close the pop-up window informing you about applying the configuration.
4. Click the **Apply Config** button. Click **OK** to close the Apply the Configuration pop-up window.
5. Calls from any extension on the first phone should work to any number category on the PSTN.

It is important to understand that even though the directory number has only limited calling, the phone CSS is allowing all the calls. Make sure to verify that the extension can call premium-rate (1-900) numbers.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-31 Assigning a CSS to a Phone



Step 4-6: Experiment with Line/Phone CSS Interaction

As demonstrated in the previous step, by combining the line CSS with the phone CSS, calls that the line CSS does not match can be completed by searching the phone CSS. However, what happens when the line CSS matches a blocked pattern? The Mad_Employee_CSS Calling Search Space allows long-distance, but blocks the premium-rate numbers. Will Mad_Unrestricted_CSS allow the call? Test this concept.

On the Cisco Unified CM Administration page, navigate to **Device > Phone**. Click **Find** if no phones are showing.

1. Click the device name of the first phone.
2. In the Association Information section, click **Line [1]** to open the Directory Number Configuration page.
3. In the Directory Number Settings section, select **Mad_Employee_CSS** from the Calling Search Space drop-down list.
4. Click the **Save** button. Wait for the phone to update the display.
5. From the first line on the first phone, call 19003334444. The call should be blocked, because the match in the line CSS has priority over the phone CSS.

Note: Do not forget that the order of the partitions *within* the CSS also determines the priority. You might wonder whether the order of the LD_PT and Block900_PT matters in Mad_Employee_CSS. In this case, it does not, as the best-match rule causes 1-900 calls to always match the blocked pattern, regardless of the order. The order of the partitions in the CSS only matters to identical matches, like the duplicate 1701 extensions in Table 10-4. To verify this, test it yourself.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 4-7: Challenge: Complete the Testing

So far, you have tested the Mad_Guest_CSS Calling Search Space on a line, and Mad_Guest_CSS and Mad_Employee_CSS on a line while the phone has Mad_Unrestricted_CSS assigned. That leaves plenty of other configurations that should be tested.

While this step might seem like busywork, understanding partitions and CSS interaction is one of the most confusing topics for new voice engineers. You will undoubtedly run into problems on a job where a call will not work when it should. Knowing the basic process of Class of Control call flow is essential. Advanced topics such as number translations only increase the complexity.

Test the following items:

1. A line with Mad_Restricted_CSS without a CSS on the phone.
2. A line with Mad_Employee_CSS without a CSS on the phone.
3. A line with Mad_Unrestricted_CSS while the phone has Mad_Employee_CSS assigned. Do the premium-rate calls still work?
4. Other combinations until you have a completely clear picture of Class of Control call flow.

Step 4-8: Cleanup

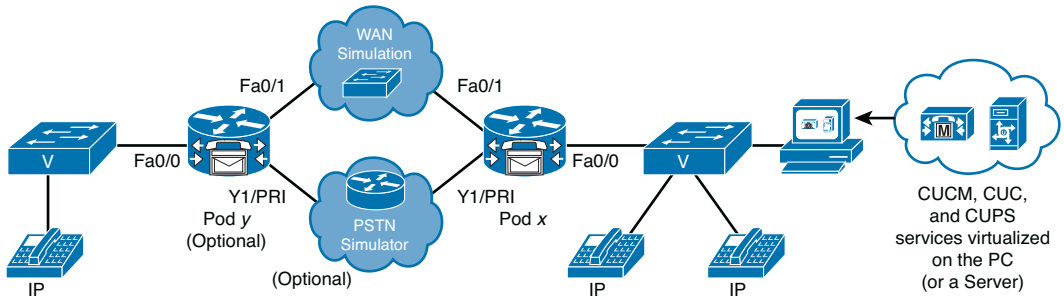
To avoid the partitions and CSSs causing problems in later labs, use BAT to set the directory numbers to **Mad_Unrestricted_CSS**. You can also use BAT to set the phones back to the **<none>** CSS. This should make it consistent that all directory numbers are able to make all calls.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 10-3: Centralized Cisco Unified Communications Manager (CUCM)–to–Branch Office Call Routing

Figure 10-32 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- Configuration from Lab 10-2
- Two or more IP Phones registered (desk phone or soft phone on PC or Windows VM)

Optional hardware components (see Scenario for details):

- Cisco router configured as a PSTN Simulator
- T1/E1/PRI Multiflex Trunk VWICs or network modules
- Digital signal processor (DSP) resources in the routers (PVDM chips) to enable the Multiflex Trunks
- Second router from another pod to act as branch office for this pod

Learning Objectives

Upon completion of this lab, you will be able to

- Understand and configure Call Admission Control (CAC)
- Understand and configure Automated Alternate Routing (AAR)
- Understand and configure Call Forward Unregistered (CFUR)
- Understand Survivable Remote Site Telephony (SRST) failover on branch routers

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Scenario

Shiny Objects Inc. (SOI) has calls working between phones at headquarters and to the PSTN. It now wants to make and receive calls from branch offices. It is rightfully concerned about not having enough WAN bandwidth, or WAN failure causing calls to fail between locations.

Note: Having T1/PRI interfaces and a PSTN Simulator is not necessary to complete the lab. However, without those items, you will not be able to test your configuration.

There are two types of call failure that impact branch offices. The first type of failure is when there is not enough bandwidth for all the voice (and video) calls on the network (especially WAN links). The second type of failure is when there is a lack of connectivity somewhere in the WAN. To solve both of these problems, calls can be routed to the PSTN, but the solutions involve different mechanisms.

This lab is based on the configuration from Lab 10-2. Verify that you can call between the VoIP phones in your pod. Troubleshoot if necessary.

Task 1: Examine Call Admission Control (CAC)

As discussed in the "Quality of Service (QoS)" section of Chapter 6, QoS allocates priority bandwidth for voice and video calls. If more simultaneous calls are put in the priority queue than the bandwidth will allow, all calls suffer in quality. To prevent this, CAC is used to limit the number of calls allowed between locations. CAC can be built into the QoS protocol, such as the Resource Reservation Protocol (RSVP), when using Integrated Services QoS. When using Differential Services QoS, the CAC needs to be provided separately. In a distributed call control environment, gateways and gatekeepers can provide this functionality. In a centralized environment, CUCM can provide the CAC functionality, which is why locations and regions were configured in Lab 9-4, Tasks 4 and 5. By changing the device pool assigned to a phone, CUCM will enforce the settings for the new region and location. This is true even if the phone does not physically move!

Step 1-1: Examine the Settings for Regions and Locations

On the Cisco Unified CM Administration page, navigate to **System > Region** and click the **Find** button if no regions are listed.

Click the **Madison Region** and verify that the Madison–to–New York bandwidth is 8 kbps and the Madison-to-Chicago bandwidth is 16 kbps (if your phone supports the iLBC codec; otherwise, it should be 64 kbps). The region determines the codec that will be used for calls within and between regions.

On the Cisco Unified CM Administration page, navigate to **System > Location** and click the **Find** button if no locations are listed. Each location should have 50 for the audio bandwidth (except the default Hub_None and Phantom, which should be Unlimited). The location determines the total bandwidth of calls into and out of a site.

Step 1-2: Examine Call Statistics on a Phone

Place a phone call between two phones, and *while the call is active*, press twice *quickly* on the Question Mark key (see Figure 10-33) on one or both phones. (If you do not press quickly enough, you get the help menu instead.) An alternate method for desk phones (does not work on soft phones) is to press the Settings button and navigate to **Status > Call Statistics**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

The call statistics on the phone show the codec used. In Figure 10-33, you can see the codec used is G.722, because both phones support it. (G.722 has the same 64-kbps bandwidth for the audio as G.711, but supports better audio quality. Not all phone models support G.722, in which case you will see the call as G.711.) Note: The call statistics on a desk phone will have more information and look slightly different than what is shown in the soft phone in Figure 10-33.

Figure 10-33 Call Statistics on a Soft Phone

Step 1-3: Change a Phone to the New York Device Pool

On the Cisco Unified CM Administration page, navigate to **Device > Phone** and click the **Find** button if no phones are listed.

1. Click the device name of an active phone to see the details.
2. In the Device Information section, change the Device Pool drop-down list to **New York DP**.
3. Click the **Save** button. A pop-up window will tell you to "Click the Apply Button to have the changes take effect." Click **OK** to close the pop-up window.
4. Click the **Apply Config** button.
5. The Apply Configuration pop-up window will open and show the devices that will be impacted. Click **OK** to close the window. You should see the phone do a quick restart before the changes take effect.

Note: If you do not see the display refresh after clicking the **Apply Config** button, repeat the step to make sure that the changes take. If you are still experiencing problems, try moving a different phone to the New York device pool. In one case, I had more than one phone that could not place calls when moved to the Chicago device pool. After ruling the phones out, I finally had to delete and re-create the Chicago region and location before a phone would work correctly in Chicago.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

6. Call from the New York phone to a phone in Madison, and while the call is active, press twice quickly the Question Mark key on one or both phones. The codec used should now be G.729, as the call is going between the New York and Madison regions. Put the call on hold on both phones.
7. Use the next **Line** button to place a second phone call between the two phones. Put this call on hold.
8. Use the next **Line** button to attempt a third call between the two phones. You will get a busy signal, and the phone will show "Not Enough Bandwidth" on the display. See Figure 10-34 for an example of this.

Figure 10-34 Not Enough Bandwidth on the Phone

9. Hang up all calls.

Step 1-4: Determine Bandwidth Needed for G.729 Calls

The CUCM is using CAC to prevent the third call between the two phones to meet the limit of the bandwidth and codec set for the regions and locations. Because the G.729 codec uses 8 kbps, you might think that 50 kbps of bandwidth between Madison and New York should allow 50 kbps / 8 kbps per call = 6 simultaneous phone calls. However, VoIP calls run the audio using the Real-time Transport Protocol (RTP) over UDP over IP (plus the Layer 2 frame overhead), so it works out that only two calls work with 50 kbps. How close (or far) are you from running a third call? Estimate what you think the total bandwidth for two G.729 calls should be.

On the Cisco Unified CM Administration page, navigate to **System > Location** and click the **Find** button if no locations are listed.

1. Click the **New York Location**.
2. In the Audio Calls Information section, enter your estimate of the bandwidth in the Audio Bandwidth kbps box.
3. Click the **Save** button.
4. Test your estimate by attempting two simultaneous calls. If you are able to place the calls, keep lowering the number of your estimate. If you cannot make two calls, raise the number of your estimate until you find the exact amount needed for two calls. From there, it should be easy to determine what the bandwidth is for just one G.729 call.

https://t.me/learningnets
From the Library of Aliwarman Tarihoran

How much bandwidth is needed for a single G.729 call? _____

Note: This number is just the amount of bandwidth that CUCM uses for calculations. It is close to, but might not be the actual, bandwidth used, as the actual bandwidth will vary based on the Layer 2 frame header size.

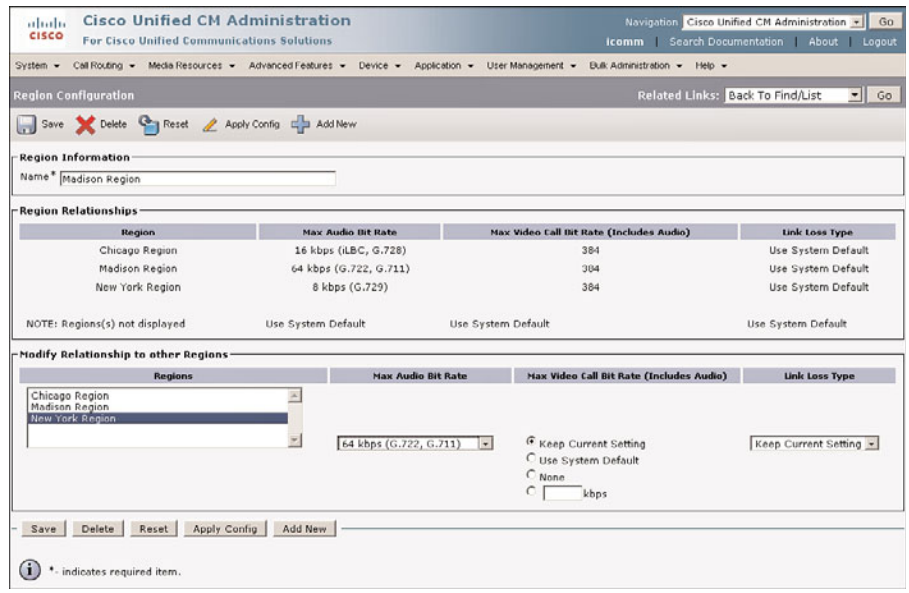
Step 1-5: Determine Bandwidth Needed for G.711 Calls

Because G.711 (and G.722) uses 64 kbps for the audio only, what is the actual bandwidth needed for a single G.711 call? To determine this, the bandwidth between Madison and New York needs to be changed.

On the Cisco Unified CM Administration page, navigate to **System > Region** and click the **Find** button if no regions are listed.

1. Click the **Madison Region**.
2. In the Modify Relationships to Other Regions section, select **New York Region** in the Regions box.
3. From the Max Audio Bit Rate drop-down list, select **64 kbps (G.722, G.711)**. See Figure 10-35 for an example of this page.

Figure 10-35 Modify Madison–to–New York Region Bandwidth



4. Click the **Save** button and the Region Relationships section will update to show the 64 kbps.

   Realize that the lower limit for *both* locations will constrain the call, so the Madison location should be increased before changing the New York location.

5. On the Cisco Unified CM Administration page, navigate to **System > Location** and click the **Find** button if no locations are listed.
6. Click the **Madison Location**.
7. In the Audio Calls Information section, enter **150** in the Audio Bandwidth kbps box.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

8. Click the **Save** button.

   Now the New York location will serve as the lowest bandwidth. Given the difference between the 8 kbps that G.729 uses for audio and the actual bandwidth needed for G.729, start with adding that value to the 64 kbps.

9. On the Cisco Unified CM Administration page, navigate to **System > Location** and click the **Find** button if no locations are listed.

10. Click the **New York Location**.

11. In the Audio Calls Information section, enter your estimate of the bandwidth in the Audio Bandwidth kbps box.

12. Click the **Save** button.

13. Test your estimate by attempting one call. If you are able to place the call, keep lowering the estimated number. If you cannot make a call, raise the estimated number until you find the exact amount needed for a single call.

How much bandwidth is needed for a single G.711 call? _____

Step 1-6: Determine Bandwidth Needed for iLBC Calls

This step assumes that you have phones that support the Internet Low Bandwidth Codec (iLBC). If you configured Madison to Chicago with G.711 in Lab 9-4, Step 4-4, skip this step. By default, iLBC in CUCM uses 15.2 kbps. Use the difference between the 8 kbps that G.729 uses for audio and the actual bandwidth needed for G.729 to develop a starting estimated value for iLBC calls. If you have a third phone, move it to the Chicago device pool, or move the New York phone to the Chicago device pool.

On the Cisco Unified CM Administration page, navigate to **Device > Phone** and click the **Find** button if no phones are listed.

1. Click the device name of an active phone to see the details.

2. In the Device Information section, change the Device Pool drop-down list to **Chicago DP**.

3. Click the **Save** button. A pop-up window will tell you to "Click the Apply Button to have the changes take effect." Click **OK** to close the pop-up window.

4. Click the **Apply Config** button.

5. The Apply Configuration pop-up window will open and show the devices that will be impacted. Click **OK** to close the window. You should see the phone do a quick restart before the changes take effect.

6. On the Cisco Unified CM Administration page, navigate to **System > Location** and click the **Find** button, if no locations are listed.

7. Click the **Chicago Location**.

8. In the Audio Calls Information section, enter your estimate of the bandwidth in the Audio Bandwidth kbps box.

9. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

10. Test your estimate by attempting one call. If you are able to place the call, keep lowering the estimated number. If you cannot make a call, raise the estimated number until you find the exact amount needed for a single call.

How much bandwidth is needed for a single iLBC call? _____

Step 1-7: Cleanup

Make sure that there is bandwidth to make only one call between Madison and both New York and Chicago phones. If necessary, change the location bandwidth and region codec to ensure that one call will work, but two will not.

Task 2: Implement Alternate Automatic Routing (AAR)

Note: This task can be configured without any router or PSTN Simulator. To be able to test this, however, you will need two routers and the PSTN Simulator. The easiest option would be to borrow a router (and the PSTN connection) from another pod.

Now that CAC is limiting calls to protect call quality, excess calls get blocked. However, these calls can be routed across the PSTN using AAR. AAR works by determining the full PSTN number for the extension of the called party and directing the call to the PSTN gateway.

Note: AAR only covers calls denied because of the oversubscription of the voice bandwidth. As such, the phone is still in contact over the data bandwidth to CUCM and is still registered. Loss of contact to the phone over the WAN is not covered by AAR; instead that is part of Call Forward Unregistered (CFUR) and Survivable Remote Site Telephony (SRST), which are covered in the next task.

This task will show just the bare minimum configuration needed to route a call from Madison that fails because of bandwidth restrictions over the PSTN to a phone at the branch office. The configuration will use the Madison CSS and will not allow the branch office phones to make calls to the local gateway to reach the PSTN. Setting this up more realistically is discussed in the challenge step at the end of the task.

Step 2-1: Set Up Branch Office Gateway

It is necessary to configure a gateway for the branch office to have AAR work. You might think that you can use your existing gateway and call out to the seven- or ten-digit number for the branch phone, but because the call will come back into the system from the gateway in Madison, the system knows the only way to get to New York is over the WAN, and will still block the call. CUCM needs to see the call enter a gateway to reach the phone without using the WAN. To set up a gateway for the New York branch office:

1. Create a CLI configuration for the branch router using the same basic configuration used for the Madison HQ router, but also do the following:
   - Change the host name to match the pod number you borrowed it from.
   - While the DHCP pools should hand out IP addresses in the range of the other pod, the option 150 still needs to point to *your* CUCM server's IP address.
   - Set the IP address on the fa0/1 physical interface on *both routers* to be 10.0.0.x /24, where *x* is the pod number.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- Connect the fa0/1 interfaces to access ports on the WAN switch if there is more than one pod completing this lab; otherwise, a crossover cable to simulate the WAN between the two routers is fine.
- Configure EIGRP on *both routers* to exchange route information.

Note: If you have another PC with a soft phone, you can connect directly to a switch to act as the branch office phone. If you are using a desk phone for the branch office, but do not have a second switch with Power over Ethernet (PoE) (or a power brick) for the phone on the branch router, just add the new data and voice VLANs on the existing PoE switch. Configure a new trunk port to the other router and a few ports using the new data and voice VLANs for the phone. This will keep them isolated from the HQ router phones.

Example 10-2 shows a brief code configuration where the branch router is borrowed from pod 2. Notice that while the IP addresses of the DHCP pools are local to the branch router, the option 150 still points to the CUCM server in *your* pod. The highlighting shows what needs to be changed if you use a different pod; adjust the configuration as necessary to match your situation.

Example 10-2 Sample Branch Office Configuration Using the Pod 2 Router

```
Router(config)# hostname RtrPod2
RtrPod2(config)# no ip domain-lookup
RtrPod2(config)# ip domain-name soi.local
RtrPod2(config)# enable secret class
RtrPod2(config)#!
RtrPod2(config)# ip dhcp excluded-address 10.20.0.1 10.20.0.10
RtrPod2(config)# ip dhcp excluded-address 10.25.0.1 10.25.0.10
RtrPod2(config)#!
RtrPod2(config)# ip dhcp pool Data
RtrPod2(dhcp-config)# network 10.20.0.0 255.255.255.0
RtrPod2(dhcp-config)# default-router 10.20.0.1
RtrPod2(dhcp-config)# option 150 ip 10.110.0.5
RtrPod2(dhcp-config)#!
RtrPod2(dhcp-config)# ip dhcp pool Voice
RtrPod2(dhcp-config)# network 10.25.0.0 255.255.255.0
RtrPod2(dhcp-config)# default-router 10.25.0.1
RtrPod2(dhcp-config)# option 150 ip 10.110.0.5
RtrPod2(dhcp-config)# !
RtrPod2(dhcp-config)# interface FastEthernet0/0
RtrPod2(config-if)# no shut
RtrPod2(config-if)# !
RtrPod2(config-if)# interface FastEthernet0/0.20
RtrPod2(config-subif)# description Data VLAN
RtrPod2(config-subif)# encapsulation dot1Q 20
RtrPod2(config-subif)# ip address 10.20.0.1 255.255.255.0
RtrPod2(config-subif)# !
RtrPod2(config-subif)# interface FastEthernet0/0.25
RtrPod2(config-subif)# description Voice VLAN
RtrPod2(config-subif)# encapsulation dot1Q 25
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
RtrPod2(config-subif)# ip address 10.25.0.1 255.255.255.0
RtrPod2(config-subif)# !
RtrPod2(config-subif)#int fa0/1
RtrPod2(config-if)# ip address 10.0.0.2 255.255.255.0
RtrPod2(config-if)# no shut
RtrPod2(config-if)#!
RtrPod2(config-if)# router eigrp 1
RtrPod2(config-router)# no auto-summary
RtrPod2(config-router)# network 10.0.0.0
RtrPod2(config-router)# passive-interface fa0/0
RtrPod2(config-router)# !
RtrPod2(config-router)# line con 0
RtrPod2(config-line)# logg sync
RtrPod2(config-line)# exec-time 120 0
RtrPod2(config-line)# line vty 0 15
RtrPod2(config-line)# pass cisco
RtrPod2(config-line)# login
RtrPod2(config-line)# exit
```

2. The existing Madison HQ router needs to be configured to allow calls over the WAN. In Example 10-3, the router for pod 11 is configured. Adjust to match your pod number.

Example 10-3 Changes to the Madison Router Configuration (for Pod 11)

```
RtrPod11(config)# interface FastEthernet0/1
RtrPod11(config-if)# ip address 10.0.0.11 255.255.255.0
RtrPod11(config-if)# no shut
RtrPod11(config-if)# exit
RtrPod11(config)# router eigrp 1
RtrPod11(config-router)# no auto-summary
RtrPod11(config-router)# network 10.0.0.0
RtrPod11(config-router)# passive-interface fa0/0
```

3. With the basic CLI completed, the MGCP gateway needs to be set up in CUCM. Repeat Lab 10-1, Steps 2-2 to 2-4 to create the gateway, but use the following:
   - The branch router host name.
   - A description of "Branch Office MGCP Gateway."
   - When setting up the interface on the gateway, do not forget to assign the New York DP device pool (so that CUCM will see the gateway in New York) and the Mad_Restricted_CSS Calling Search Space (to allow incoming calls to access the phones assigned the Internal_PT partition).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-2: Enable AAR Service Parameter

By default, CUCM does not allow AAR calls. On the Cisco Unified CM Administration page, navigate to **System > Service Parameters**.

1. Select the IP address of the server from the Server drop-down list.
2. The Service drop-down list will appear. Select **Cisco CallManager (Active)**.
3. Scroll down (way down) to the Clusterwide Parameters (System – CCM Automated Alternate Routing) section.
4. Select **True** from the Automated Alternate Routing Enable drop-down list.
5. Click the **Save** button.

Step 2-3: Create AAR Groups

The essence of AAR is that when the WAN call is blocked, the call is directed to the PSTN. Calls sent to the PSTN for branch offices might be local, long-distance, or international. AAR groups allow the system to determine the correct outside-line access digit and PSTN localization (for example, adding a 1 to a number to make it long-distance) needed to make the call complete.

Note: If the Globalized Design Approach to Dial Plans discussed in the *Cisco Unified Communications System 8.x SRND* document is implemented, AAR groups are not needed, as every phone number has the necessary digits to be routed (with modifications for the local gateway).

On the Cisco Unified CM Administration page, navigate to **Call Routing > AAR Group**.

1. Click the **Add New** button.
2. In the Name field, enter **Mad_AAR**.
3. Click the **Save** button. The Prefix Digits Within Mad_AAR section now shows. Because there is no need for AAR within the Madison area, leave this blank. The actual configuration requires more than one AAR group, in much the same way that regions required more than one to effectively configure.
4. Click the **Add New** button.
5. In the Name field, enter **NYC_AAR**.
6. Click the **Save** button. Now the Prefix Digits Between NYC_AAR and Other AARGroups section shows.
7. In both Dial Prefix fields, enter **9**, as this is the number needed for an outside access line. (You do not need to add the 1 for long-distance, because the pod numbers are in the same area code and exchange.) See Figure 10-36 for an example of this page.
8. Click the **Save** button.

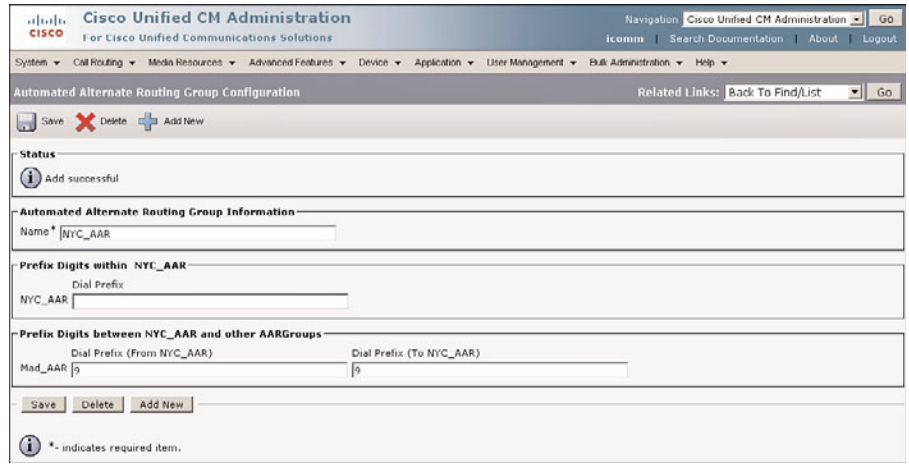
Note: Please do not email Cisco Press or the author about the absurdity of having both Madison, Wisconsin, and New York, New York, in the same area code (which is actually assigned to the San Francisco Bay area), let alone the same exchange! The PSTN Simulator becomes a nightmare to configure when using large numbers of pods in different area codes.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-36 Automated Alternate Routing Group Configuration



Step 2-4: Update Device Pools

Devices (such as phones and gateways) need to have an AAR group and AAR Calling Search Space assigned. You might wonder why there is a CSS for AAR, when the phone or directory number should already have a CSS. The problem is when a phone or directory number has a limited CSS, when AAR redirects the call to the PSTN, the CSS will not allow access to the route patterns. For example, in this lab, you configured the Mad_Restricted_CSS Calling Search Space, which only allows calls to internal and 911 calls. If a user with the Mad_Restricted_CSS Calling Search Space tries to call an internal extension at a branch office, because of insufficient bandwidth, AAR redirects the call. However, Mad_Restricted_CSS does not allow access to the route patterns for local or long-distance, so the call would fail. By assigning a CSS for AAR calls, access to partitions that can complete the call is assured. A separate AAR CSS could be created, but for this lab, Mad_Employee_CSS will be used, as it allows both local and long-distance calls.

The easiest way to apply the AAR group to all the gateways and phones is to use the device pool to apply the settings to all devices at once.

On the Cisco Unified CM Administration page, navigate to **System > Device Pool** and click **Find** if no device pools are showing.

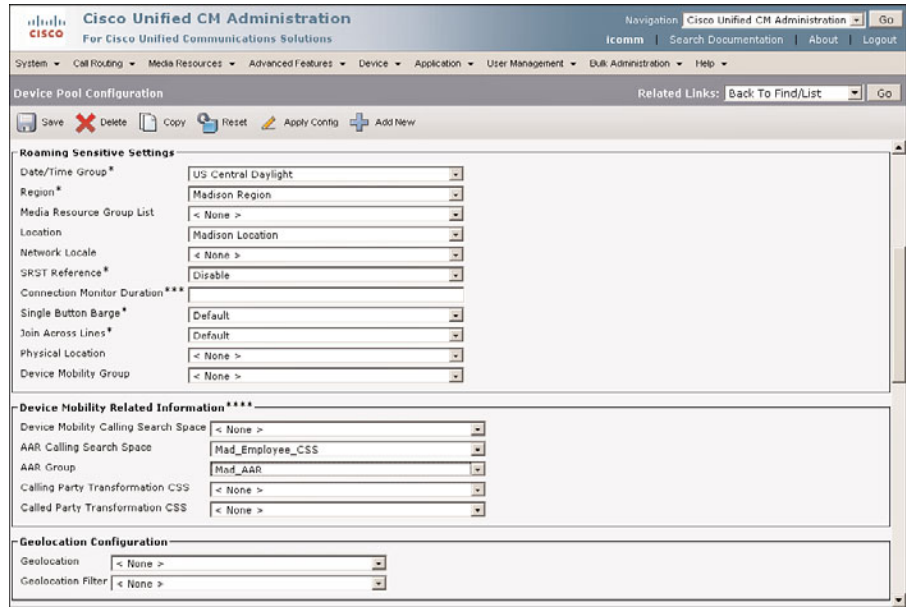
1. Click the hyperlinked **Madison DP** name.
2. Scroll down to the Device Mobility Related Information Section, and select **Mad_Employee_CSS** from the AAR Calling Search Space drop-down list.
3. Select **Mad_AAR** from the AAR Group drop-down list. See Figure 10-37 for an example of this page.
4. Click the **Save** button.
5. The status section informs you that the Reset button is necessary to apply the changes. Click the **Reset** button.
6. The Device Reset pop-up window opens. Click the **Reset** button. The devices will all reset; while you wait for them to boot back up, click the **Close** button to exit the pop-up window.

Repeat this step for the New York DP, but use **NYC_AAR** for the AAR group.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-37 Automated Alternate Routing in Device Pool Configuration



Step 2-5: Configure a Branch Office Phone

Because the calls for the branch office will be inbound from the PSTN Simulator using the interface of another pod, the phone used for the branch office needs to have directory numbers that match the range used by the other pod. On the Cisco Unified CM Administration page, navigate to **Device > Phone** and click **Find**.

1. If you have a phone registered to the New York DP device pool, use that phone. Otherwise, select one of your existing phones for the New York branch office, and change the Device Pool field to **New York DP**.
2. In the Association Information section, click **Line [1]** to open the Directory Number Configuration page.
3. In the Directory Number Information section, enter an extension from the other pod in the Directory Number field.

Note: When you enter the new directory numbers on the lines, the old directory numbers will not be deleted. You can easily switch back to the previous directory numbers later.

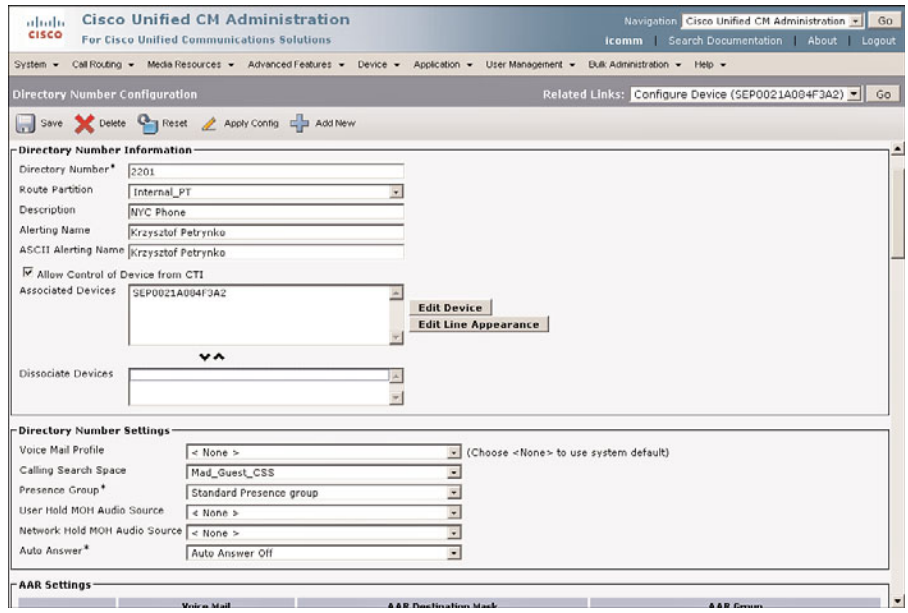
---

4. Make sure that the Route Partition field is **Internal_PT**.
5. Change the Description to **NYC Phone**.
6. Enter a name from the Appendix B table for the other pod for the Alerting Name and ASCII Alerting Name fields.
7. In the Directory Number Settings section, make sure that the Calling Search Space is **Mad_Guest_CSS**. See Figure 10-38 for an example of this page using Pod 2.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-38 Example of Remote Pod Directory Number Using Pod 2



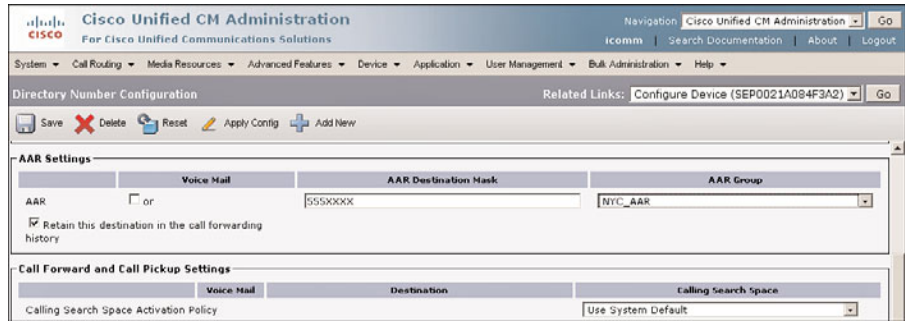
8. In the AAR Settings section, enter **555XXXX** in the AAR Destination Mask field.

Note: If there was an entry in the External Phone Number Mask field in the Line *X* on Device section, that mask would be used to convert the four-digit number to match a seven-digit or long-distance route pattern. Because this lab is not going into advanced dial planning, the External Phone Number Mask field is blank (the mask is currently applied at the route patterns). As a result, the AAR Destination Mask field is used to convert the four-digit number to match a route pattern for local calls. The central office exchange (555 in the labs) is added to the extension to make a seven-digit number. The leading 9 will be added from the AAR group to build a complete local number that matches the local-calls route pattern.

---

9. Select **NYC_AAR** from the AAR Group drop-down list. See Figure 10-39 for an example of this page.

Figure 10-39 AAR Settings on a Directory Number



10. In the Line *X* on Device section, enter the name again for the Display and ASCII Display fields.

11. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Repeat this step to change all the directory numbers on this phone. (If you are setting up a new phone, you will need at least two directory numbers.)

Step 2-6: Testing

Test to verify that AAR is routing the call over the PSTN when there is oversubscription on the WAN link. Remember that this configuration only allows calls from Madison to New York to use AAR. The phone in New York is still using the Madison gateway for outbound calls, instead of the New York gateway. (The New York phone can only receive calls from the New York gateway.)

To verify that the remote office gateway is being used:

1. Use the CLI command **debug isdn q931** on the New York router to monitor the PRI. (If you are able to, use the same command to monitor the Madison gateway at the same time.)
2. Make a call from a line on a Madison phone to the four-digit internal extension of a line on the New York phone. Answer this call and place it on hold, on both sides.
3. Use the next **Line** button on the Madison phone to make a second call to the New York phone. The display on the Madison phone should show "Network congestion, rerouting" and the New York phone should ring. See Figure 10-40 for an example of the Madison phone display.

Figure 10-40 Example of AAR in Action

If the AAR call does not connect, troubleshoot by double-checking all the steps in this task. If the phone display shows "Network congestion, rerouting" but you get a busy signal, the most likely problem is an incorrect AAR Destination Mask on the New York directory number.

4. Answer the second call. The New York router debug will show the incoming call. In Example 10-4, the call to Pod 2 shows the name and number of both the calling and called parties.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Example 10-4 Debug ISDN Q931 of AAR Call to Pod 2

```
RtrPod2# debug isdn q931
debug isdn q931 is              ON.
RtrPod2#
*Sep 23 05:50:57.933: ISDN Se0/1/0:23 Q931: RX <- SETUP pd = 8  callref = 0x0084
        Bearer Capability i = 0x8090A2
                Standard = CCITT
                Transfer Capability = Speech
                Transfer Mode = Circuit
                Transfer Rate = 64 kbit/s
        Channel ID i = 0xA98381
                Exclusive, Channel 1
        Display i = 'Lon Sherman'
        Calling Party Number i = 0x0081, '15105552005'
                Plan:Unknown, Type:Unknown
        Called Party Number i = 0xA1, '5105552201'
                Plan:ISDN, Type:National
        Redirecting Number i = 0x000081, '2201'
                Plan:Unknown, Type:Unknown
*Sep 23 05:50:58.013: ISDN Se0/1/0:23 Q931: TX -> CALL_PROC pd = 8  callref = 0x8084
        Channel ID i = 0xA98381
                Exclusive, Channel 1
RtrPod2#
*Sep 23 05:50:58.013: ISDN Se0/1/0:23 Q931: TX -> ALERTING pd = 8  callref = 0x8084
        Progress Ind i = 0x8088 - In-band info or appropriate now available
RtrPod2#
*Sep 23 05:51:01.545: ISDN Se0/1/0:23 Q931: TX -> CONNECT pd = 8  callref = 0x8084
        Display i = 'Krzysztof Petrynko'
*Sep 23 05:51:02.545: ISDN Se0/1/0:23 Q931: TX -> CONNECT pd = 8  callref = 0x8084
        Display i = 'Krzysztof Petrynko'
RtrPod2#
*Sep 23 05:51:02.557: ISDN Se0/1/0:23 Q931: RX <- CONNECT_ACK pd = 8  callref =
  0x0084
```

5. When you are done testing, hang up all the calls.

Step 2-7: Verify That the AAR CSS Is Working

As discussed in Step 2-4, the device pool has the AAR CSS configured to allow calls over the PSTN, even if the phone and directory number do not have a CSS that allows such access. To test this, follow these steps:

1. Pick one Madison phone, and verify that it has **< None >** as the CSS assigned to it.
2. Change the CSS on all the directory numbers on that phone to **Mad_Restricted_CSS**, which only allows internal and emergency calls.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. Attempt to call the NYC extensions using the seven-digit PSTN number. This should fail because of the restricted CSS.
4. Make a call from a line on a Madison phone to the four-digit internal extension of a line on the New York phone. Answer this call and place it on hold on both sides.
5. Use the Next Line button on the Madison phone to make a second call to the New York phone. The display on the Madison phone should show "Network congestion, rerouting" and the New York phone should ring. The AAR CSS made the call work, even though the line CSS did not have access to the route patterns.
6. When you are done testing, hang up all the calls.
7. Change all the Madison directory numbers back to **Mad_Unrestricted_CSS**.

Step 2-8: Branch Office Dial Plan Challenge

As mentioned at the start of the task, this configuration is the minimum necessary to demonstrate AAR for calls from Madison to the New York branch office. If this was a production system, the phones in New York should be using the New York gateway to place calls, and they should have AAR for calls to Madison, because a single call over the WAN blocks all other calls from New York connecting over the WAN. Additionally, if there are no calls on the WAN, a 911 call from New York goes out the Madison gateway, which should not happen.

Review the steps in Labs 10-1, 10-2, and 10-3 to plan out what would be necessary to make the configuration work as it might be expected to function. After you have your plan established, check out the "Tips to Complete Branch Office Dial Plan" section at the end of this lab to see whether your ideas are correct.

For an (optional) extra challenge, and to improve your understanding of the topics, implement your plan and verify that it works as expected.

Task 3: Implement Survivable Remote Site Telephony (SRST) and Call Forward UnRegistered (CFUR)

Note: This task can be configured without any router or PSTN Simulator. To be able to test this, however, you will need two routers and the PSTN Simulator. The easiest option would be to borrow a router (and the PSTN connection) from another pod.

In the previous task, if calls are blocked by CAC, the calls can be routed across the PSTN using AAR. However, what happens if the WAN is down? In a centralized CUCM deployment, there are two effects:

- All phones at the branch office essentially go dead (unless they are currently on a call). Without a call agent, the phones cannot perform any functions. The solution to this problem is to have the phones register temporarily with the local gateway, which will act as a Survivable Remote Site Telephony (SRST) call agent. SRST is essentially a lightweight configuration of Cisco Unified Communications Manager Express (CUCME).
- CUCM sees the phone as unregistered, so a call from headquarters automatically fails or goes to voicemail (if configured). If the phones at the branch office are able to get access to a call agent, both incoming and outgoing calls could be directed over the PSTN. (Note that this case is different than AAR. In this situation, the CUCM system no longer has any contact with the

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

phone and assumes it no longer active.) The solution to this is the Call Forward UnRegistered (CFUR) setting to direct the call to the correct gateway.

To demonstrate this, disconnect the cable for the WAN link on the Madison router. After a timeout value, the NYC phone will go blank, as it can no longer reach the CUCM system. Reconnect the cable, and after another timeout value, the NYC phone will reregister with CUCM.

There are three ways to configure SRST:

- **Cisco Unified SRST:** The gateway functions as the SRST call agent with basic functionality.
- **SRST Fallback Mode using Cisco Unified CME:** The gateway goes into CME mode when the WAN link goes down. It has more functionality for the phones than Cisco Unified SRST.
- **Cisco Unified Enhanced SRST (ESRST):** Provides the best experience for remote phones, as the SRST configuration is populated and updated by the CUCM system as changes are made. ESRST requires that a Cisco Unified Messaging Gateway be configured.

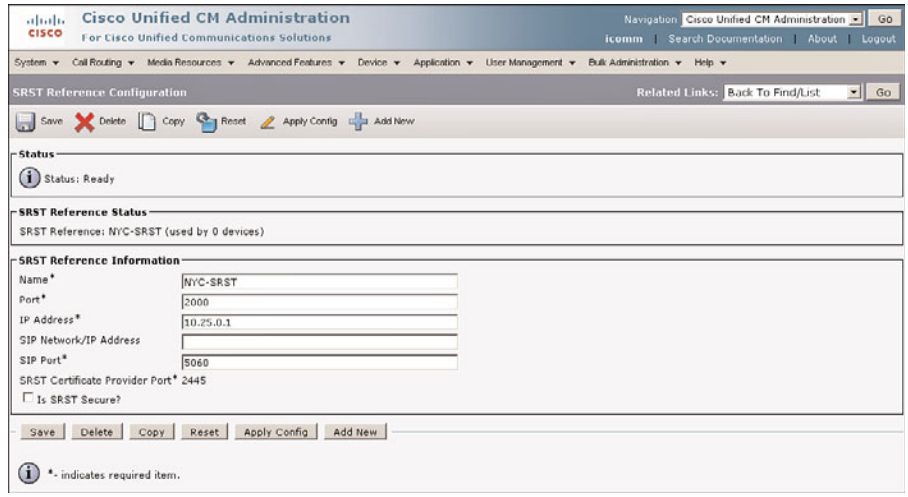
Configuring SRST is not part of the CCNA Voice certification, so this task will show just the bare minimum configuration to have the system function with SRST Fallback Mode using Cisco Unified CME.

Step 3-1: Configure SRST Reference in CUCM

The CUCM system needs to know about the SRST router so that all devices at the location can be told to register to the SRST as a secondary call agent. On the Cisco Unified CM Administration page, navigate to **System > SRST**.

1. Click the **Add New** button.
2. In the Name field, enter **NYC-SRST**.
3. In the IP Address field, enter the IP address of the NYC router voice VLAN subinterface. Make sure that you use the IP address of the LAN side, as the WAN interface might be down and unreachable. (This example will continue to use the pod 2 router from Task 2.) See Figure 10-41 for an example of this page.

Figure 10-41 SRST Reference Configuration



4. Click the **Save** button.

https://t.me/learningnets

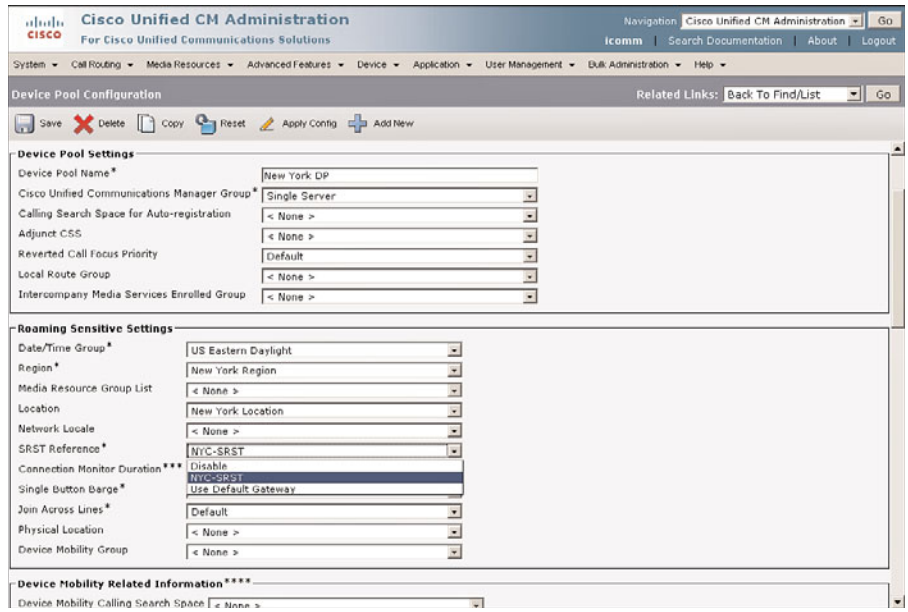
From the Library of Aliwarman Tarihoran

Step 3-2: Apply SRST Reference to Device Pool

By configuring the SRST reference on the device pool, all devices in that pool will know the SRST call agent will be secondary and fail over to it when the CUCM is unreachable. On the Cisco Unified CM Administration page, navigate to **System > Device Pool**. Click **Find** to see the device pools.

1. Click the **New York DP** hyperlinked name.
2. In the Roaming Sensitive Settings section, select **NYC-SRST** from the SRST Reference drop-down list. See Figure 10-42 for an example of this page.

Figure 10-42 SRST Reference on Device Pool



3. Click the **Save** button.
4. The status section informs you that the **Reset** button is necessary to apply the changes. Click the **Reset** button.
5. The Device Reset pop-up window opens. Click the **Reset** button. The devices will all reset; while you wait for them to boot back up, click the **Close** button to exit the pop-up window.
6. After the New York phone is back up, verify the SRST configuration. Press the **Settings** button and navigate to **Device Configuration**.
7. (Soft phones can skip this step.) In the device configuration, select **Unified CM Configuration**.
8. The display should show Unified CM 1 as Active and Unified CM 2 SRST. See Figure 10-43 for an example of the phone display.
9. Press the **Exit** softkey to return to the normal phone display.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-43 Viewing SRST Reference on the Phone

Step 3-3: Configure Router for SRST

The router needs to be told how to reach the CUCM system. There are two parts to this. First, the router needs to be configured to act as SRST, and second, because the PRI is controlled by MGCP from CUCM, the router needs to take over MGCP call processing when the WAN is down. In the following example, *x* is the pod number of the NYC router. It should result in the IP address of the NYC router voice VLAN subinterface. The *yy* needs to be replaced with the first two digits of the extensions of the NYC pod, which vary depending on the pod you use. (For example, Pod 4 has extensions 2400 to 2499, so replace *yy* with 24.) The final step is to force the PRI to start with channel 1 for outgoing calls, because the MGCP configuration has set the router to use more channels than the PSTN Simulator supports. If your PRI interface is in a different slot than 0/2/0, adjust as necessary.

Note: The following commands assume that the IOS is Release 12.3(14)T or later.

```
RtrPodx(config)# call-manager-fallback
*Sep 23 22:59:49.851: %LINEPROTO-5-UPDOWN: Line protocol on Interface EDSP0, changed
state to up
RtrPodx(config-cm-fallback)# ip source-address 10.x5.0.1
RtrPodx(config-cm-fallback)# max-ephones 3
RtrPodx(config-cm-fallback)# max-dn 5 dual-line
RtrPodx(config-cm-fallback)# dialplan-pattern 1 510555yy.. extension-length 4
RtrPodx(config-cm-fallback)# exit
RtrPodx(config)# ccm-manager fallback-mgcp
RtrPodx(config)# application
RtrPodx(config-app)# global
RtrPodx(config-app-global)# service alternate Default
RtrPodx(config-app-global)# interface s0/2/0:23
RtrPodx(config-if)# isdn bchan-number-order ascending
RtrPodx(config-if)# exit
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-4: Configure Dial Peers for SRST

After the SRST router takes over the MGCP gateway role, it needs to be able to route calls properly. A subset of the dial peers used in Lab 6-5 needs to be configured. If your PRI is in a different slot than 0/2/0, adjust as necessary. The last dial peer allows the NYC phones to still call phones in Madison using four digits. (A voice-translation profile would also have worked, but would be more complex.)

```
RtrPodx(config)# dial-peer voice 911 pots
RtrPodx(config-dial-peer)# description Emergency Services
RtrPodx(config-dial-peer)# destination-pattern 911
RtrPodx(config-dial-peer)# prefix 911
RtrPodx(config-dial-peer)# port 0/2/0:23

RtrPodx(config-dial-peer)# dial-peer voice 9911 pots
RtrPodx(config-dial-peer)# description 9+Emergency Services
RtrPodx(config-dial-peer)# destination-pattern 9911
RtrPodx(config-dial-peer)# prefix 911
RtrPodx(config-dial-peer)# port 0/2/0:23

RtrPodx(config-dial-peer)# dial-peer voice 97 pots
RtrPodx(config-dial-peer)# description 7 digit local numbers
RtrPodx(config-dial-peer)# destination-pattern 9[2-9]......
RtrPodx(config-dial-peer)# port 0/2/0:23

RtrPodx(config-dial-peer)# dial-peer voice 9110 pots
RtrPodx(config-dial-peer)# description 1+10 digit long-distance
RtrPodx(config-dial-peer)# destination-pattern 91[2-9]..[2-9]......
RtrPodx(config-dial-peer)# prefix 1
RtrPodx(config-dial-peer)# port 0/2/0:23

RtrPodx(config-dial-peer)# dial-peer voice 123 pots
RtrPodx(config-dial-peer)# description Inbound calls
RtrPodx(config-dial-peer)# incoming called-number 510555....
RtrPodx(config-dial-peer)# direct-inward-dial
RtrPodx(config-dial-peer)# port 0/2/0:23

RtrPodx(config-dial-peer)# dial-peer voice 2000 pots
RtrPodx(config-dial-peer)# description Four-digit failover
RtrPodx(config-dial-peer)# destination-pattern [2-4]...
RtrPodx(config-dial-peer)# prefix 555
RtrPodx(config-dial-peer)# port 0/2/0:23
RtrPodx(config-dial-peer)# exit
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-5: Configure Maximum Redirects

The CFUR settings cause an interesting side effect when the remote office is not in SRST mode. Suppose that a phone is unplugged (or in the case of a soft phone, the laptop is shut down). The CUCM sees the phone as unregistered. If someone calls the directory number, the CUCM sends the call out to the PSTN, and when the remote gateway gets the call, it forwards it back to headquarters, which sends it to the PSTN, which sends it. . . You get the idea—a call that loops until all resources are exhausted. One solution is to set the "Max Forward UnRegistered Hops to DN" service parameter. The default is 0 (unlimited), but a value of 2 should work in most situations. On the Cisco Unified CM Administration page, navigate to **System > Service Parameters**.

1. Select the IP address of the server from the Server drop-down list.
2. The Service drop-down list will appear. Select **Cisco CallManager (Active)**.
3. Scroll down (midway down) to the Clusterwide Parameters (Feature – Forward) section.
4. Enter **2** in the Max Forward UnRegistered Hops to DN field.
5. Click the **Save** button.

Step 3-6: Configure CFUR

If the WAN to the branch office is down, and a phone user at the headquarters dials the four-digit extension for a branch office phone, the call can be routed to the PSTN (or to voicemail). Because the branch office phone is registered to SRST, CUCM needs to know how to route the call. On the Cisco Unified CM Administration page, navigate to **Call Routing > Directory Number**. Click **Find** to see the directory numbers.

1. Click on an extension assigned to the NYC phone.
2. Scroll down to the Call Forward and Call Pickup Settings section, and enter **9555XXXX** in the Destination field after the Forward Unregistered Internal label. (This will automatically be copied to the Forward Unregistered External field when you leave the field.)
3. Select **Mad_Employee_CSS** from the Calling Search Space drop-down list after the Forward Unregistered Internal label. (This selection will automatically be copied to the Forward Unregistered External field when you leave the field.)
4. Select the **Voice Mail** check box after the Forward Unregistered External label. (We have not configured voicemail yet, so this is a setting for the future.) See Figure 10-44 for an example of this page.
5. Click the **Save** button.
6. In this case, it might be necessary to click the **Apply Config** button, and then click **OK** in the pop-up window to have the changes applied to the phone.

Note: While the "Max Forward UnRegistered Hops to DN" service parameter does prevent the loops, it then drops the call. A better solution is explained by William Bell,[1] where the call loop is broken by using the difference between the internal and external Forward Unregistered settings (as shown in this lab). To summarize, when a user in the company calls the unregistered phone, the call uses the Unregistered Internal setting and sends it to the PSTN. However, when the call comes in the gateway (that is not in SRST), it is now treated as an external call, which forwards to voicemail, and thus the loop is broken, and better yet, the call is not dropped.

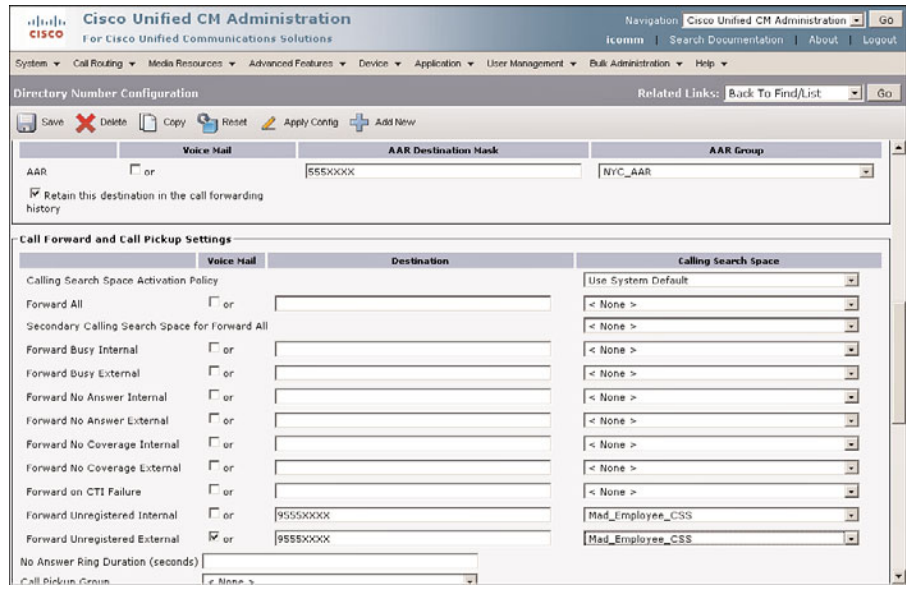
---

[1] "What about Non-SRST Unregistered Devices?" section at http://www.netcraftsmen.net/resources/blogs/using-call-forwarding-to-support-srst-mode.html

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-44 CFUR Settings on the Directory Number



Step 3-7: Test SRST Failover and CFUR Behavior

At this point, the SRST is configured to allow the phones at the branch office to register and even to make calls to 911, local, and long-distance numbers. Follow these steps to test this:

1. Disconnect the cable for the WAN link on the Madison router. By default, the phone sends keepalives every 30 seconds, but waits for three failed keepalives before it determines that the CUCM is nonresponsive and registers with the SRST system.
2. After the phone registered with SRST, the phone display shows "CM Fallback Service Operating."
3. If you examine the device settings on the phone, the Unified CM 2 SRST will be listed as Active.
4. Call from one NYC extension to another NYC extension. The call should ring.
5. Call from a NYC extension to 911, a seven-digit number, and a long-distance number. All those calls should work. Be aware that while in SRST mode, all extensions at the branch can make premium-rate-number (1-900) calls. Class of Restriction (not covered in this lab book) would have to be implemented to prevent this during failover.
6. Call from a NYC extension to the four-digit extension of a Madison phone. The call should work. Both phone displays show the number, but not the name, of the calling or called party.
7. Call from a Madison phone to the four-digit extension of the NYC phone. When the NYC phone rings, the display on the NYC phone will show that the call was redirected by the NYC extension to the same extension! See Figure 10-45 for an example of the phone display.
8. Reconnect the WAN cable. After the gateway connects, the SRST mode ends. However, after the CUCM is reachable, the phone will wait for 120 seconds before reregistering to avoid a flapping link, making the phone constantly switch between call agents. This results in phones not working for a few minutes during the failback to CUCM. You can tell that the phone is reregistered when the "CM Fallback Service Operating" message disappears from the phone display.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-45 CFUR Call Forwarding on a Phone Display

Tips to Complete Branch Office Dial Plan

As discussed in Step 2-7, the branch office is not ready for production. The items left to configure are as follows:

- Partitions for the New York location. To make the local gateway separate from the Madison location, partitions are needed. Specifically, the following are necessary:
  - NYC_911_PT
  - NYC_Local_PT
  - NYC_Services_PT

Consider this: As discussed in Lab 10-2, Task 1-5, SOI is directing all long-distance calls to the Madison site to get better phone call rates. (The long-distance route pattern is not site specific.) If the WAN becomes congested, all long-distance calls fail, because there is no long-distance route pattern pointing to a local gateway. A long-distance route pattern using the New York gateway would be needed, but this would cause all long-distance calls to use the local gateway. To make this function optimally:

- Configure a new partition called NYC_LD_Failover_PT and later assign it to a new NYC_LD_Failover long-distance route pattern. The NYC_LD_Failover_PT pattern should only be assigned to a new NYC_AAR_CSS Calling Search Space. (The NYC_AAR_CSS Calling Search Space should also have the other local gateway patterns.) NYC_AAR_CSS is then assigned as the AAR CSS in the New York DP device pool. This setup causes long-distance calls to route over the WAN normally, but when AAR is activated, it can route the long-distance calls over the PSTN through the local gateway.
- CSSs for NYC are almost the same as for Madison, but with the NYC partitions instead of the Madison ones. There is one new CSS (NYC_AAR_CSS), as discussed in the previous consideration.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- The complete call flow needs to be established: device (gateway), route group, route list, and route patterns. Assign the correct partition when creating the route patterns. There only needs to be route patterns for the following:
  - NYC emergency (both 911 and 9911)
  - NYC local (both seven- and ten-digit)
  - NYC service codes
  - NYC LD failover (for AAR)

Tip: If you want to save time, and are careful, you can copy the existing route patterns and change only the Route Partition, Description, and Gateway/Route List fields on each.

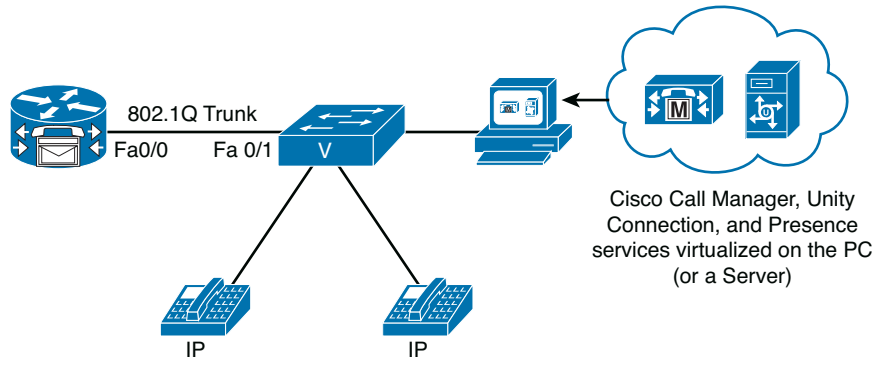
- The NYC gateway should have the NYC version of the CSS applied to the interface.
- The directory numbers on the NYC phones need to be updated with the correct CSS for NYC. (The Internal_PT partition does not need to be changed.)
- If the NYC phones have a CSS assigned, the CSS needs to be updated.
- For AAR from NYC to Madison to function, all the Madison directory numbers need to have the AAR destination mask and AAR group assigned.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 10-4: Hunt Groups

Figure 10-46 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS
- Switch that supports voice VLANs
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- Configuration from Lab 9-5 or later
- Two or more IP Phones registered (desk phone or soft phone on PC or Windows VM)

Note: You can leave the remote pod setup from Lab 10-2 or 10-3, as long as you have enough directory numbers in the Madison location. (A minimum of six lines is needed.) If necessary, move the NYC phone back to Madison and reassign the previous Madison directory numbers to it.

Learning Objectives

Upon completion of this lab, you will be able to

- Configure line groups in CUCM
- Configure hunt lists in CUCM
- Configure hunt pilots in CUCM

Scenario

SOI wants to sell lots of shiny objects. To make this happen, it wants to have sales agents pool together to answer calls. If none of the sales agents are able to answer the calls, the calls should fail over to a group of managers to provide call coverage. This is just one scenario for using hunt groups. Hunt groups can be used in almost any situation where the call is not destined for a single phone user.

Note: Cisco has software for call centers that integrates phone calls, email contacts, and web-support chat into one solution, while providing call center management and reports. See the Cisco Unified Contact Center Express and Cisco Unified Contact Center Enterprise solutions for details.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

This lab is based on the configuration from Lab 9-5 or later. Ideally you should have three or more phones, with six or more unique directory numbers in total. One directory number will be used to call the hunt pilot, three (or more) directory numbers will be needed for the sales agents, and another two (or more) directory numbers are used for the managers group. (For best results, the two managers' directory numbers should not be on the same phone.) Verify that you can call between the VoIP phones. Troubleshoot if necessary.

Task 1: Configure Hunt Groups

There will be two line groups: one for sales agents and another for the managers.

Step 1-1: Configure Sales Agents Line Group

Line groups are collections of directory numbers that are grouped together to receive calls. The calls to a line group can be distributed in four different ways:

- **Top down:** The calls always follow the same sequence of directory numbers.
- **Circular:** The calls go around in a circle, where every directory number gets a call in turn.
- **Longest idle time:** The call goes to the directory number that has waited the longest since taking a call.
- **Broadcast:** The call goes to all directory numbers at the same time. This is useful for incoming calls from the PSTN for a small business where any employee might need to answer a call. (Note: Do not assign any directory number that is shared on more than one phone to a broadcast group.)

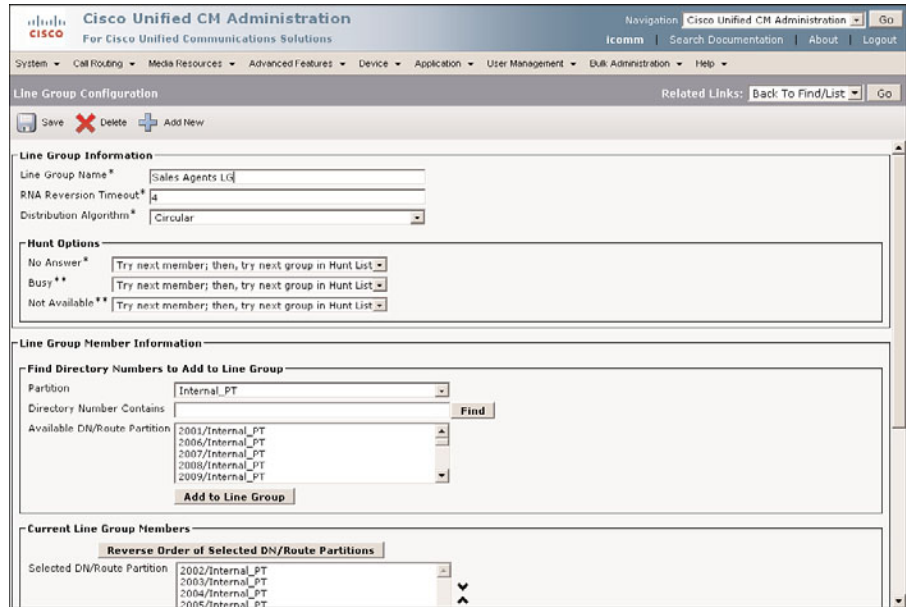
On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Line Group**.

1. Click the **Add New** button.
2. In the Line Group Name field, enter **Sales Agents LG**.
3. Enter **4** in the RNA Revision Timeout field to avoid waiting in the lab for ten seconds for each extension. The RNA revision timeout is how long a call tries a directory number in the group before moving on to the next line.
4. Select **Circular** from the Distribution Algorithm drop-down list.
5. In the Line Group Member Information section, select **Internal_PT** from the Partition drop-down list.
6. In the Available DN/Route Partition box, hold the **Ctrl** key while clicking three or more active directory numbers. (Do not forget that you need to have one unused directory number to call the groups and two directory numbers left for the manager group.)
7. Click the **Add to Line Group** button. See Figure 10-47 for an example of this page.
8. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-47 Line Group Configuration



Step 1-2: Configure Managers Line Group

Now, you need to create the line group for the managers that will be the failover for the sales line group.

1. Click the **Add New** button.
2. In the Line Group Name field, enter **Managers LG**.
3. Enter **6** in the RNA Revision Timeout field.
4. Select **Broadcast** from the Distribution Algorithm drop-down list.
5. In the Line Group Member Information section, select **Internal_PT** from the Partition drop-down list.
6. In the Available DN/Route Partition box, hold the **Ctrl** key while clicking two or more active directory numbers (that were not used previously).
7. Click the **Add to Line Group** button.
8. Click the **Save** button.

Step 1-3: Configure Hunt List

The hunt list is an ordered list of line groups. The hunt list will send calls first to the sales agent line group and then fail over to the manager line group. On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Hunt List**.

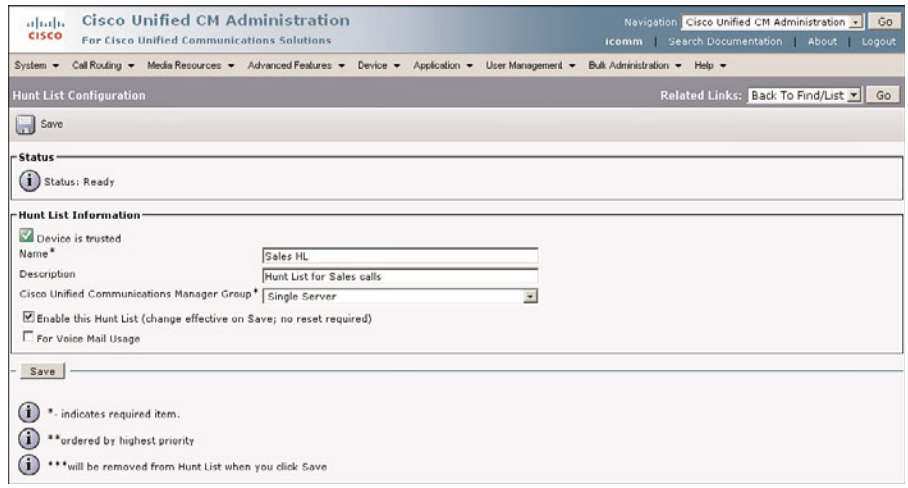
1. Click the **Add New** button.
2. In the Name field, enter **Sales HL**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. Enter **Hunt List for Sales calls** in the Description field.
4. Select **Single Server** from the Cisco Unified Communications Manager Group drop-down list.
5. Select the **Enable this Hunt List** check box. See Figure 10-48 for an example of this page.

Figure 10-48 Hunt List Configuration

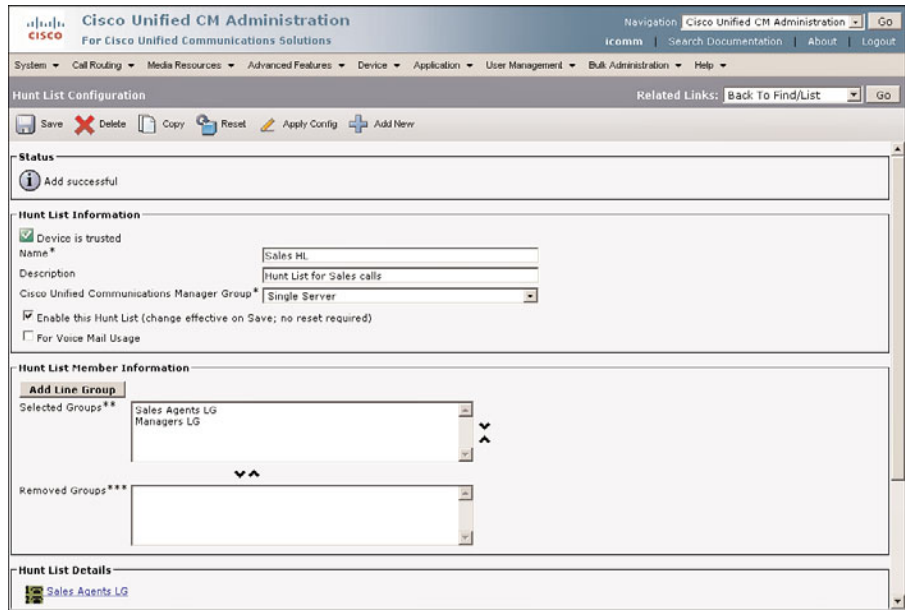


6. Click the **Save** button.
7. The page updates to show the Hunt List Member Information section. Click the **Add Line Group** button.
8. The Hunt List Detail Configuration page opens. From the Line Group drop-down list, select **Sales Agents LG**.
9. Click the **Save** button. A pop-up window will inform you about changes to the hunt list. Click **OK** to close the window.
10. Click the **Add Line Group** button, and this time select **Managers LG** from the Line Group drop-down list.
11. The Selected Groups box should show both list groups, with the Sales Agents LG listed above the Managers LG. (If not, use the arrows on the right side of the box to order them correctly.) See Figure 10-49 for an example of this page.
12. Click the **Save** button. A pop-up window will tell you to reset for the changes to take effect. Click **OK** to close the window.
13. Click the **Reset** button. The Device Reset pop-up window will open. Click the **Reset** button. Click the **Close** button to close the pop-up window.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-49 Hunt List Member Configuration



Step 1-4: Configure Hunt Pilot

The hunt pilot is the target number that is dialed to reach the list groups in the order they are specified in the hunt list. The hunt pilot can be a number outside the range of extensions for your pod. On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Hunt Pilot**.

1. Click the **Add New** button.
2. In the Hunt Pilot field, enter **1500**.
3. Select **Internal_PT** from the Route Partition drop-down list.
4. Enter **Sales and Managers** in the Description field.
5. Select **Sales HL** from the Hunt List drop-down list.
6. Enter **Sales Hunt List** in the Alerting Name field and the ASCII Alerting Name field.
7. Deselect the **Provide Outside Dial Tone** check box. See Figure 10-50 for an example of this page.
8. Click the **Save** button.

Step 1-5: Testing

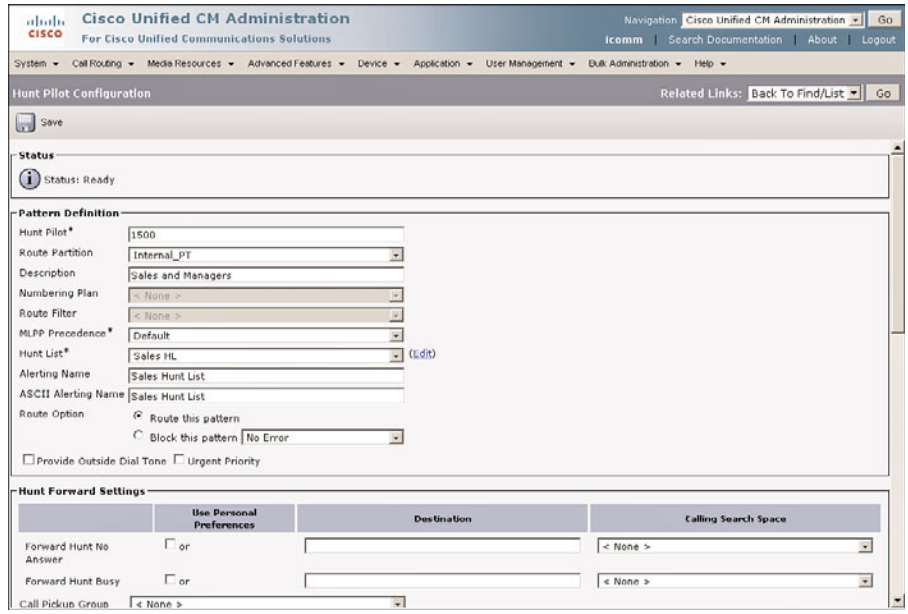
Make a phone call to 1500 from the one directory number that is not assigned to any line group. Do not answer the call. The number should proceed to ring for four seconds on each of the lines in the Sales LG. When none of them is answered, all lines in the Manager LG will ring at the same time. If the call is not answered in the next six seconds, it will disconnect and give a busy signal to the caller.

If you call 1500 a second time, the next number on the Sales LG will be the first to ring. Again, when all the lines in the Sales LG have rung for four seconds, all lines in the Manager LG will ring at the same time. Every time the hunt pilot is dialed, the next directory number in the Sales LG list will be the first to ring.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 10-50 Hunt Pilot Configuration



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

This page intentionally left blank

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

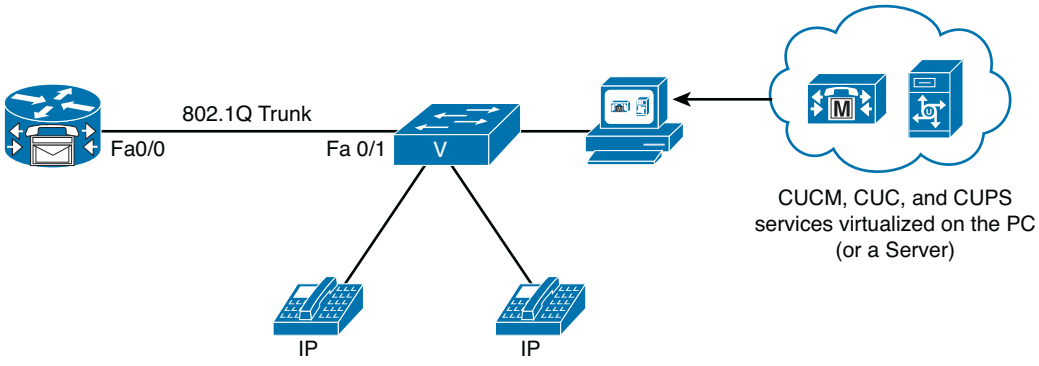
CHAPTER 11

CUCM Telephony Features

This chapter explores some of the telephony features found with Cisco Unified Communications Manager (CUCM). Although there are a number of features available to the users of this system, this chapter focuses on extension mobility and call coverage features, such as Call Forward, Call Barge, Call Pickup, and Call Park. Although Call Hunting is also considered a call coverage feature, it will not be covered in this chapter, as it was covered in Lab 10-4, "Hunt Groups."

Lab 11-1: Extension Mobility

Figure 11-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- CUCM Server or PC with VMware Workstation installed and a VM of CUCM
- Configuration from Lab 10-2 or later
- One or more IP phones registered (desk phone or soft phone on PC or Windows VM)

Learning Objectives

Upon completion of this lab, you will be able to

- Activate extension mobility services
- Configure extension mobility service parameters
- Configure extension mobility phone service
- Create user device profiles
- Associate a user device profile with a user
- Enable the Extension Mobility Service on a phone

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Scenario

Shiny Objects Inc. (SOI) has a large outside sales staff, and many of the salespeople rarely come into the office. To save space and money, these salespeople do not have permanent workspaces in the office. However, it is still important that they have an office phone number and a place to work when they do come into the office. SOI has created a number of shared workspaces that the salespeople can use when needed. They have also assigned dedicated phone numbers for each salesperson that can be configured to ring the person's cell phone when not in the office. However, when salespeople are in the office, they would prefer to use a Cisco IP Phone to place and receive calls. Because they do not have a permanent workspace, extension mobility must be deployed so that they can log in to a phone at any of the shared workspaces.

Task 1: Activate Extension Mobility Services and Configure Service Parameters

A number of items must be configured to implement extension mobility. Because certain tasks depend on other tasks already having been completed, the order in which these tasks are done is important. First, you must enable the extension mobility service and configure the extension mobility service parameters.

Step 1-1: Activate Extension Mobility Service

Connect to the CUCM web pages using the methods discussed in Chapter 8, "Administrative Interfaces."

1. Log in with your application username (icomm) and accept any security certificate warnings. Use the Navigation drop-down list in the upper right to select **Cisco Unified CM Serviceability** and click **Go**.
2. Navigate to **Tools > Service Activation**. Select the desired server from the Server drop-down list.
3. Select the check box next to the **Cisco Extension Mobility** service.
4. Click the **Save** button.
5. The Cisco Extension Mobility service will now activate. This can take a few minutes to complete. After the page refreshes, ensure that the Cisco Extension Mobility service is activated.

Step 1-2: Configure Extension Mobility Service Parameters

The configuration of service parameters is done from the Cisco Unified Communications Administration page, so you must first navigate to that page. Use the Navigation drop-down list in the upper right to select **Cisco Unified CM Administration** and click **Go**.

1. On the Cisco Unified CM Administration page, navigate to **System > Service Parameters**.
2. Select the **Communications Manager IP Address** from the **Server** drop-down list.
3. Select **Cisco Extension Mobility** from the **Service** drop-down list.
4. From here you can configure seven different parameters that will impact a user's experience when using extension mobility. The **Enforce Intra-cluster Maximum Login Time** field determines whether the value in the **Intra-cluster Maximum Login Time** field is enforced. This determines the amount of time a user within the cluster can be logged in to extension mobility.

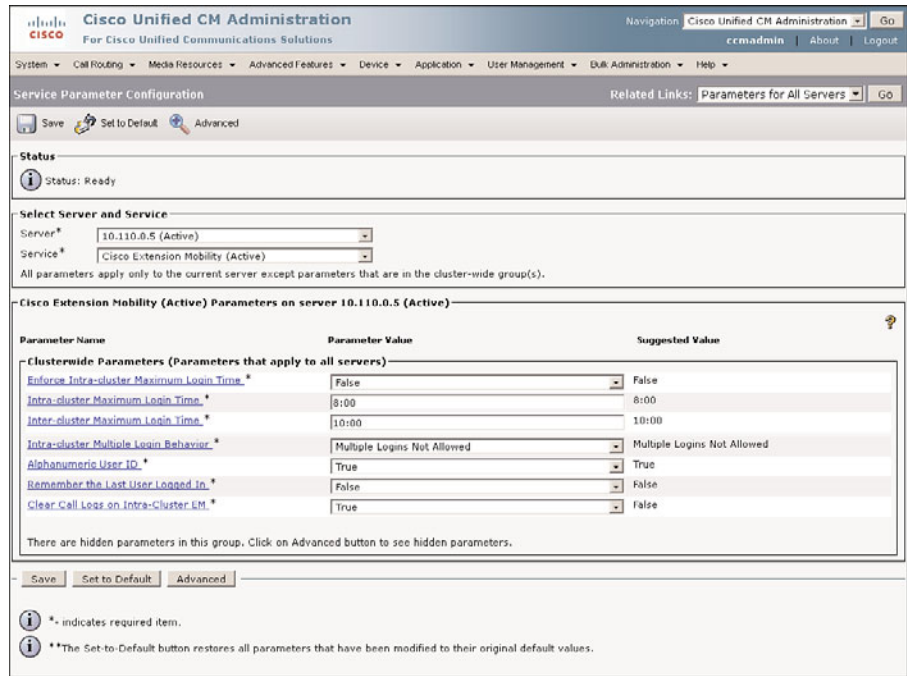
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Because many SOI employees might need to stay logged in for multiple days, this value will be left set at **False**.

5. Because we are setting the **Enforce Intra-cluster Maximum Login Time** field to False, the **Intra-cluster Maximum Login Time** field is ignored by the system, so you can leave it set to the default value.
6. The **Inter-cluster Maximum Login Time** field determines the amount of time after which phones will automatically log out when logged in remotely. Because SOI has only one cluster, the value in this field is of no consequence, and you can leave it at the default value.
7. Because we don't want employees to log in to multiple phones at the same time, select **Multiple Logins Not Allowed** from the **Intra-cluster Multiple Login Behavior** drop-down list.
8. To make it easier for the salespeople to log in, SOI could have used numeric-only user IDs. By doing this, the salesperson would have simply entered their extension number when prompted for a user ID. However, because the user ID has already been created with alphanumeric characters, we will need to set **Alphanumeric User ID** to **True**.
9. Set the **Remember the Last User Logged In** to **False** so that the previous user ID is not cached.
10. Set the **Clear Call Logs on Intra-Cluster EM** value to **True** so that the calls the previous user placed are not retained in the call log. See Figure 11-2 for an example of this page.
11. Click the **Save** button.

Figure 11-2 Extension Mobility Service Parameter Configuration



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: Configure Extension Mobility IP Phone Service

For a user to be able to log in to extension mobility, an IP phone service extension mobility must be configured. After it is configured, you must ensure that any phone that is going to be used for extension mobility purposes is subscribed to this service.

Step 2-1: Configure the Extension Mobility IP Phone Service

On the Cisco Unified CM Administration page, navigate to **Device > Device Settings > Phone Services**. On the next page, select **Add New**.

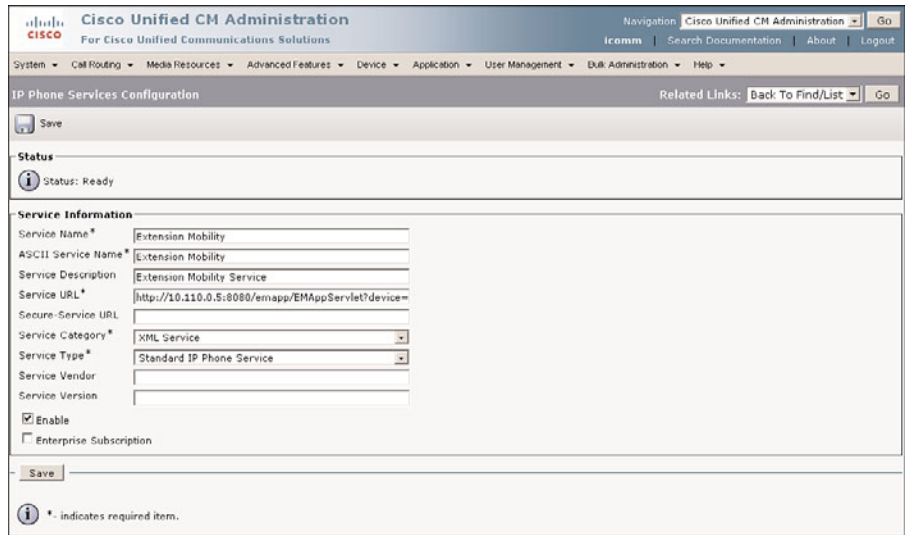
1. Enter **Extension Mobility** in the **Service Name** and the **ASCII Service Name** fields. In the **Service Description** field, enter **Extension Mobility Service**.
2. Enter the URL for the extension mobility service. This service is already installed on the Cisco Unified Communications server. Enter **http://10.110.0.5:8080/emapp/EMAppServlet?device=#DEVICENAME#** in the **Service URL** field. (Replace the highlighted part with your CUCM server's IP address.)

Note: The service URL is case sensitive, so be sure to enter the URL exactly as it appears in this step.

3. Select **XML Service** from the **Service Category** drop-down list.
4. Select **Standard IP Phone Server** in the **Service Type** field.

   The **Service Vendor** and **Service Version** fields are optional and will be left blank for this lab.
5. Select the **Enable** check box. See Figure 11-3 for an example of this page.
6. Click the **Save** button.

Figure 11-3 IP Phone Service – Extension Mobility



Note: The service is only available to device that subscribe to it. If you want this service to be available on all devices without subscribing, you can select the **Enterprise Subscription** check box. This field cannot be modified after the service is configured, so make sure that you set it properly. Leave it unselected for this lab.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 3: Create and Associate Device Profiles

Step 3-1: Create Default Device Profile

The default device profiles will be used by the phone when a mobility user logs out. They can be automatically created by the system, but it is better if they are manually created.

On the Cisco Unified CM Administration page, navigate to **Device > Device Settings > Default Device Profile**.

1. From the **Device Profile Type** drop-down list, select the model of phone on which this profile is based and click **Next**.
2. Select the protocol the device will use from the **Device Protocol** drop-down list. Select **SCCP** and click **Next**.
3. The only option that is required to be selected is the **Phone Button Template**. From the drop-down list, select the **Custom Button Template** you created for the phone model in Task 7 of Lab 9-4.
4. Click the **Save** button.

Step 3-2: Create Device Profile

The process of creating a device profile is very similar to creating a phone. Because you already know how to create a phone, much of this will look familiar.

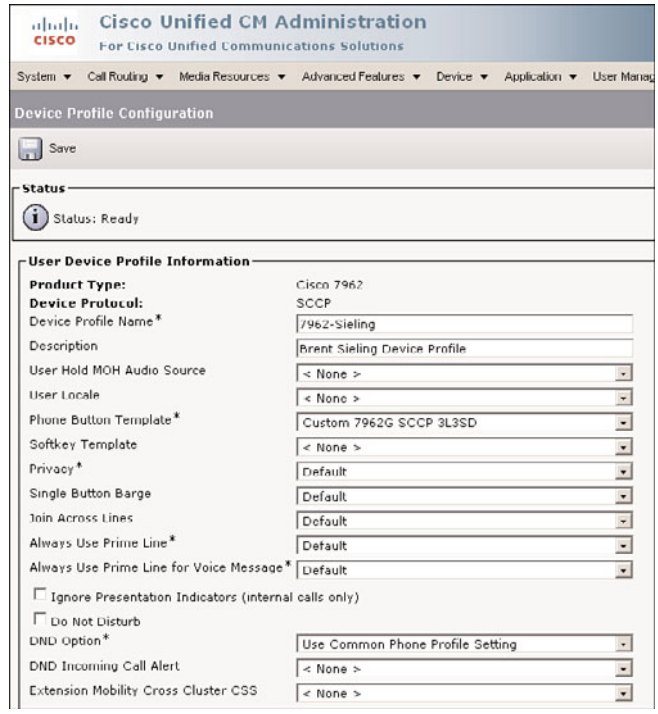
On the Cisco Unified CM Administration page, navigate to **Device > Device Settings > Device Profile**. On the next page,

1. Click the **Add New** button.
2. From the **Device Profile Type** drop-down list, select the type of phone on which this profile is based and click **Next**.
3. Select the protocol the device will use from the **Device Protocol** drop-down list. Select **SCCP** and click **Next**.
4. The next screen that appears looks very similar to the Phone Configuration screen. For this lab, we will only enter the required information. In the **Device Profile Name** field, enter a name for this profile, for example, **7962-<*your last name*>**.
5. In the **Description** field, enter a description that helps identify this profile, such as **<*Your Full Name*> Device Profile**.
6. Select the appropriate phone button template from the **Phone Button Template** drop-down list. See Figure 11-4 for an example of this page.
7. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 11-4 Device Profile



Step 3-3: Configure Lines for the Device Profile

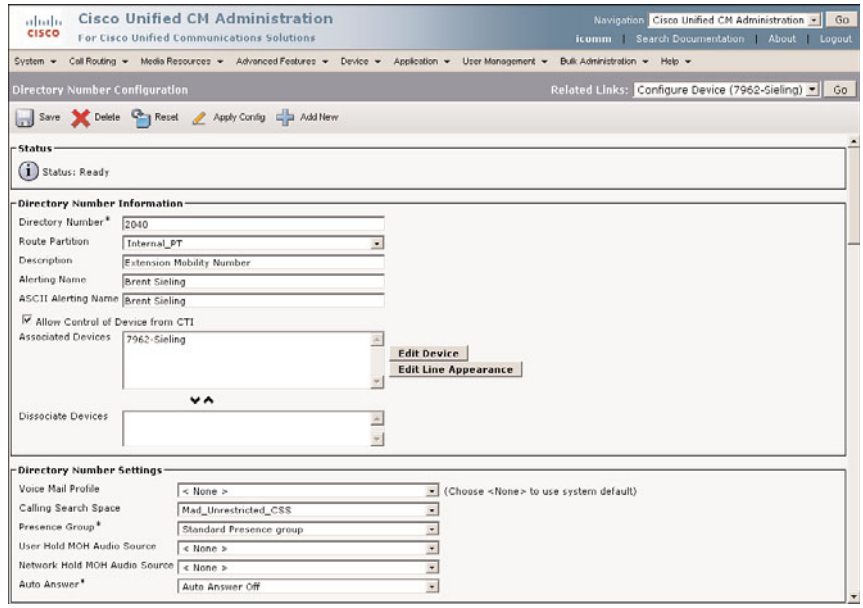
After you create a device profile, you need to configure lines for the profile. The process for this is similar to that of adding lines to a phone:

1. Click the **Line [1]** – **Add a new DN** link.
2. In the **Directory Number** field, enter the next unassigned directory number in your range.
3. Select **Internal_PT** from the **Route Partition** drop-down list.
4. Enter **Extension Mobility Number** in the **Description** field.
5. Enter ***<your name>*** in the **Alerting Name** field.
6. In the Directory Number Settings section, select **Mad_Unrestricted_CSS** from the **Calling Search Space** drop-down list. See Figure 11-5 for an example of this page.
7. In the Line 1 on Device section, enter ***<your name>*** in the **Display (Internal Caller ID)** field.
8. Click the **Save** button.
9. Use the **Related Links** to return to configuring the device.
10. Only one line is needed, but you can configure more if you want. After all of the lines are configured, you must add the extension mobility service to this profile. Select **Subscribe/Unsubscribe Services** from the Related Links drop-down menu and click **Go**.
11. Select **Extension Mobility** from the **Select a Service** drop-down list and click **Next**.
12. Click the **Subscribe** button and close the window after it refreshes.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 11-5 Device Profile – Directory Number

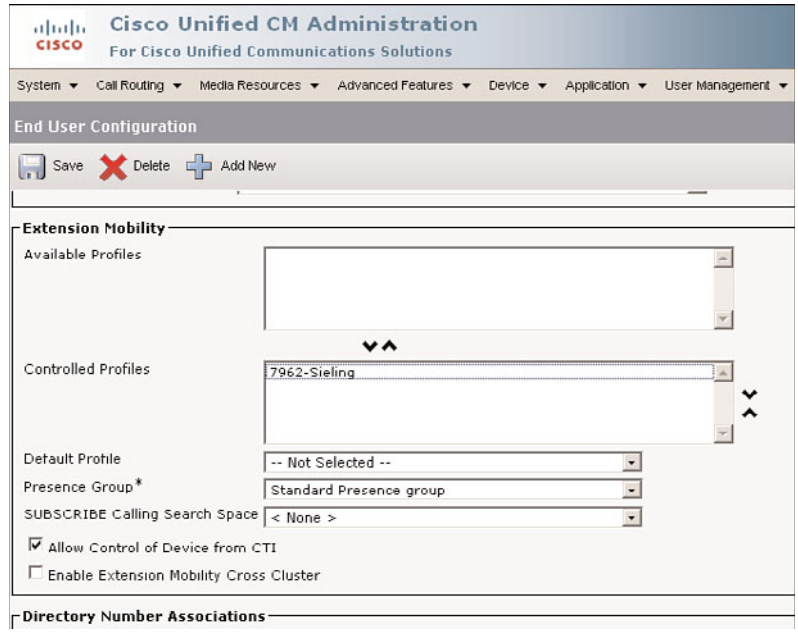


Step 3-4: Associate a Device Profile with a User

Next, you must associate the device profile you just created with a Communications Manager user. On the Cisco Unified CM Administration page, navigate to **User Management > End User**.

1. Click **Find** and select the user that you created in Chapter 9 using your name.
2. In the Extension Mobility section, make sure that the **Allow Control of Device from CTI** check box is selected. If it isn't, select the box and click **Save**.
3. In the Extension Mobility section, highlight the profile you just created from the **Available Profiles** box and click the down arrow below that box to move the profile to the **Controlled Profiles** box. See Figure 11-6 for an example of this page.

Figure 11-6 Associate Device Profile



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. Click the **Save** button.

Step 3-5: Enable Extension Mobility on a Phone

After device profiles are configured and associated with a user, extension mobility must be enabled on the phones. This requires that the phone is subscribed to the Extension Mobility Service and that the extension mobility parameters are configured on the phone. The following steps show how to complete the tasks.

1. On the Cisco Unified CM Administration page, navigate to **Device > Phone**. Click **Find** and select the first HQ phone.
2. Scroll down to the Extension Information section, and select the **Enable Extension Mobility** check box.
3. Click the **Save** button.
4. You should see a pop-up window telling you to click the Apply Config button. Click **OK** to close the pop-up window.
5. Click the **Apply Config** button. A window will appear informing you to save changes before applying config. Click **OK**.
6. Next, you must configure this phone so that it is subscribed to the Extension Mobility Service. To do this, select **Subscribe/Unsubscribe Services** from the **Related Links** drop-down menu and click **Go**.
7. Select **Extension Mobility** from the **Select a Service** drop-down list and click **Next**.
8. Click the **Subscribe** button and close the window after it refreshes.

Task 3: Validate Extension Mobility

To validate,

1. Press the **Services** button (the icon looks like a globe) on the first HQ phone.

Note: If you get the message "No Services Configured" on the phone display, first verify you have the Extension Mobility service assigned to both the user and the phone. If you still have problems, see the tip about clearing the Certificates on the phone in the Hardware section.

---

2. Select Extension Mobility from the list of available services.
3. When prompted, enter your username. Entering letters can be a little tricky. You have to press a number key repeatedly to choose the letter you want from the three or four on the key. (This is why choosing numerical usernames and restricting login to numbers only can make extension mobility log in faster.) See Figure 11-7 for an example of this page.

Tip: The computer keyboard can be used to enter the log in on softphones.

---

4. Navigate down to enter the PIN you assigned for your username.
5. Press the **Submit** softkey.

   The phone should now have the extension that you assigned to the device profile.

   When you are done, press the **Services** button and press the **Yes** softkey to log out. The phone will now revert back to the previous line configuration.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

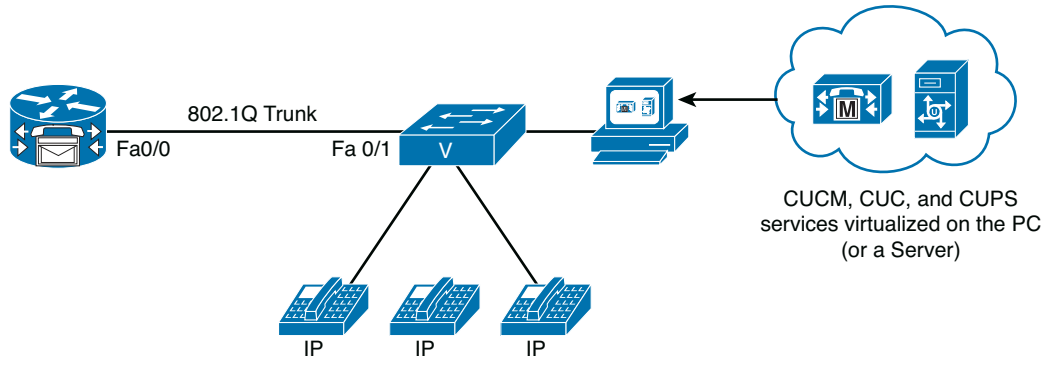
Figure 11-7 Extension Mobility Login on the Phone

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 11-2: Call Coverage Features

Figure 11-8 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- CUCM Server or PC with VMware Workstation installed and a VM of CUCM
- Configuration from Lab 10-2 or later
- Three or more IP Phones (desk phone or soft phone on PC or Windows VM)

Learning Objectives

Upon completion of this lab, you will be able to

- Configure Call Park
- Configure Directed Call Park
- Configure Call Pickup
- Configure Shared Lines
- Configure Barge and Privacy
- Configure Intercoms
- Configure Native Presence

Scenario

There are a number of features that SOI wants to have deployed on its system. Although some features work out of the box, such as Call Forward, others require configuration to be available to the users. In this lab, you will be configuring Call Park, Call Pickup, Shared Lines, Barge, Intercoms, and the Native Presence features.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Configure Call Park and Directed Call Park

Call Park places the call on hold and parks it on a virtual directory number. By dialing that number, you can retrieve the call from a different phone. A common use for Call Park is to have an attendant or operator park the calls and then announce the call using an overhead paging system.

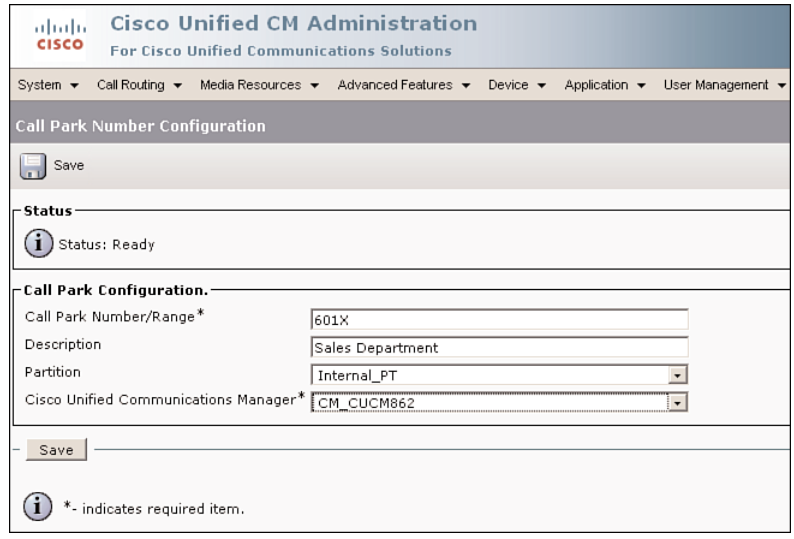
Often users want to select the number on which the call will be parked. Communications Manager includes the Directed Call Park feature. To use this feature, the user transfers a call to the Directed Call Park number by pressing the Transfer softkey and the Directed Call Park number where they want the call parked.

Step 1-1: Configure Call Park

On the Cisco Unified CM Administration page, navigate to **Call Routing > Call Park**.

1. Click the **Add New** button.
2. In the **Call Park Number/Range** field enter **601X**. This will create ten Call Park numbers, 6010–6019. The wildcards used for Call Park ranges are the same as those used for route patterns.
3. In the **Description** field, enter **Sales Department**. The description helps identify the purpose of this Call Park pattern. For example, perhaps you are going to create a Call Park range for each department. You could enter the department's name in this field.
4. To restrict who can use a Call Park range, a partition can be assigned to the Call Park number. Only devices that have access to the assigned partition can retrieve the parked call. For this lab, we are going to allow all devices to use this range, so select **Internal_PT** from the **Partition** drop-down list.
5. Call Park numbers are unique for each Communications Manager in the cluster. This means that you will need to create a range for each Communications Manger that has phones registered to it. For this lab, select **CM_CUCM862** from the **Cisco Unified Communications Manager** drop-down list. See Figure 11-9 for an example of this page.
6. Click the **Save** button.

Figure 11-9 Call Park Configuration



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 1-2: Test Call Park

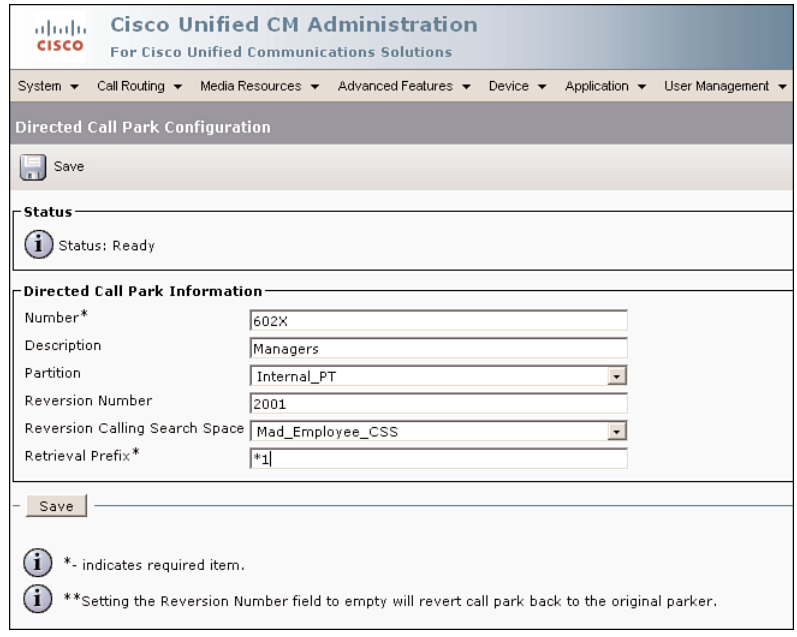
From the third phone in you pod, call the first HQ phone. Answer the call and press the softkey labeled **Park** (you might need to press the **more** softkey to see the park option). The phone will display the number on which the call was parked; take note of that number. Go off-hook on the second HQ phone and dial the displayed call parked number. The call should connect to the second phone.

Step 1-3: Configure Directed Call Park

On the Cisco Unified CM Administration page, navigate to **Call Routing > Directed Call Park**. On the next page, select **Add New**.

1. In the **Number** field enter **602X**. This will create ten Directed Call Park numbers, 6020–6029.
2. In the **Description** field, enter **Managers**. The description helps identify the purpose of this Call Park pattern. For example, perhaps you are going to create a Directed Call Park range for each department, so you could enter the department's name in this field.
3. To restrict who can use a Directed Call Park range, a partition can be assigned to the Call Park number. For this lab, we are going to allow all devices to use this range, so select **Internal_PT** from the **Partition** drop-down list.
4. In the **Reversion Number** field, enter the extension number of the first HQ phone. The parked call is forwarded to this number if it is not retrieved.
5. From the **Reversion Calling Search Space** drop-down list, select **Mad_Employee_CSS**. This calling search space needs to have access to the partition that the extension number of the first HQ phone is in. This is required so that the Directed Call Parked feature can transfer the call to the extension number entered in the Reversion Number field.
6. Enter ***1** in the **Retrieval Prefix** field. By dialing this number followed by a Directed Call Park number, Communications Manager knows you are trying to pick up a call that was parked using Directed Call Park. See Figure 11-10 for an example of this page.
7. Click the **Save** button.

Figure 11-10 Directed Call Park Configuration



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 1-4: Test Directed Call Park

From the third phone in you pod, call the first HQ phone. Answer the call and press the softkey labeled **Transfer**, enter **6021**, and press **Transfer** again. Go off-hook on the second HQ phone and dial ***16021**. The call should connect to the second phone.

Task 2: Configure Call Pickup

Call pickup groups allow people to answer a line that is ringing on another phone from their phone. For example, if extension 1005 is ringing, the call can be answered from a phone that does not have 1005 as an extension. There are two ways this can happen. The first is called Call Pickup. Call Pickup allows a call to be picked up from another phone if both phones are in the same pickup group. The second type of call pickup is called Group Call Pickup. Group Call Pickup allows a call to be picked up from another phone if both phones are not in the same pickup group.

Step 2-1: Create a Call Pickup Group

On the Cisco Unified CM Administration page, navigate to **Call Routing** > **Call Pickup Group**. On the next page, select **Add New**.

1. Enter **Sales** for the Call Pickup Group Name field.

Note: The call pickup group name is used when assigning a pickup group to a line, so it is best to make it as descriptive as possible.

---

2. In the **Call Pickup Number** field, enter the **6501**. This number must be unique in that it is not assigned to any other function or device.
3. In the **Description** field, enter **Madison Sales Group.**
4. Select **Internal_PT** from the **Partition** drop-down list.
5. The remaining fields are only required if you want an alert sent to all the users in the group if the call is not picked up. For this lab, we will leave the remaining fields set to default. See Figure 11-11 for an example of this page.
6. Click the **Save** button.

Step 2-2: Assign a Call Pickup Group to a Phone

On the Cisco Unified CM Administration page, navigate to **Device** > **Phone**.

1. Click **Find** and select the first HQ phone. Now select the first directory number.
2. In the Call Forward and Call Pickup Settings section, select **Sales in Internal_PT** from the **Call Pickup Group** drop-down list. See Figure 11-12 for an example of this page.
3. Click the **Save** button.
4. Repeat this step and assign the **Sales** call pickup group to the first directory number of the second HQ phone.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 11-11 Call Pickup Group Configuration

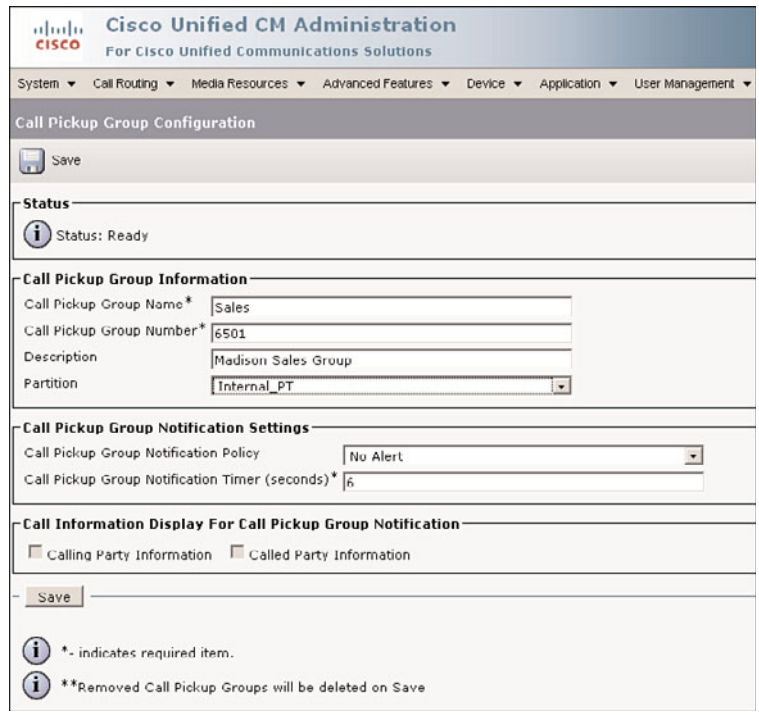
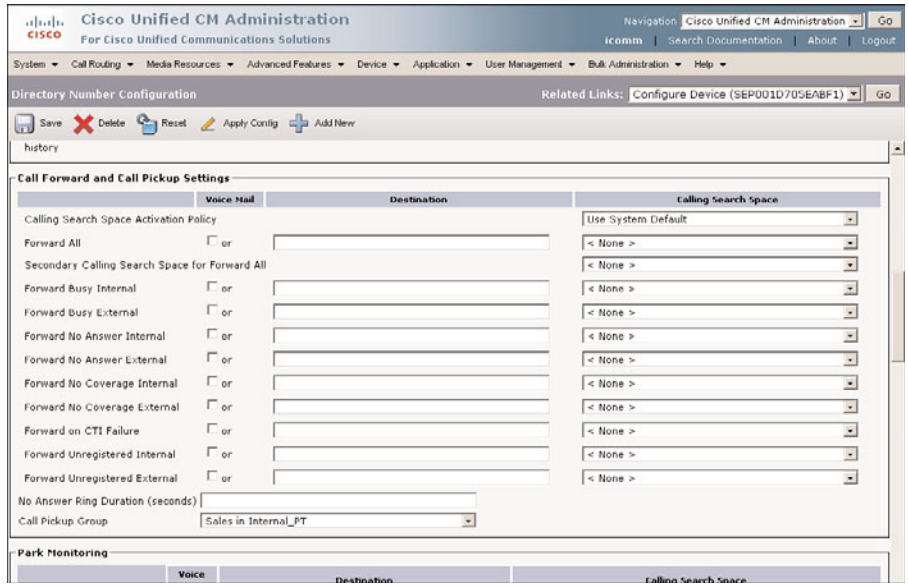


Figure 11-12 Call Pickup Group Assignment



Step 2-3: Test Call Pickup

From the third phone in your pod, call the first HQ phone. *Do not* answer the call. Go **off-hook** on the second HQ phone and press the **Pickup** softkey. The phone should ring; press the **Answer** softkey. The call should be connected to the second phone.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 3: Configure Shared Lines

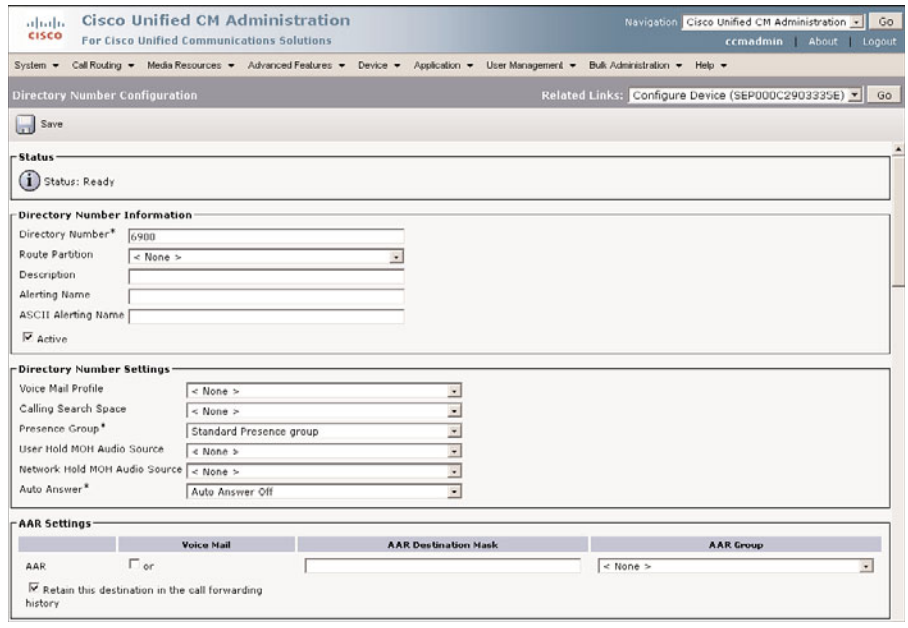
A shared line means assigning the same DN (in the same partition) to two or more phones. When this DN is dialed, all phones that share that line will ring. When a call on a shared line is placed on hold, it can be picked up from any of the shared lines. Another feature that can be enabled on shared lines is Barge. Barge will be explored next, but first you need to create a shared line.

Step 3-1: Create a New Directory Number

On the Cisco Unified CM Administration page, navigate to **Device > Phone**.

1. Click **Find** and select the first HQ phone. Select a line that is currently not configured. If all lines are configured, select **Line 2**.
2. Enter **6900** in the **Directory Number** field.
3. The rest of the fields can be left at default for this lab. See Figure 11-13 for an example of this page.
4. Click the **Save** button.

Figure 11-13 New Directory Number



Step 3-2: Assign Directory Number to Second Phone

On the Cisco Unified CM Administration page, navigate to **Device > Phone**.

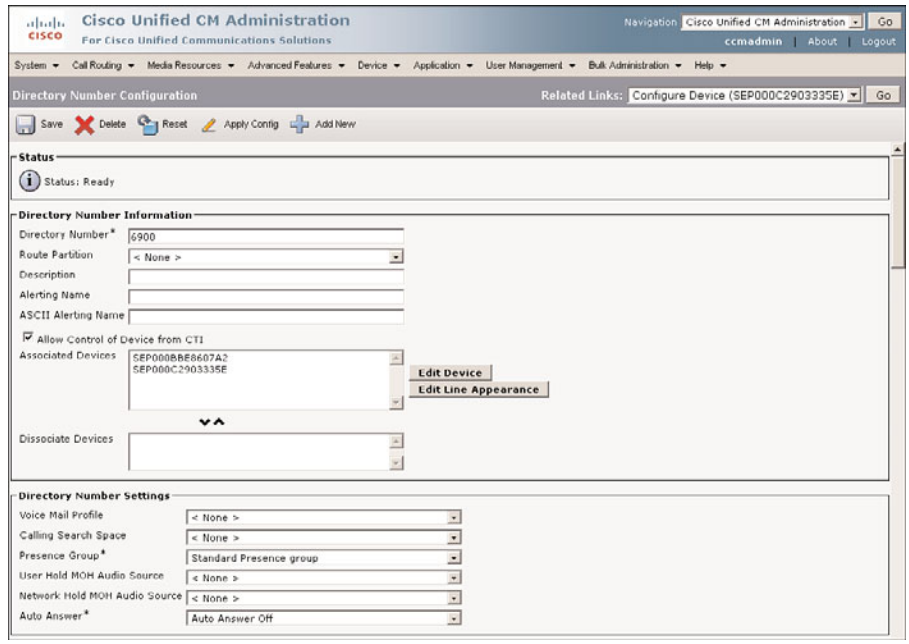
1. Click **Find** and select the second HQ phone. Select a line that is currently not configured. If all lines are configured, select **Line 2**.
2. Enter **6900** in the **Directory Number** field and then select the **Description** field.
3. You will see that screen update, and it now shows a field called **Associated Devices**. This tells you that the directory number you are assigning to this line is already assigned to another device. In other words, if you add it to this device, it will be a shared line. See Figure 11-14 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. Click the **Save** button.

Figure 11-14 Shared Line



Step 3-3: Test Shared Lines

From the third phone in your pod, dial 6900. The second line on both the HQ phones should ring.

Task 4: Configure Barge and Privacy

Barge allows users to join another user's call if both user phones have a shared line. SOI feels this would be beneficial for salespeople to have when they are training someone new. They want the salesperson to be able to join the new trainee's call, but they do not want the trainee to join the salesperson's calls.

Let's assume that the first HQ phone is the salesperson's phone and the second HQ phone is the trainee's.

Step 4-1: Configure System Parameters for Barge

Because there might be other uses for this feature, we are going to enable it globally and then disable it on the phones that won't be using this feature. On the Cisco Unified CM Administration page, navigate to **System > Service Parameters**.

1. Select the Communications Manager **IP Address** from the **Server** drop-down list.
2. Select **Cisco CallManager** from the **Service** drop-down list.
3. Scroll down to the **Clusterwide Parameters (Device-Phone)** section and select **On** from the **Builtin Bridge Enable** drop-down list. A message might appear informing you that 7960s and 7940 with encryption enabled cannot use the Barge feature and informing you to reset the phone for this setting to take effect. Click **OK**.

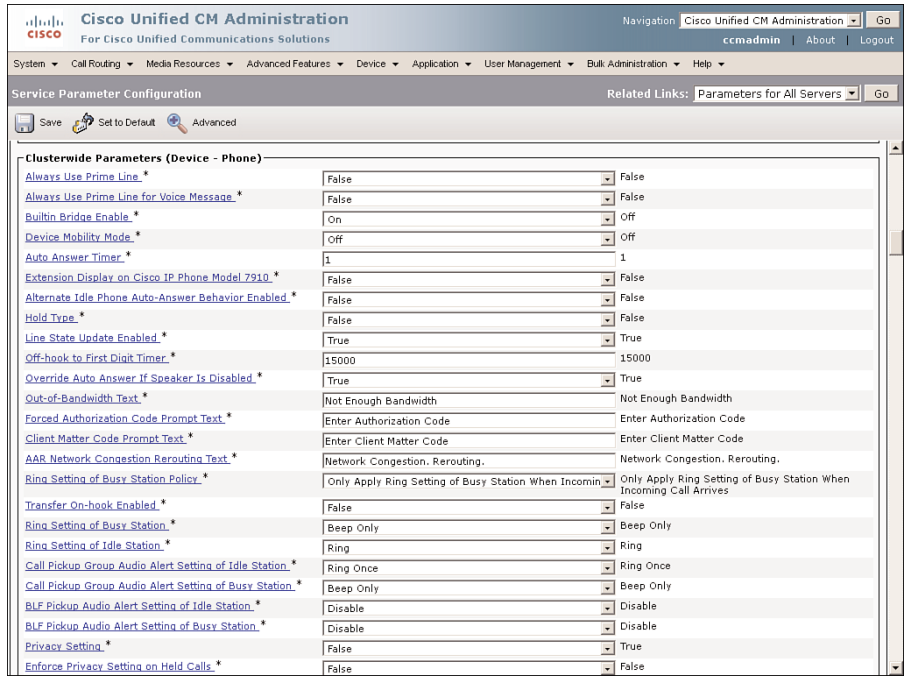
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. In the same section, you will find the **Privacy Setting** field. Select **False** from the drop-down list. A message might appear informing you to reset the phone for this setting to take effect. Click **OK**. See Figure 11-15 for an example of this page.

5. Click the **Save** button.

Figure 11-15 Built-In Bridge and Privacy



Step 4-2: Disable Barge on a Phone

In the last step, we enabled this feature for all phones that have a shared line. In the case of the salesperson and the trainee, we do not want the trainee to barge into a call that the salesperson might be on.

1. On the Cisco Unified CM Administration page, navigate to **Device > Phone**.

2. Click **Find** and select the first HQ phone.

3. In the Device Information section, scroll down to the **Privacy** parameter and select **On** from the drop-down list. By setting Privacy to On, every call placed from the salesperson's phone is assumed to be private, and barging will be disabled. However, because we did not change this on the trainee's phone, the salesperson will be able to barge in to the trainee's calls. See Figure 11-16 for an example of this page.

4. Click the **Save** button.

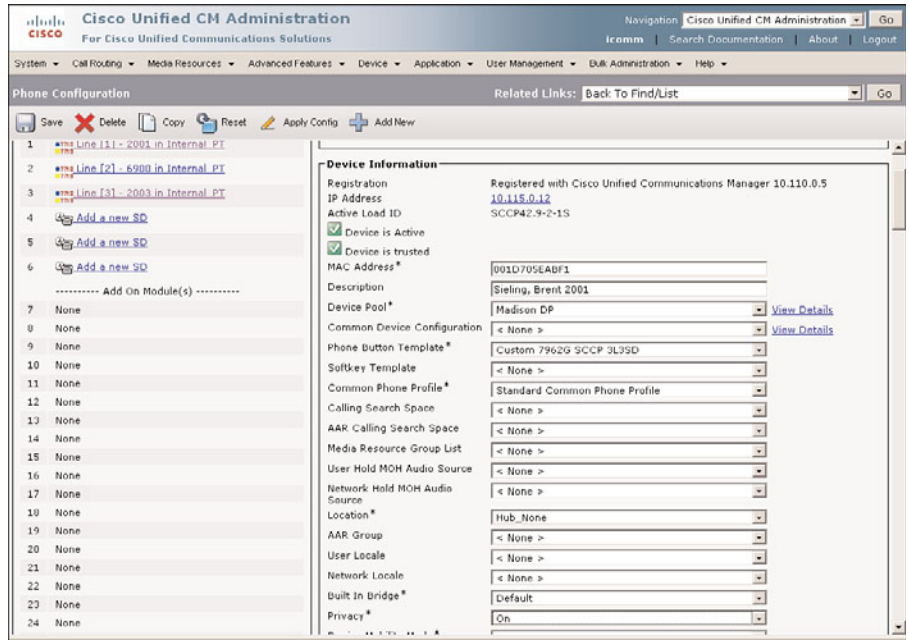
5. Click the **Apply Config** button.

6. On the second HQ phone (the trainee) just click the **Apply Config** button or reset the phone to have barge applied.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 11-16 Phones Privacy Configuration



Step 4-3: Testing Barge

From the third phone in your pod, call the shared line (6900). Answer the call on the trainee's phone and leave it off-hook. Next, on the salesperson's phone, press the **shared line** button (it should be lit up red) and then the softkey labeled **Barge**. A three-way call between all phones should now be set up. Hang up all phones.

Next, from the third phone in your pod, call the shared line (6900). Answer the call on the salesperson's phone and leave it off-hook. Now attempt to barge in to the call form the trainee's phone; this should be unsuccessful.

Task 5: Configure Intercom

Another feature that SOI wants to deploy is Intercom. The company has a number of executives that require an intercom system to communicate with their assistants. CUCM intercoms work by first setting up a one-way audio stream. The user at the other end can then accept the call, at which point, a two-way stream is set up. This prevents someone from overhearing sensitive information when he initiates an intercom call.

Step 5-1: Create Intercom Partitions

Intercom partitions are similar to standard partitions. They are assigned to intercom directory numbers. The calling intercom line must have an intercom Calling Search Space (CSS) that allows access to the intercom partition assigned to the destination intercom directory number.

1. On the Cisco Unified CM Administration page, navigate to **Call Routing > Intercom > Intercom Route Partition** and click **Add New**.
2. There is only one entry field on this screen. In the **Name** field, enter **SalesExec_Intercom, Sales Executive Intercom** and click **Save**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

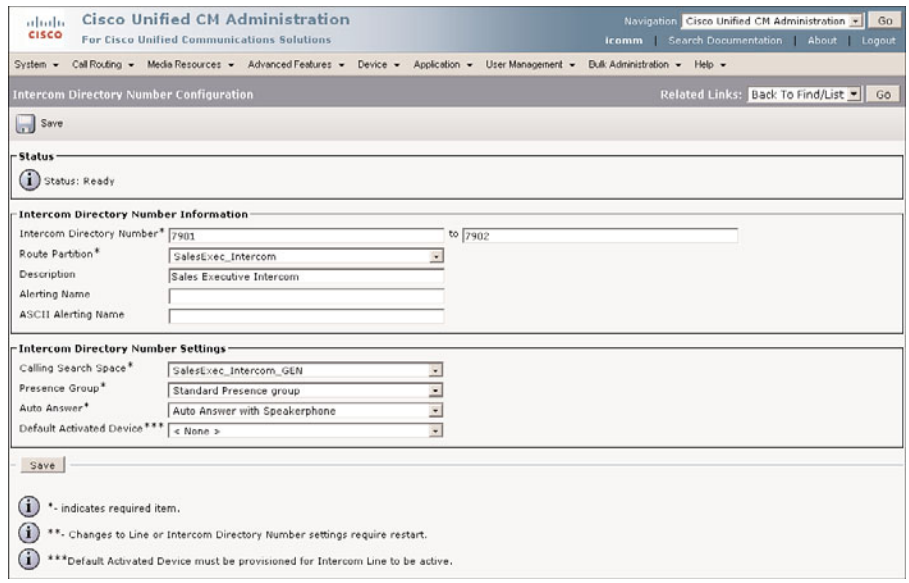
3. You are now returned to the main Intercom Partition page. Click **Find**, if the partition you just created did not appear.
4. Now navigate to **Call Routing > Intercom > Intercom Calling Search Space** and click **Find**.
5. A CSS named **SalesExec_Intercom_GEN** should be in the list. Intercom calling search spaces are automatically generated when you add an intercom partition.

Step 5-2: Create Intercom Numbers

On the Cisco Unified CM Administration page, navigate to **Call Routing > Intercom > Intercom Directory Number**.

1. Click the **Add New** button.
2. To create a range of intercom DNs, enter a starting directory number in the Intercom Directory Number field and then an ending number in the next field to the right. Because we are only going to create two intercom directory numbers, enter **7901** in the first **Intercom Directory Number** field and **7902** in the second field.
3. From the **Route Partition** drop-down list, select **SalesExec_Intercom**.
4. In the **Description** field, enter **Sales Executive Intercom**.
5. From the **Calling Search Space** drop-down list, select **SalesExec_Intercom_GEN**. This is the CSS that was automatically created when you created the intercom partition. By selecting this CSS, the intercom lines will only be able to call each other. See Figure 11-17 for an example of this page.
6. Click the **Save** button.
7. Navigate to **Call Routing > Intercom > Intercom Directory Number** and click **Find**. 7901 and 7902 should appear in the list.

Figure 11-17 Intercom Directory Numbers



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Note: The 7960 and 7940 models of the phone will not support intercoms configured this way. See the *Intercom Support for Cisco Unified IP Phones* section of the *Features and Services Guide* for your version of CUCM.[1]

Step 5-3: Configure Intercom on First Phone

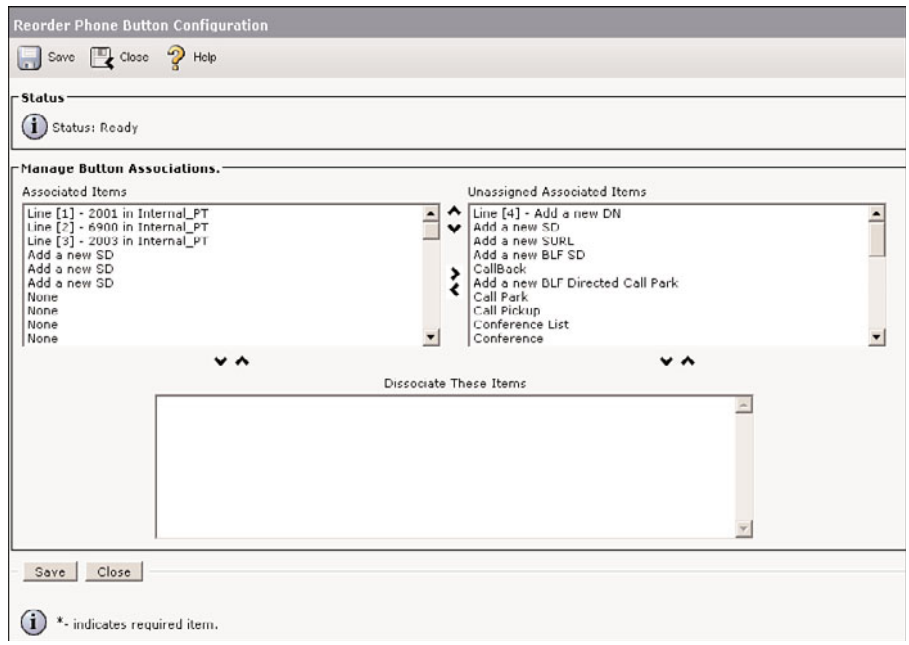
On the **Cisco Unified CM Administration** page, navigate to **Device > Phone**.

Click **Find** and select the first HQ phone. You now need to configure phone button number 6 to be an intercom button. Most likely, the phone button template assigned to the phone has button number 6 configured as a speed dial button. Typically, to change this button you would need to create a new softkey template and apply it to the phone, which is the recommended method. However, in this lab, we use a different method that allows us to change it directly from the device configuration page.

Warning: Using the method described next will cause a new phone button template to be added to the system. This means that if you were to use this method on ten phones, you would add ten phone button templates to your system. This could result in difficulties when trying to manage the system.

1. To change button 6 to an intercom button, click **Modify Button Items**, which is on the left side of the page at the top of the **Association Information** section. You might receive a warning informing you that unsaved changes will be lost; click **OK**. The Reorder Phone Button Configuration page will open. See Figure 11-18 for an example of this page.

Figure 11-18 Modify Phone Buttons Part 1



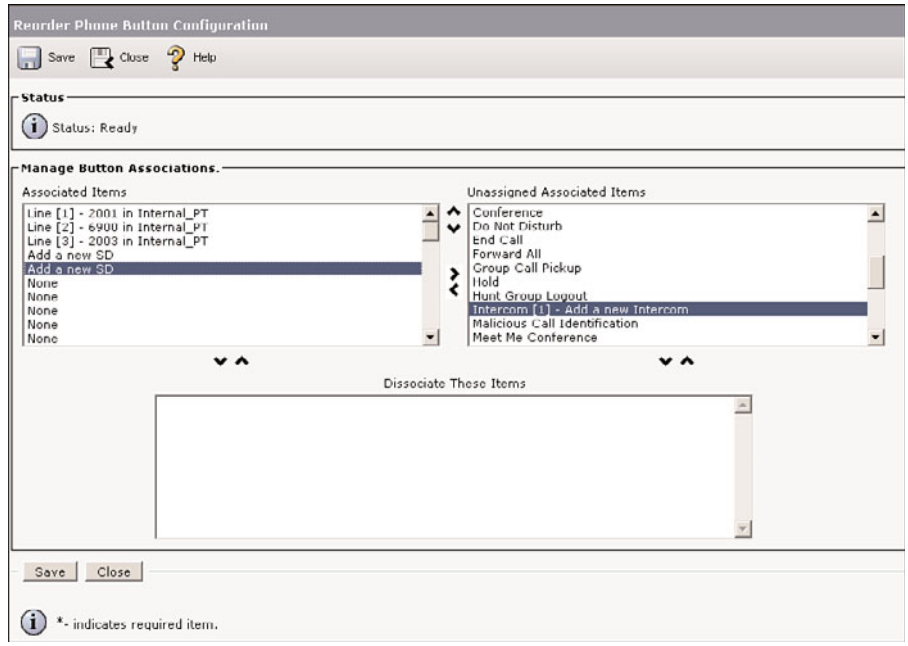
2. Highlight the sixth item in the **Associated Items** list and click the arrow that points to the right.
3. Highlight the fifth item in the **Associated Items** list and highlight the **Intercom [1] – Add a new Intercom** item in the **Unassigned Associated Items** list. See Figure 11-19 for an example of this page.

[1] Franske, Ben; Inver Hills Community College

https://t.me/learningnets

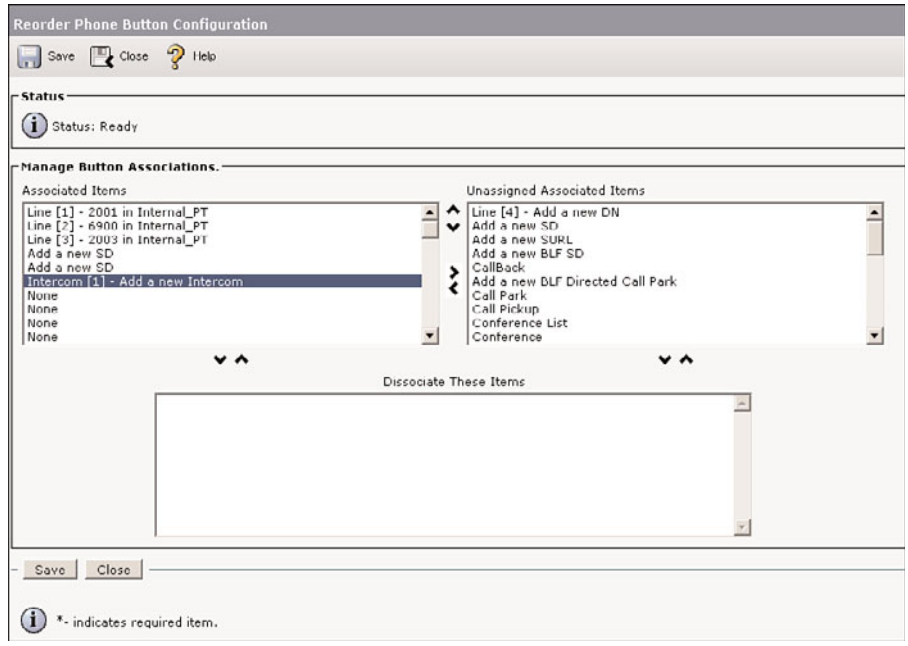
From the Library of Aliwarman Tarihoran

Figure 11-19 Modify Phone Buttons Part 2



4. Click the arrow that points to the left. This should make the sixth item on Associated Items list an intercom button. See Figure 11-20 for an example of this page.

Figure 11-20 Modify Phone Buttons Part 3



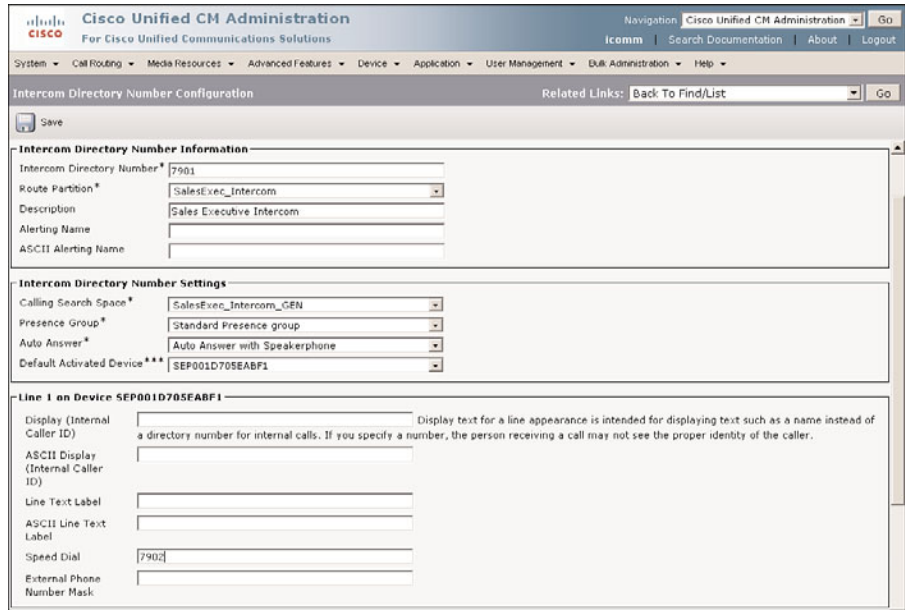
5. Click the **Save** button, and after the page has updated, click **Close**.
6. Write down the MAC Address of the phone (from the MAC Address field).
7. Button 6 should now read **Intercom [1] – Add a new Intercom**. Click this link

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

8. On the next page, enter **7901** in the **Intercom Directory Number** field. Notice that when you click somewhere else on the screen, a "Loading, please wait" alert appears and the page refreshes. Look at the **Intercom Directory Number Settings** and see that these fields have automatically been populated based on how you configured the intercom directory number when you created it.
9. In the **Default Activated Device** drop-down list, select the MAC address of the first phone that you wrote down.
10. In the **Line 1 on Device *<SEP and MAC address of phone>*** section **Speed Dial** field, enter the other intercom directory number (for this lab, use **7902**). See Figure 11-21 for an example of this page.

Figure 11-21 Intercom Directory Number Configuration



11. Click the **Save** button.
12. Click the **Apply Config** button. Click **OK** to close the pop-up window.

Step 5-4: Configure Intercom on Second Phone

Next, you need to assign an intercom line to the second HQ phone. Navigate to **Device > Phone**. Click **Find** and select the second HQ phone.

1. You will need to configure button 6 as an intercom DN just as you did on the first HQ phone. You might need to refer to the instruction in Step 5-3. However, this time when you configure the Intercom directory number, you will need to reverse where you enter the 7902 and 7901 numbers.
2. After you configure the button 6 intercom DN, click the **Intercom [1] – Add a new Intercom** link.
3. Enter **7902** in the **Intercom Directory Number** field and **7901** in the **Speed Dial** field. The result of this is the intercom on the first phone (7901) causes 7902 on the second phone to

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

auto-answer (muted), while the intercom on the second phone (7902) causes 7901 on the first phone to auto-answer (muted).

Step 5-5: Testing Intercom

Press line button 6 on the first HQ phone. This should cause a one-way audio stream to be open between the two HQ phones. Now go off-hook or press the intercom line button on the second HQ phone, and a two-way stream should be set up.

Note: You have to use the line button to unmute the intercom on the softphone. If you press the speakerphone icon, the call ends.

If you press line button 6 on the second phone, the intercom on the first phone should auto-answer muted.

Step 5-6: Intercom Challenge

Currently, the intercom appears on the phone display as just 7901 or 7902. When the intercom is activated on one phone, the other phone just displays the other intercom number. The staff at SOI want to know if you can change the display on the phone next to the button to show not just the intercom number, but also include a short description, such as "Intercom to Trainee 7901." In the future, there may be more than one intercom on a phone, so the employees would also like an incoming intercom call to show a description. Where would you make changes, and to what fields, to achieve this?

Implement your answer to test.

Task 6: Configure Native Presence

One issue that SOI had with its old phone system was that there was no way for an executive assistant to know whether their boss was on the phone. This resulted in assistants transferring calls to people who were already on calls. To help avoid this issue, SOI has decided to implement Presence. This feature will allow assistants to see the status of their boss's phone.

Step 6-1: Configure Phone Button Template (BLF Speed Dials)

One way to use Presence to monitor the status of another line is to create a Busy Lamp Field (BLF) speed dial button. The Busy Lamp Field will not only be a speed dial (press to call the number), it also shows the status of the configured directory number. To do this, you will need to have one of the phone buttons defined as a speed dial BLF button by creating a new phone button template. In Task 5, you did this by modifying the template at the device level, which resulted in a new phone button template automatically being created for that phone. In this task, we will manually create a new phone button template.

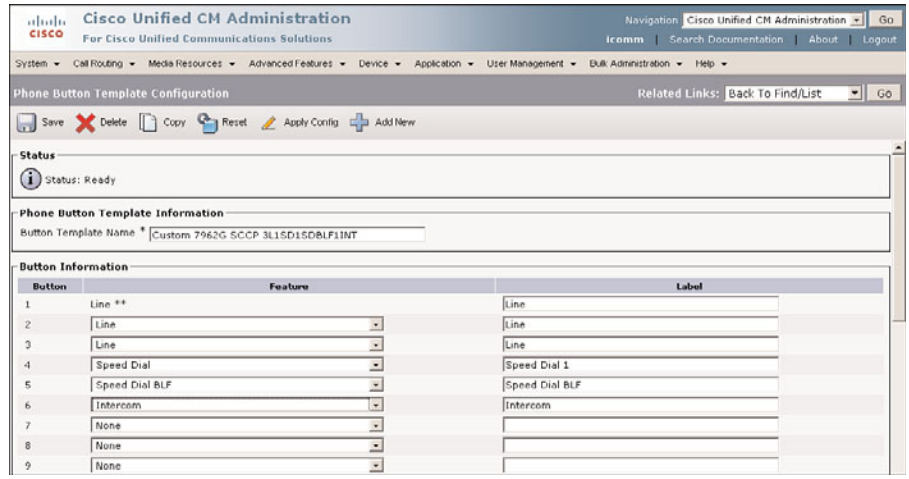
1. On the Cisco Unified CM Administration page, navigate to **Device > Device Settings > Phone Button Template** and click **Find**.
2. Scroll down the list that appears and select the one of the custom phone button templates you created in Task 7 of lab 9-4 (Example: Custom 7962 SCCP 3L3SD).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. On the next screen, click **Copy**.
4. Enter new name for this template by changing the name to something like this: Custom 7962G SCCP 3LD1SD1SDBLF1INT, which would let you know this template is for a 7962 phone, using SCCP, with 3 lines, 1 speed dial, 1 speed dial busy lamp field, and one intercom.
5. Click the **Save** button.
6. In the **Button 5** drop-down list, select **Speed Dial BLF**.
7. In the **Button 6** drop-down list, select **Intercom**. See Figure 11-22 for an example of this page.

Figure 11-22 Phone Button Template with Speed Dial BLF



8. Click the **Save** button.
9. If necessary, repeat this step to create a similar template for all other models of phones you have.

Step 6-2: Enable BLF Speed Dials

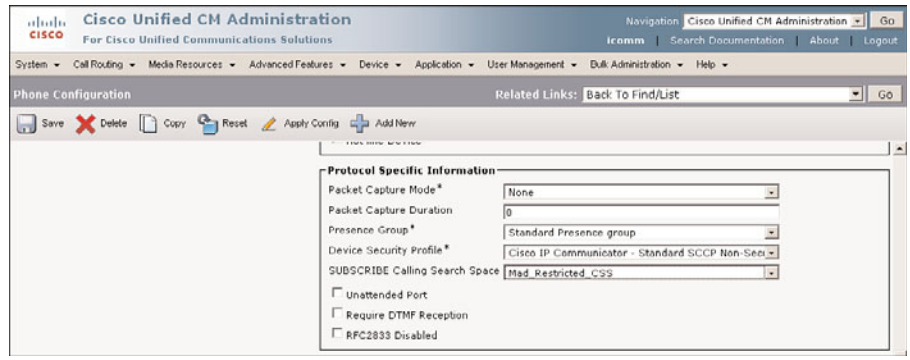
Before another phone can monitor the status of another directory number that has a partition assigned, the phone needs a Subscribe Calling Search Space (CSS) that includes the partition. Since all the directory numbers were assigned partitions in Lab 10-2, this phone must have a Subscribe CSS that includes the Internal_PT. Navigate to **Device > Phone** and click **Find**. Select the second HQ phone.

1. Scroll down to the Protocol Specific Information section and select **Mad_Restricted_CSS** from the **SUBSCRIBE Calling Search Space** drop-down list. See Figure 11-23 for an example of this page.
2. Scroll-back up to the Device Information section and select the phone button template you just created from the **Phone Button Template** drop-down list.
3. Click the **Save** button.
4. A pop-up window opens telling you to click the Apply Config button. Click OK to close the pop-up window.
5. Click the **Apply Config** button. A pop-up window will inform you of the devices impacted. Click **OK**.

https://t.me/learningnets

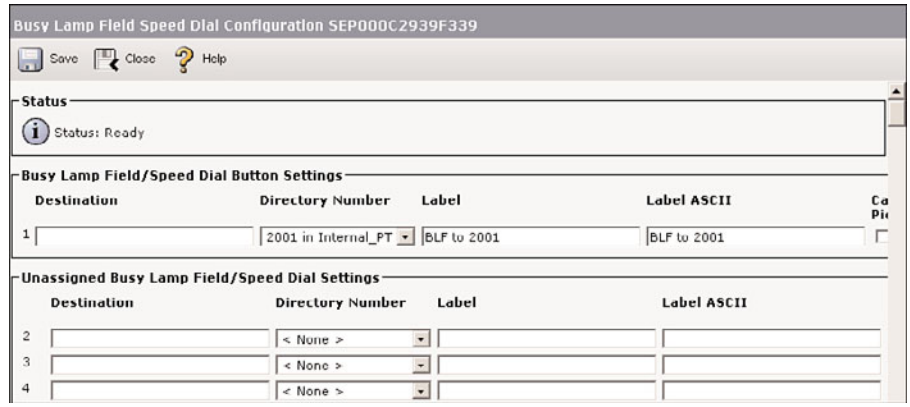
From the Library of Aliwarman Tarihoran

Figure 11-23 SUBSCRIBE Calling Search Space



6. In the Association Information section, click the new line called **Add a new BLF SD**.
7. From the Directory Number drop-down list near the top of the page, select the extension of the first HQ phone.
8. Enter descriptive text, such as "**BLF to *<directory number>***" in the **Label** field, and then click outside of the field. See Figure 11-24 for an example of this page.

Figure 11-24 Busy Lamp Field Speed Dial Configuration



9. Click the **Save** button.
10. After the page refreshes, click **Close**. Look at the second HQ phone. The icon next to the BLF button should show a phone icon in front of a phone keypad. (If you have just the keypad [9 squares], the SUBSCRIBE CSS is not correct or applied to the phone.)
11. Go off-hook on the first HQ phone. Look at the fifth button on the second HQ phone; it should indicate that the first HQ phone is off-hook with the icon showing two handsets over the keypadHang the phone back up.
12. On the second HQ phone, press the BLF line button. It will speed dial the monitored number.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

This page intentionally left blank

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CHAPTER 12

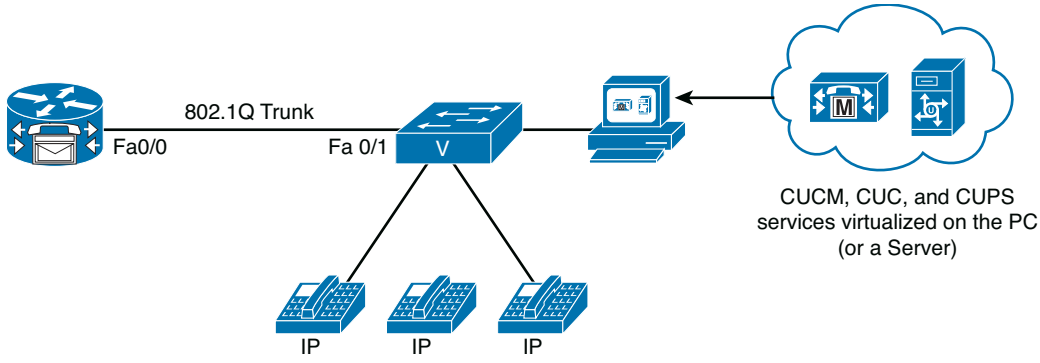
CUCM Mobility Features

This chapter explores Cisco Unified Communications Manager's (CUCM's) mobility features, which includes Mobile Connect and Mobile Voice Access (MVA). Mobile Connect allows a call placed to a Cisco IP Phone to ring at additional phones, such as a cell or home phone. This allows the caller to only need to know one number in order to reach someone no matter where he or she might be. This is often referred to as Single Number Reach (SNR). In addition, Mobile Connect allows a user to transfer a call from one device to another without placing the call on hold. For example, a user might answer a call on her office phone just before she leaves the office. After answering this call, she realizes that the call is not going to be a short one. She can press a softkey on the Cisco IP Phone, and her cell phone will begin to ring. She can answer her cell phone and the call will be transferred to that phone.

MVA allows all calls placed by a user to appear as if they are originating from the person's office phone. One benefit of this is that it continues to present a single-number appearance. For example, the number a customer is used to dialing when calling his account representative is the same number he will see as the caller ID when the account representative calls him. Often this feature is used when the user is using his mobile phone, but it can also be used when using any phone other than the user's primary office phone.

Lab 12-1: Mobile Connect

Figure 12-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- CUCM Server or PC with VMware Workstation installed and a VM of CUCM
- Three or more IP phones registered (desk phone or soft phone on PC or Windows VM)
- Configuration from Lab 11-2

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Learning Objectives

Upon completion of this lab, you will be able to

- Enable users and phones for Mobile Connect
- Define remote destinations
- Configure and apply access lists

Scenario

Shiny Objects Inc. (SOI) has a large outside sales staff, and many of the salespeople rarely come into the office. To allow the salespeople to leverage the company's CUCM, SOI has decided to deploy Mobile Connect. This will give salespeople the ability to receive calls on their cell phone when a customer calls their office number. It will also allow them to transparently transfer calls between their office and cell phones.

Task 1: Enable Users and Phones for Mobile Connect

Mobile Connect is a feature that most often is not enabled for every user on the system. As you can imagine, there often wouldn't be a need for such a feature for individuals who do all their work from the office and don't find themselves on the road often. Because the feature isn't used by everyone, you will need to do some configuration for the users and phones that will require this feature.

Step 1-1: Configure User to Use Mobile Connect

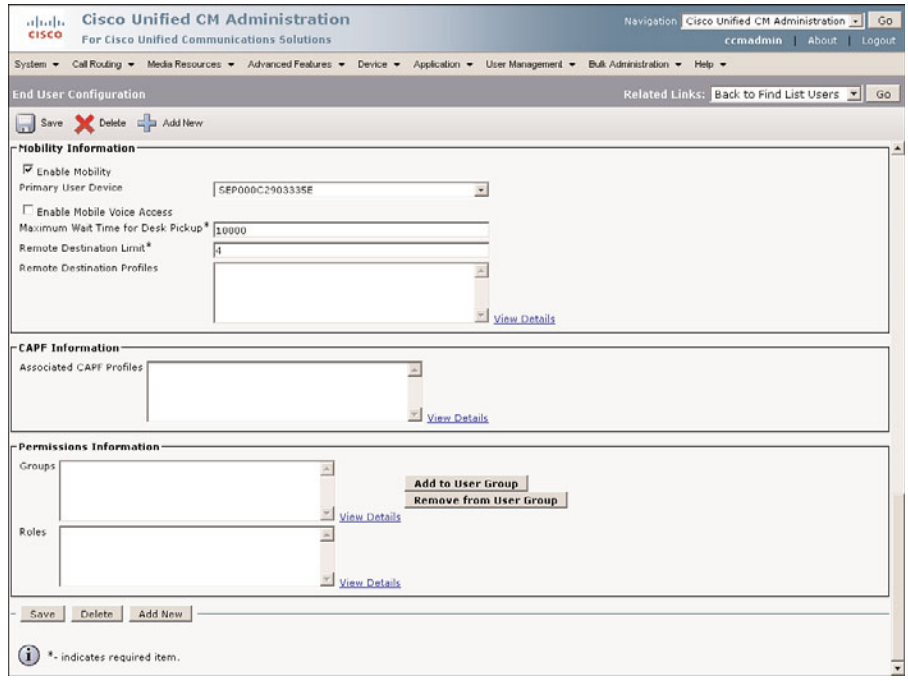
On the Cisco Unified CM Administration page, navigate to **Device > Phone**. Click **Find** if no phones are listed.

1. Back in Chapter 9, "Managing Services, Phones, and Users," you assigned a user account with your name to a phone. From the **Device Name** column, write down the MAC address of that phone (the characters listed right after the SEP).
2. On the Cisco Unified CM Administration page, navigate to **User Management > End User**. Click **Find** if no users are listed.
3. Select the user with your name.
4. Scroll down to the **Mobility Information** section. Select the **Enable Mobility** check box. By selecting this box, you are enabling Mobile Connect for this user, but not MVA. We will enable MVA later.
5. In the **Primary User Device** field**,** select the MAC address of the phone associated with this user (that you wrote down above). This is done is so that less licensing units are used. If you do not associate a phone to this user in the Primary User Device field, four additional Device License Units (DLU) are required for Mobile Connect. By associating a physical device, only two additional DLUs are required. See Figure 12-2 for an example of this page.
6. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 12-2 User Configuration for Mobile Connect



Step 1-2: Configure Softkey Template

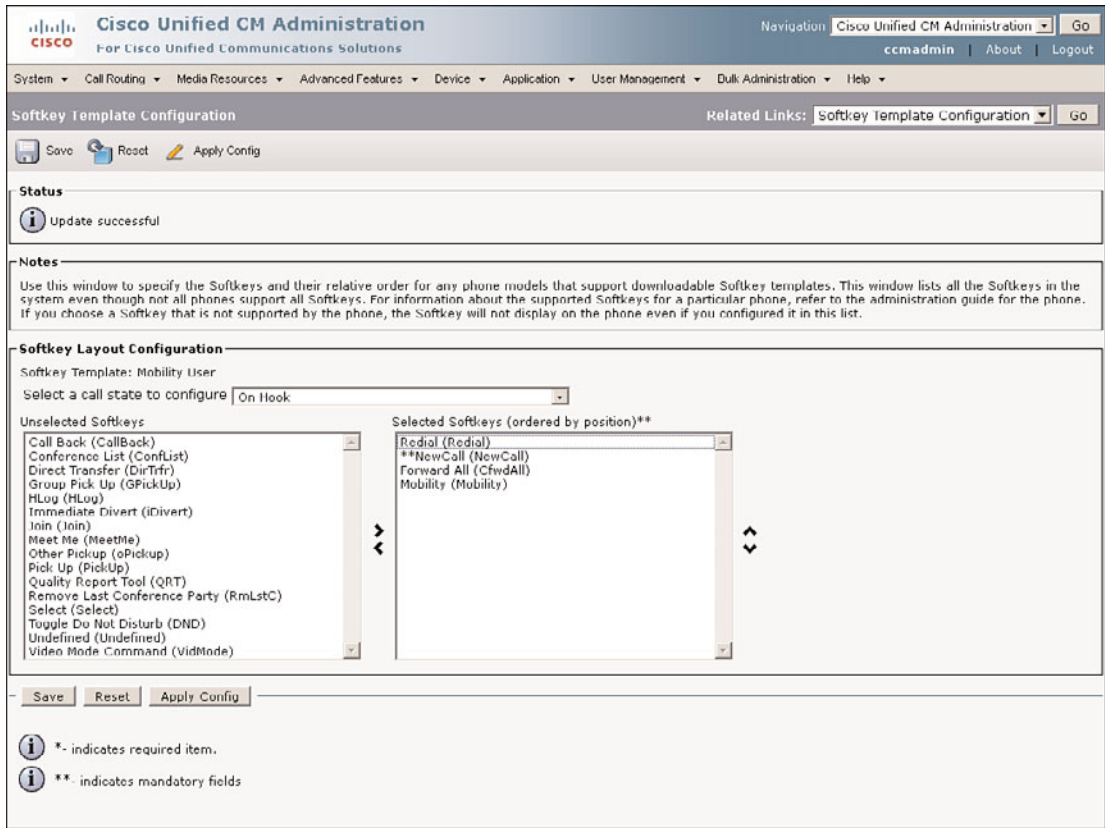
A softkey template will be needed to add the Mobility button to the users phone so they can transfer calls from the desk phone to their cell phone. Navigate to **Device > Device Settings > Softkey Templates**.

1. Click the **Add New** button**.** On the next page, you must select an existing softkey template on which to base the new template.
2. Select **Standard User** from the drop-down list in the **Create a softkey template based on** field.
3. Click the **Copy** button.
4. On the next screen, enter **Mobility User** in the **Name** field.
5. The description should help identify the features associated with the template, so enter **Standard Template + Mobility** in the **Description** field.
6. Leave the **Applications** field set to **Cisco CallManager**
7. Click the **Save** button.
8. With the **Related Links** drop-down set to **Configure Softkey Layout**, click **Go**.
9. From the **Select a call state to configure** drop-down list, select **On Hook**.
10. In the **Unselected Softkeys** list, select **Mobility (Mobility)** and click the arrow that points to the right (it looks like a greater-than sign [>]). This will move the **Mobility (Mobility)** item over to the **Selected Softkeys** list. See Figure 12-3 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 12-3 Add Mobility Softkey to On Hook State

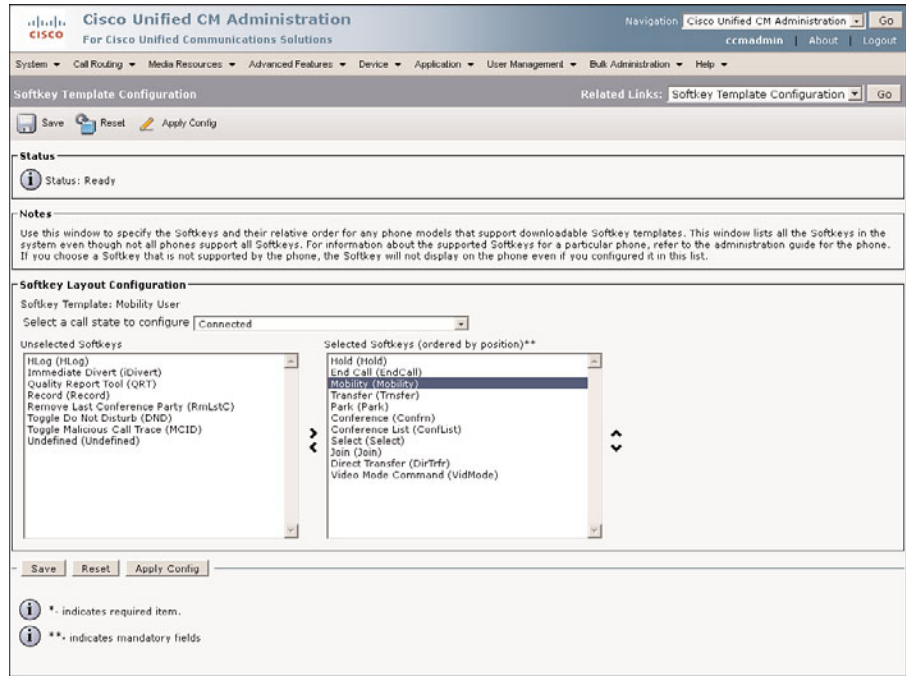


11. Click the **Save** button.
12. From the **Select a call state to configure** field**,** select **Connected** from the drop-down list.
13. In the **Unselected Softkeys** list, select **Mobility (Mobility)** and move it over to the **Selected Softkeys** list.
14. You will notice that it is at the bottom of the list, which means that a user will have to press the **More** softkey three times before she has access to this softkey. Use the up arrow to the right of the list to move **Mobility (Mobility)** to the third position from the top. This will cause it to be the third softkey when the phone is in the connected call state. See Figure 12-4 for an example of this page.
15. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 12-4 Add Mobility Softkey to Connected State



Step 1-3: Configure Phone for Mobile Connect

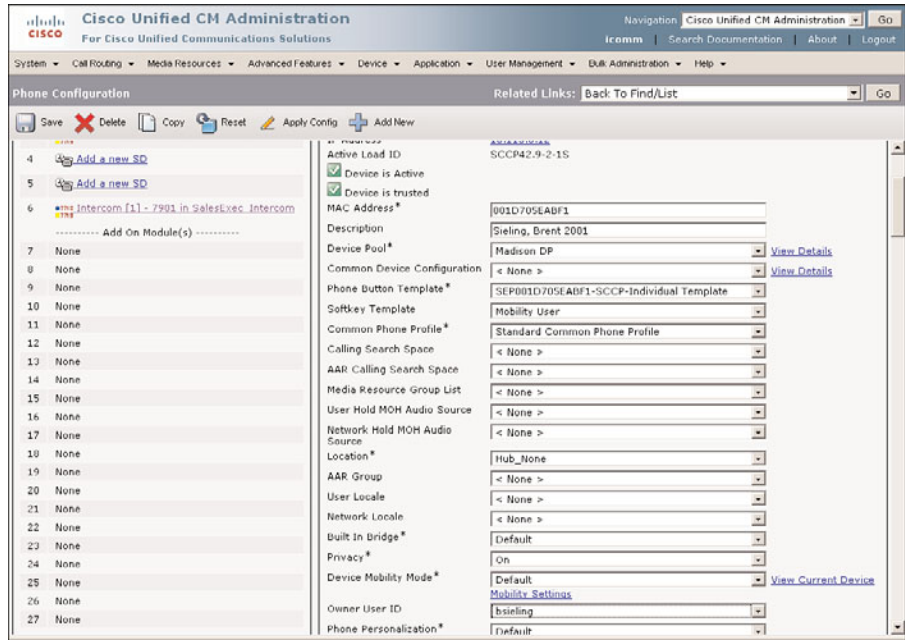
On the Cisco Unified CM Administration page, navigate to **Device > Phone**. Click **Find** if no phones are listed.

1. Select the first HQ phone (should be the phone assigned to your user account).
2. Check to see whether extension mobility is enabled. To do this, scroll down to the Extension Information selection and see whether the **Enable Extension Mobility** check box is selected. If it is, deselect it and click **Save**. This should be done to associate an owner ID to this phone, which cannot be accomplished if extension mobility is enabled.
3. Now, scroll to the top, and in the Device Information section, select **Mobility User** from the **Softkey Template** drop-down list.
4. Select the user you enabled Mobile Connect for (in Step 1-1) from the **Owner User ID** drop-down list. See Figure 12-5 for an example of this page.
5. Click the **Save** button. You should see a pop-up window telling you to click the Apply Config button. Click **OK** to close the pop-up window.
6. Click the **Apply Config** button. A pop-up window will appear informing you to save changes before applying config. Click **OK**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 12-5 Configure Phone for Mobile Connect



Task 2: Create Remote Destinations and Remote Destination Profiles

A remote destination profile must be configured for each extension that is going to support the Mobile Connect feature. The remote destination profile can be thought of as a virtual phone that shares the same extension number as the user's office phone. It is, in fact, a shared line. As you recall, when a call is placed to a shared line, all the devices that have the shared line assigned ring; the same thing happens in this case. The call is extended to the office phone and to the remote destination profile. The remote destination profile has remote destinations associated with it and extends the call to those remote destinations.

A remote destination is configured for each outside phone you want to use with Mobile Connect or MVA. For example, a remote destination would have to be configured for a user's cell phone because we want Mobile Connect to ring that phone when a call comes in to the user's office phone.

Step 2-1: Create Remote Destination Profile

On the Cisco Unified CM Administration page, navigate to **Device > Device Settings > Remote Destination Profile**

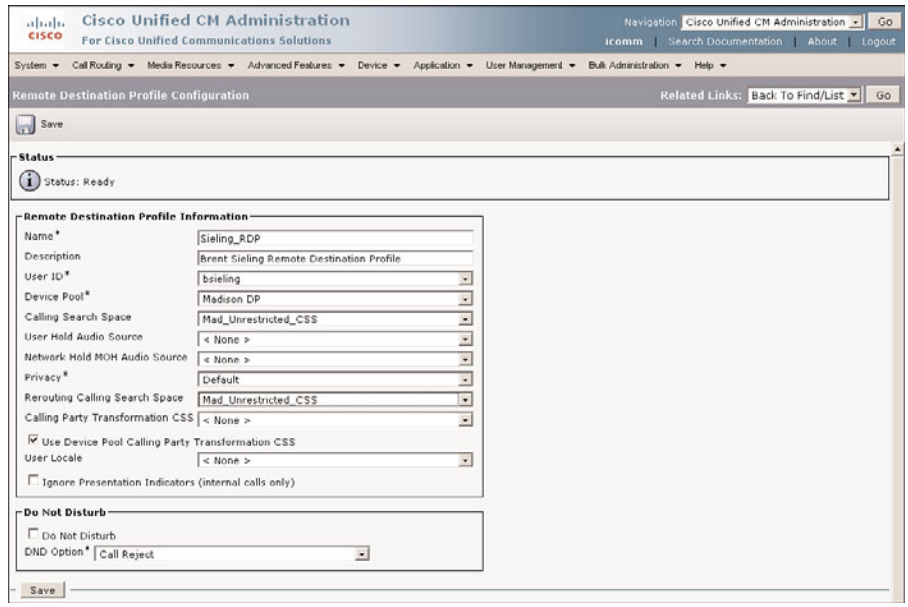
1. Click the **Add New** button.
2. In the Name field, enter your last name followed by **_RDP**.
3. Enter a description of your choice in the **Description** field.
4. Select ***your user ID*** from the **User ID** drop-down list.
5. Select the **Madison DP** from the **Device Pool** drop-down list.
6. Select the **Mad_Unrestricted_CSS** from the **Calling Search Space** drop-down list. The Calling Search Space (CSS) selected needs to have access to all partitions. This CSS is used when calls are placed using MVA.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

7. Select the **Mad_Unrestricted_CSS** from the **Rerouting Calling Search Space** drop-down list. This CSS is used to route calls to remote destinations. For this lab, the remainder of the fields can be left at default settings. See Figure 12-6 for an example of this page.

Figure 12-6 Remote Destination Profile



8. Click the **Save** button.
9. Click the **Line [1]** – **Add a new DN** link.
10. The parameters on the page should match those on the line of the phone that Mobile Connect is being configured for. For the lab, set the **Directory Number** to the first directory number on the first HQ phone.
11. Select **Internal_PT** from the **Route Partition** drop-down list.
12. Click the **Save** button. After you save the directory number, the Associated Devices will show both the MAC address of the phone and remote device profile, indicating the shared line nature of this directory number.
13. In the Directory Number Setting section, select **Mad_Unrestricted_CSS** from the **Calling Search Space** drop-down list.
14. Click the **Save** button.

Step 2-2: Create Remote Destinations.

On the Cisco Unified CM Administration page, navigate to **Device > Remote Destinations**.

1. Click the **Add New** button.
2. The Name field will normally contain a descriptive name such as DSmith Cell Phone. For this lab, simply enter ***<your last name>*** **Remote Phone** in the **Name** field.
3. Typically, the Destination Number field is where you would enter the user's cell phone number. Destination numbers must be numbers that are registered to a system other than your CM cluster. Because we can't send a call to a cell phone in the lab environment, we will have to use

https://t.me/learningnets
From the Library of Aliwarman Tarihoran

another phone that is registered to a system other than your cluster but is accessible from your cluster. If you have a partner pod in your lab environment, you can use one of those phones. Enter the full PSTN number to reach the extension number of one of your partner pod's phones in the **Destination Number** field. The number should be formatted exactly the way it would be dialed on a phone, so do not forget to include the outside line access digit. If you do not have any phones in your lab that are not part of your cluster, enter **95554101**.

Note: If you do not have any phones in your lab that are registered to a system other than your cluster, you will not be able to fully test Mobile Connect. You might be able to connect an analog phone to an FXS port on the PSTN simulator, or configure a VoIP phone on the PSTN simulator, to create an external phone number to call. If you use a phone number such as 95554101 that would be auto-answered on the PSTN simulator by an audio file, the Answer Too Soon Timer (covered next) will prevent it from being used. The number would have to be excluded from the PSTN simulator's local dial peer.

4. The Answer Too Soon Timer field is used to prevent a call from being answered by the cell phone voicemail when the cell phone is off. The default is 1500 milliseconds, which means that if the call is answered by the cell phone within one and a half seconds, it is assumed that the phone is off and has been forwarded to the cell phone voicemail. In this case, CUCM will pull the call back and not extend it to the cell phone's voicemail. For this lab, you can leave this set to default.
5. The Answer Too Late Timer field simply determines how long a cell phone will ring before the call is pulled back by CUCM. The default is 19000 milliseconds (19 seconds). Set the **Answer Too Late Timer** field to **10000** (10 seconds).
6. The Delay Before Ringing Timer field determines how long CUCM will wait before sending the call to the cell phone. This helps prevent the cell phone from ringing when a user is at their desk and is able to quickly answer the phone. Set the **Delay Before Ringing Timer** field to **2000** (2 seconds).
7. From the Remote Destination Profile drop-down list, select the remote destination profile you created in the previous step. Select the **Mobile Phone** check box. This will allow you to transfer a call to this remote destination from the office phone.
8. Select the **Enable Mobile Connect** check box so that incoming calls to the office number will also ring this remote destination.
9. The next section allows you to create a schedule that determines when calls are allowed to be sent to this remote destination. For this lab, we will leave the schedule set to **All the time**. After we configure access lists, we will come back to this screen and configure the last two fields. See Figure 12-7 for an example of this page.
10. Click the **Save** button. An informational window will appear telling you to make sure that the associated phone has the Mobility softkey; click **OK**.
11. When the page refreshes, you will see the Association Information section with the Line [1]. Select the **Line Association** checkbox for **Line 1**. See Figure 12-8 for an example of this page.
12. Click the **Save** button. An informational window will appear telling you to make sure that the associated phone has the Mobility softkey; click **OK**.

Note: In this step, you created a remote destination for a single user. In the real world, each mobility user will require his own remote destinations, and the values, such as the destination number used to create these, will be different for each user.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 12-7 Remote Destination Configuration

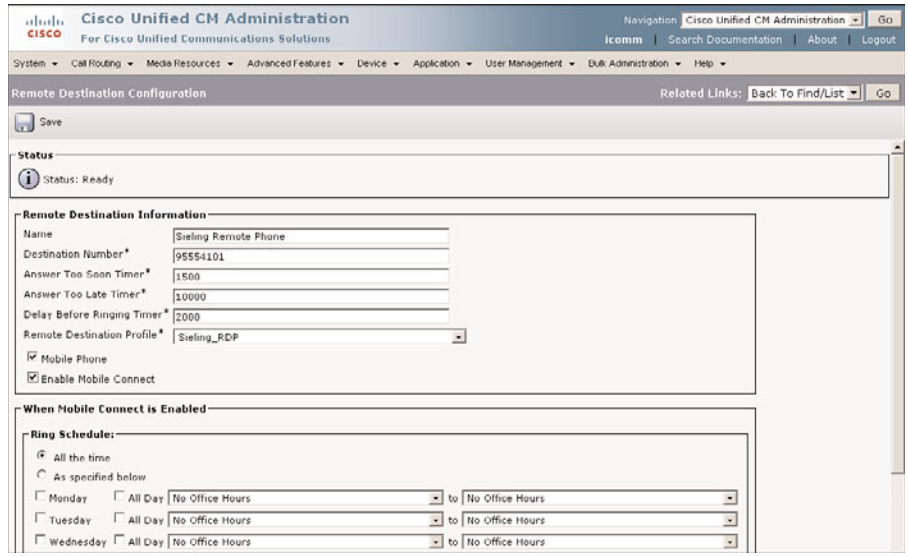
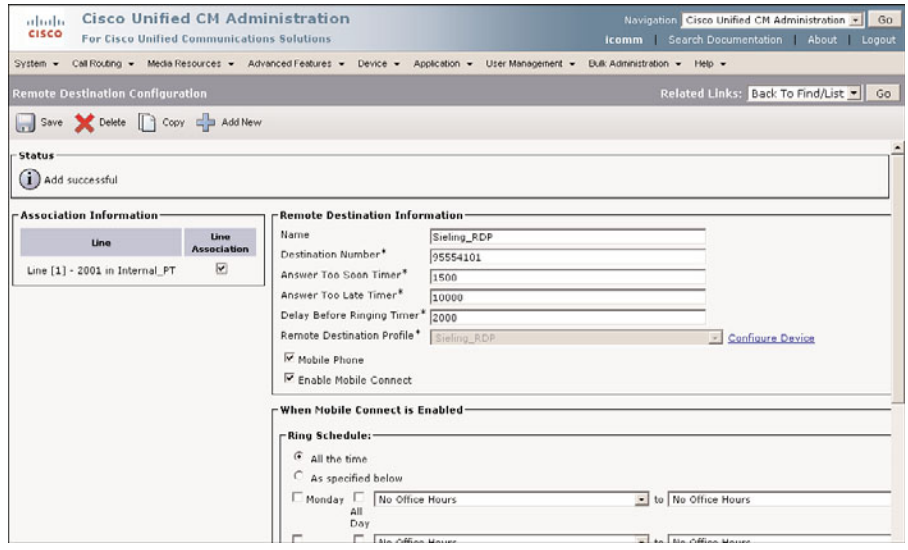


Figure 12-8 Remote Destination Line Association



Task 3: Configure and Apply Access Lists

Not all calls are equal, and there might be some calls that we do not want to ring remote destinations. For example, if one of your more important customers is calling, you will want that call sent to your cell phone. But, if it is that cousin of yours that is always looking for a handout, you might just want that one to find its way to your voicemail. Access lists can be configured so that you can decide which calls are permitted and which are denied access to remote destinations.

https://t.me/learningnets

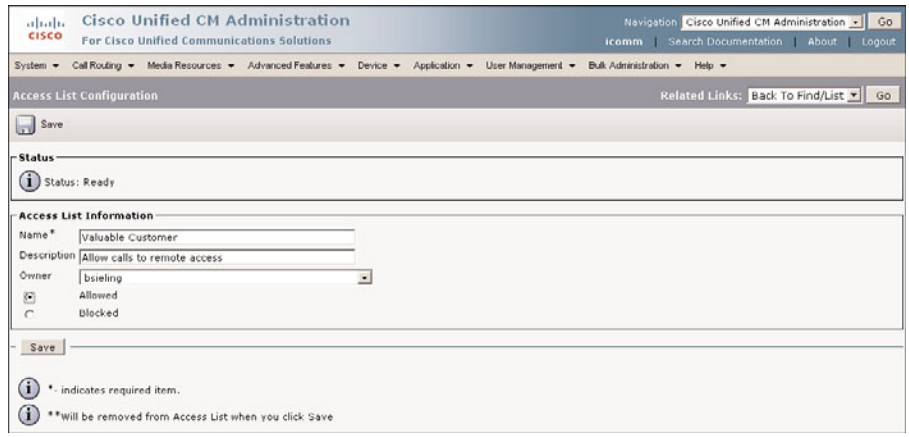
From the Library of Aliwarman Tarihoran

Step 3-1: Create Allowed Number Access List

On the Cisco Unified CM Administration page, navigate to **Call Routing** > **Class of Control** > **Access List**.

1. Click the **Add New** button.
2. Enter **Valuable Customer** in the **Name** field.
3. Enter **Allow calls to remote access** in the **Description** field. Typically, an access list will have more than one number in it, and the description would be something like "West Coast Customers" or whatever best describes the numbers in the list.
4. From the **Owner** drop-down list, select ***<your user name>***.
5. Select the **Allowed** radio button. See Figure 12-9 for an example of this page.

Figure 12-9 Access List Configuration Part 1

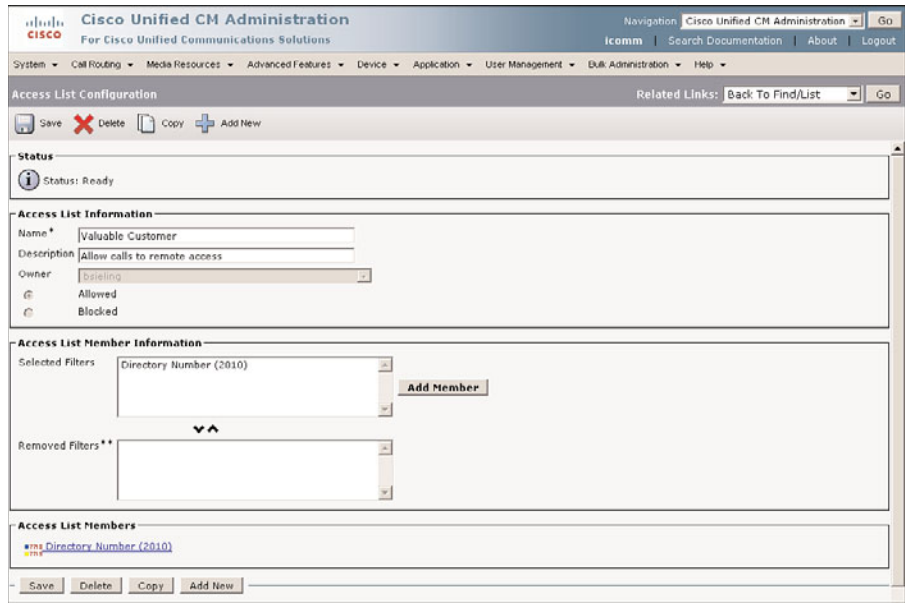


6. Click the **Save** button.
7. On the next page, click the **Add Member** button.
8. The Access List Member Detail page will open. Select **Directory Number** from the **Filter Mask** drop-down list.
9. Enter the first extension number on the third phone in the **DN Mask** field.
10. Click the **Save** button to return to the Access List Configuration page. See Figure 12-10 for an example of this page.
11. Click the **Save** button to save the Access List.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 12-10 Access List Configuration Part 2



Step 3-2: Create Blocked Number Access List

Next, you create an access list that will be used to prevent certain callers from being transferred to the remote destination.

1. Click the **Add New** button.
2. Enter **Block Third Phone Extension 2** in the **Name** field.
3. Enter **Block Second Extension of Third Phone** in the **Description** field.
4. From the **Owner** drop-down list, select ***<your user name>***.
5. Select the **Blocked** radio button.
6. Click the **Save** button.
7. On the next page, click **Add Member**.
8. The Access List Member Detail page will open. Select **Directory Number** from the **Filter Mask** drop-down list.
9. Enter the second extension number on the third phone in the **DN Mask** field.
10. Click the **Save** button to return to the Access List Configuration page.
11. Click the **Save** button to save the Access List.

The page should look similar to the one shown in Figure 12-9, except that the one you just created is configured to block the caller while the one previously created is configured to allow the caller.

https://t.me/learningnets

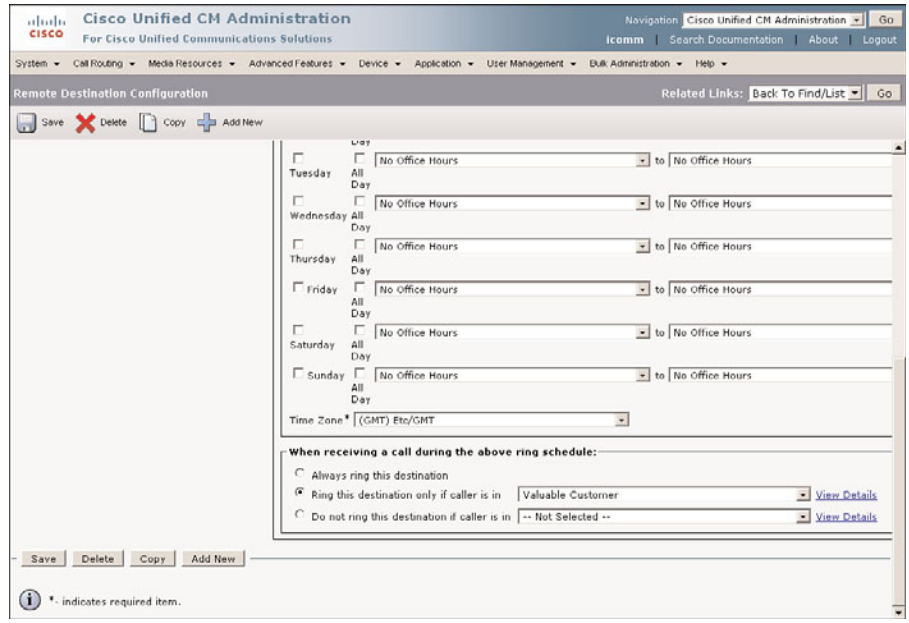
From the Library of Aliwarman Tarihoran

Step 3-3: Apply Access Lists

Now that the access lists have been created, you are going to apply them to a remote destination. Remote destinations do not require that an access list be assigned to them; they are only used when you want to filter which callers are forwarded to remote destinations. On the Cisco Unified CM Administration page, navigate to **Device > Remote Destination** and click **Find** if no remote destinations are listed.

1. Select the remote destination you created earlier in this lab.
2. Scroll down to the **When receiving a call during the above ring schedule** section of the page. Select the **Ring this destination only if caller is in** radio button.
3. Select **Valuable Customer** from the corresponding drop-down list. This will allow calls placed from the first extension on the third phone to the first HQ phone to ring both the first HQ phone and the remote destination (phone 2), but calls from any other phone will only ring the first HQ phone. See Figure 12-11 for an example of this page.

Figure 12-11 Apply Access List to Remote Destination



4. Click the **Save** button. An informational window will appear telling you to make sure that the associated phone has the Mobility softkey; click **OK**.

Task 4: Testing Mobile Connect

Step 4-1: Mobile Connect—Forwarding to Remote Destination

From your third phone, place a call to the first extension of the first HQ phone. The first HQ phone should ring and shortly after that the remote destination phone should start to ring. Answer the call on the first HQ phone.

Note: If you do not have any phones in your lab that are registered to a system other than your cluster, only the first phone will ring.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Now press the **Mobility** softkey and then the **Select** softkey, and the remote destination phone should start to ring.

Note: If you do not have any phones in your lab that are registered to a system other than your cluster, you will receive an error on phone one stating that it failed to send the call to the mobile phone. This is to be expected because you do not have a legitimate remote destination.

You can answer the call on the remote destination phone and the call will be transferred. You do not need to press any other keys other than the Mobility softkey on the first HQ phone.

At this point, only the numbers on the allowed access list will cause the remote phone to ring. Since the first extension on the third phone is the only number on that list, it is the only number that will cause the remote destination phone to ring. If you call from the second directory number on the third phone, or the first extension on the second phone, the remote phone will not ring. However, calls from all phones can still be transferred from the desk phone to the remote phone.

Step 4-2: Mobile Connect—Blocking

Note: If you do not have any phones in your lab that are registered to a system other than your cluster, this testing is not possible.

On the Cisco Unified CM Administration page, navigate to **Device > Remote Destination** and click **Find** if no destinations are listed.

1. Select the remote destination you created earlier in this lab.
2. Scroll down to the **When receiving a call during the above ring schedule** section of the page. Select the **Do not ring this destination if caller is in** radio button.
3. Select **Block Third Phone Extension 2** from the corresponding drop-down list.
4. Click the **Save** button. An informational window will appear telling you to make sure that the associated phone has the Mobility softkey; click **OK**.
5. Now using the second extension on the third phone, place a call to the first extension of the first HQ phone. The HQ phone should ring, but the remote destination phone should not. However, the first extension on the second phone, as well as the first extension on the third phone can cause the remote phone to ring.

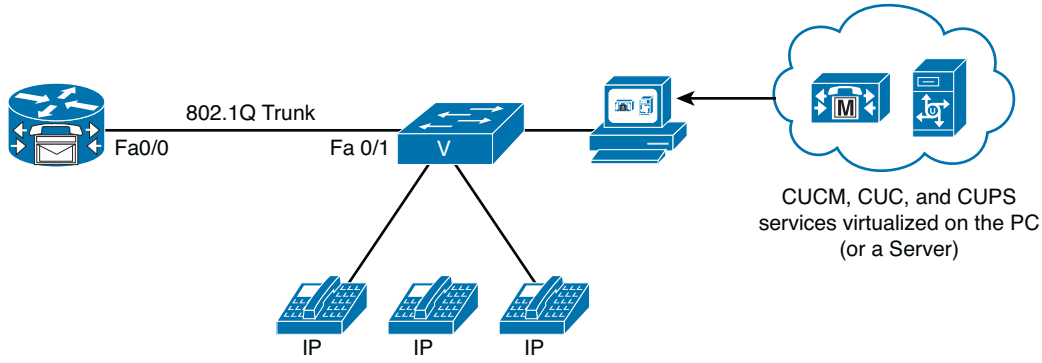
   At this point, only the numbers on the blocked access list will not cause the remote phone to ring. Any extension (that is not on the blocked list) that calls the first extension on the first HQ phone will cause the remote phone to ring.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 12-2: Mobile Voice Access

Figure 12-12 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- CUCM Server or PC with VMware Workstation installed and a VM of CUCM
- Configuration from Lab 12-1

Learning Objectives

Upon completion of this lab, you will be able to

- Enable MVA
- Configure users for MVA
- Configure MVA

Scenario

SOI has also decided that it wants to deploy MVA. It knew this at the time of deployment, so its integrator configured a Voice Extensible Markup Language (VMXL) gateway that will act as the Interactive Voice Response (IVR) system. This information comes as a great relief to you because this type of task is not a CCNA Voice–level task. However, you do know how to configure the CUCM portion of this solution.

Note: This feature requires an H.323 gateway configured with a VXML application. This lab environment does not include this gateway. Furthermore, the VXML application configuration is not part of the CCNA Voice curriculum. Because of these reasons, and a few other factors, the MVA feature will not be able to be tested at the end of this lab. However, if the steps found in this lab are followed accurately, you will have successfully completed the MVA configuration tasks covered in the CCNA curriculum.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Enable MVA

Just like a number of CUCM features, a service must be activated and service parameters configured before the feature can be used.

Step 1-1: Activate the MVA Service

From within the CUCM web pages, use the Navigation drop-down list in the upper right to select the **Cisco Unified Serviceability** item and click **Go**.

1. Navigate to **Tools > Service Activation**.
2. Select the desired server from the **Server** drop-down list.
3. Select the check box next to **Cisco Unified Mobile Voice Access Service** and click **Save**.
4. A message will appear telling you that this process might take a while. Click **OK**. The Cisco Unified Mobile Voice Access Service will now activate.
5. When the page refreshes, ensure that the Cisco Unified Mobile Voice Access Service is activated.

Step 1-2: Configure Service Parameters for MVA

Configuration of service parameters is done on the Cisco Unified Communications Administration page, so you must first navigate to that page. Use the Navigation drop-down list in the upper right to select the **Cisco Unified CM Administration** item and click **Go**.

1. On the Cisco Unified CM Administration page, navigate to **System > Service Parameters**.
2. Select the Communications Manager **IP Address** from the **Server** drop-down list.
3. Select **Cisco CallManager** from the **Service** drop-down list.
4. Scroll down to the **Clusterwide Parameters (System – Mobility)** section. You see that there are a number of parameters that can be configured here, but there is only one that must be changed to enable MVA. Select **True** from the **Enable Mobile Voice Access** drop-down list.
5. Click the **Save** button.

Task 2: Configure Users for MVA

Just as you had to do when you configured Mobile Connect, you will have to enable users to be able to use the MVA feature. Also, when you configured the remote destinations, there was one setting you did not select that will need to be selected to allow MVA to work properly.

Step 2-1: Enable MVA for the User

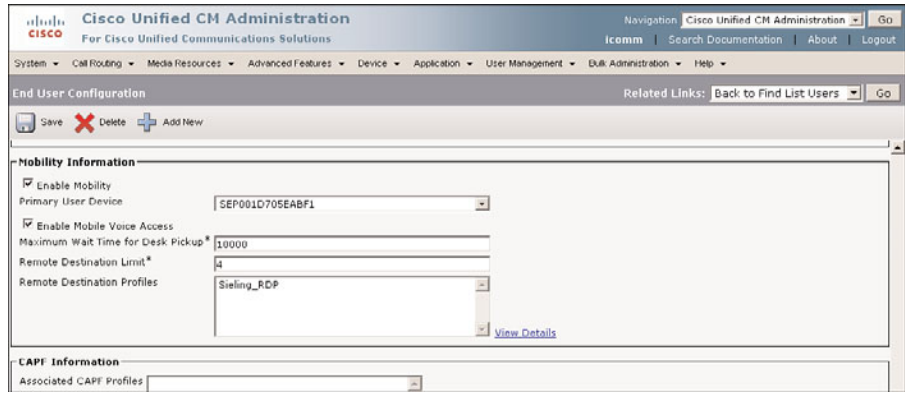
On the Cisco Unified CM Administration page, navigate to **User Management > End User**. Click **Find** if no users are listed.

1. Select the user that you created in Chapter 9 using your name.
2. Scroll down to the **Mobility Information** section. The **Enable Mobility** check box should be selected because you did that in the previous lab. To enable MVA, you must select the **Enable Mobile Voice Access** check box. See Figure 12-13 for an example of this page.
3. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 12-13 Enable MVA for a User



There are three more parameters listed under the Enable Mobile Voice Access check box. This leads some people to think they apply to MVA. In actuality, they do not apply specifically to MVA, but rather to mobility as a whole. You can leave this as a default, but because they do affect the Mobility feature, they are briefly described in the following list:

- **Maximum Wait Time for Desk Pickup:** Determines how long the desk phone will ring when a call is transferred from the cell phone. This is set in milliseconds.
- **Remote Destination Limit:** Determines the maximum number of phones a user can transfer a call to when using the desk phone.
- **Remote Destination Profiles:** Lists the remote destination profiles associated with this user.

Task 3: Configure MVA

When you enable the Cisco Mobile Voice Access service, an MVA media resource is created. This resource must be configured with a directory number. This is the number that the gateway will forward inbound MVA calls to.

MVA also requires a VXML application be running on an H.323 gateway. The configuration of this is outside the CCNA Voice curriculum, but you will be provided a brief description of this configuration.

Step 3-1: Configure MVA Media Resource

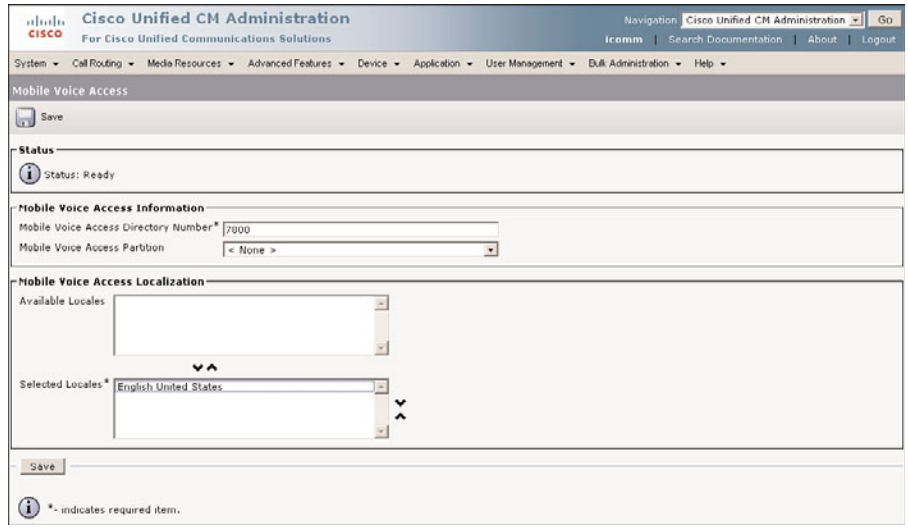
On the Cisco Unified CM Administration page, navigate to **Media Resources > Mobile Voice Access**.

1. The Mobile Voice Access Directory Number field defines the internal number that the VXML application forwards the call to. In this lab, enter **7800** in the **Mobile Voice Access Directory Number** field.
2. The **Mobile Voice Access Partition** field is simply the partition that the Mobile Voice Access directory number is part of. For this lab, we will not be assigning a partition.
3. The **Mobile Voice Access Localization** section allows you to configure which locales (languages) are associated with MVA. Select the **English United States** in the **Available Locales** box and click the down arrow to move the item to the **Selected Locales** box. See Figure 12-14 for an example of this page.
4. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 12-14 MVA Media Resource Configuration



Step 3-2: Examine IOS Gateway Configuration

As stated previously, the gateway configuration portion of the MVA is not a CCNA Voice–level topic. This step is provided so that you can see what is typically configured on a properly provisioned H.323 gateway hosting the VXML application.

The VMXL application is used to authenticate MVA callers. When an outside caller dials the MVA phone number, the call is connected to the VXML application and credentials are checked. The configuration in the H.323 gateway allows the gateway to identify incoming calls as being MVA calls. It also defines where the gateway should send these calls after the destination number has been entered.

Table 12-1 lists the commands found in the H.323 gateway along with a description.

Table 12-1 H.323 Gateway Configuration Command

Commands	Description

`Application`
`service mva http:// <CUCM Server IP address>/`
`ccmivr/pages/IVRMainpage.xml`
	Defines where the MVA application is located

`dial-peer voice 7800 pots`
`service mva`
`incoming called-number 5105557800`
`direct-inward-dial`
	Associates the MVA service with inbounds calls to 510-555-7800

`dial-peer voice 7800 voip`
`destination-pattern 5105557800`
`session target ipv4:<CUCM Server IP address>`
`dtmf-relay h245-alphanumeric`
`codec g711ulaw`
`no vad`
	Routes MVA calls to the CUCM

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

After the steps in this lab are completed and the H.323 gateway is properly configured, MVA is provisioned and should be ready for use. However, because the H.323 gateway configuration is not part of the CCNA Voice curriculum, it is not configured in the lab environment. Therefore, no further validation of this feature is possible.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

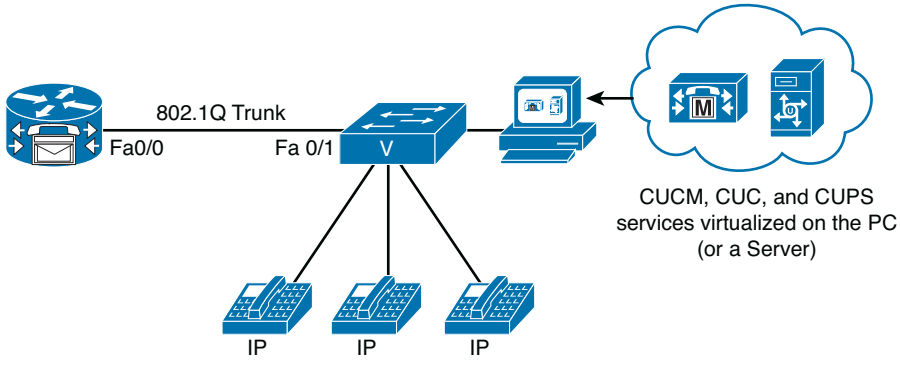
CHAPTER 13

Cisco Unity Connection

This chapter explores adding Cisco Unity Connection (CUC) to the Cisco Unified Communications Manager (CUCM) system. These labs will introduce integrating both CUC and CUCM to allow voice mail messages, configuring user templates, and configuring user voice mail accounts. CUC supports more advanced integration with email systems, such as Microsoft Exchange, to unify voice mail, email, and faxes into one place, but that will not be covered in these labs.

Lab 13-1: Integrating CUC with CUCM

Figure 13-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- Cisco Unity Connection (CUC) Server or PC with VMware Workstation installed and a VM of CUC
- Three or more IP Phones registered (desk phone or soft phone on PC or Windows VM)
- Lab configuration from Lab 10-4 or later

Learning Objectives

Upon completion of this lab, you will be able to

- Configure voice mail ports on the CUCM system
- Configure line groups on the CUCM system
- Configure hunt list and hunt pilot on the CUCM system
- Configure voice mail pilot on the CUCM system

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- Configure voice mail profile on the CUCM system
- Configure SIP trunk for voice mail on the CUCM system
- Configure phone system in CUC
- Configure ports and port groups in CUC
- Configure phones to forward messages to CUC

Scenario

Shiny Objects Inc. (SOI) is finally getting the phone system it wants, and it works beautifully during work hours. After hours and on weekends, however, the phones just ring and ring. While you could set up Mobile Connect for every employee, as shown in Lab 12-1, and try to get employees to answer their phones 24 hours a day, seven days a week, that would use a lot of licenses, and it would break numerous labor laws for hourly employees.

The solution is to set up a voice mail system. The CUCM system needs to be configured to send calls to CUC. There are two ways to connect CUCM to CUC: SCCP ports or SIP trunks. This lab will explore both options.

Task 1: Create SCCP Ports for CUCM Connections to CUC

This task adds Skinny Client Control Protocol (SCCP) integration between CUCM and CUC. The CUCM system uses ports (essentially virtual phone extensions) to send the calls to CUC. The number of ports determines the number of simultaneous connections allowed. This includes not only people leaving messages, but also users retrieving messages, as well as the CUC system calling CUCM to signal it to turn on (or off) the message-waiting light on phones, indicating that a message has been left for the user. Because there can be multiple ports, CUCM organizes them much like the call-routing process: into multiple stages for maximum flexibility in configuration. The phones have a **Voice Mail** button on them, and CUCM needs to know what to do when that button is pressed. The voice mail profile tells the system the voice mail pilot number to dial for voice mail by default. Because there might be multiple voice mail ports, CUCM uses the same Hunt Pilot > Hunt List > Line Group construction discussed in Lab 10-4 to send calls to the voice mail ports. See Figure 13-2 to see the call flow. Conveniently, CUCM includes a wizard to configure the voice mail ports and line group all at once.

Step 1-1: Add Voice Mail Ports Using the Wizard

On the Cisco Unified CM Administration page, navigate to **Advanced Features > Voice Mail > Cisco Voice Mail Port Wizard**.

1. In the wizard (on the left side of the page), choose **Add a new voice mail server**.
2. Leave the default of **CiscoUM1** for the Add Ports to a New Cisco Voice Mail Server Using This Name field. (This name is important later when you configure CUC.) See Figure 13-3 for an example of this page.
3. Click the **Next** button (at the bottom of the page).

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-2 SCCP Voice Mail Integration Components in CUCM

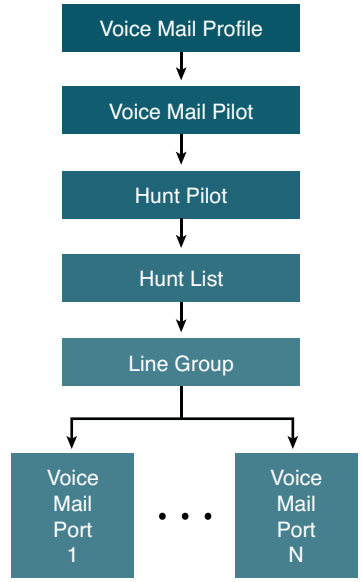
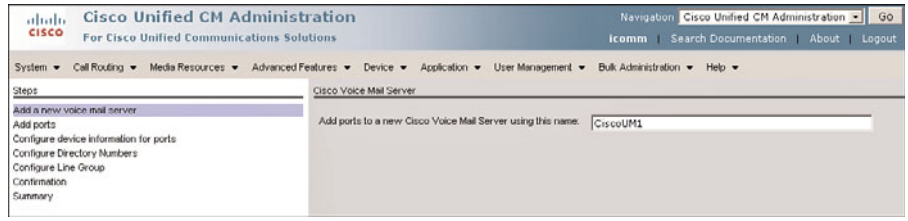


Figure 13-3 Voice Mail Port Wizard—Add Cisco Voice Mail Server



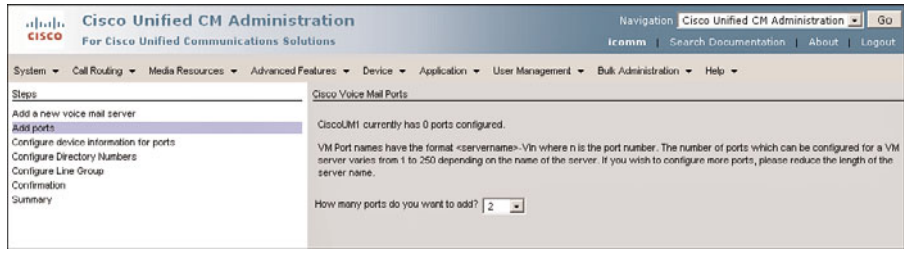
Step 1-2: Add Ports Using the Wizard

Follow these items to add ports using the wizard:

1. In the wizard, choose **Add ports**. Select **2** from the How Many Ports Do You Want to Add drop-down list. See Figure 13-4 for an example of this page.

Note: The number of ports that CUC accepts is controlled by licenses and hardware capacity. If you are using the demo copy of CUC without licenses, it only supports two ports. You will only use one of the two configured here, because the other port will be used by the Session Initiation Protocol (SIP) trunk, but it is useful to see the wizard create more than one port.

Figure 13-4 Voice Mail Port Wizard—Add Ports



2. Click the **Next** button.

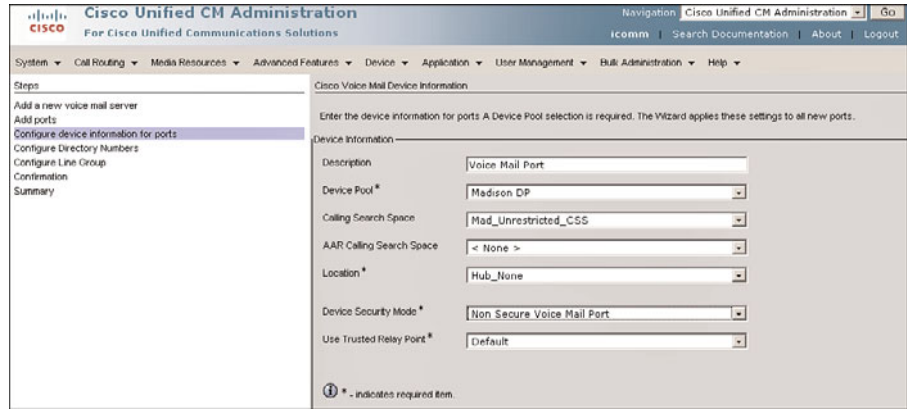
https://t.me/learningnets
From the Library of Aliwarman Tarihoran

Step 1-3: Configure Device Information Using the Wizard

Follow these items to configure device information:

1. Enter **Voice Mail Port** in the Description field.
2. Select **Madison DP** from the Device Pool drop-down list.
3. Select **Mad_Unrestricted_CSS** from the Calling Search Space drop-down list. CUC uses this CSS to send calls to user phones, so it should have access to all partitions.
4. Select **Hub_None** from the Location drop-down list.
5. Select **Non Secure Voice Mail Port** from the Device Security Mode drop-down list. See Figure 13-5 for an example of this page.

Figure 13-5 Voice Mail Port Wizard—Device Information for Ports



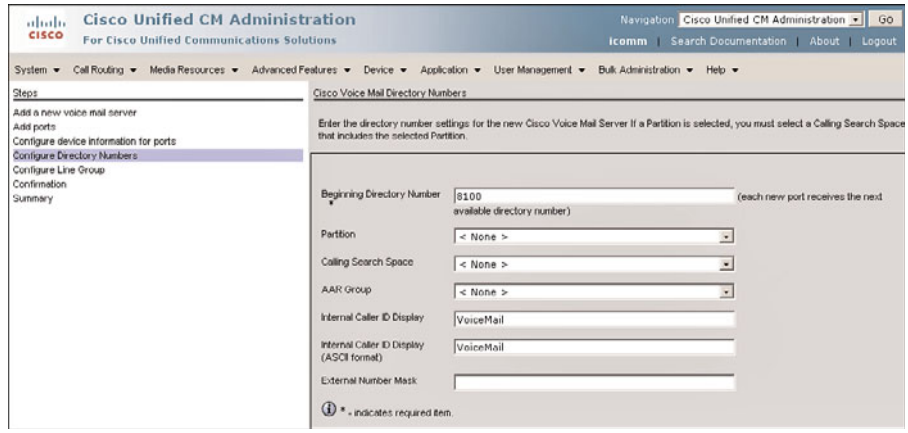
6. Click the **Next** button.

Step 1-4: Configure Directory Numbers Using the Wizard

Follow these items to configure directory numbers:

1. Enter **8100** in the Beginning Directory Number field. See Figure 13-6 for an example of this page.

Figure 13-6 Voice Mail Port Wizard—Configure Directory Numbers



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Note: The number 8100 will be assigned to the first voice mail port, and 8101 for the second port. Users are not expected to dial these numbers. They will call the pilot number, which will be defined later.

The Partition and Calling Search Space fields listed here are only used if you created separate partitions and CSSs to keep people from dialing the voice ports directly. This is not covered in this lab, so leave them set to **< None >**.

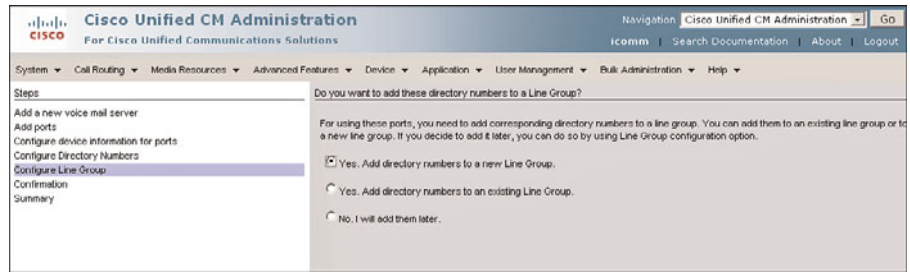
2. Click the **Next** button.

Step 1-5: Configure Line Group Using the Wizard

Follow these items to configure a line group:

1. Click the **Yes. Add directory numbers to a new Line Group** radio button. See Figure 13-7 for an example of this page.

Figure 13-7 Voice Mail Port Wizard—Configure Line Group



2. Click the **Next** button.
3. Leave the Line Group Name field set to **CiscoUM1**.
4. Click the **Next** button.

Step 1-6: Wizard Confirmation

Follow these items to confirm the wizard settings:

1. Double-check all settings. See Figure 13-8 for an example of this page.
2. Scroll down to click the **Finish** button.

Step 1-7: Wizard Summary

The wizard will show the summary page, with the details of creating the two voice ports at 8100 an 8101. See Figure 13-9 for an example of this page.

Notice that the ports are created with the name CiscoUM1-VI*x*, where *x* is the port number. The name used by CUCM will be entered in CUC to link them together. Because the wizard created all the voice ports and the line group, it tells you that the next step is to create the hunt list and then the hunt pilot.

Click the **Hunt List** hyperlink in the **(1) Add this Line Group to a new or existing Hunt List** line in the wizard.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-8 Voice Mail Port Wizard—Confirmation

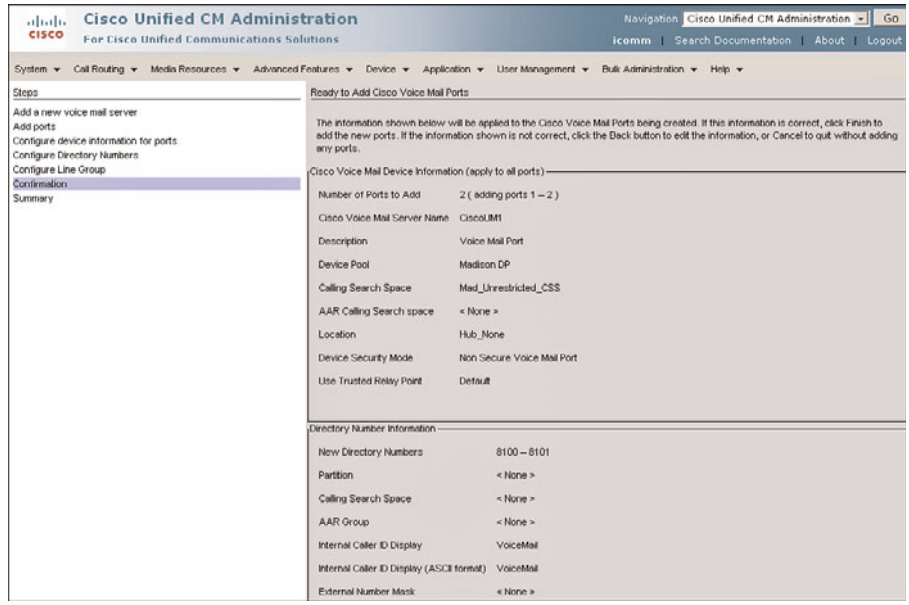
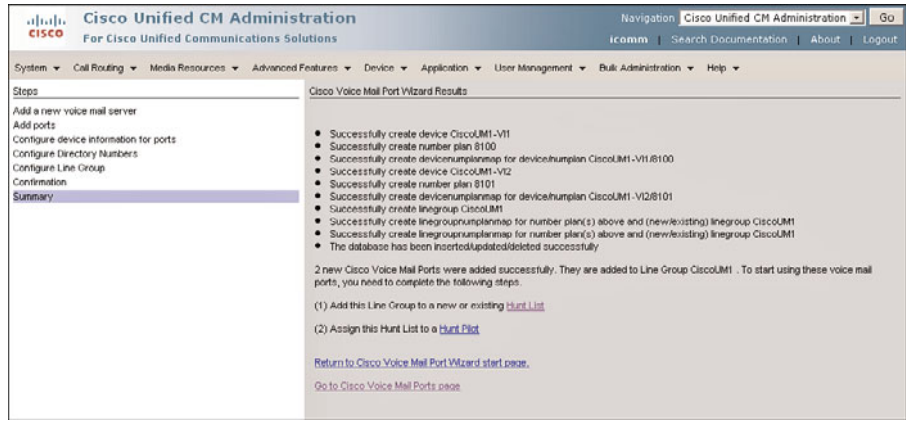


Figure 13-9 Voice Mail Port Wizard—Summary



Step 1-8: Create Hunt List

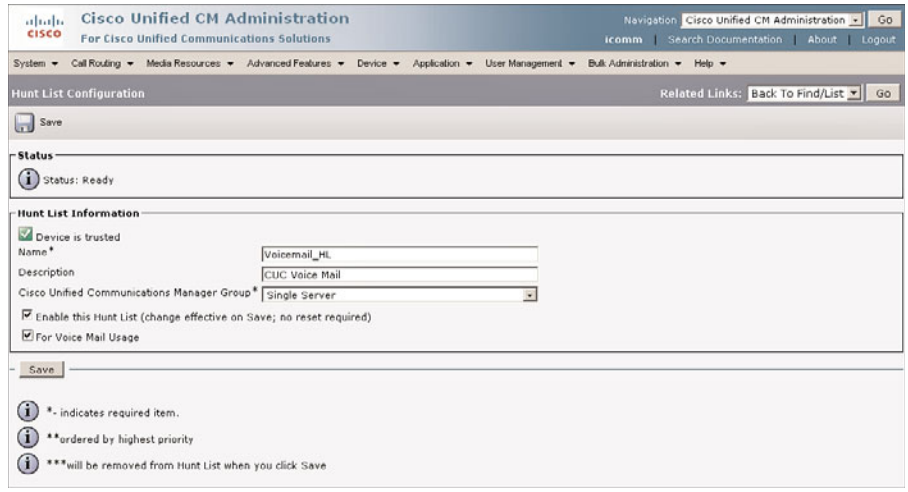
If the wizard did not direct you to the hunt list, on the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Hunt List**.

1. Click the **Add New** button.
2. Enter **Voicemail_HL** in the Name field.
3. Enter **CUC Voice Mail** in the Description field.
4. Select **Single Server** from the Cisco Unified Communications Manager Group drop-down list.
5. Select the **Enable this Hunt List** check box.
6. Select the **For Voice Mail Usage** check box. See Figure 13-10 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-10 Voice Mail Hunt List



7. Click the **Save** button. The page updates to show the Hunt List Member Information section.
8. Click the **Add Line Group** button. The Hunt List Detail Configuration page opens.
9. Select **CiscoUM1** from the Line Group drop-down list.
10. Click **Save** to return to Hunt List page.
11. On the Hunt List page, click the **Save** button. Click **OK** to close the pop-up window.
12. Click the **Reset** button to apply the changes.
13. The Device Reset pop-up window opens. Click the **Reset** button. Click the **Close** button to exit the pop-up window.

Step 1-9: Create Hunt Pilot

On the Cisco Unified CM Administration page, navigate to **Call Routing** > **Route/Hunt** > **Hunt Pilot**.

1. Click the **Add New** button.
2. Enter **8000** in the Hunt Pilot field. This is the number that users will call to access voice mail.

Note: The Route Partition field listed here is only used if you created separate partitions and CSSs to keep people from dialing the voice ports directly. This is not covered in this lab, so leave it set to **< None >**.

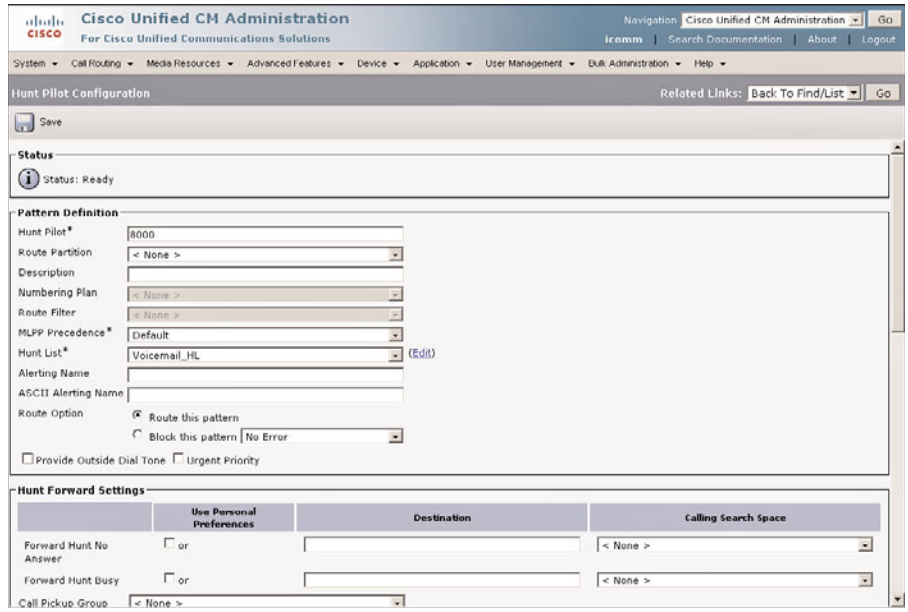
---

3. Select **Voicemail_HL** from the Hunt List drop-down list.
4. Deselect the **Provide Outside Dial Tone** check box. See Figure 13-11 for an example of this page.
5. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-11 Voice Mail Hunt Pilot

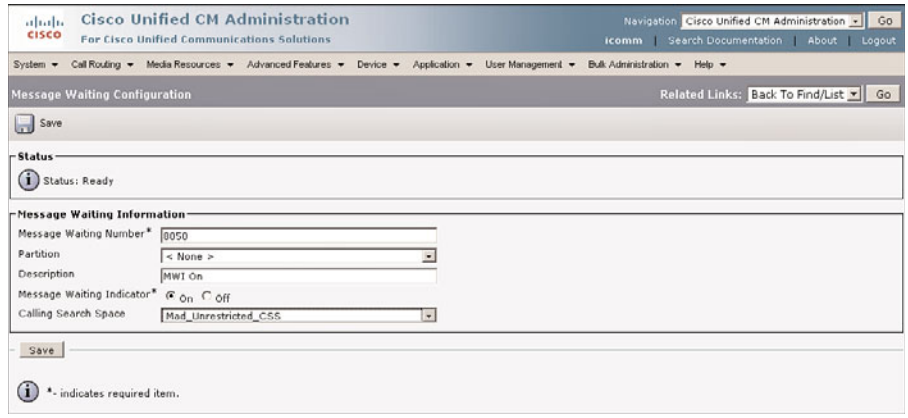


Step 1-10: Create Message Waiting Indicator On

Before you finish the call flow by creating the voice mail pilot and the voice mail profile, take a detour and configure the Message Waiting Indicators (MWI). The MWI-On is how the CUC calls the CUCM system to signal CUCM to turn on the New Message indicator on a phone. On the Cisco Unified CM Administration page, navigate to **Advanced Features > Voice Mail > Message Waiting**.

1. Click the **Add New** button.
2. Enter **8050** in the Message Waiting Number field.
3. Enter **MWI On** in the Description field.
4. Select the **On** radio button for the Message Waiting Indicator.
5. Select **Mad_Unrestricted_CSS** from the Calling Search Space drop-down list. CUC uses this CSS to send calls to user phones, so it should have access to all partitions. See Figure 13-12 for an example of this page.

Figure 13-12 Message Waiting Configuration



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

6. Click the **Save** button.

Step 1-11: Create Message Waiting Indicator Off

Follow these items to turn the MWI off:

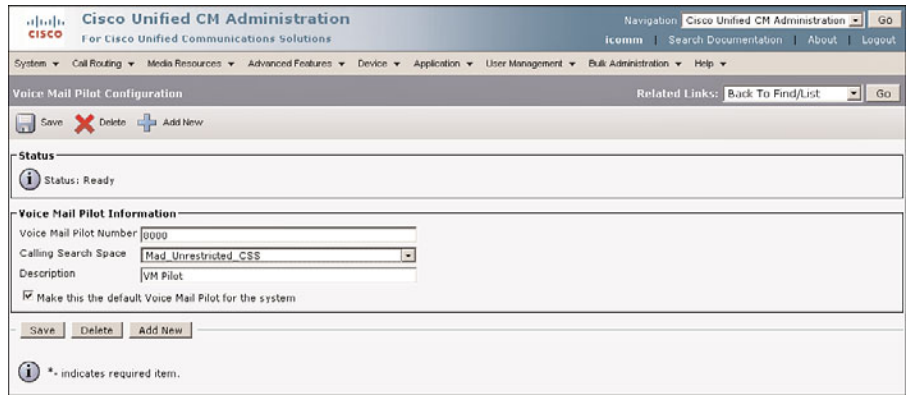
1. Click the **Copy** button.
2. Change the Message Waiting Number field to **8051**.
3. Change the Description field to **MWI Off**.
4. Select the **Off** radio button for the Message Waiting Indicator.
5. Click the **Save** button.

Step 1-12: Create Voice Mail Pilot

With the MWIs created, it is time to finish the last two components for the SCCP voice mail. On the Cisco Unified CM Administration page, navigate to **Advanced Features > Voice Mail > Voice Mail Pilot**.

1. Click the **Add New** button.
2. Enter **8000** in the Voice Mail Pilot Number field. This number is the same as used for the hunt pilot, as this is basically handing off all voice mail calls to the hunt pilot.
3. Select **Mad_Unrestricted_CSS** from the Calling Search Space drop-down list.
4. Enter **VM Pilot** in the Description field.
5. Select the **Make this the default Voice Mail Pilot for the system** check box. A pop-up message will warn you about the default pilot; click **OK**. See Figure 13-13 for an example of this page.

Figure 13-13 Voice Mail Pilot Configuration



6. Click the **Save** button.

https://t.me/learningnets

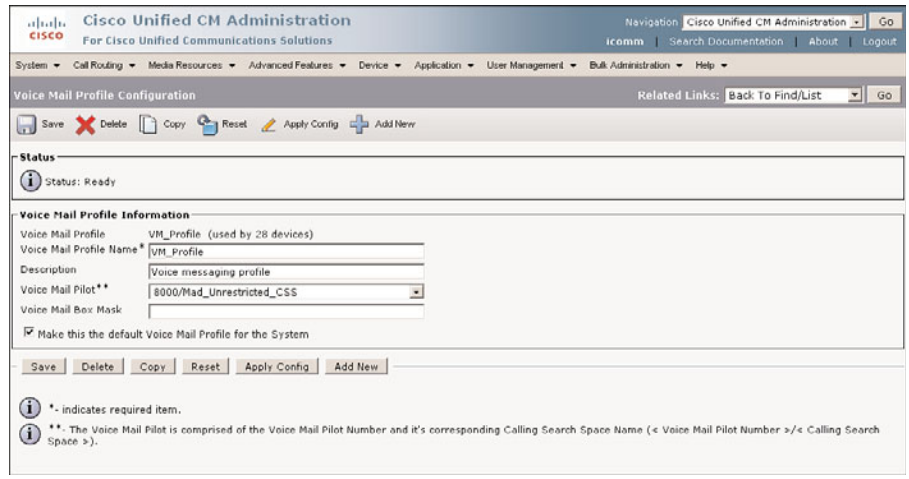
From the Library of Aliwarman Tarihoran

Step 1-13: Create Voice Mail Profile

On the Cisco Unified CM Administration page, navigate to **Advanced Features** > **Voice Mail** > **Voice Mail Profile**. Click **Find** if no profiles are listed.

1. Click the **Default** profile.
2. Enter **VM_Profile** in the Voice Mail Profile Name field.
3. Change the Description field to **Voice messaging profile**.
4. Select **8000/Mad_Unrestricted_CSS** from the Voice Mail Pilot drop-down list.
5. Select the **Make this the default Voice Mail Profile for the System** check box. See Figure 13-14 for an example of this page.

Figure 13-14 Voice Mail Profile Configuration



6. Click the **Save** button.

Task 2: Configure CUC for SCCP Connection to CUCM

Now that the CUCM call flow to CUC is configured, it is time to configure CUC to accept the calls. While CUCM is mostly configured from pull-down menus along the top of the page, CUC uses a navigation pane on the left, with a tree structure to navigate between pages in CUC. For the CUC to connect to the SCCP ports on the CUCM system, there are three elements that need to be configured: the phone system, the port group, and the ports.

Step 2-1: Configure Phone System

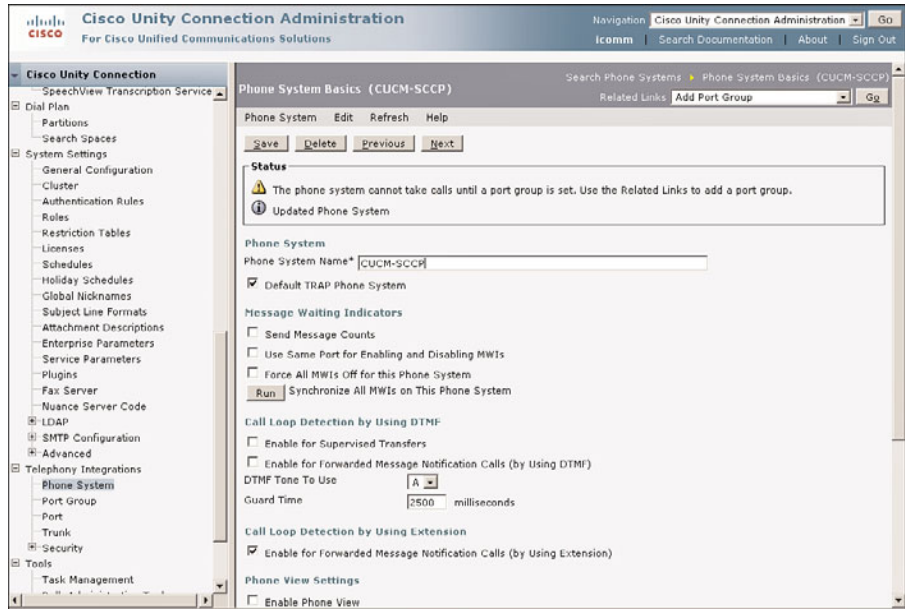
Connect to the CUC web page at IP address **10.*x*0.0.8** (where *x* is your pod number). Log in with your application username (icomm) and accept any security certificate warnings. On the Cisco Unity Connection Administration page, navigate down to **Telephony Integrations** > **Phone System**.

1. Click the hyperlinked **PhoneSystem** name.
2. Change the **Phone System Name** field to **CUCM-SCCP**. See Figure 13-15 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-15 CUC Phone System Basics



3. Click the **Save** button.
4. The status box shows that the system will not take calls until a port group is set. With the Related Links drop-down list set to **Add Port Group**, click the **Go** button. The New Port Group page opens.

Step 2-2: Configure Port Group

On the New Port Group page:

1. Leave the Display Name field set to **CUCM-SCCP-1**.
2. Enter **CiscoUM1-VI** in the Device Name Prefix field. (Note: This is case sensitive, and it stands for **Cisco U**nified **M**essaging **1**–**V**irtual **I**nterface.) It is the CUCM Server name, as configured in Step 1-1, with a –VI suffix added to the end.

Note: The Device Name Prefix field can be anything, but it must be exactly the same (including case) when entered into the CUC server.

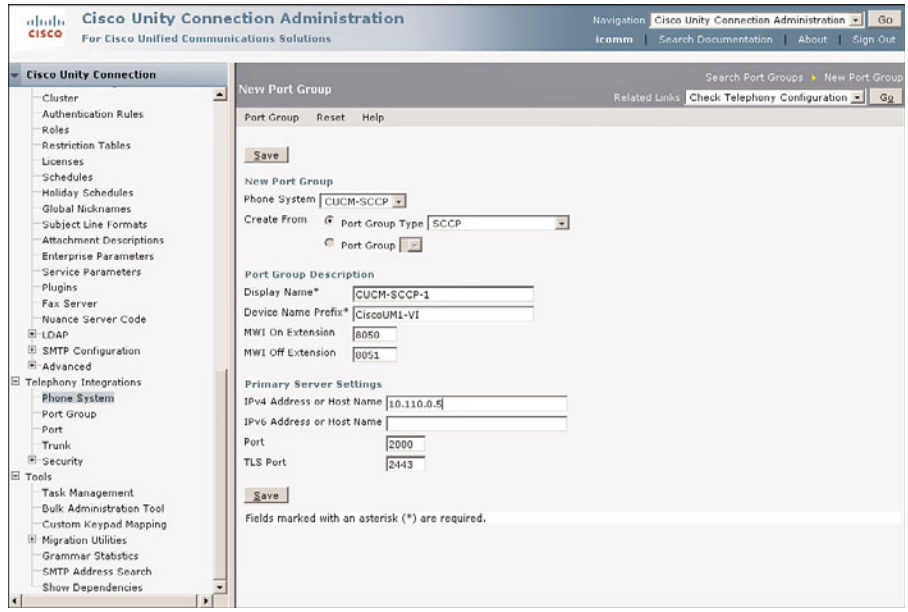
---

3. Enter **8050** for the MWI On Extension field.
4. Enter **8051** for the MWI Off Extension field.
5. Enter the IP address of your CUCM server (10.*x*0.0.5) in the IPv4 Address or Host Name field. See Figure 13-16 for an example of this page.
6. Click the **Save** button.
7. The status will show that the system cannot take calls without ports. With the Related Links drop-down list set to **Add Ports**, click the **Go** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-16 CUC New Port Group



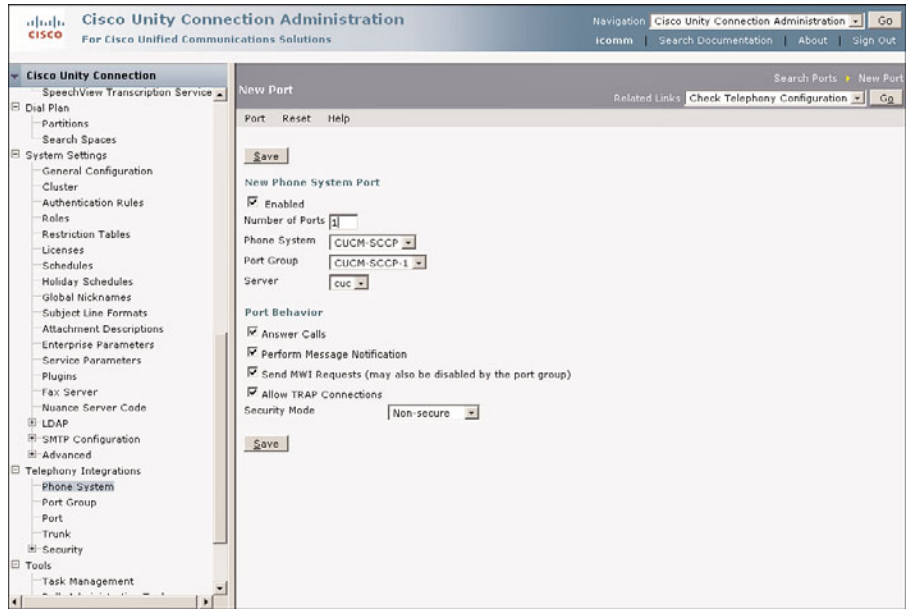
Step 2-3: Configure SCCP Port

Note: This lab assumes that you are using the CUC in demo mode, which only allows two ports. One port will be saved for the SIP trunk from CUCM, so only configure one port here.

The New Port page opens. Follow these items to configure the SCCP port:

1. Leave the Number of Ports field set to **1**. See Figure 13-17 for an example of this page.

Figure 13-17 CUC New Port

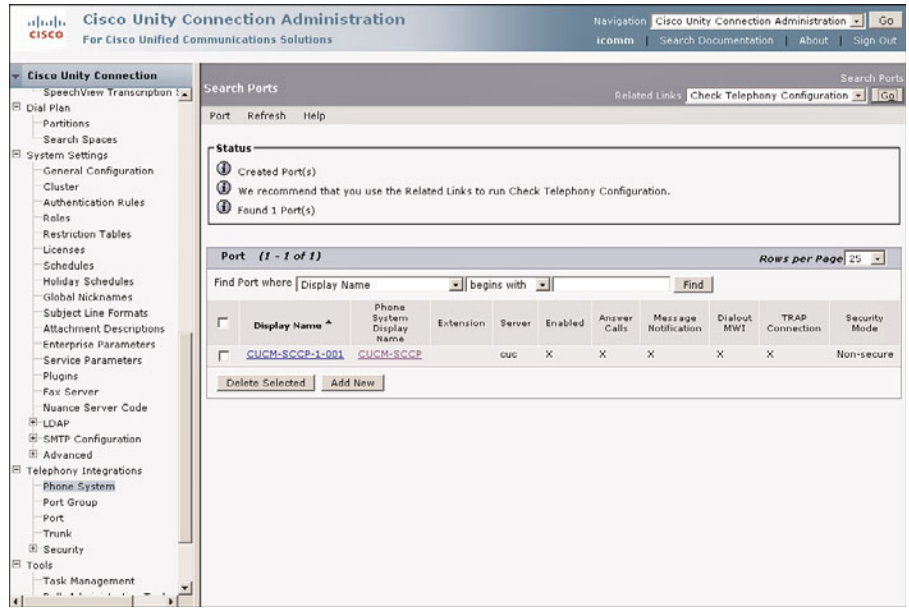


https://t.me/learningnets

From the Library of Aliwarman Tarihoran

2. Click the **Save** button. The page will change to the Search Ports page, which shows the status of the port just created. See Figure 13-18 for an example of this page.

Figure 13-18 CUC Search Ports



3. With the Related Links drop-down list set to **Check Telephony Configuration**, click the **Go** button.

4. The Task Execution Results pop-up window should show **No Problems Detected**. Click the **Close** button.

Step 2-4: Test the CUCM-to-CUC Connection

Because the voice mail profile was already created, if you press the **Messages** button (it looks like an envelope) on a phone, it should automatically connect to the CUC main operator prompt. You should hear a female voice say something like this: "Hello! Cisco Unity Connection Messaging System. From a touch-tone phone . . ." Hang up before the message gets to the end. Normally, the **Messages** button would connect you to your voice mailbox, but those have not been configured yet.

If you did not hear the message, check to see whether the phone display shows a connection to extension 8000. Start by checking all the steps in Tasks 1 and 2 to troubleshoot.

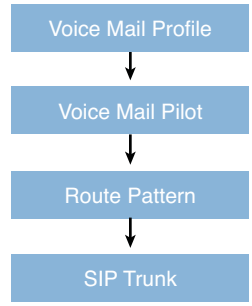
Task 3: Create SIP Trunk for CUCM Connections to CUC

This task will explore adding SIP protocol integration between CUCM and CUC. The CUCM system uses SIP trunks to send the calls to CUC. The call flow for SIP is easier to configure. Because there is already a default voice mail profile and voice mail pilot, you will configure nondefault versions to assign to a specific directory number for testing. The voice mail pilot will call a special route pattern that connects to the SIP trunk. See Figure 13-19 to see the call flow.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-19 SIP Voice Mail Integration Components in CUCM

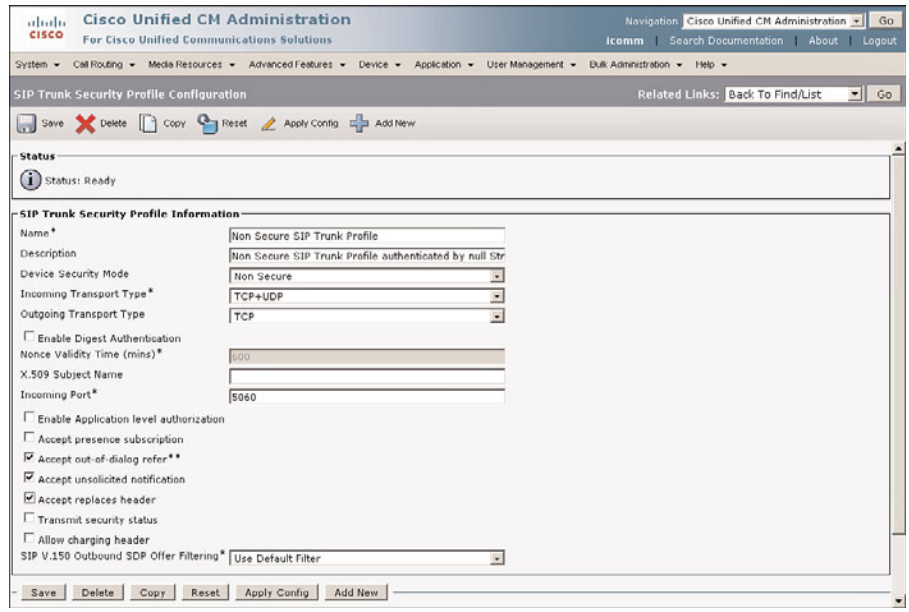


Step 3-1: Configure SIP Trunk Security Profile

On the Cisco Unified CM Administration page, navigate to **System > Security > SIP Trunk Security Profile**. Click **Find** if no profiles are listed.

1. Click the default **Non Secure SIP Trunk Profile**.
2. Select the **Accept out-of-dialog refer** check box.
3. Select the **Accept unsolicited notification** check box.
4. Select the **Accept replaces header** check box. See Figure 13-20 for an example of this page.

Figure 13-20 SIP Trunk Security Profile Configuration



5. Click the **Save** button. There are no trunks at this point, so you can ignore the status message to reset trunks.

https://t.me/learningnets

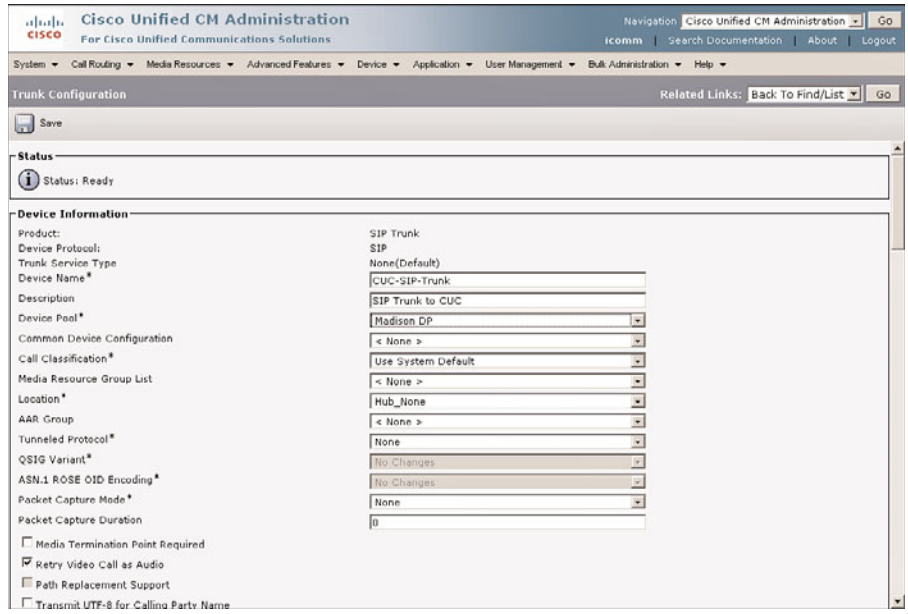
From the Library of Aliwarman Tarihoran

Step 3-2: Configure SIP Trunk

On the Cisco Unified CM Administration page, navigate to **Device** > **Trunk**.

1. Click the **Add New** button.
2. Select **SIP Trunk** from the Trunk Type drop-down list.
3. Click the **Next** button. The Trunk Configuration page opens.
4. Enter **CUC-SIP-Trunk** in the Device Name field.
5. Enter **SIP Trunk to CUC** in the Description field.
6. Select **Madison DP** from the Device Pool drop-down list. See Figure 13-21 for an example of this page.

Figure 13-21 SIP Trunk Configuration Part 1



7. Scroll down to the Inbound Calls section, and select **Mad_Restricted_CSS** from the Calling Search Space drop-down list.
8. Select the **Redirecting Diversion Header Delivery – Inbound** check box. See Figure 13-22 for an example of this page.
9. In the Outbound Calls section, select the **Redirecting Diversion Header Delivery – Outbound** check box.
10. In the SIP Information section, enter the IP address of the CUC server (10.*x*0.0.8) in the Destination Address field.
11. Select **Non Secure SIP Trunk Profile** from the SIP Trunk Security Profile drop-down list.
12. Select **Standard SIP Profile** from the SIP Profile drop-down list. See Figure 13-23 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-22 SIP Trunk Configuration Part 2

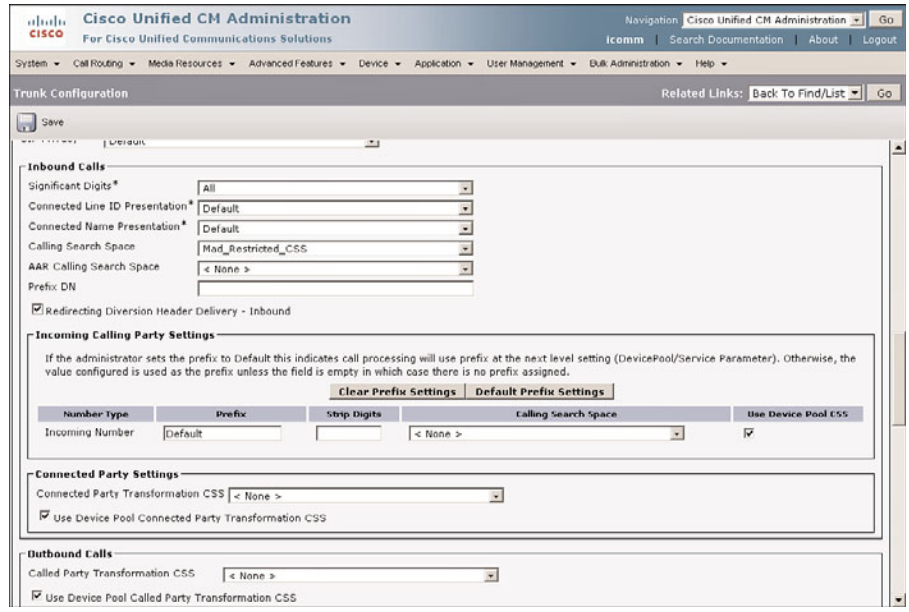
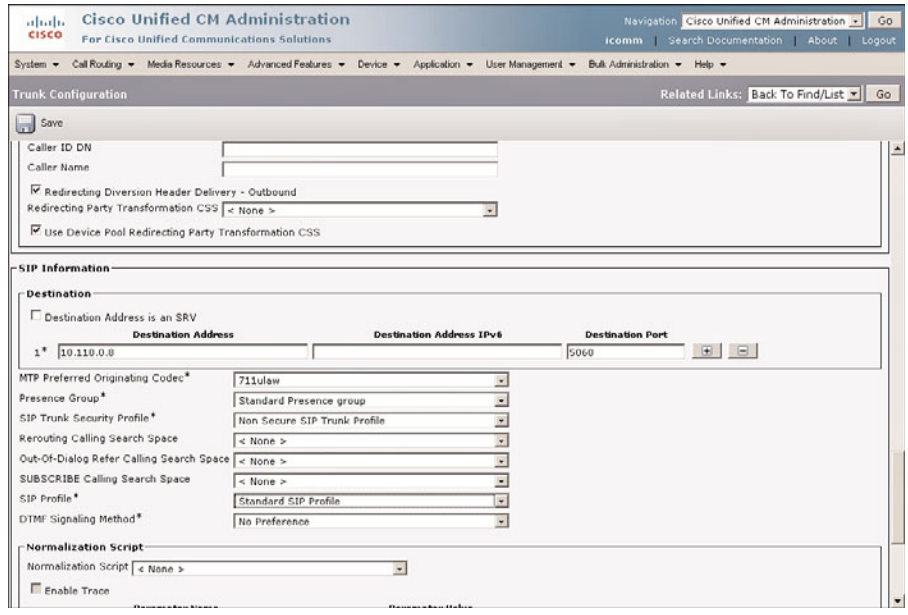


Figure 13-23 SIP Trunk Configuration Part 3



13. Click the **Save** button. The trunk was just created, so you can ignore the status message to reset the trunk.

Step 3-3: Configure Route Pattern

On the Cisco Unified CM Administration page, navigate to **Call Routing > Route/Hunt > Route Pattern**.

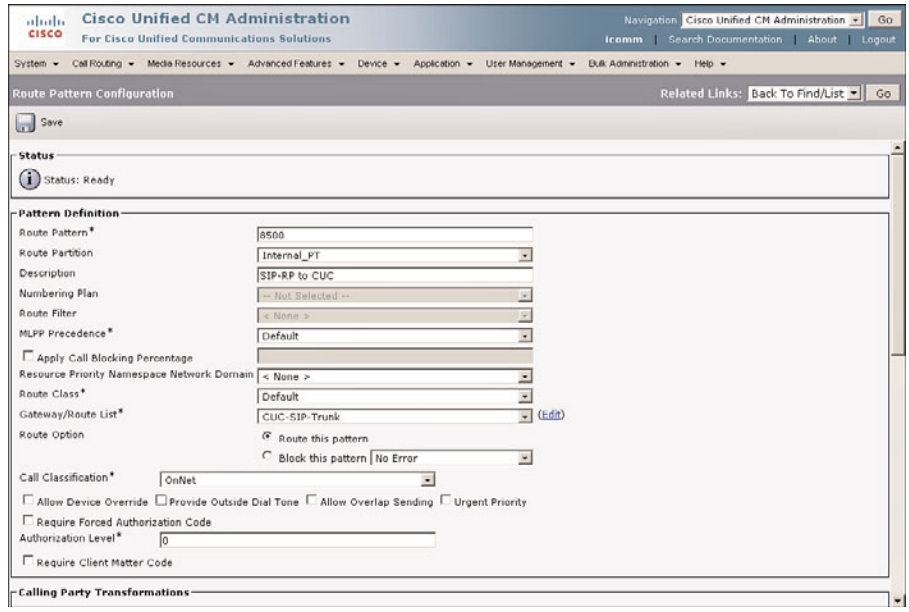
1. Click the **Add New** button.
2. Enter **8500** in the Route Pattern field.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. Select **Internal_PT** from the Route Partition drop-down list.
4. Enter **SIP-RP to CUC** in the Description field.
5. Select **CUC-SIP-Trunk** from the Gateway/Route List drop-down list.
6. Deselect the **Provide Outside Dial Tone** check box. (This action will automatically change the Call Classification field to **OnNet**. Leave it set to OnNet.) See Figure 13-24 for an example of this page.

Figure 13-24 SIP Trunk Route Pattern



7. Click the **Save** button.
8. Click **OK** for both of the pop-up windows.

Step 3-4: Create SIP Voice Mail Pilot

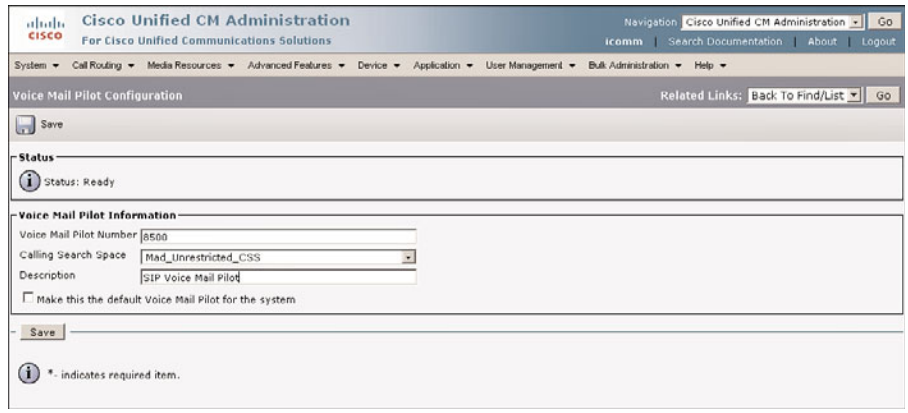
Unlike the SCCP connection, you do not need MWI ports for SIP trunks. However, because you already have a voice mail pilot pointing to the SCCP hunt pilot, create a nondefault voice mail pilot that will be assigned to a SIP voice mail profile, which will be manually assigned to a directory number. On the Cisco Unified CM Administration page, navigate to **Advanced Features > Voice Mail > Voice Mail Pilot**.

1. Click the **Add New** button.
2. Enter **8500** in the Voice Mail Pilot Number field. This number is the same as used in the SIP route pattern that you created in the previous step, as this is basically making a call that will match the route pattern, which will send it to the SIP trunk and on to the CUC server.
3. Select **Mad_Unrestricted_CSS** from the Calling Search Space drop-down list.
4. Enter **SIP Voice Mail Pilot** in the Description field.
5. Deselect the **Make this the default Voice Mail Pilot for the system** check box. If you see a pop-up message warning you about the default pilot, click **OK** and double-check your work. See Figure 13-25 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-25 Voice Mail Pilot Configuration



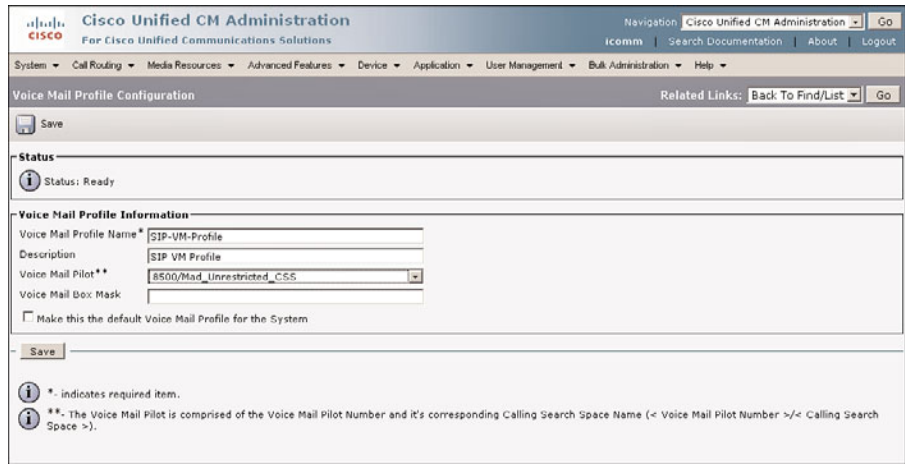
6. Click the **Save** button.

Step 3-5: Create Voice Mail Profile

With the SIP voice mail pilot created, create a SIP voice mail profile, which will be manually assigned to a directory number. On the Cisco Unified CM Administration page, navigate to **Advanced Features > Voice Mail > Voice Mail Profile**. Click **Find** if no profiles are listed.

1. Click the **Add New** button.
2. Enter **SIP-VM-Profile** in the Voice Mail Profile Name field.
3. Enter **SIP VM Profile** in the Description field.
4. Select **8500/Mad_Unrestricted_CSS** from the Voice Mail Pilot drop-down list.
5. Deselect the **Make this the default Voice Mail Profile for the System** check box. If you see a pop-up message that warns you about the default profile, click **OK** and double-check your work. See Figure 13-26 for an example of this page.

Figure 13-26 SIP Voice Mail Profile Configuration



6. Click the **Save** button.

https://t.me/learningnets

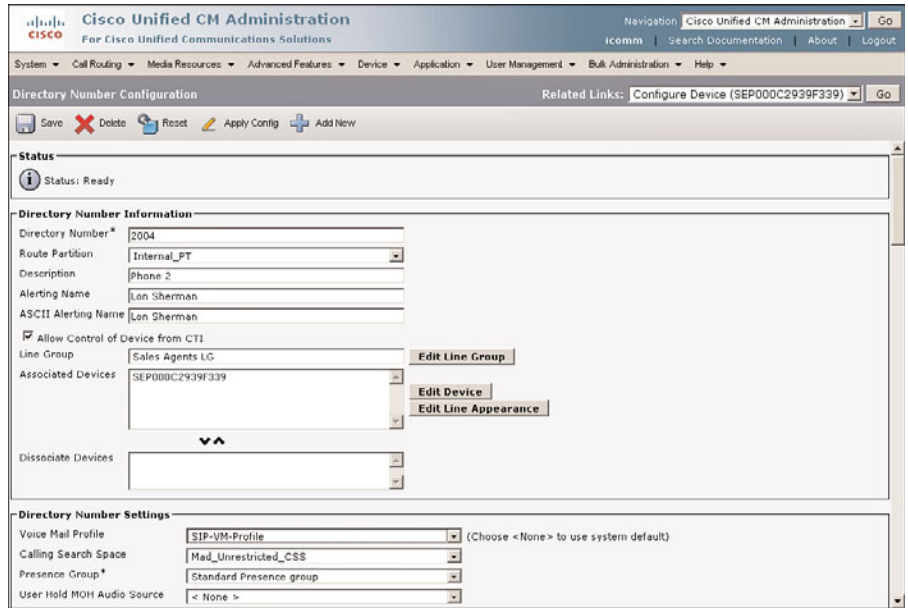
From the Library of Aliwarman Tarihoran

Step 3-6: Assign SIP Voice Mail Profile to a Phone

Because all phones will use the default voice mail profile, which connects to CUC through the SCCP port, you need to configure a directory number to use the SIP voice mail profile. On the Cisco Unified CM Administration page, navigate to **Device > Phone**. Click **Find** if no phones are listed.

1. Click the second HQ phone.
2. In the Association Information section, click the **Line [1]** hyperlink.
3. In the Directory Number Settings section, select **SIP-VM-Profile** from the Voice Mail Profile drop-down list. See Figure 13-27 for an example of this page.

Figure 13-27 SIP Voice Mail Profile on the Directory Number



4. Click the **Save** button.

Task 4: Configure CUC for SIP Connection to CUCM

Now that the SIP CUCM call flow to CUC is configured, it is time to configure CUC to accept the SIP calls. For the CUC to connect to the SIP trunk on the CUCM system, three elements need to be configured: the phone system, the port group, and the ports.

Step 4-1: Configure Phone System

Connect to the CUC web page. On the Cisco Unity Connection Administration page, navigate down to **Telephony Integrations > Phone System**.

1. Click the **Add New** button.
2. Enter **CUCM-SIP** in the Phone System Name field.
3. Click the **Save** button.
4. The status box shows that the system will not take calls until a port group is set. With the Related Links drop-down list set to **Add Port Group**, click the **Go** button.

https://t.me/learningnets

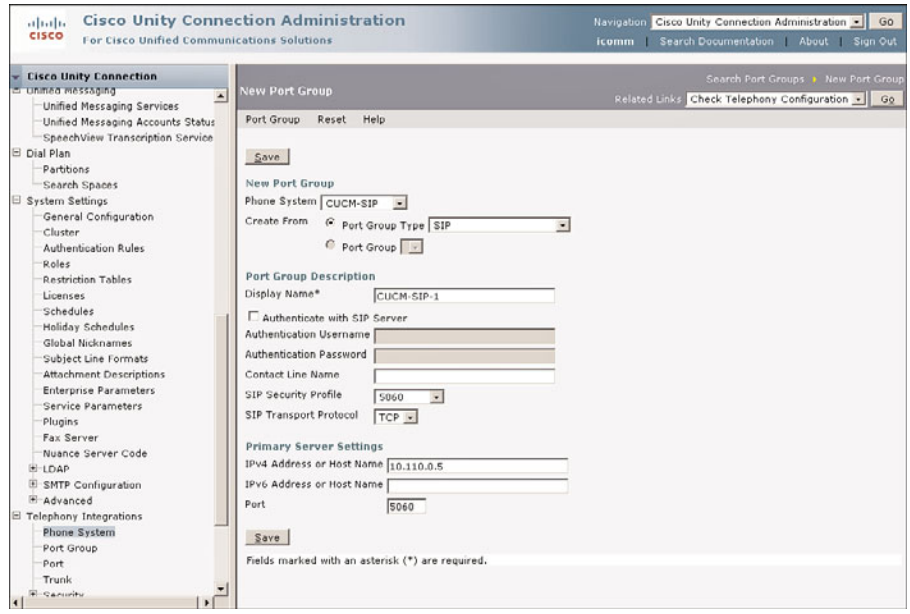
From the Library of Aliwarman Tarihoran

Step 4-2: Configure SIP Port Group

The New Port Group page opens. Follow these items to configure the SIP port group:

1. Leave the Display Name field set to **CUCM-SIP-1**.
2. Select **SIP** from the Port Group Type drop-down list after the **Create From** radio button. The page will update with changed information, because of selecting the SIP type.
3. Enter the IP address of your CUCM server (10.*x*0.0.5) in the IPv4 Address or Host Name field. See Figure 13-28 for an example of this page.

Figure 13-28 CUC SIP New Port Group



4. Click the **Save** button. The status will show that the system cannot take calls without ports.
5. Select the **Register with SIP Server** check box.
6. Click the **Save** button. The status will show that the system cannot take calls without ports and the port group needs to be reset.
7. Under the Port Group section, click the **Reset** button.
8. With the Related Links drop-down list set to **Add Ports**, click the **Go** button.

Step 4-3: Configure SIP Port

Note: This lab assumes that you are using the CUC in demo mode, which only allows two ports. One port was saved for the SIP trunk from CUCM, so only configure one port here.

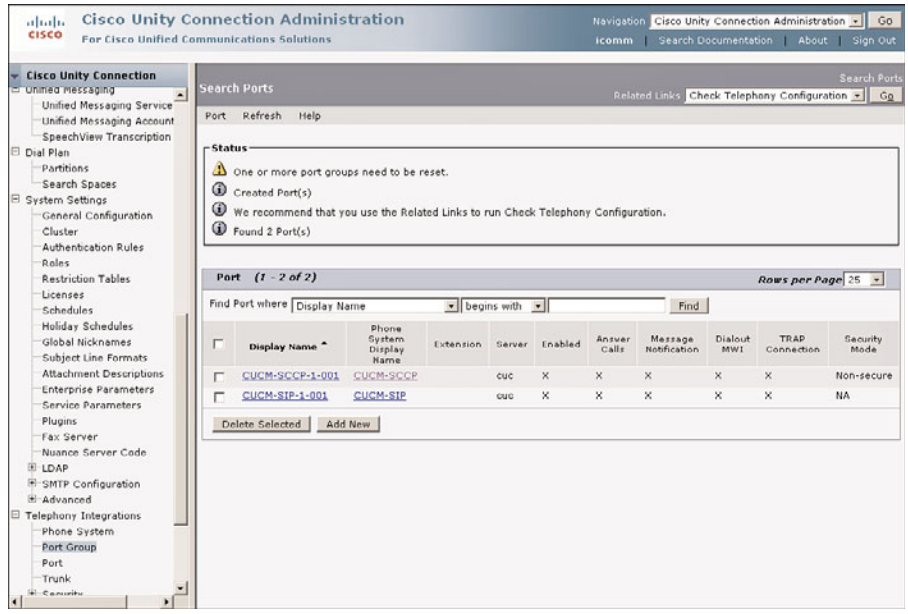
The New Port page opens. Follow these items:

1. Leave the Number of Ports field set at **1**.
2. Click the **Save** button. The page will change to the Search Ports page, which shows the status of both ports. See Figure 13-29 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-29 CUC Search Ports



3. With the Related Links drop-down list set to **Check Telephony Configuration**, click the **Go** button.
4. The Task Execution Results pop-up window should show **No Problems Detected**. Click the **Close** button.

Step 4-4: Test the CUCM-to-CUC Connection

Because the voice mail profile was already created, if you press the **Messages** button on the second HQ phone, it should automatically connect to the CUC main operator prompt. You should hear the same prompt that you heard on the other phones. Hang up before the message gets to the end.

How do you know that the SIP trunk was used? Use the Cisco Unified Real-Time Monitoring Tool (RTMT). This is one of the best methods to examine the functions of the CUC system.

Task 5: Using the Real-Time Monitoring Tool (RTMT) to Examine Voice Mail Call Flow

RTMT is a client application that is downloaded and run on your PC. The details of RTMT will be covered in the troubleshooting chapters, but it is useful to examine the call routing now.

Step 5-1: Download and Install RTMT

The version of RTMT used needs to match the version of the server you are connecting to. To download the software, on the Cisco Unity Connection Administration page, navigate down to **System Settings > Plugins**. Click the **Find** button if no plugins are listed.

Note: In CUCM, the RTMT is found in the **Application > Plugins** menu, along with many other tools useful for CUCM.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Download the correct version of RTMT for your operating system (currently Linux and Windows are supported) and run the installer. When the installer finishes, click the icon to launch RTMT.

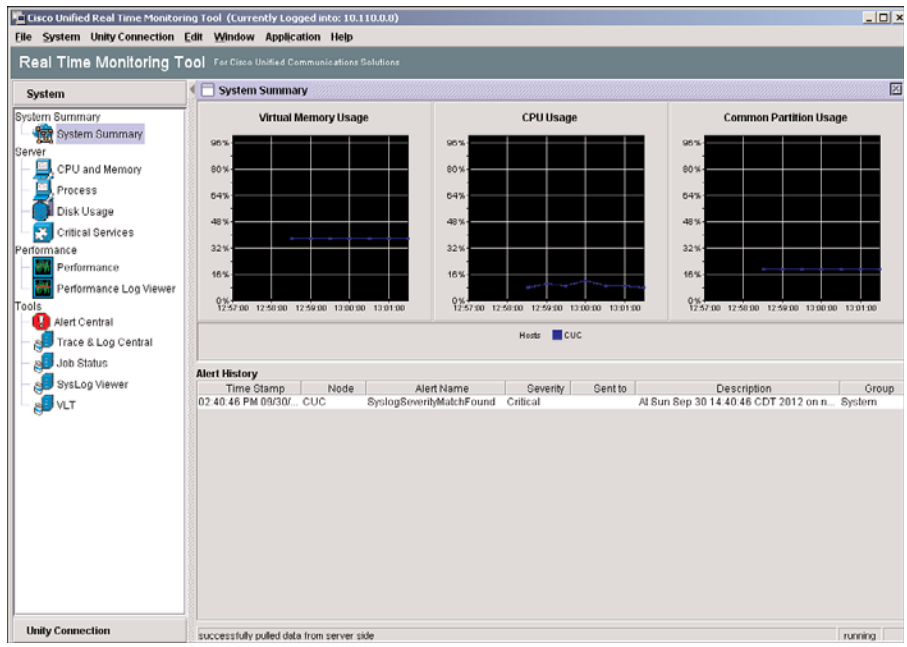
Note: The details of the screens might change with each release of RTMT, so your windows might not look exactly the same as shown in the following figures. The important thing is to use the right version of RTMT for your servers.

Step 5-2: Examine Voice Mail Ports Using RTMT

When RTMT is open, it asks for the IP address of the system to monitor. Follow these items to examine voice mail ports using RTMT:

1. Enter the CUC Server IP address (10.*x*0.0.8). Click the **OK** button.
2. An authentication window will open. Enter your application username (icomm) and password.
3. A pop-up window appears asking you to select a configuration. At this time, only the default exists, so click **OK**.
4. The default configuration opens to the System Summary pane. This pane shows useful information about the server hardware and alerts. See Figure 13-30 for an example of this page.

Figure 13-30 RTMT System Summary



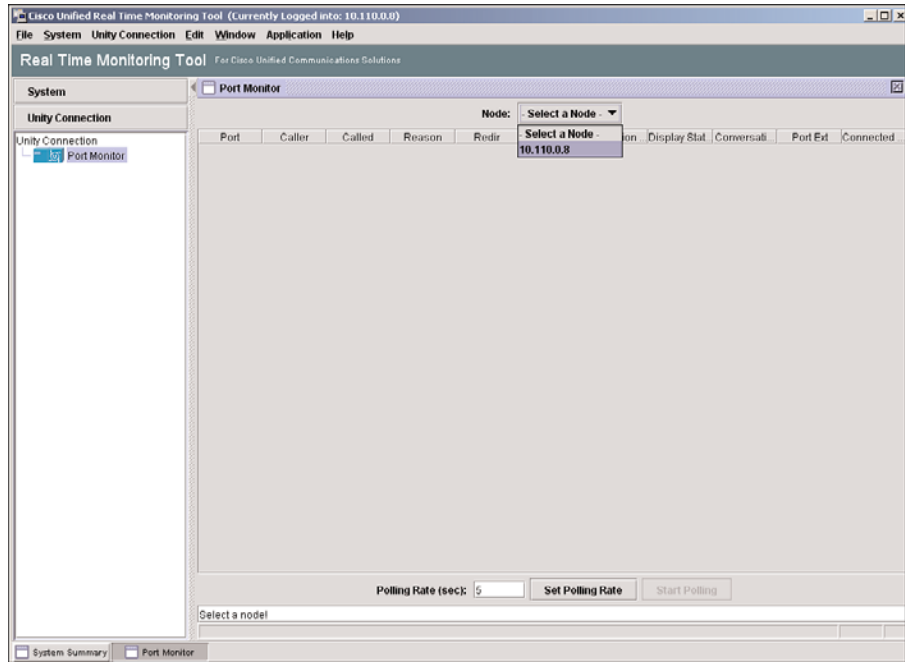
5. Click the **Unity Connection** button in the lower-left corner to see the Port Monitor. (If you do not see Unity Connection, verify that you are connected to your CUC server, and not to your CUCM server.)
6. Under Unity Connection (near the upper left), click the **Port Monitor** item.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

7. From the Node drop-down menu (top center), select the IP address of your CUC Server. See Figure 13-31 for an example of this page.

Figure 13-31 RTMT Port Monitor Node Selection



8. Because you do not need to worry about loading the lab system down, enter **1** in the Polling Rate field and click the **Set Polling Rate** button.

9. Click the **Start Polling** button. The ports will show up in the Port Monitor pane. If you look at the Port column, you see two entries, one for the SCCP port and one for the SIP trunk. If necessary, hover over the port name to see a tooltip with the full port name.

Tip: If you do not have room to open the window to see more details in the columns, click the left-facing triangle next to the Port Monitor title bar to collapse the navigation pane. You can also reduce the size of columns that are not needed at the time. For now, the Redir and Last Redir columns are not used, so they can be reduced by hovering the mouse over the line between the column names and dragging. This method also allows you to expand columns, such as Port and Conversation Status, that are more useful for now.

---

10. Press the **Messages** button on the second HQ phone. The SIP trunk should show the incoming call. The caller information shows the phone calling and the call reason is Direct. The Status columns show that the standard greeting is being played. Hang up before the message gets to the end. See Figure 13-32 for an example of this page.

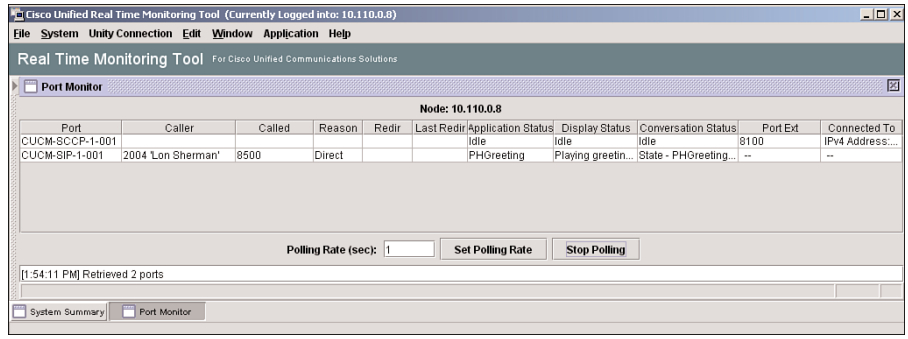
11. If you press the **Messages** button on the first HQ phone, the SCCP port should be used.

12. When done, click the **Stop Polling** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-32 RTMT Port Monitor

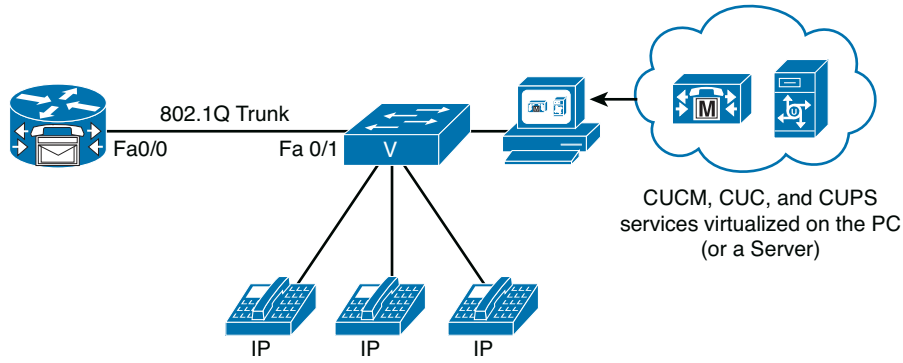


https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 13-2: Configuring Cisco Unity Connection (CUC) Templates and Manually Adding a User

Figure 13-33 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- Cisco Unity Connection (CUC) Server or PC with VMware Workstation installed and a VM of CUC
- Three or more IP Phones registered (desk phone or soft phone on PC or Windows VM)
- Lab configuration from Lab 13-1

Learning Objectives

Upon completion of this lab, you will be able to

- Configure CUC system-wide parameters
- Configure templates for CUC end users
- Configure authentication rules for CUC end users
- Configure user account manually in CUC
- Configure CUCM to forward busy or unanswered calls to CUC

Scenario

SOI is happy that there is a voice mail system, but the only thing it does is allow employees to press the **Messages** button to hear the standard greeting—not that impressive. SOI wants voice mails to be left for employees and to have the employees be able to retrieve the voice mails. Like many other computer systems, if the default parameters are adjusted before adding users to the system, there are fewer problems than trying to implement changes later.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: CUC Authentication Rules and Class of Service

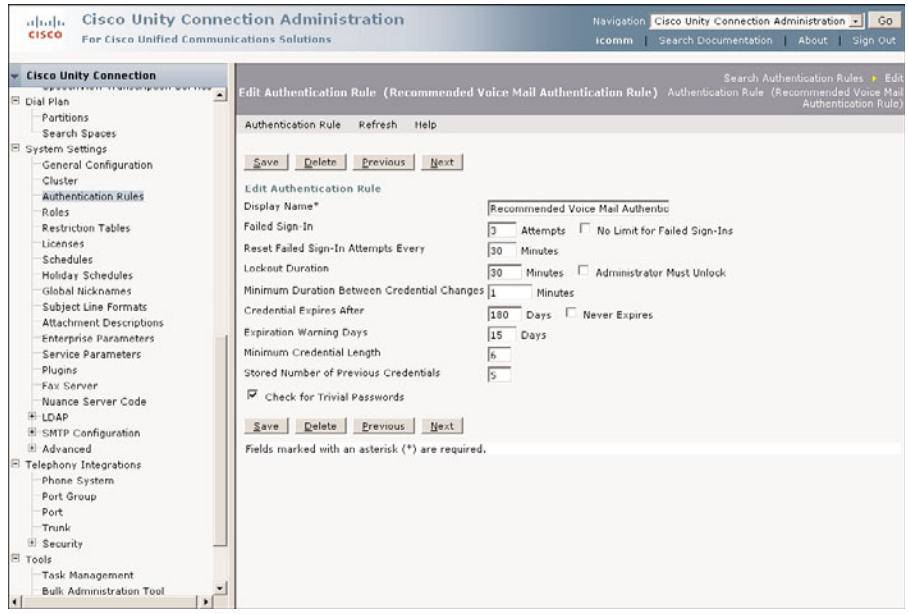
The real functionality of CUC is the numerous options provided for administrators to use in customizing the system to meet the needs of a business. The downside of all these options is deciding how to organize and configure them. As you will discover, CUC has an orderly system of templates and rules that works well to minimize the amount of work to create and manage user accounts. However, the template only works when applied at user creation, so lots of time can be saved if the desired settings are configured before the users are created. It might take you some time to discover the settings to meet the needs of a company, so it can be helpful to create a user or two to test the setting before creating the users in bulk. Start by examining the default settings and creating alternate rules.

Step 1-1: Examine Authentication Rules

There are two default authentication rules: one for users connecting to voice mail from their phones and another for connecting from a web interface. On the Cisco Unity Connection Administration page, navigate to **System Settings > Authentication Rules**.

1. Click the hyperlinked **Recommended Voice Mail Authentication Rule**. The Edit Authentication Rule pane will open. See Figure 13-34 for an example of this page.

Figure 13-34 Recommended Voice Mail Authentication Rule



2. As you can see, the rule will lock a user out for 30 minutes after three failed attempts within 30 minutes. The user will need to change his password every 180 days, the past five passwords cannot be reused, the password has to have a minimum length of six characters, and the password cannot be trivial. Trivial passwords have all the same digits (for example, 111111) or consecutive digits (for example, 123456), or are the same as the user's extension. Click the **Next** button to see the Web Application Authentication Rule.

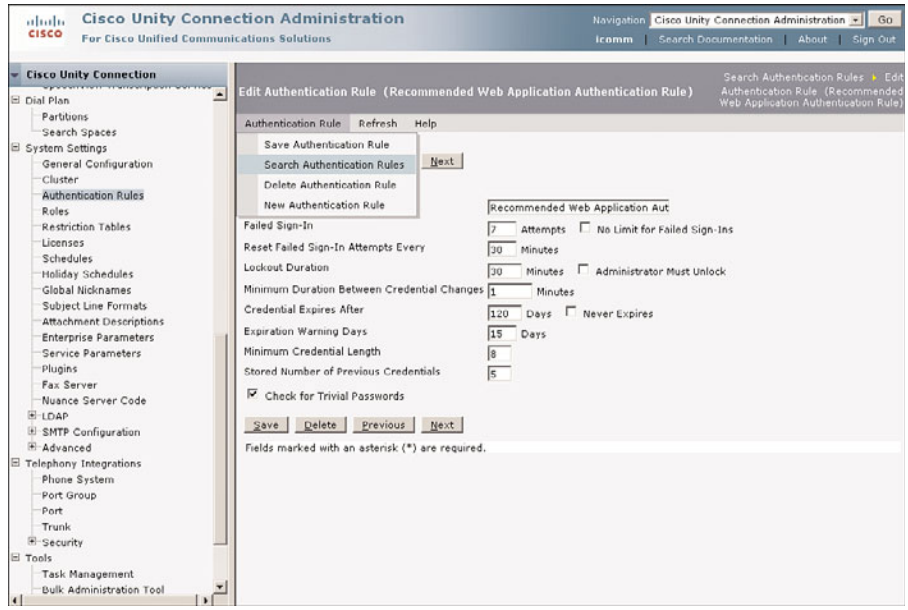
3. The Web Application Authentication Rule is almost identical, except it takes seven failed log ins to lock out, the password expires every 120 days, and the password must have a minimum length of eight characters. In the Edit Authentication Rule pane, select the Authentication Rule

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

menu and then select the **Search Authentication Rules** item. See Figure 13-35 for an example of this page.

Figure 13-35 Recommended Web Application Authentication Rule



Step 1-2: Configure Authentication Rules

Rather than change the default rules, create your own. This will allow you to experiment with having more than one rule to select in the templates for the user. By creating a custom template, you are on the safe side, so if you make mistakes, you can easily start again. If you are not already on the Search Authentication Rules pane, on the Cisco Unity Connection Administration page, navigate to **System Settings > Authentication Rules**.

1. Click the **Add New** button.

Note: These settings might be appropriate only for lab usage.

---

2. Enter **Low Security** in the Display Name field.
3. Change the Lockout Duration field to **1** minute.
4. Select the **Never Expires** check box for Credential Expires After.
5. Change the Minimum Credential Length field to **3**.
6. Change the Stored Number of Previous Credentials field to **0**.
7. Deselect the **Check for Trivial Passwords** check box. See Figure 13-36 for an example of this page.
8. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

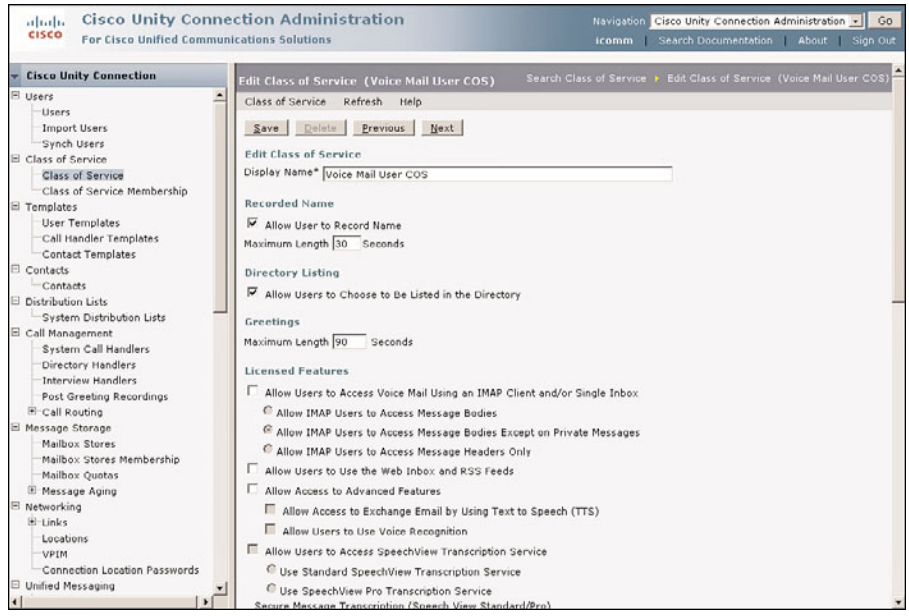
Figure 13-36 Custom Authentication Rule

Step 1-3: Examine Class of Service

On the Cisco Unity Connection Administration page, navigate to **Class of Service > Class of Service**. Click the hyperlinked **Voice Mail User COS**.

On this page, you will see the options for many settings, such as allowing the user to record her own name and the length of the recording. See Figure 13-37 for an example of this page.

Figure 13-37 CUC Class of Service



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 2: CUC User Template

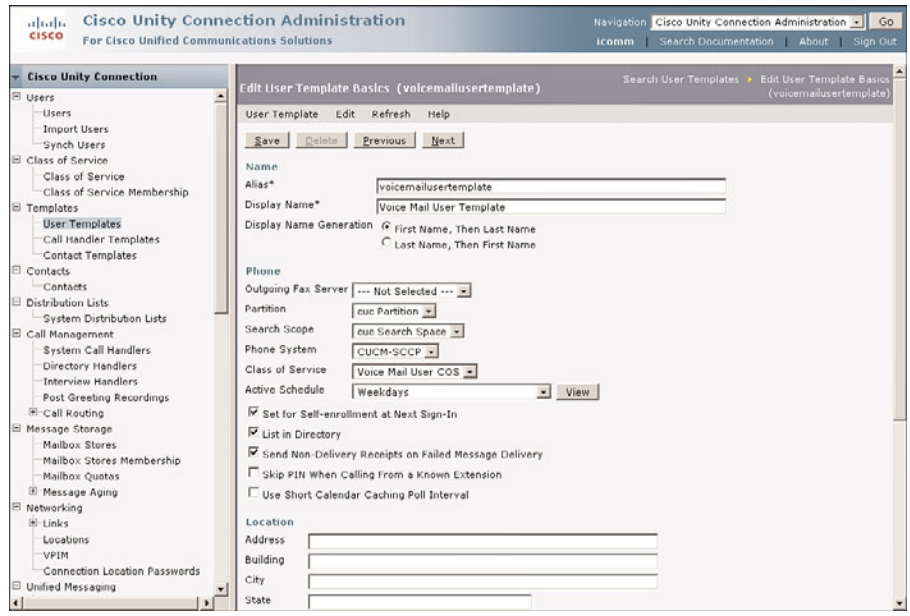
After examining the class of service settings and creating a custom authentication rule, it is time to see how these apply to user creation.

Step 2-1: Examine the User Template

On the Cisco Unity Connection Administration page, navigate to **Templates > User Templates**.

1. Click the hyperlinked **voicemailusertemplate**. See Figure 13-38 for an example of this page.

Figure 13-38 Custom Authentication Rule

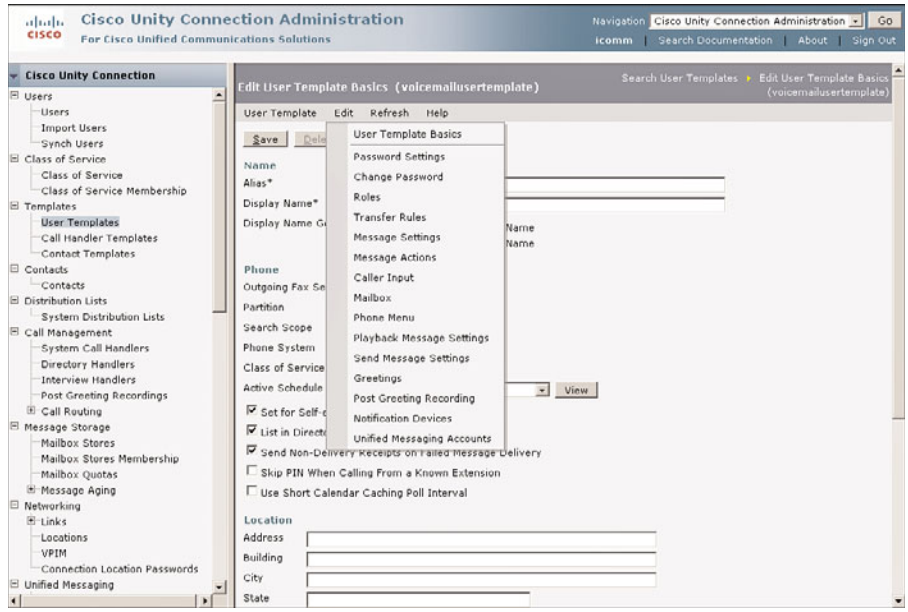


2. As you examine the template, notice the Partition and Search Scope fields in the Phone section. CUC implements these the same way that CUCM implements partitions and CSSs. The default for CUC is one partition, with everyone in the same CSS.
3. Notice that the Class of Service field is selected in the Phone section. All users created with this template will be assigned **Voice Mail User COS**.
4. Farther down the pane are the location and time zone defaults. So far, the template does not seem that complex. That is because most of the settings are organized into separate panes.
5. Select the Edit menu at the top of the pane. See Figure 13-39 for an example of this page.
6. Here is where you start to see the vast number of options that are configurable as part of the template. Select **Edit > Password Settings**. This pane includes the password settings and the authentication rule.
7. Select **Edit > Roles**. This pane has roles for users. (The Assigned Roles field is blank, as most voice mail users will not have a role.)
8. Select **Edit > Message Settings**. This pane includes the settings for message length and message options.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-39 Custom Authentication Rule



9. Select **Edit > Change Password**. This pane is where a password can be assigned (or on a user account, changed).
10. Explore the rest of the menu options to see what other settings are available. Don't change any of them at this point.

Step 2-2: Create a User Template

Again, rather than modify the default template, to be on the safe side, create your own template, so if you make mistakes, you can easily start again. You can create as many templates as needed, so you can customize the settings for each group of users that need common settings. On the Cisco Unity Connection Administration page, navigate to **Templates > User Templates**.

1. Click the **Add New** button.
2. Enter **Sales Agent Template** in the Alias field.
3. Enter **Sales Agent Template** in the Display Name field. See Figure 13-40 for an example of this page.
4. Click the **Save** button. The pane will change to the Edit User Template Basics pane.
5. Deselect the **Set for Self-enrollment at Next Sign-In** check box. The self-enrollment is a script that helps users set up their mailbox. (While it is great for new users, you will quickly get sick of it on every account you create.) See Figure 13-41 for an example of this page.
6. Click the **Save** button.
7. From the Edit menu, select **Password Settings**.
8. Leave the Choose Password drop-down list set to **Voice Mail**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-40 Copy User Template

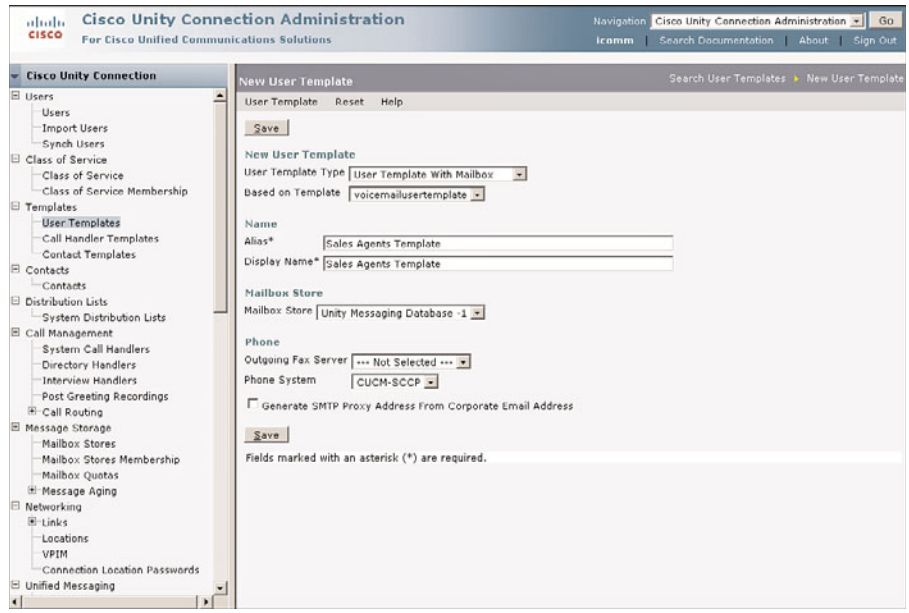
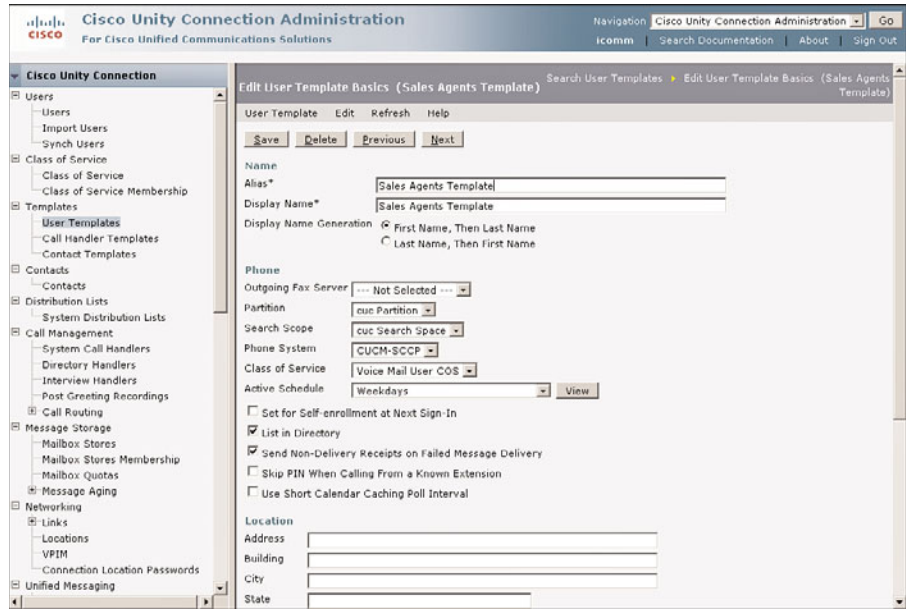


Figure 13-41 Edit User Template Basics

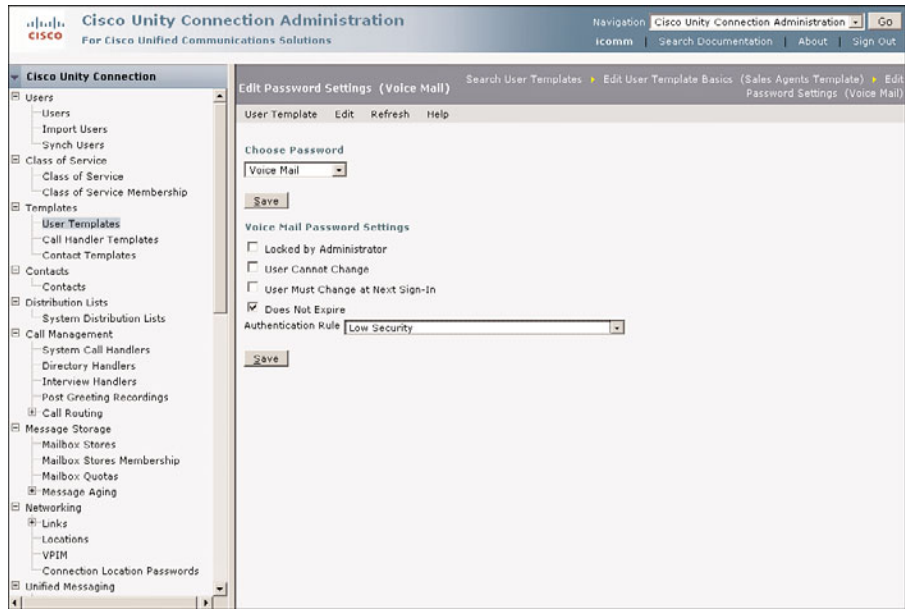


9. Deselect the **User Must Change at Next Sign-In** check box.
10. Select the **Does Not Expire** check box.
11. Select **Low Security** from the Authentication Rule drop-down list. See Figure 13-42 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-42 Edit Password Settings



12. Click the **Save** button.
13. From the Edit menu, select **Change Password**.
14. Leave the Choose Password drop-down list set to **Voice Mail**.
15. Enter **123** for the Password and Confirm Password fields.
16. Click the **Save** button.

Task 3: Configure CUC Users

Now that templates have been created and modified, it is time to manually create a user account. The account you set up first will be for the first extension on the first HQ phone (which should be the extension in CUCM where you created a user account with your name).

Step 3-1: Configure User with the Custom Template

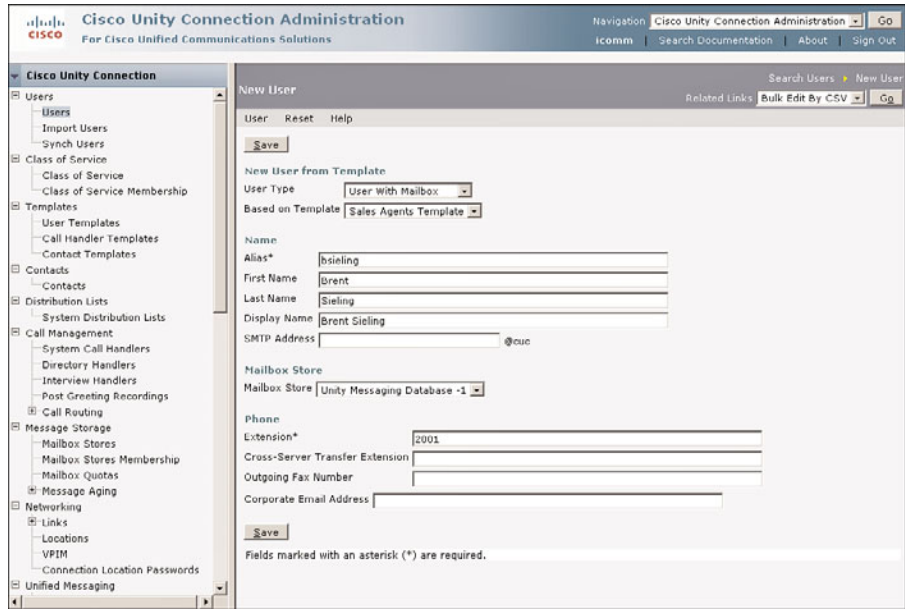
On the Cisco Unity Connection Administration page, navigate to **Users > Users**.

1. Click the **Add New** button.
2. Make sure that the Based on Template field is set to your custom **Sales Agent Template**.
3. Enter your user login name (example: bsieling) in the **Alias** field. This value must be unique in the CUC system, and ideally matches the account name you created for yourself in CUCM.
4. Enter your first name and your last name in the First Name and Last Name fields. These values will automatically fill in the Display Name field.
5. In the Phone section, in the Extension field, enter the primary extension number for your username. See Figure 13-43 for an example of this page.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

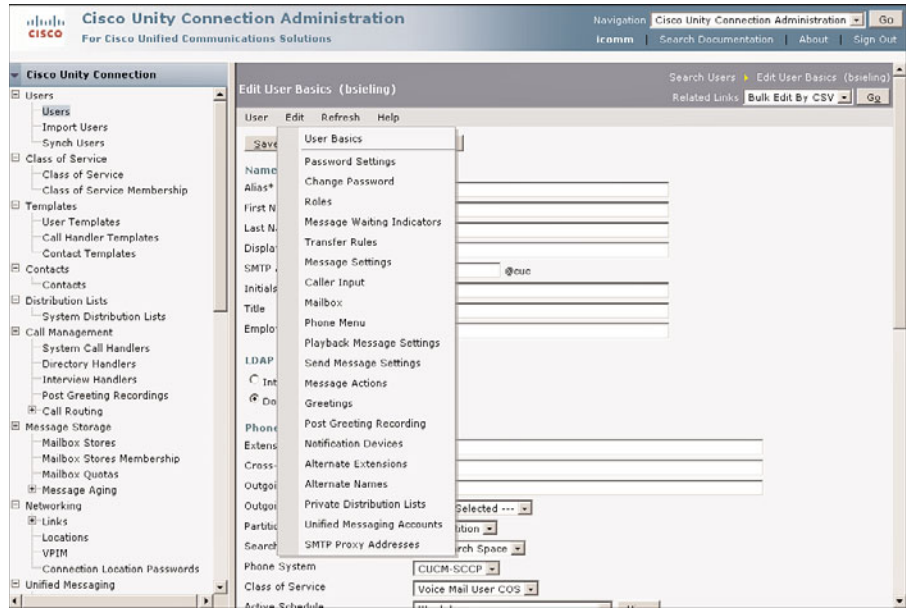
Figure 13-43 New User



6. Click **Save**.

7. After the user is created, all the Edit options become available. Click the Edit menu and notice that there are more options than the Template option. See Figure 13-44 for an example of this page.

Figure 13-44 New User Edit Menu



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-2: Test User Voice Mailbox

It is time to take your new voice mailbox for a test drive:

1. On the first HQ phone, press the **Messages** button. You should be asked to enter your PIN.
2. Enter **123#**. The system responds by speaking your name and "Hello, to send a message . . ." (Cisco has found that some people hate to create a custom greeting for their mailbox.) CUC uses text-to-speech recognition of the mailbox owner's name to provide a better experience for people leaving a message, even for the standard greeting message.
3. To test the setting once, go back to your CUC user account, and in the Edit User Basics pane, select the **Set for Self-enrollment at Next Sign-In** check box.
4. Click the **Save** button.
5. On the first HQ phone, press the **Messages** button. You should be asked to enter your PIN, and then the system will prompt you to change various options. Complete this step by answering the prompts.
6. When you go back to the user account again, you will notice that the system has deselected the self-enrollment, because you have completed it.

Task 4: Update CUCM Directory Numbers to Use Voice Mail

At this point, only one phone user has a voice mailbox, and no one can leave messages yet.

Step 4-1: Configure Voice Mail on a Directory Number

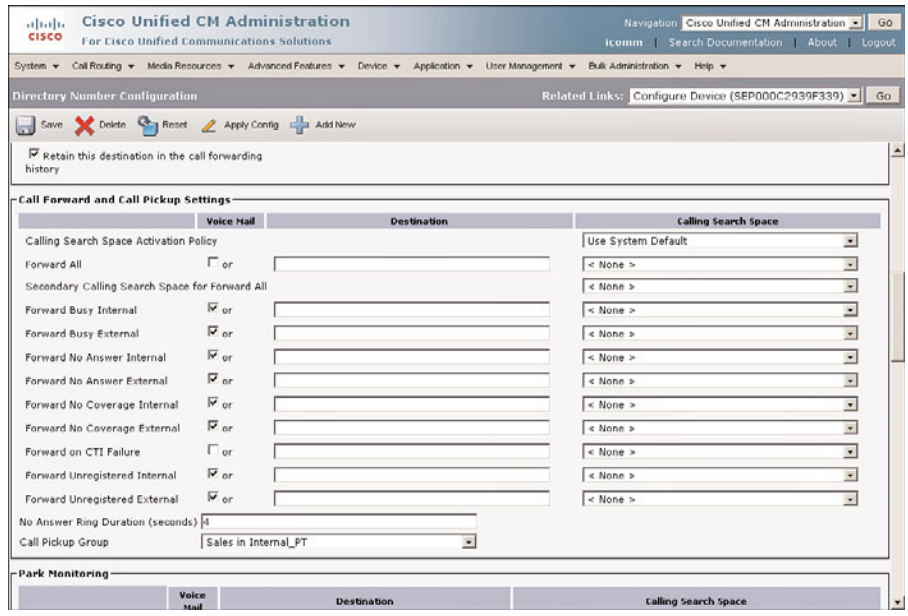
On the Cisco Unified CM Administration page, navigate to **Device > Phone**. Click **Find** if no phones are listed.

1. Click the second HQ phone.
2. In the Association Information section, click the **Line [1]** hyperlink. (This should be the extension with the SIP-VM-Profile assigned.)
3. Scroll down to the Call Forward and Call Pickup Settings section. Because the voice mail profile was defined, you can just select the Voice Mail check box for the following items:
   - **Forward Busy Internal**
   - **Forward Busy External**
   - **Forward No Answer Internal** (which will automatically select the **Forward No Answer External**, **Forward Unregistered Internal**, and **Forward Unregistered External** check boxes)
   - **Forward No Coverage Internal**
   - **Forward No Coverage External**
4. Enter **4** in the No Answer Ring Duration field. See Figure 13-45 for an example of this page.
5. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-45 Directory Number Call Forwarding Settings

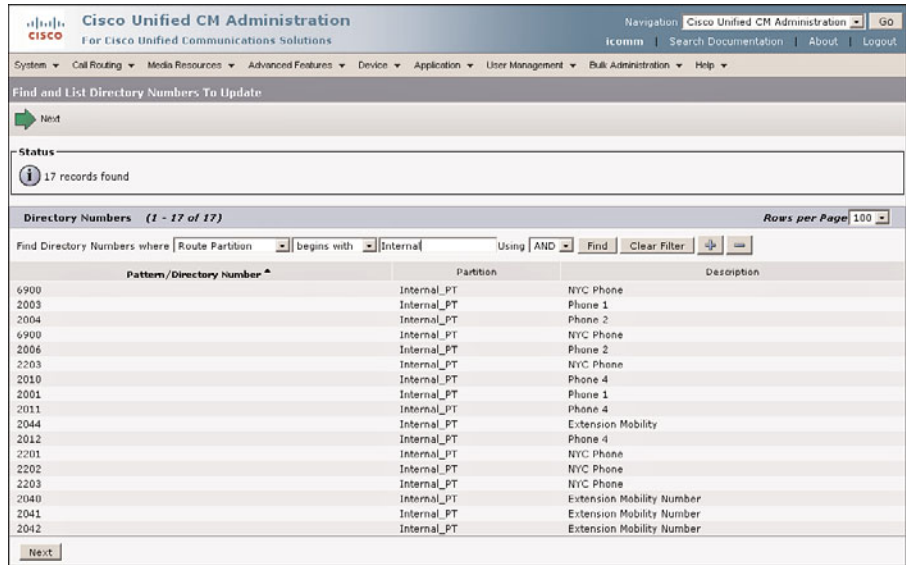


Step 4-2: Configure Voice Mail on a Directory Number

The thought of having to do this for all the directory numbers could be rather depressing (time to hire an intern!), but you can use the Bulk Administration Tool (BAT) to do the update for directory numbers in bulk. On the Cisco Unified CM Administration page, navigate to **Bulk Administration > Phones > Add/Update Lines > Update Lines**.

1. Select **Route Partition** from the Find Directory Numbers Where drop-down list, and enter **Internal** in the Begins With field to find the active directory numbers. Click the **Find** button. See Figure 13-46 for an example of this page.

Figure 13-46 Find and List Directory Numbers to Update

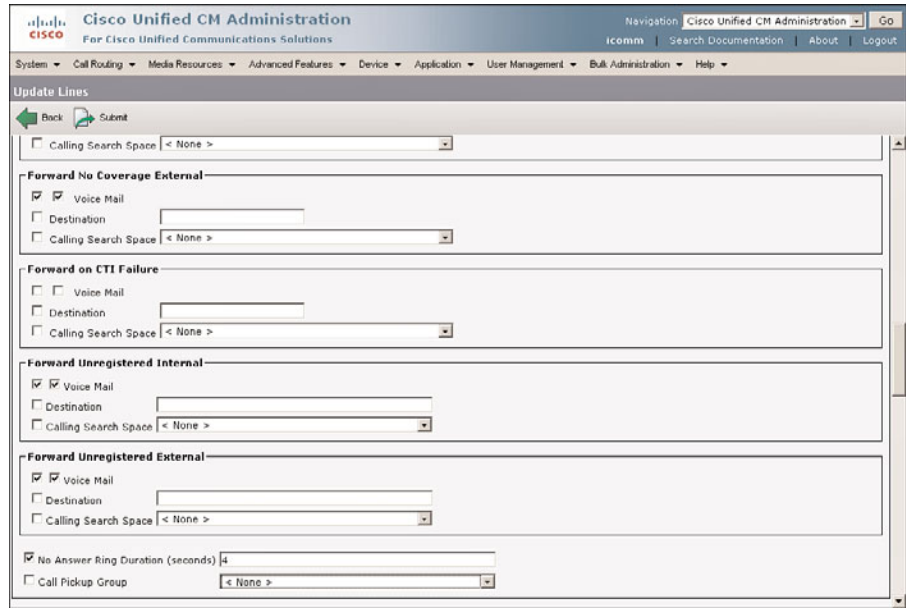


https://t.me/learningnets

From the Library of Aliwarman Tarihoran

2. Click the **Next** button.
3. Scroll down to the Call Forward and Call Pickup Settings section. Select both check boxes before Voice Mail, for the following items:
   - **Forward Busy Internal**
   - **Forward Busy External**
   - **Forward No Answer Internal**
   - **Forward No Answer External**
   - **Forward No Coverage Internal**
   - **Forward No Coverage External**
   - **Forward Unregistered Internal**
   - **Forward Unregistered External**
4. Enter **4** in the No Answer Ring Duration field. See Figure 13-47 for an example of this page.

Figure 13-47 Update Lines



5. Scroll down to the Job Information section and click the **Run Immediately** radio button.
6. Click the **Submit** button.

Check the Job Scheduler to see the results of your job.

Step 4-3: Test Call Forwarding to Voice Mail

Time to leave your first voice mail with the CUC system:

1. From the second or third HQ phone, call the first extension on the first HQ phone. *Do not answer*. After four seconds, the voice mail system should answer and play the personal greeting.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

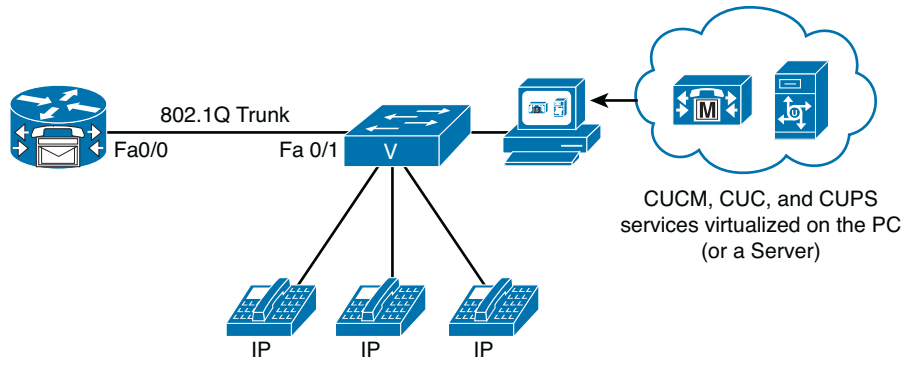
2. Leave a short message and hang up.
3. After a second or so, the red light on the handset will light up, and the icon next to the line button will show a blinking envelope, to let you know there is a new message.
4. Press the **Messages** button on the first HQ phone and enter your PIN. Listen to your message and delete or save it. Hang up when you are done.
5. In a second or two, the Message Waiting Indicators will turn off.
6. If you repeat this process while watching RTMT, you will discover the difference between the two main types of calls: direct calls (when the user accesses his voice mail account) and forwarded calls (when the phone is not answered and a caller is leaving a message for the phone user). Forwarded calls show Reason and Redir information from CUCM in the RTMT columns. This is how CUC knows when to play the leave-a-message script, and when to ask for a PIN. It is also interesting to watch RTMT show the Conversation Status while leaving and retrieving voice mails. You can watch the audio scripts and response mechanisms working.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 13-3: Adding Users to Cisco Unity Connection (CUC) from Cisco Unified Communications Manager (CUCM) and Using the Bulk Administration Tool (BAT)

Figure 13-48 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- Cisco Unity Connection (CUC) Server or PC with VMware Workstation installed and a VM of CUC
- Three or more IP Phones registered (desk phone or soft phone on PC or Windows VM)
- Lab configuration from Lab 13-2

Learning Objectives

Upon completion of this lab, you will be able to

- Import user accounts into CUC from CUCM
- Import user accounts into CUC using BAT

Scenario

SOI is happy that there is a voice mail system and that you have one voice mail account working. Now SOI wants voice mailboxes for all employees, and it still will not let you hire an intern. Take advantage of ways to save time creating voice mail accounts by importing users from CUCM or by using BAT.

Task 1: Configure CUC to Import Users from CUCM

To enable the exchange of records between CUCM and CUC, the AXL service and user need to be configured before you can import users. AXL stands for Administrative XML (where XML stands for eXtensible Markup Language). It is a protocol used to exchange data between web-based applications.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 1-1: Activate AXL Web Service on CUCM

If Cisco AXL Web Service is not already active on CUCM, follow the steps in Lab 9-2, Task 3 to activate it.

Step 1-2: Create AXL User Account

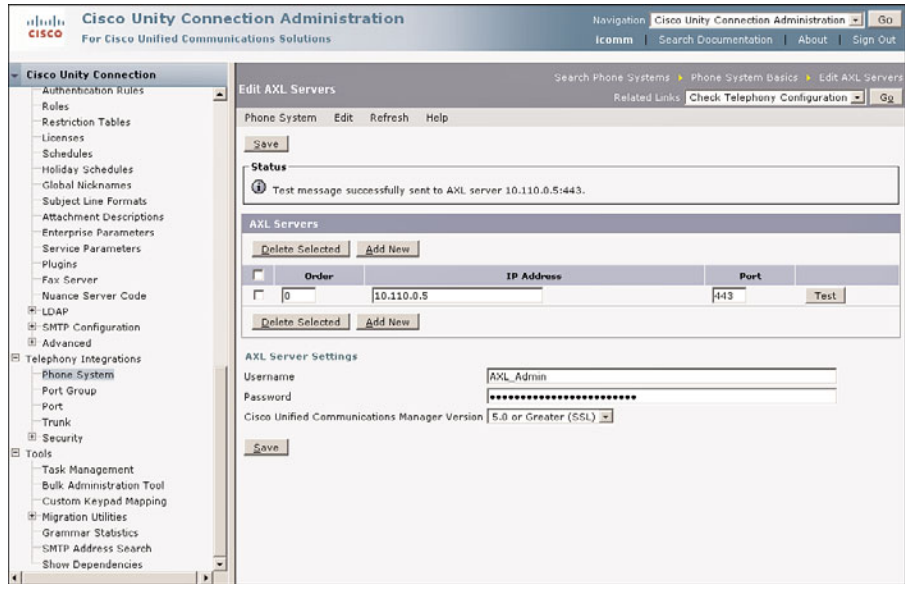
If you have not completed Lab 9-7, Tasks 4 and 5 to create the AXL user account, follow the steps now to create the account. (It is a bad practice to use the Application Administrator account. If the password is ever changed in the future, the link to CUC would also need to be updated. A far better practice is to have a separate application user account for the AXL service access.)

Step 1-3: Configure AXL Services in CUC

On the Cisco Unity Connection Administration page, navigate to **Telephony Integrations > Phone System**.

1. Click the hyperlinked **CUCM-SCCP** name.
2. On the Phone System Basics (CUCM-SCCP) page, use the Edit menu to select **Cisco Unified Communications Manager AXL Servers**.
3. Enter the AXL username created in Step 1-2 (**AXL_Admin**) and the password of **cisco**.
4. Click the **Save** button.
5. On the AXL Servers section of the page, click the **Add New** button.
6. Enter the IP address of the CUCM server (10.*x*0.0.5) in the IP Address field and enter **443** in the Port field.
7. Click the **Test** button. You should see the Status display "Test message successfully sent to AXL server." See Figure 13-49 for an example of this page.

Figure 13-49 Edit AXL Servers



8. Click the **Save** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

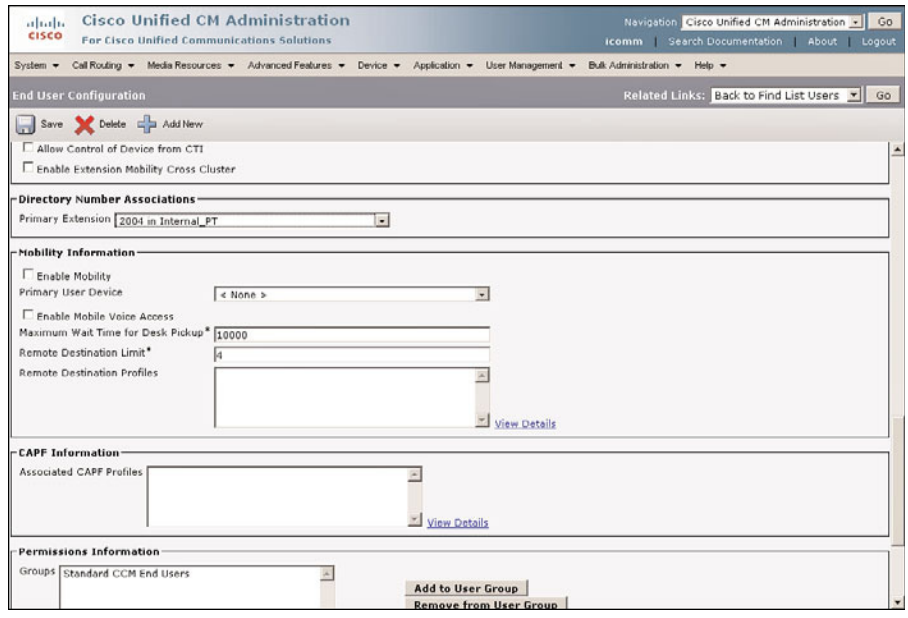
If you had more than one CUCM server, you could add each in the preferred ordered of usage. (For example Sub1, then Sub 2, then Pub.)

Step 1-4: Configure User Accounts in CUCM

Before the user accounts can be imported into CUC, the primary extension for the user needs to be identified. On the Cisco Unified CM Administration page, navigate to **User Management > End User** and click the **Find** button to see any existing users.

1. Click a username.
2. Scroll down to the Device Information section and see whether there is a device listed in the Controlled Devices box. If there is, proceed to item 6. If there are no devices listed, click the **Device Association** button, next to the Controlled Devices box.
3. Because no devices have been associated yet, click the **Find** button. You will see a list of the individual directory numbers for all phones. Select the check boxes for the phone lines on the phone that you have registered for this user. (This is where using the name in the phone description is handy.)
4. Click the **Save Selected/Changes** button. The page will refresh to show all directory numbers (on the same phone) that you selected at the top of the list.
5. With the Related Links set at **Back to User**, click the **Go** button to return to the end user.
6. Scroll down to the Directory Number Associations section and select the first extension on the phone from the Primary Extension drop-down list. See Figure 13-50 for an example of this page.

Figure 13-50 End User Primary Extension



7. Click the **Save** button.

Use the Related Links drop-down list to return to the find users list and repeat this step for all the user accounts that have phones.

https://t.me/learningnets

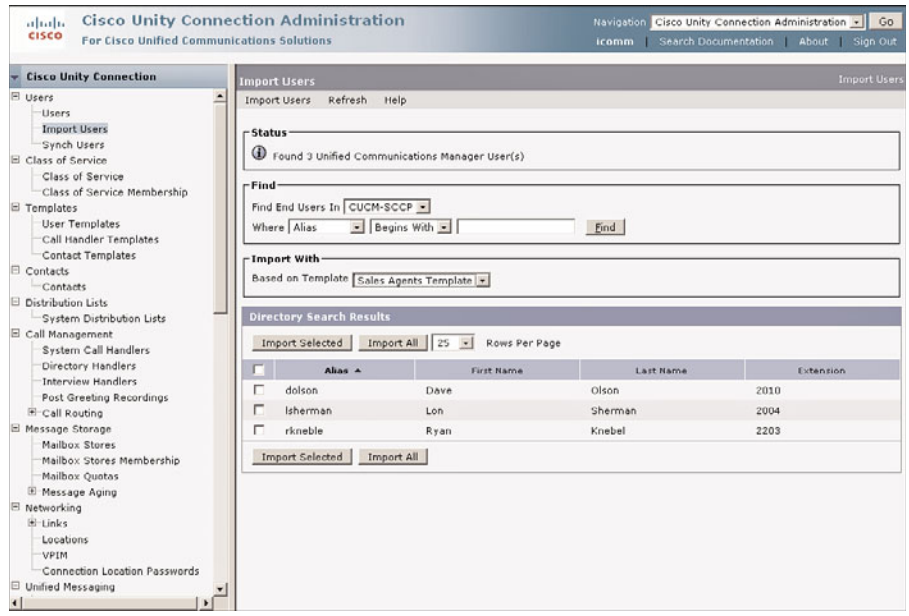
From the Library of Aliwarman Tarihoran

Step 1-5: Import CUCM Users into CUC

On the Cisco Unity Connection Administration page, navigate to **Users > Import Users**.

1. Select **CUCM-SCCP** from the Find End Users In drop-down list.
2. Click the **Find** button. You should see all the users listed that have primary extensions assigned.
3. Select **Sales Agents Template** from the Based on Template drop-down list. See Figure 13-51 for an example of this page.

Figure 13-51 Import Users



4. Select the check box in front of individual users (that do not exist in CUC already) and click **Import Selected**. (If the alias already exists in CUC, you will get an error report.)
5. A pop-up window will ask whether you are sure. Click **OK**.
6. The pane will update with the status. Hopefully you have all records as successes and zero failures.

Voice mailboxes for everyone!

Step 1-6: Examine Imported User

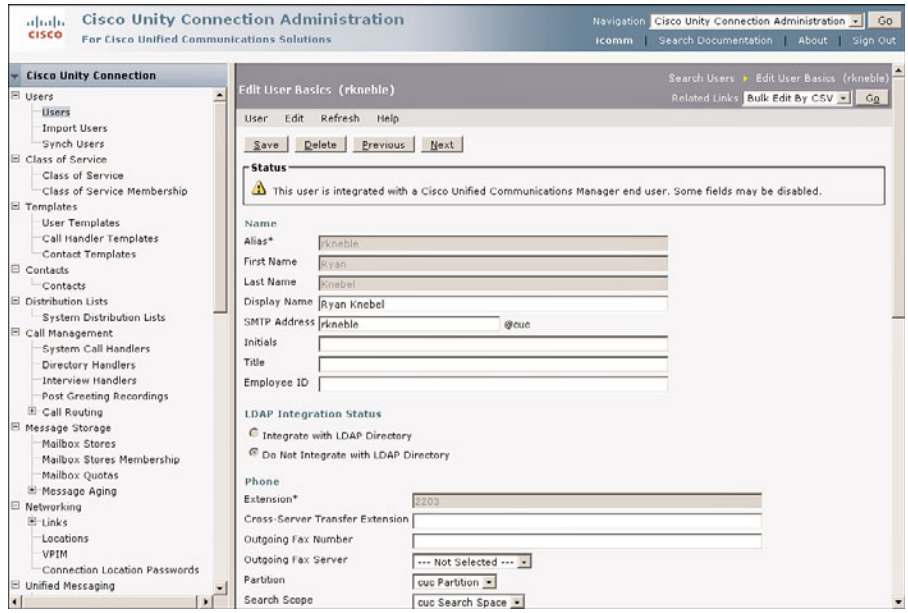
On the Cisco Unity Connection Administration page, navigate to **Users > Users**. Click one of the usernames you just imported. You will notice that some of the fields are grayed out, as is the information from CUCM. See Figure 13-52 for an example of this page.

If the information is changed in CUCM, it is not automatically updated in CUC. To have the changes brought into CUC, the **Users > Synch Users** selection can be run to capture any changes.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 13-52 Import End User Accounts



Task 2: Use BAT to Import Users into CUC

CUC can use BAT in much the same way that CUCM uses it to import, export, and modify records. The good news is that the process is much easier than in CUCM, but the bad news is that there are not as many features and there is no spreadsheet to simplify the process. The best way to create a file for import is to export some existing users to discover the file format.

Step 2-1: Export Users

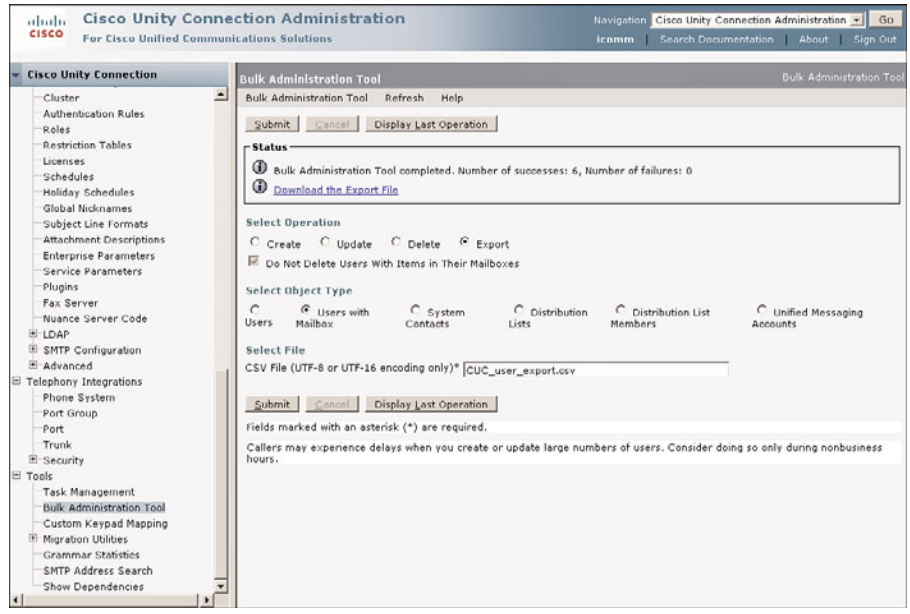
On the Cisco Unity Connection Administration page, navigate to **Tools > Bulk Administration Tool**.

1. Select the **Export** radio button.
2. Enter **CUC_user_export.csv** in the CSV File field.
3. Click the **Submit** button. The job will process.
4. When the process is done, a hyperlink to download the file will show in the status. See Figure 13-53 for an example of this page.
5. Click the link to download the file.
6. Open the file in a spreadsheet program. Use the existing records to assist you in creating a new row. Use a name like Test Import, and assign it one of the directory numbers created from the BAT import of the phone to CUCM.
7. Delete the existing user rows from the file.
8. Save the file as **CUC_user_import.csv.**
9. In CUC, select the **Create** radio button.
10. Select the **Yes** radio button and **Sales Agents Template** from the drop-down list.

https://t.me/learningnets

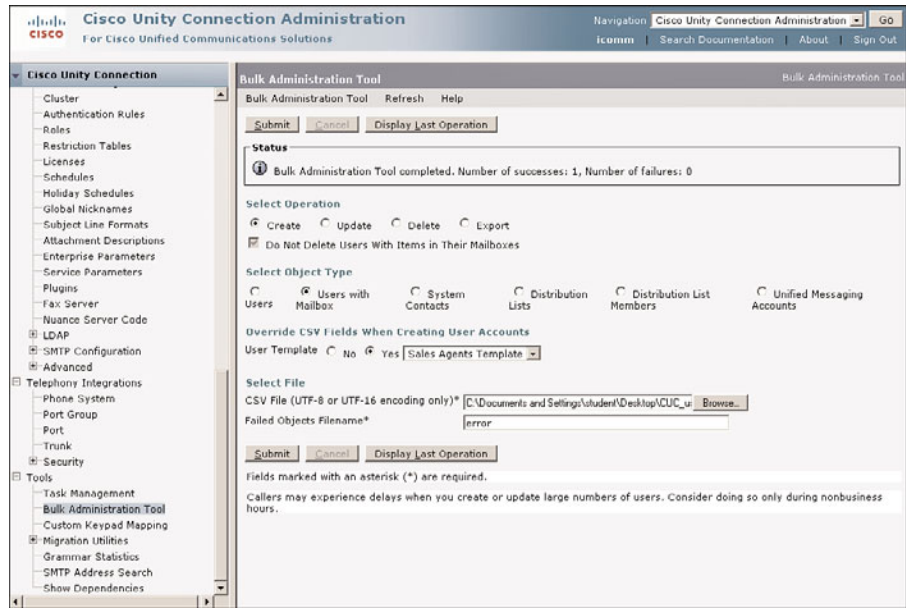
From the Library of Aliwarman Tarihoran

Figure 13-53 BAT User Export



11. Click the **Browse** button and navigate to where the CUC_user_import.csv file is saved.
12. Enter **error** in the Failed Objects Filename field.
13. Click the **Submit** button. The job will process.
14. The status should show one success and zero failures. See Figure 13-54 for an example of this page.

Figure 13-54 BAT User Import



15. Examine **Users** > **Users** to see the new user account.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

This page intentionally left blank

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

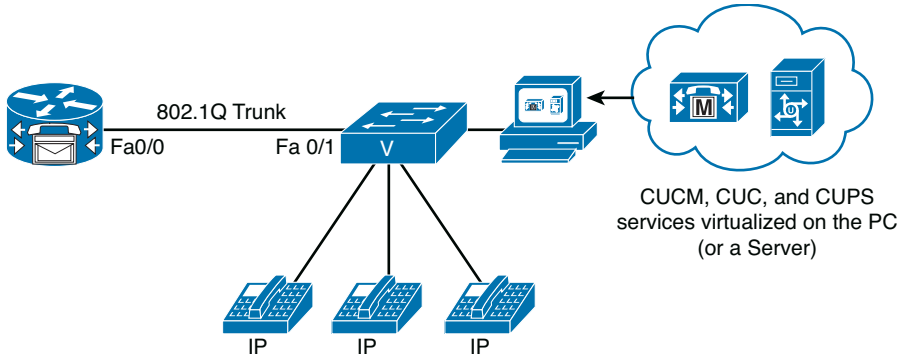
CHAPTER 14

Cisco Unified Presence

Cisco Unified Presence provides real-time status information for user contacts along with Instant Messaging (IM), desk phone control, integrated soft phone, video, and other related capabilities. The Cisco Unified Personal Communicator (CUPC), now known as Jabber, provides the client-side interface, while the Cisco Unified Presence Server (CUPS) provides the server-side processes that make this function properly behind the scenes. In this lab, you will go through the steps necessary to configure CUPS to function with Cisco Unified Communications Manager (CUCM) and the CUPC/Jabber client.

Lab 14-1: Configuring Cisco Unified Presence Server

Figure 14-1 Topology Diagram



Equipment Required

- Cisco router
- Switch that supports voice VLANs
- Fully installed Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- A newly installed (OS install Only) CUPS server
- Cisco Unity Connection (CUC) Server or PC with VMware Workstation installed and a VM of CUC (optional)
- Two or more IP Phones registered (desk phone or soft phone on PC or Windows VM)
- One or more PCs with the Cisco Jabber client software installed
- Lab configuration from Lab 13-3

Note: If your PC or server does not have enough resources to run all the servers at the same time, the Cisco Unity Connection server can be considered optional.

If you do not have the CUPC/Jabber software, you can configure the lab, but you will not be able to test the functionality.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Learning Objectives

Upon completion of this lab, you will be able to

- Configure CUCM for CUPS functionality
- Configure CUPS connectivity to CUCM
- Configure CUPC/Jabber profile
- Configure CSF devices in CUCM

Task 1: Configure CUCM for CUPS Functionality

To function properly, the Presence Server must make contact with the CUCM Publisher on a number of fronts using various protocols. To facilitate these connections, some configuration changes must be made on the CUCM Publisher before the CUPS server attempts to make first contact. These are as follows:

- Add CUPS as an application server
- Add an AXL group
- Add an AXL user
- Add a CTI-enabled group
- Add a CTI user
- Add an IP Phone messenger user
- Add the IP Phone messenger service
- Add a SIP Trunk Security Profile
- Add a SIP publish trunk
- Enable users for Presence in CUCM

Step 1-1: Activate Services

On the CUCM server, activate the CTI Manager Service and verify that the AXL Web Service is active. If necessary, follow the steps in Lab 9-2, Task 3 to activate them.

Step 1-2: Add CUPS as an Application Server

Follow these steps to add CUPS as an application server:

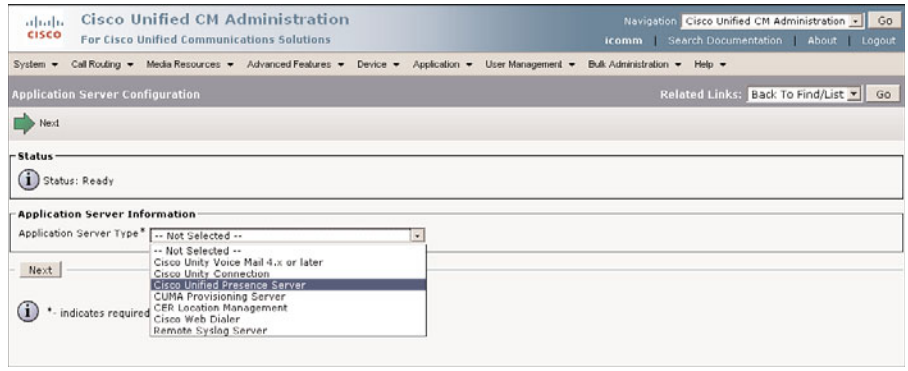
1. Access the CUCM CCMAdmin page.
2. Navigate to **System > Application Server** to access the Application Server configuration page.
3. Click the **Add New** button.
4. Select **Cisco Unified Presence Server** from the Application Server Type drop-down list.

   Figure 14-2 shows the Application Server Type selection.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 14-2 Application Server Type Selection



5. Click the **Next** button.

   The next screen provided is the Application Server information screen.

6. Enter the host name of the CUPS server. (If you followed the instruction in Lab C-3 to build the CUPS server, the name should be CUPS, plus the version of CUPS you are using. For example, **CUPS863**.)

7. Enter the URLs for its admin and user pages. The URL format for CUPS is as follows:

   URL: https://<*cups-ip-address*>/cupadmin

   End User URL: https://<*cups-ip-address*>/cupuser

8. After the required information is added, click the **Save** button.

Step 1-3: Add an AXL Group and User

If you have not completed Lab 9-7, Tasks 4 and 5 to create the AXL_Admin account, follow the steps now to create the account.

Step 1-4: Add a CTI-Enabled Group

To enable desk phone control and other aspects of Presence functionality, computer telephony integration (CTI) control must be enabled between CUPS and CUCM. Follow these steps:

1. Navigate to **User Management > User Group** and create a new group.

   As always, choose a name that is descriptive and unambiguous. Because all the roles we'll be assigning are CTI related, the name CTI-Enabled-Group is sufficient.

2. Enter **CTI-Enabled-Group** in the Name field, and then click **Save**.

3. On the User Group Configuration page, select **Assign Role to User Group** from the Related Links drop-down list at the upper right.

4. Click **Go**.

5. Click **Assign Role to Group**, and then click **Find** in the pop-up window that appears.

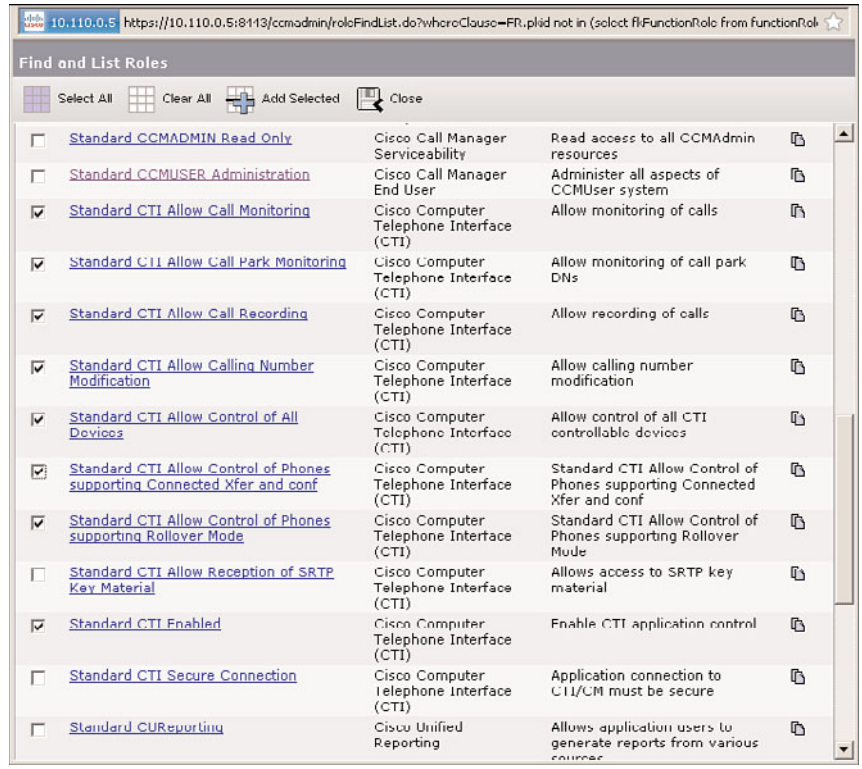
6. Select all CTI-related roles *except* **Standard CTI Allow Reception of SRTP Key Material** and **Standard CTI Secure Connection**.

   Figure 14-3 shows the necessary check boxes selected.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 14-3 Find and List Roles Screen for CTI



7. Click **Save**.

Step 1-5: Add a CTI User

As with the Administrative XML Layer (AXL) user that was configured, a CTI user needs to be created to connect with CUPS. By default, in the CUPS configuration, the username is CtiGw. With that in mind, follow these steps to create a new application user and assign it to the newly created CTI-enabled group:

1. Navigate to **User Management > Application User**.
2. Click **Add New**.
3. Enter **CtiGw** (case sensitive) in the User ID field.
4. Enter **cisco** in the Password and Confirm Password fields. In a production environment, always use a strong password. In the lab, an easy password is fine.
5. Assign the user to the group you created in Step 1-3.
6. Click **Save** and verify that the roles have autopopulated in the Roles box at the bottom of the page.

Step 1-6: Add an IP Phone Messenger User

IP Phone Messenger (IPPM) is a service that allows the user of the Cisco IP Phone to maintain/check the presence status of individual contacts. To enable the service, a user must be created on the CUCM Publisher. The CUPS configuration will default the name on its end to PhoneMessenger, so use that name for this lab.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

1. Navigate to **User Management > Application User**.
2. Click **Add New**.
3. Enter **PhoneMessenger** in the User ID field.
4. Enter **cisco** in the Password and Confirm Password fields. In a production environment, always use a strong password.
5. Click **Save** and continue to the next step.

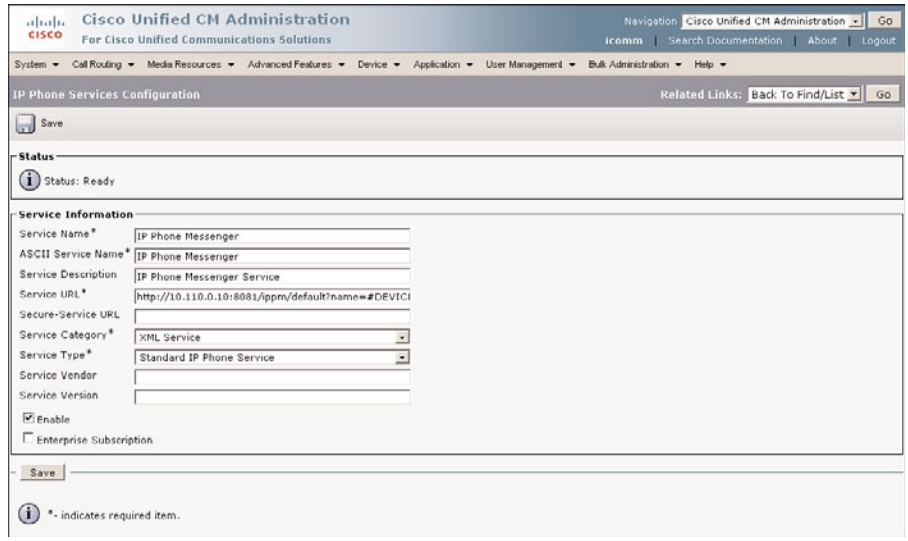
Step 1-7: Add the IP Phone Messenger Service

To use the IPPM functionality, a service must be created and phones subscribed to that service. Follow these steps:

1. To create a new service, navigate to **Device > Device Settings > Phone Services**.
2. Click **Add New**.
3. Enter the following parameters:
   - Service Name field: **IP Phone Messenger**
   - ASCII Service Name field: **IP Phone Messenger** (autopopulated)
   - Service Description field: **IP Phone Messenger Service**
   - Service URL field: **http://**<*cup-server-ip*>**:8081/ippm/default?name=#DEVICE-NAME#**
   - Service Category field: **XML Service**
   - Service Type field: **Standard IP Phone Service**
   - **Enable** check box: Select
   - **Enterprise Subscription** check box: Deselect

   See Figure 14-4 for an example of this page.

Figure 14-4 IP Phone Messenger Service



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

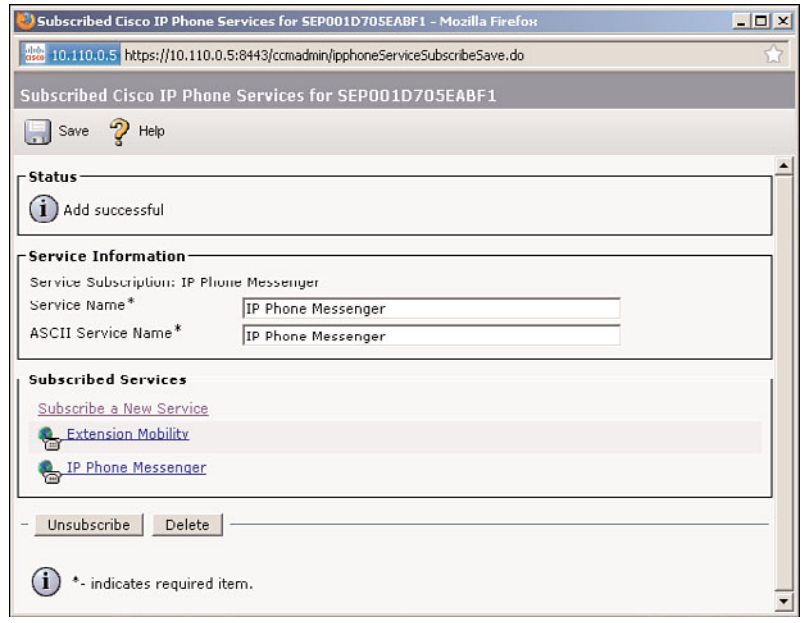
4. Click **Save** to complete the service creation.

Step 1-8: Subscribe Phones to IP Phone Messenger

Cisco IP Phones can be subscribed to the service from the individual phone's device screen. Navigate to **Device > Phone**, click **Find**, and follow these steps:

1. Select the phone to which you want to add the service and click its device name.
2. Select **Subscribe/Unsubscribe Services** from the Related Links drop-down list.
3. Click **Go**. Select the IP Phone Messenger Service from the drop-down menu in the resulting pop-up window.
4. Click **Next**.
5. Click **Subscribe**. Figure 14-5 shows the pop-up window.

Figure 14-5 Service Subscription Pop-up Window



6. Click **Save** to complete the process. You can close the pop-up window at this point.

Step 1-9: Add a SIP Trunk Security Profile

CUCM and CUPS communicate through SIP. To facilitate that communication, a SIP trunk needs to be created with specific parameters. Those specific parameters are primarily taken from a SIP Trunk Security Profile. Follow these steps to add a SIP Trunk Security Profile:

1. Navigate to **System > Security > SIP Trunk Security Profile** to begin this configuration task.
2. Click **Add New**.
3. Enter **CUPS Non-secure SIP Trunk Profile** in both the Name and Description fields.

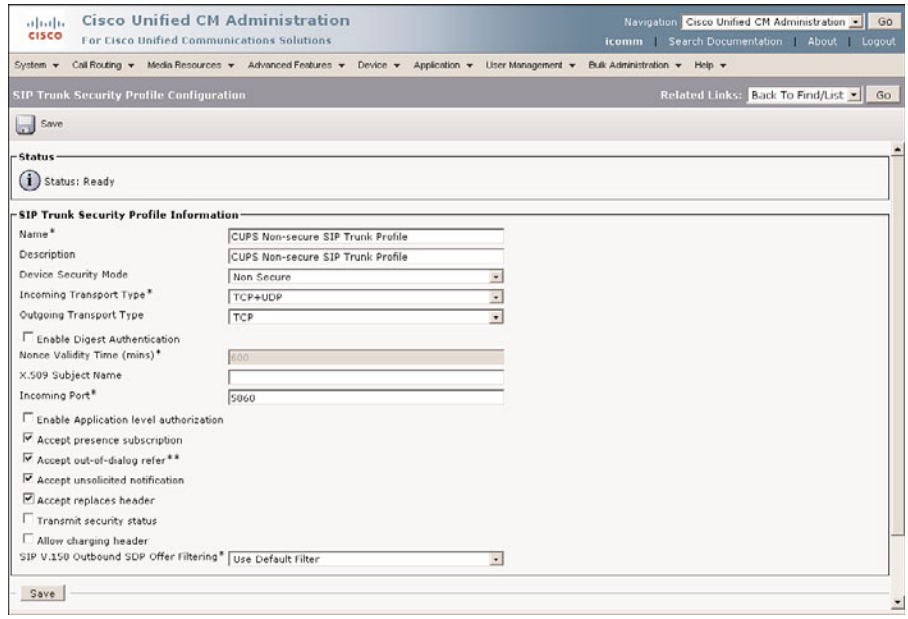
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. Verify that the following parameters are selected:
   - Device Security Mode field: **Non Secure**
   - Incoming Transport Type field: **TCP+UDP**
   - Outgoing Transport Type field: **TCP**
5. Select the following check boxes:
   - **Accept presence subscription**
   - **Accept out-of-dialog refer**
   - **Accept unsolicited notification**
   - **Accept replaces header**

   Figure 14-6 shows the SIP Trunk Security Profile Configuration screen.

Figure 14-6 SIP Trunk Security Profile Configuration



6. Click **Save**.

Step 1-10: Add SIP Publish Trunk

With the security profile created, it is now time to create the SIP trunk over which the communications between CUCM and CUPS will flow. Follow these steps:

1. Navigate to **Device > Trunk**.
2. Click **Add New** to bring up the Trunk Configuration screen.
3. As this will be a SIP trunk, select **SIP Trunk** from the Trunk Type drop-down list. The Device Protocol field will autopopulate with **SIP**.
4. Leave the Trunk Service Type field at its default setting (it's a new field and might not exist in your version of CUCM).

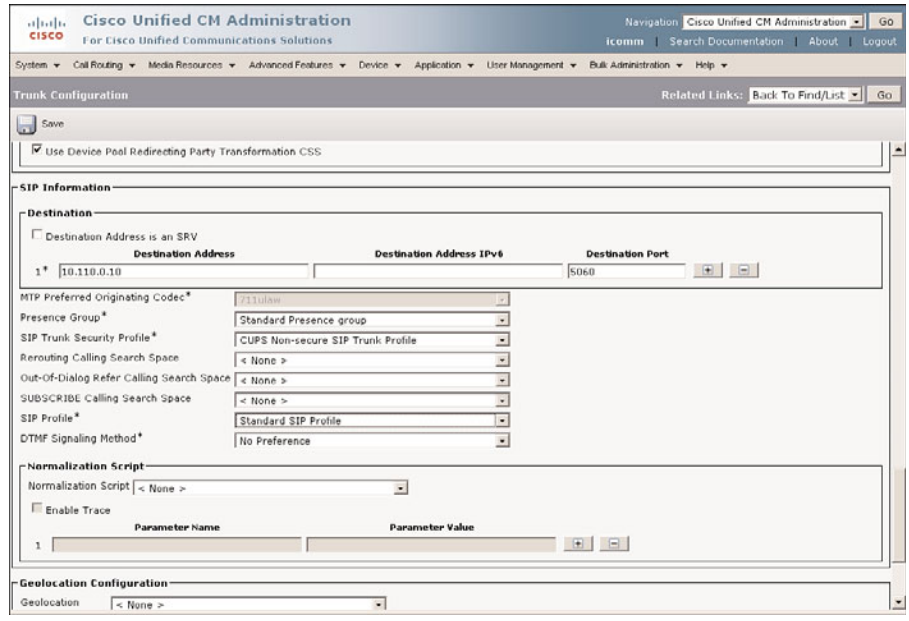
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

5. Click **Next**.
6. Enter **CUPS-SIP-Trunk** in the Device Name and Description fields.
7. Select **Madison DP** from the Device Pool drop–down list.
8. Scroll all the way to the bottom of the screen to the SIP Information section. The Destination Address field must be configured to point to the Presence Server's IP address (10.*x*0.0.10).
9. Select **CUPS Non-secure SIP Trunk Profile** from the SIP Trunk Security Profile drop-down list to tie the two together.
10. Select **Standard SIP Profile** from the SIP Profile drop-down list.

    Figure 14-7 provides a reference for this part of the task.

Figure 14-7 SIP Publish Trunk Configuration



11. Click **Save**.

Step 1-11: Enable Users for Presence Functionality

The final step in this task is to enable individual users for Presence and CUPC functionality.

1. Navigate to **System > Licensing > Capabilities Assignment** to begin.
2. Click the **Find** button to view all system users.

Note: This task assumes that all users have been added to CUCM through Lightweight Directory Access Protocol (LDAP). LDAP integration is required for proper operation of the CUPC/Jabber client. If no users appear upon clicking the **Find** button, it is likely that this integration is not properly complete or that the two systems have not yet synchronized.

---

3. From this screen, individual assignments can be made or they can be done in bulk. To assign Presence and CUPC/Jabber capabilities to all listed users on the page, select the check boxes by each name, click the **Select All** button, or select the check box at the upper-left corner of the table.

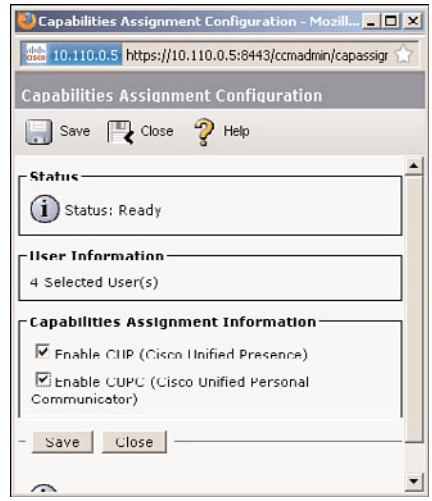
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. Click the **Bulk Assignment** button. Clicking this button brings a pop-up window that shows the number of selected users and two check boxes. (Individual users can be configured one by one as well, should you want to be selective.)

   Figure 14-8 shows the Capabilities Assignment Configuration pop-up screen.

Figure 14-8 Capabilities Assignment Configuration



5. Select both check boxes.
6. Click **Save**.

The pop-up will disappear and checks will now appear in the CUP Enabled and CUPC Enabled columns next to the selected users' names.

This completes the CUCM configuration tasks.

Task 2: Configure CUPS Connectivity to CUCM

Now that the CUCM-side connection dependencies are all in place, we're ready to access CUPS for the first time. You will need all the information configured in Task 1, including usernames, passwords, trunk names, and so on to complete this task. The steps that follow include

- Access the CUPS web administration page
- Upload a license file
- Activate services
- Add a Presence gateway
- Activate desk phone control
- Activate the IP Phone Messenger

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-1: Access the CUPS Web Administration Page

Accessing the CUPS web administration page for the first time after the initial OS installation launches a postinstall wizard. This wizard must be fully and properly completed to establish connectivity with the CUCM Publisher. Follow these steps to complete the post-installation wizard:

1. Open a browser and enter the URL of the Presence Server. It will be in the format of

   https://<*cups-ip-address*>/cupadmin

2. Log in using the application administration username and password, as noted in Lab 8-1. This username and password were created during the installation of the CUPS operating system.

   After you are logged in, the postinstall wizard will launch automatically if it wasn't already completed in a prior lab. If the wizard has already been run, you can skip to the next step.

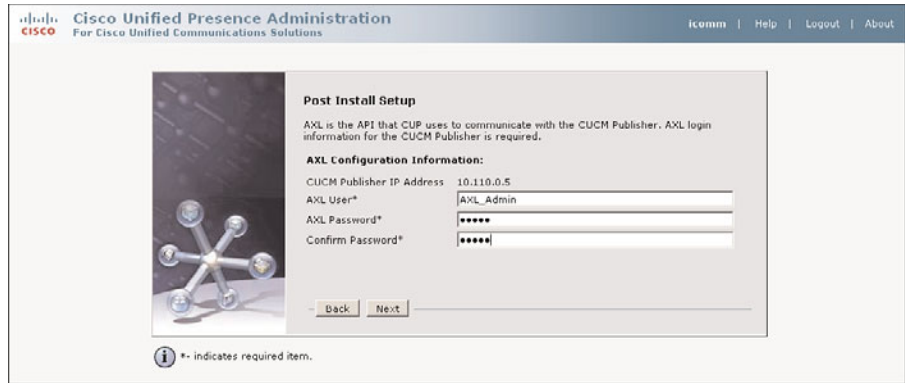
Note: To make contact, the Presence Server must have been added as an application server and the AXL user must have been configured in the CUCM before this step is completed. If Task 1 of this lab is incomplete, do not continue.

---

3. Provide the host name (not fully qualified domain name [FQDN]) and IP address of the CUCM Publisher.

4. Click **Next**. The next screen allows the entry of the AXL information you created in Task 1. Figure 14-9 shows the AXL Configuration Information screen.

Figure 14-9 AXL Configuration Information Screen



It will populate the application administration credentials automatically. It is not recommended that these credentials be utilized.

5. Enter the username (**AXL_Admin**) and password (**cisco**) of the AXL user created in Task 1.

6. Click **Next**.

   Assuming successful validation of the AXL user information, the wizard progresses to the Security Password Configuration entry. The security password was created during the OS install and should be provided by your instructor. (In Lab C-1, the password was set as **ccnacert**.) This security password must match that which was configured on the CUCM Publisher upon its initial installation. The security password is necessary to provide synchronization access to the Publisher for outside applications, even its own cluster subscribers.

7. Enter the security password in each field, and then click **Next**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

8. Finally, you arrive at the wizard's confirmation screen. It will present the information you've entered for validation.

   a. If all is well, click **Confirm**.

   b. If not, click **Back** and alter any necessary entries.

9. Upon confirmation, the postinstall wizard is complete. Click the **Home** button to access the CUPS administration page.

Feel free to explore the System Dashboard and/or Topology pages if so desired. Regardless of which option you select, you'll need to log in. To do this, enter the application administration credentials and click **Login**.

Step 2-2: Upload a License File (Optional)

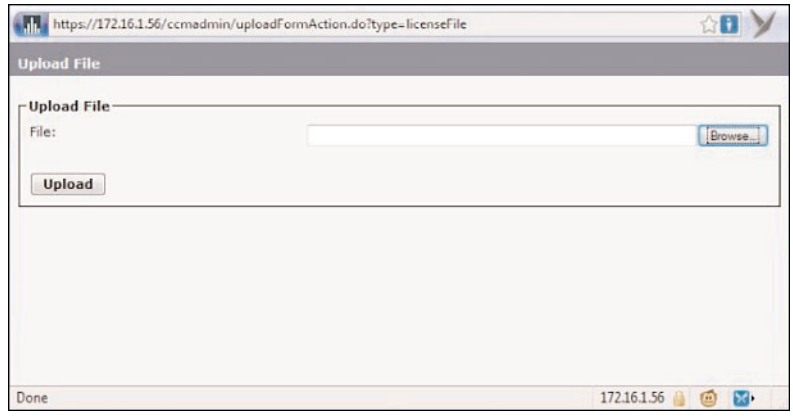
The license file is crucial to maintain operation of the Presence Server. It will operate in Evaluation mode for 90 days postinstall to provide adequate time to acquire and install a valid license file. Fortunately, that also provides more than ample time for our purposes for these labs. No functionality will be lost or hampered by the lack of a license file until the 90-day timer expires.

After it is acquired, the license file can be installed through the CUPS Administration page. Follow these steps:

1. Navigate to **System > Licensing > License File Upload**.

   Figure 14-10 shows the License File Upload screen.

Figure 14-10 License File Upload Screen



2. Click the **Upload License File** button.
3. Click the **Browse** button.
4. Select the directory in which the license file is stored.
5. Click the license file itself and click **Open**.
6. Click **Upload**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-3: Activate Services

By default, all services are deactivated on the Presence Server. To function properly, these services must be activated. Services are administered through the Serviceability page. Follow these steps to activate services:

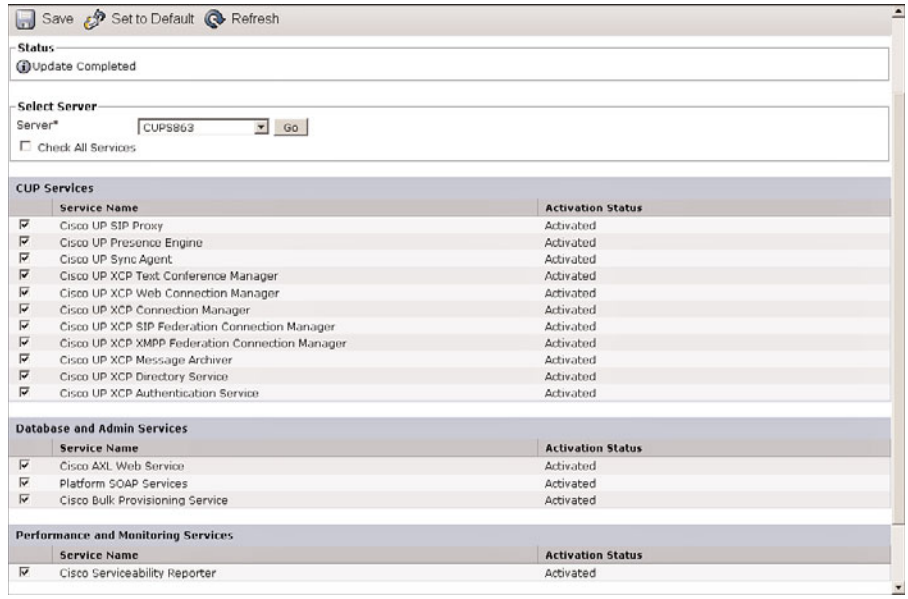
1. From the CUPS Administration page, click the Navigation drop-down list in the upper-right corner of the screen and select **Cisco Unified Serviceability**.
2. Click **Go**.

Note: The first step here is to activate services. Only activated services will start. Deactivated services will not respond to system requests until activated.

3. Navigate to **Tools > Service Activation** to see the status of all services. Note the Activation Status column. All services should show as Deactivated.
4. The most efficient way to get all services going is to select the **Check All Service** check box near the top of the screen.
5. Click **Save**.

Figure 14-11 shows the resulting Service Activation page after the **Save** button has been clicked. It can take a couple of minutes for the screen to refresh initially.

Figure 14-11 Service Activation Screen



Once again, note the Activation Status column. All services should show as Activated as in the figure. It will take from a few minutes to a half-hour for all services to properly start on a fully populated production system. A new lab installation usually will take ten minutes or less for all services to start. Be patient with it.

Note: To monitor service progress, navigate to **Tools > Control Center-Feature Services**. Some services, such as those dealing with XCP functions, do not start until they are actually needed and called upon by the system.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-4: Add a Presence Gateway

Return to the Cisco Unified Presence Administration page using the Navigation drop-down list at the upper right of the screen. We've already established initial connectivity between CUCM and CUPS with regard to AXL functions. Follow these steps to add a the CUCM Publisher as a Presence Gateway:

1. To verify this, navigate to **System > CUCM Publisher**. It will make contact and send test messages to CUCM and return results to you after a moment. AXL, of course, isn't the only connectivity dependency we configured on the CUCM side. You also built SIP and CTI connections. In this step, you will establish the SIP connectivity between CUCM and CUPS.
2. Navigate to **Presence > Settings**.
3. Verify that **CUPS-SIP-Trunk** (created in CUCM) is selected in the CUCM SIP Publish Trunk drop-down list.
4. Leave the other parameters on this screen at their default settings.
5. Click **Save**.

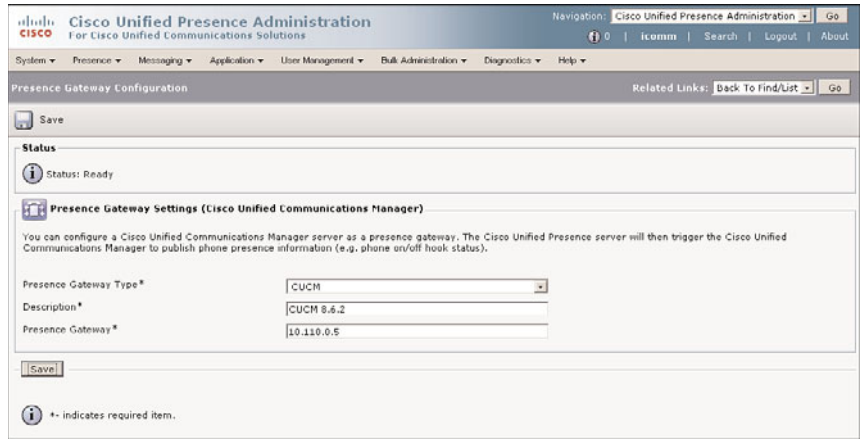
Step 2-5: Add CUCM as a Presence Gateway

In this case, we're adding the CUCM as a Presence gateway so that phone presence status (on-/off-hook) can be exchanged. Follow these steps:

1. Navigate to **Presence > Gateways**.
2. Click **Add New**.

   Figure 14-12 shows the Presence Gateway Settings page.

Figure 14-12 Presence Gateway Settings



3. Leave the Presence Gateway Type field defaulted to **CUCM**.
4. Enter a relevant description.
5. Enter the Publisher's IP address (10.*x*0.0.5, where *x* is the pod number).
6. Click **Save**.

Note: If you have access to Microsoft Exchange, you should create an additional Presence gateway. Specify the gateway type as **Exchange – WebDav** for Exchange 2003, or **Exchange – ESW Server** for Exchange 2007/2010. Enter a username and password with permission to view rights on the Exchange server. With that, you have just enabled integration with Outlook and Calendaring.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-6: Activating Desk Phone Control/Microsoft RCC

Desk phone control is accomplished using CTI functions. This is one of the more useful and powerful functions available with Cisco Unified Presence. It allows the control of desk phone functions through a soft client on the desktop.

Note: Newer versions of CUPS changed the names of some menus. Follow the steps based on the version you have.

1a. (If using CUPS version 8.6.3 or later) Navigate to **Application > Microsoft RCC > Settings** to configure the features.

1b. (If using an earlier version of CUPS) Navigate to **Application > Desk Phone Control > Settings** to configure the features.

2. By default, desk phone control is turned off. Select **On** from the Application Status drop-down list.

Note: The Application Username field is prepopulated. The username defaults to CtiGw. This is the CTI user we configured in Task 1. Assuming that you kept the same name as recommended, no change is necessary. If you did change the CTI username, enter the name you configured previously.

---

3. No username is complete without a password, so enter **cisco** in the appropriate fields as well.

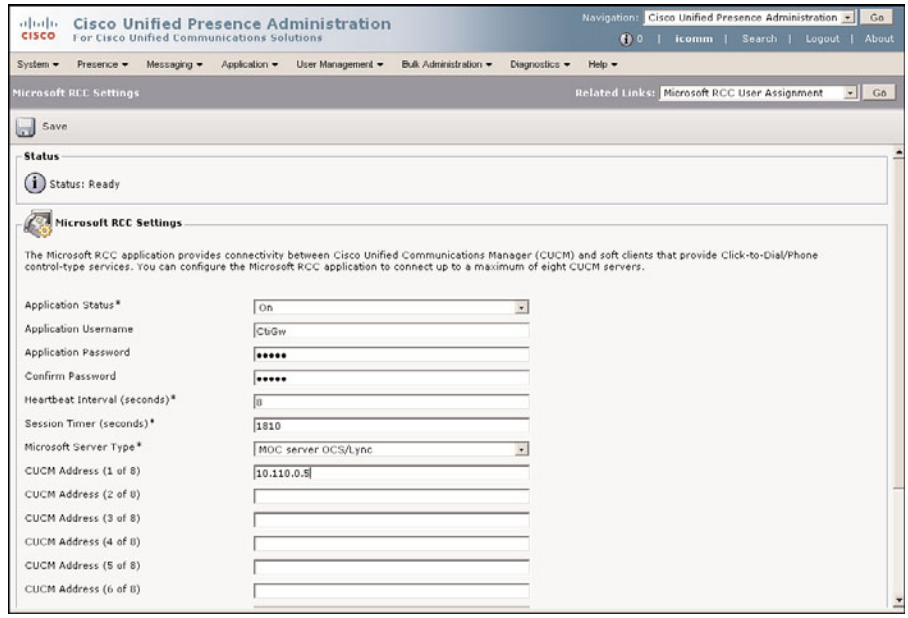
4. Enter the CUCM Publisher's IP address (10.*x*0.0.5, where *x* is the pod number) in the CUCM Address (1 of 8) field.

5. If you have CUCM subscribers in the lab, enter their IP addresses in the CUCM Address (2 of 8) field and so on.

6. The remaining fields can be left at their default settings.

Figure 14-13 shows the Desk Phone Control Settings page with these parameters filled out. **Note:** Your CUCM address will be different than what is shown.

Figure 14-13 Desk Phone Control/Microsoft RCC Settings



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-7: Enable Users for Desk Phone Control/Microsoft RCC

The next step is to enable users for Desk Phone Control/Microsoft RCC. Follow these steps:

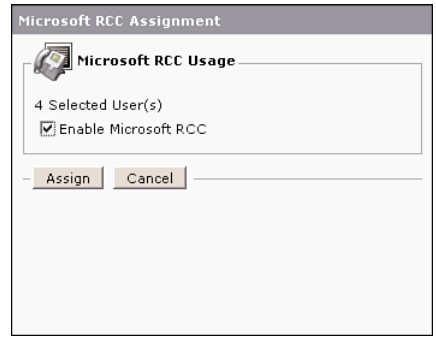
1a. (If using CUPS version 8.6.3 or later) Navigate to **Application > Microsoft RCC > User Assignment**.

1b. (If using an earlier version of CUPS) Navigate to **Application > Desk Phone Control > User Assignment**.

2. Click **Find**. Note that the Assigned Desk Phone Control (Microsoft RCC in CUPS 8.6.3) column on the right side of the screen is blank.

Figure 14-14 shows the Desk Phone Control Usage page.

Figure 14-14 Desk Phone Control/Microsoft RCC Usage



3. Select the check boxes for users who should be provided this feature, and then click **Assign Selected Users**. A pop-up window will appear stating the number of selected users.

4a. (If using CUPS version 8.6.3 or later) Select the **Enable Microsoft RCC** check box and click **Assign**.

4b. (If using an earlier version of CUPS) Select the **Enable Desk Phone Control** check box and click **Assign**.

You should now see a check mark next to each selected username in the Assigned Desk Phone Control/Microsoft RCC column.

Step 2-8: Activate the IP Phone Messenger

Some of the IPPM configuration was done on the CUCM side in Task 1. The final piece of that configuration is here on the CUPS side. Follow these steps:

1. Navigate to **Application > IP Phone Messenger > Settings** to continue the configuration.

2. The service should be set to **On** in the IPPM Application Status drop-down list. If it is not, select **On**.

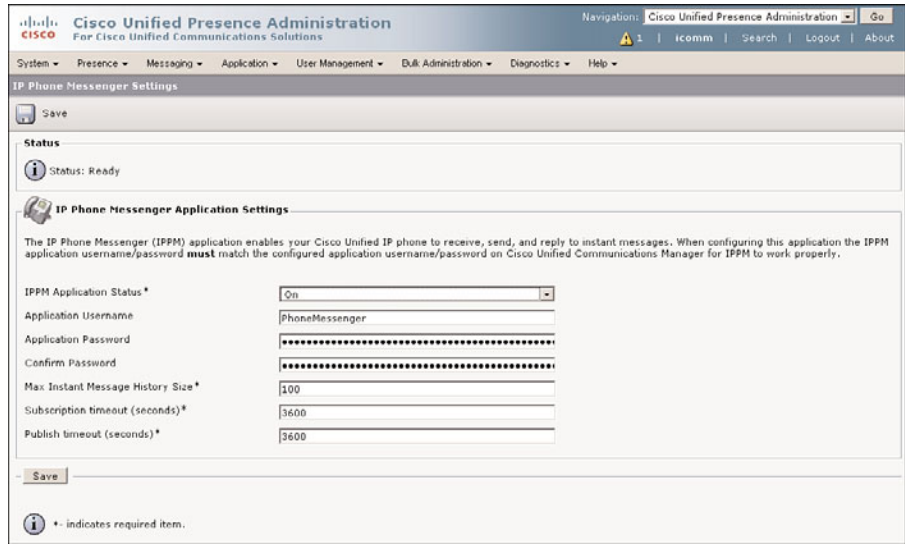
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. If you used PhoneMessenger for the IPPM user configured on CUCM as suggested earlier, leave the Application Username field as it is and simply enter **cisco** for the password information in the relevant blanks.

   Figure 14-15 shows the IP Phone Messenger Application Settings page.

Figure 14-15 IP Phone Messenger Application Settings



4. Click **Save**.

Task 3: Configure CUPC/Jabber Profile

The configuration pieces dealing with the CUPS-CUCM interaction is complete. What remains is to configure the client-related aspects that will control the user experience with the desktop client. CUPC, or Jabber as it's now called, gets its configuration parameters from both the CUPS server and CUCM. CUPS provides profile-specific information that will be configured in the tasks to come. CUCM provides call control for the client in both soft phone and desk phone modes. The following steps need to be completed for users to log in to the CUPC/Jabber client:

- Configure CUPC settings
- Configure CUPC voicemail
- Configure CUPC conferencing
- Configure CUPC CTI access
- Configure CUPC LDAP access
- Configure a CUPC audio profile
- Configure a CUPC CCMCIP profile
- Enable user calendar integration

Note: As you complete these steps, you will often need to add users to the various profiles created in this section. Also keep in mind that some of the profiles (for example, CTI Profile) are automatically created a short time after the installation is complete. Be sure to mark one instance of each profile as the default for the system. This will provide some automation of the profile selection as users are added.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-1: Configure CUPC Settings

The basic settings necessary for CUPC/Jabber to function are similar to those of any Cisco IP Phone. At the core of the functionality of the phone lies the TFTP server. Follow these steps to configure CUPC settings:

1a. (If using CUPS version 8.6.3 or later) Navigate to **Application > Cisco Jabber > Settings**.

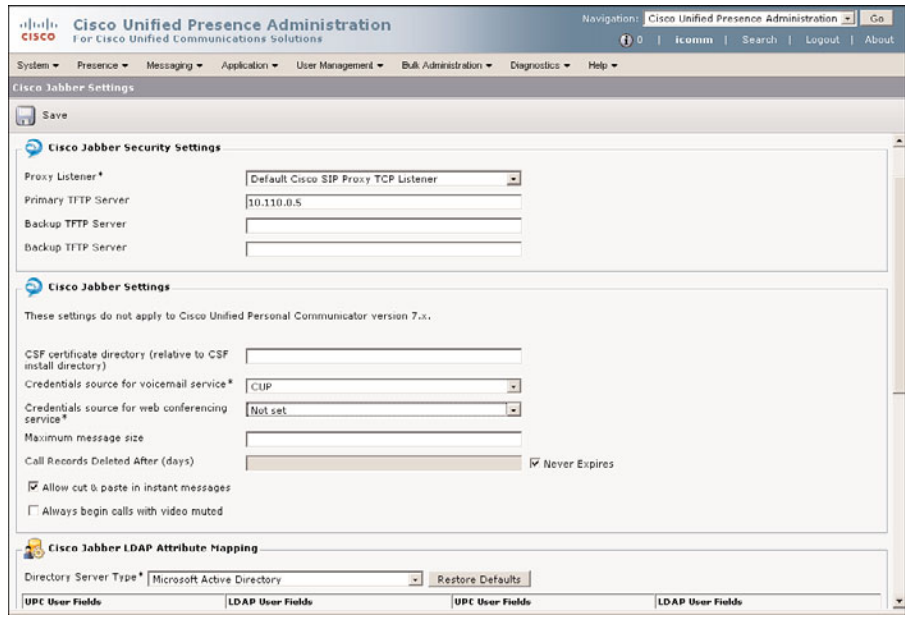
1b. (If using an earlier version of CUPS) Navigate to **Application > Cisco Unified Personal Communicator > Settings**.

2. Enter the TFTP server address (usually the Publisher's IP address) in the Primary TFTP Server field.

3. If you want the Presence Server to utilize the same login credentials for Cisco Unity Connection voicemail as they use to log in to CUPC/Jabber, select **CUP** from the Credentials Source for Voicemail Service drop-down list.

Figure 14-16 shows the Unified Personal Communicator Settings screen.

Figure 14-16 Unified Personal Communicator Settings



4. Leave the remaining fields at their default settings for purposes of this lab.

5. Click **Save** to complete the configuration.

Step 3-2: Configure CUPC Voicemail—Voicemail Server

Voicemail configuration is comprised of three components. These are the Voicemail Server, Mailstore, and Voicemail Profile. To that end, each needs to be configured individually. Follow these steps to configure the Voicemail Server:

1a. (If using CUPS version 8.6.3 or later) To configure the Voicemail Server, navigate to **Application > Cisco Jabber > Voicemail Server**.

1b. (If using an earlier version of CUPS) To configure the Voicemail Server, navigate to **Application > Cisco Unified Personal Communicator > Voicemail Server**.

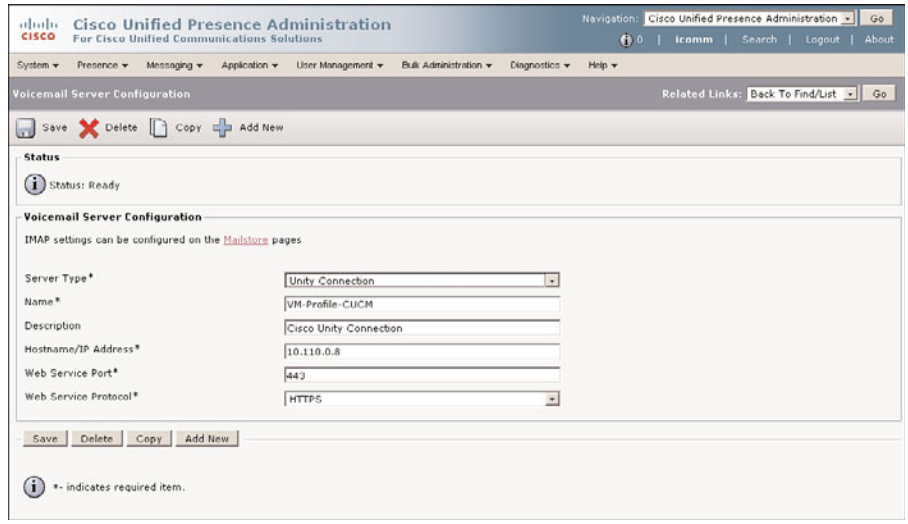
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

2. Click **Add New**.

   Figure 14-17 shows the Voicemail Server Configuration screen.

Figure 14-17 Voicemail Server Configuration



3. Select **Unity Connection** from the Server Type drop-down list.
4. Enter **VM-Profile-CUCM** in the Name field.
5. Enter **Cisco Unity Connection** in the Description field.
6. Enter the IP address of the Voicemail Server (10.*x*0.0.8, where *x* is your pod number) in the Hostname/IP Address field.
7. The Web Service Port field should be set to **443**.
8. The Web Service Protocol field should be set to **HTTPS**.
9. Don't forget to click **Save** before exiting this screen.

Step 3-3: Configure CUPC Voicemail—Mailstore

The next step is the Mailstore configuration. Follow these steps:

1a. (If using CUPS version 8.6.3 or later) Navigate to **Application > Cisco Jabber > Mailstore** to begin this configuration.

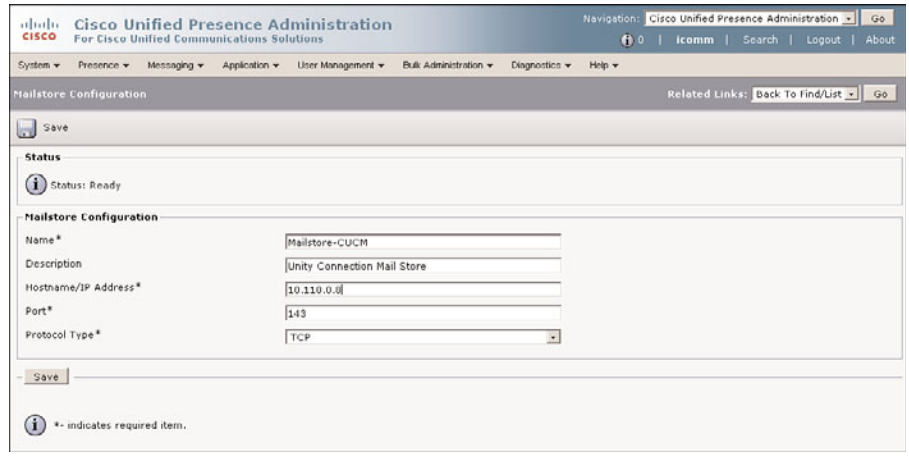
1b. (If using an earlier version of CUPS) Navigate to **Application > Cisco Unified Personal Communicator > Mailstore** to begin this configuration.

Figure 14-18 shows the Mailstore Configuration screen.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 14-18 Mailstore Configuration



2. Enter **Mailstore-CUCM** in the Name field.
3. Enter **Unity Connection Mail Store** in the Description field.
4. Enter the IP address of the Unity Connection server 10.*x*0.0.8, where *x* is your pod number.
5. Leave the Port field set to **143** and the Protocol Type field set to **TCP**.
6. Click **Save** to complete the configuration.

Step 3-4: Configure CUPC Voicemail—Voicemail Profile

The Voicemail Profile ties the two previous components together and is associated with the user(s). Configure the Voicemail Profile by following these steps:

1a. (If using CUPS version 8.6.3 or later) Navigate to **Application > Cisco Jabber > Voicemail Profile**.

1b. (If using an earlier version of CUPS) Navigate to **Application > Cisco Unified Personal Communicator > Voicemail Profile**.

2. Click **Add New** to begin this configuration.

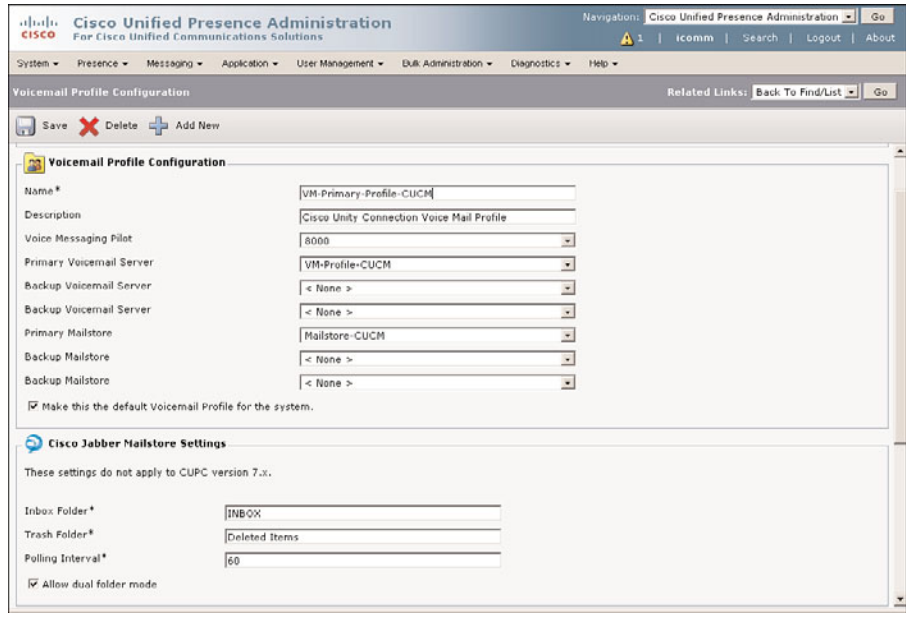
   Figure 14-19 shows the Voicemail Profile Configuration screen.

3. Enter **VM-Primary-Profile-CUCM** in the Name field.
4. Enter **Cisco Unity Connection Voice Mail Profile** in the Description field.
5. Select **8000** from the Voice Messaging Pilot drop-down list. The voicemail pilot number is the same one used on the phones in CUCM (this is synced from CUCM).
6. Select **VM-Profile-CUCM** from the Primary Voicemail Server drop-down list.
7. Select **Mailstore-CUCM** from the Primary Mailstore drop-down list.
8. Select the **Make this the default Voicemail Profile for the system** check box. This will allow autoassignment of users to this profile unless otherwise configured.
9. A pop-up window will open informing you that changing the default will not update users already synced from CUCM. Click **OK** to close the window.
10. Add users to the profile by clicking the **Add Users to Profile** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 14-19 Voicemail Profile Configuration



11. A pop-up window will appear that will allow the selection of users. When all desired users are selected, click **Add Selected** to close the pop-up window. The users selected will populate to the bottom of the screen.

12. Click **Save** to complete the process.

Step 3-5: Configure CUPC Conferencing (Optional)

Cisco conferencing solutions provide both on-premise and cloud-based solutions. Fortunately, either can be configured for CUPC/Jabber users. (Skip this step if you do not have a MeetingPlace or WebEx account.) Follow these steps to configure CUPC Conferencing:

1a. (If using CUPS version 8.6.3 or later) Navigate to **Application > Cisco Jabber > Conferencing Server**.

1b. (If using an earlier version of CUPS) Navigate to **Application > Cisco Unified Personal Communicator > Conferencing Server**.

2. Click **Add New** to begin the configuration.

   Figure 14-20 shows the Conferencing Host Configuration screen.

3. Provide a meaningful name and description.

4. Enter the IP address or host name of the conferencing server.

5. Leave the Port field set to **80** and the Protocol field set to **HTTP**.

6. Select the server type appropriate to your situation.

   The drop-down list includes MeetingPlace Classic, MeetingPlace Express, and WebEx. If you choose a WebEx integration, you'll need to provide the Site ID and Partner ID as well.

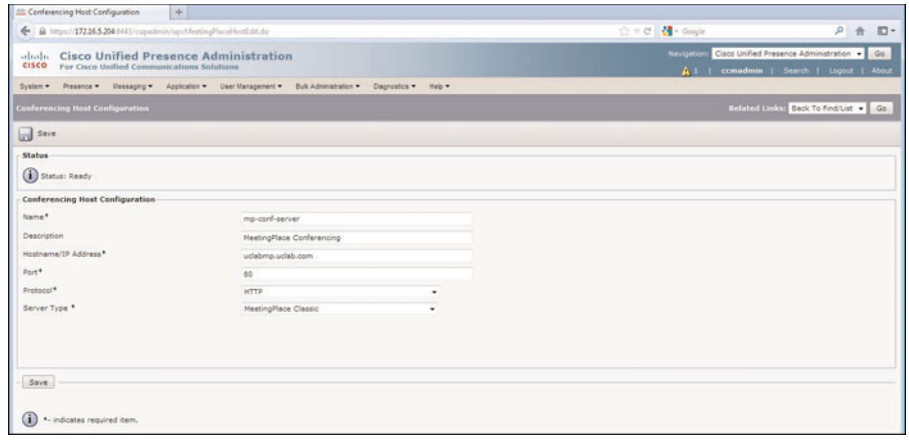
7. Click **Save** to complete the configuration.

   The next part of the conferencing configuration is the Conferencing Profile.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

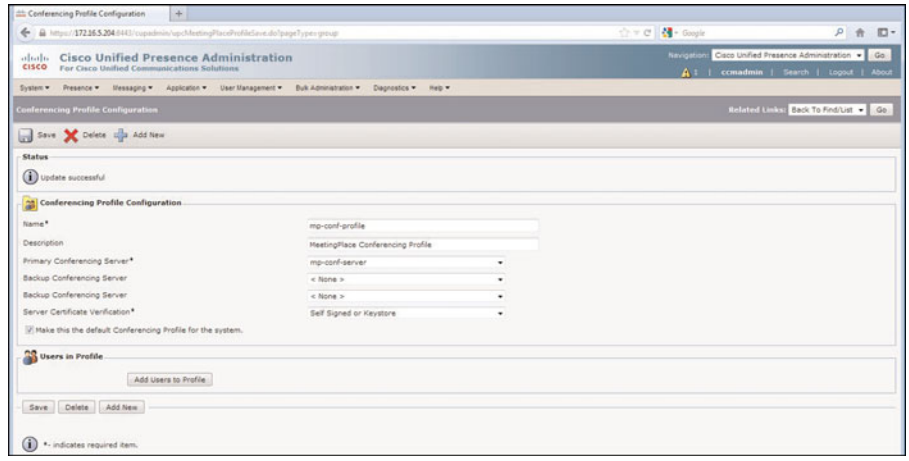
Figure 14-20 Conferencing Host Configuration



8. Navigate to **Application > Cisco Unified Personal Communicator > Conferencing Profile**.
9. Click **Add New** to continue.

   Figure 14-21 shows the Conferencing Profile Configuration screen.

Figure 14-21 Conferencing Profile Configuration



10. Provide a meaningful name and description.
11. In the Primary Conferencing Server field, select the conferencing server you just configured. If so desired, select the **Make this the default Conferencing Profile for the system** check box.
12. Add users to the profile by clicking the **Add Users to Profile** button.
13. A pop-up window will appear that will allow the selection of users. When all desired users are selected, click **Add Selected** to close the pop-up window. The users selected will populate to the bottom of the screen.
14. Click **Save** to complete the process.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-6: Configure CUPC CTI Access

Note: The CTI server list is automatically created, so feel free to skip this step and move directly to the CTI Gateway Profile creation. However, if you want to create your own, feel free to do so.

For CUPC/Jabber to make use of the CTI settings configured thus far, a CTI profile has to be created. Like other profiles in this task, a server is configured and the profile ties to it. Follow these steps to select the CTI Server:

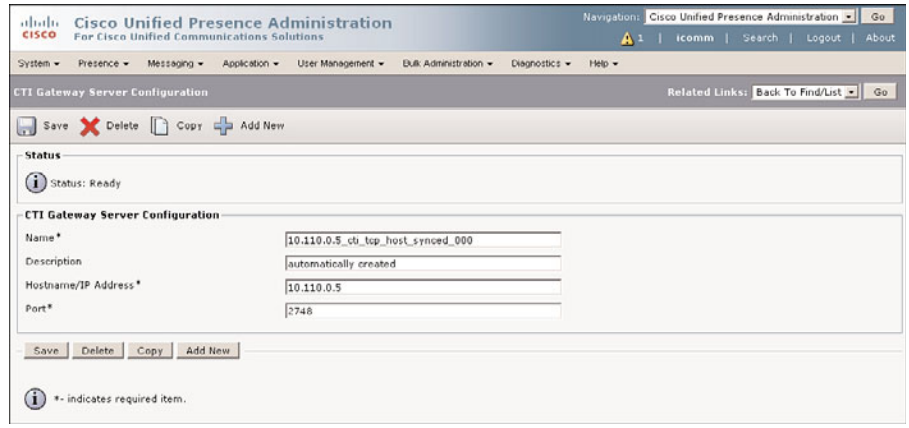
1a. (If using CUPS version 8.6.3 or later) To create a CTI server configuration, navigate to **Application > Cisco Jabber > CTI Gateway Server**.

1b. (If using an earlier version of CUPS) To create a CTI server configuration, navigate to **Application > Cisco Unified Personal Communicator > CTI Gateway Server**.

2. Click **Add New**.

Figure 14-22 shows the CTI Gateway Server Configuration screen.

Figure 14-22 CTI Gateway Server Configuration



3. Provide a meaningful name and description.

4. Enter the CUCM Publisher's address or host name.

5. Leave the Port field set at **2748**.

6. Click **Save**.

Step 3-7a : Configure CUPC CTI Gateway Profile for CUPS Version 8.6.3 or Greater

If you are using an earlier version of CUPS, skip to Step 3-7b. Otherwise, follow these steps to configure a CTI Gateway Profile:

1. Configure a new CTI Gateway Profile by navigating to **Application > Cisco Jabber > CTI Gateway Profile**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

2. The CTI Gateway Profiles are already created; one for each of the device pools on CUCM. Click **Find**.
3. Click the Profile Name field with the **Madison DP** in the name.
4. Select the **Make this the default CTI Gateway Profile for the system** check box.
5. Add users to the profile by clicking the **Add Users to Profile** button.
6. A pop-up window will appear that will allow the selection of users. When all desired users are selected, click **Add Selected** to close the pop-up window. The users selected will populate to the bottom of the screen.
7. Click **Save** to complete the process.

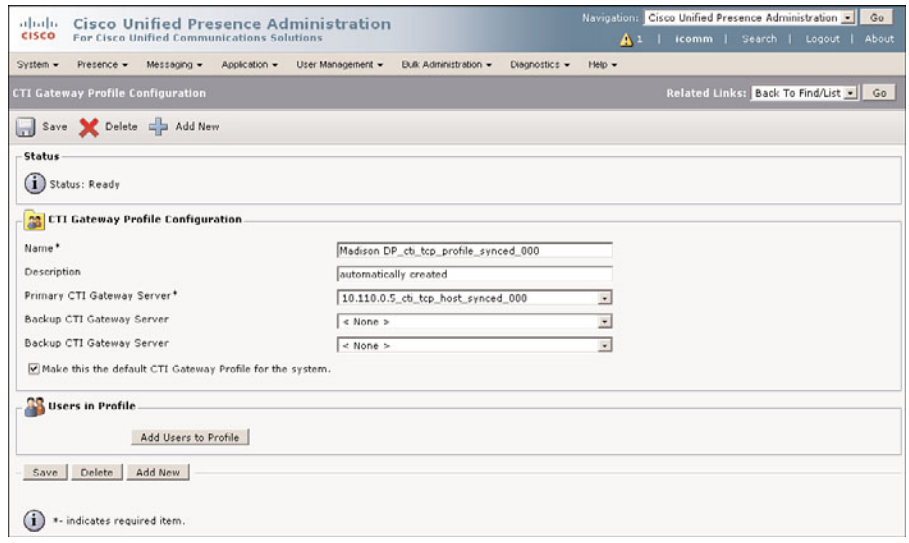
Step 3-7b: Configure CUPC CTI Gateway Profile CUPS Version Prior to 8.6.3

If you are using the 8.6.3 version or later of CUPS, skip to Step 3-8. Otherwise, follow these steps to configure a CTI Gateway Profile:

1. Configure a new CTI Gateway Profile by navigating to **Application > Cisco Unified Personal Communicator > CTI Gateway Profile**.
2. Click **Add New**.

   Figure 14-23 shows the CTI Gateway Profile Configuration screen.

Figure 14-23 CTI Gateway Profile Configuration



3. Provide a meaningful name and description.
4. In the Primary CTI Gateway Server field, click the drop-down list and choose either the server profile you created or one of the automatically created profiles.
5. Select the **Make this the default CTI Gateway Profile for the system** check box.
6. Add users to the profile by clicking the **Add Users to Profile** button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

7. A pop-up window will appear that will allow the selection of users. When all desired users are selected, click **Add Selected** to close the pop-up window. The users selected will populate to the bottom of the screen.

8. Click **Save** to complete the process.

Step 3-8: Configure CUPC LDAP Access

User searches and authentication requests are handled through LDAP integration. The information configured in this step should match that configured in CUCM's LDAP integration configuration.

To configure LDAP, we need a server and a profile. Follow these steps:

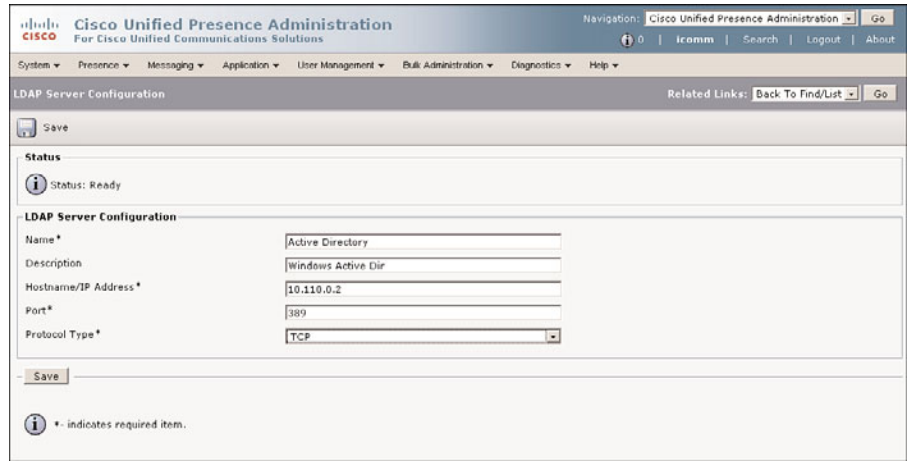
1a. (If using CUPS version 8.6.3 or later) To create the LDAP Profile, navigate to **Application > Cisco Jabber > LDAP Server**.

1b. (If using an earlier version of CUPS) To create the LDAP Profile, navigate to **Application > Cisco Unified Personal Communicator > LDAP Server**.

2. Click **Add New**.

   Figure 14-24 shows the LDAP Server Configuration page.

Figure 14-24 LDAP Server Configuration



3. Provide a meaningful name and description.

4. Enter the IP address of the LDAP server.

Note: The port number should typically be left at 389, though in some cases it will change. For example, it will be 3268 if connecting to an Active Directory Global Catalog Server, 3269 if using SSL connecting to the Global Catalog Server, or 636 if using SSL to connect to a non-Global Catalog Server. In most cases, 389 works just fine.

---

5. Click **Save** to complete the process.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

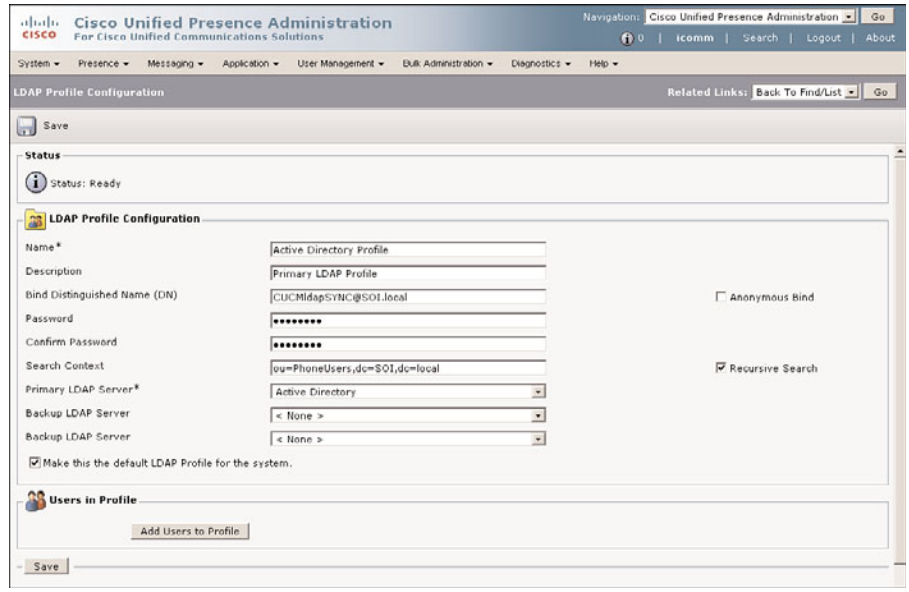
Step 3-9: Configuring CUPC LDAP Access

Follow these steps to create the LDAP Profile:

1. Navigate to **Application > Cisco Unified Personal Communicator > LDAP Profile**.
2. Click **Add New**.

   Figure 14-25 shows the LDAP Profile Configuration screen.

Figure 14-25 LDAP Profile Configuration



3. Provide a meaningful name and description.
4. The Bind Distinguished Name, Password, and Search Context fields can be copied from CUCM's LDAP configuration (**System > LDAP > LDAP Directory** on the CCMAdmin page). Enter the distinguished name, password, and search context.

Note: The search context should optimally be as specific as possible while still maintaining visibility to all user containers. Typically, when using Active Directory, users are in the Users container. In the Search Context field shown in Figure 14-24, the search context then would be cn=Users,dc=domain,dc=com. Instead of "cn," it is also possible to use "ou". If you're unsure of the proper context, download and install one of the many free LDAP browsers and use it to find the proper contexts.

---

5. In the Primary LDAP Server drop-down list, select the LDAP server you just created. If you specified additional LDAP servers, choose them in order of preference for backup LDAP servers. If so desired, select the **Make this the default LDAP Profile for the system** check box.
6. Add users to the profile by clicking the **Add Users to Profile** button.
7. A pop-up window will appear that will allow the selection of users. When all desired users are checked, click **Add Selected** to close the pop-up window. The users selected will populate to the bottom of the screen.
8. Click **Save** to complete the process.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-10: Configure a CUPC Audio Profile

CUPC 8.0 and Jabber support traditional voice tweaking parameters such as Voice Activity Detection (VAD), automatic gain control, echo cancellation, and so on. Follow these steps to configure a CUPC Audio Profile:

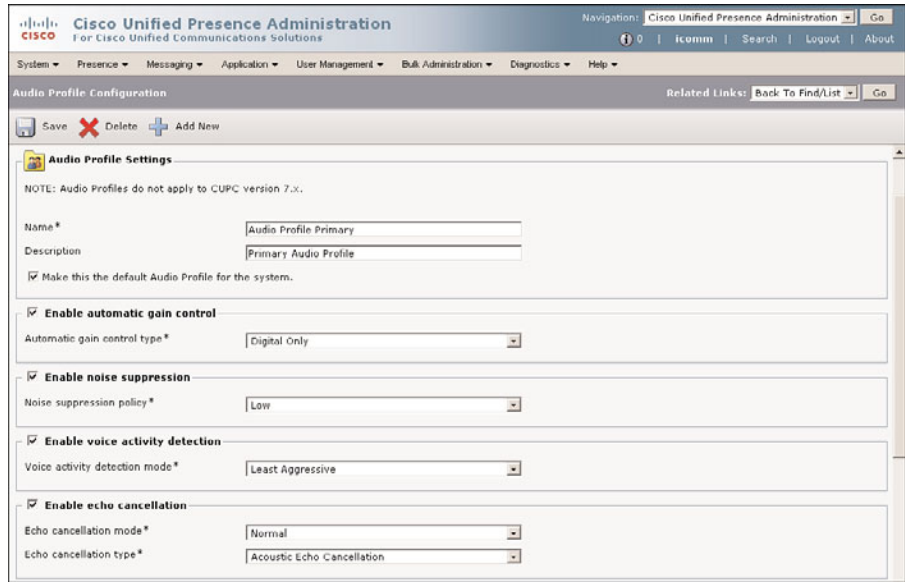
1a. (If using CUPS version 8.6.3 or later) To create a new Audio Profile, navigate to **Application > Cisco Jabber > Audio Profile** (for CUPC 8.0 and higher).

1b. (If using an earlier version of CUPS) To create a new Audio Profile, navigate to **Application > Cisco Unified Personal Communicator > Audio Profile** (for CUPC 8.0 and higher).

2. Click **Add New**.

Figure 14-26 shows the Audio Profile Configuration screen.

Figure 14-26 Audio Profile Configuration



The settings for this one really consist of just the Name and Description fields. Typically, there's no reason to alter any of the default settings. Do feel free to experiment with them, of course. But, for lab purposes, we need not make any changes.

3. Select the **Make this the default Audio Profile for the system** check box.

4. Add users to the profile by clicking the **Add Users to Profile** button.

5. A pop-up window will appear that will allow the selection of users. When all desired users are selected, click **Add Selected** to close the pop-up window. The users selected will populate to the bottom of the screen.

6. Click **Save** to complete the process.

Step 3-11: Configure a CUPC CCMCIP Profile

To retrieve the list of devices associated to a user in CUCM, the Cisco CallManager Cisco IP Phone (CCMCIP) service must be running on CUCM (the CCMCIP is active by default as a network service on CUCM) and a CCMCIP profile must exist on the Presence Server. Follow these steps to create a CUPC CCMCIP Profile:

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

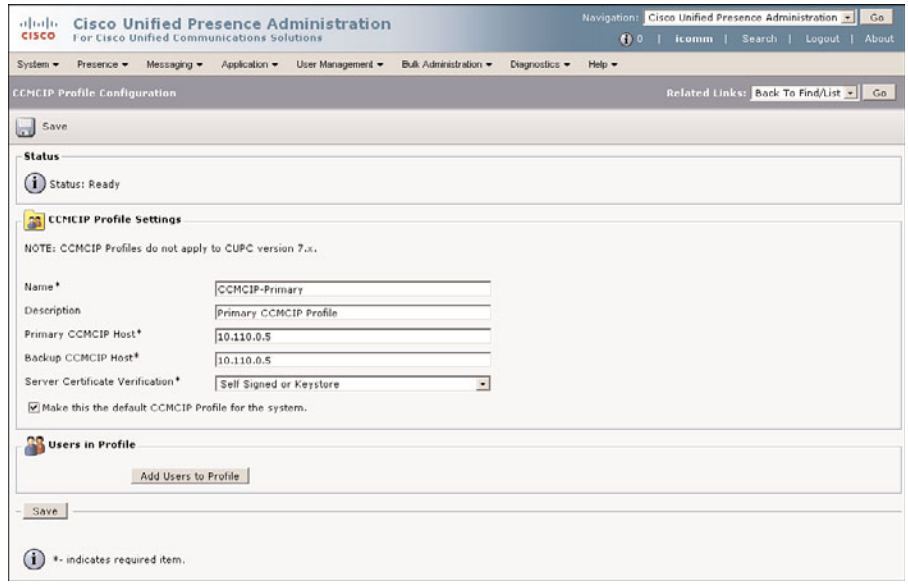
1a. (If using CUPS version 8.6.3 or later) To create a new CCMCIP Profile, navigate to **Application > Cisco Jabber > CCMCIP** (for CUPC 8.0 and higher).

1b. (If using an earlier version of CUPS) To create a new CCMCIP Profile, navigate to **Application > Cisco Unified Personal Communicator > CCMCIP** (for CUPC 8.0 and higher).

2. Click **Add New**.

Figure 14-27 shows the CCMCIP Profile Configuration screen.

Figure 14-27 CCMCIP Profile Configuration



3. Enter a meaningful name and description.

4. The CCMCIP service runs on CUCM, so specify the Publisher in the Primary CCMCIP Host field and Subscriber in the Backup CCMCIP Host field. (Use the Publisher's IP address again if you do not have a Subscriber, as the Backup CCMCIP is a required field.)

5. Leave the Server Certificate Verification field at its default setting.

6. Select the **Make this the default CCMCIP Profile for the system** check box.

7. Add users to the profile by clicking the **Add Users to Profile** button.

8. A pop-up window will appear that will allow the selection of users. When all desired users are selected, click **Add Selected** to close the pop-up window. The users selected will populate to the bottom of the screen.

9. Click **Save** to complete the process.

Step 3-12: Enable User Calendar Integration (Optional)

Note: This option might not show.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Calendaring integration is enabled on a per-user basis at this time. Each user must log in to the CUPUser page and manually enable it. Follow these steps to enable user calendar integration:

1. To do so, have the user open a browser and navigate to

   http://<*cups-ip-address*>/cupuser

2. Navigate to **User Options > Preferences**.
3. At the bottom of the page is a field labeled Include Calendar Information in my Presence Status. Have the user set it to **On.**
4. Click **Save**.

Currently, each user must do this for himself or herself. There is no global or administrative means to do so.

Task 4: Create CSF Devices in CUCM

The Presence Server configuration is complete as is its integration with CUCM. The final element that needs to be put in place is the CSF device in CUCM. This is a phone definition for the CUPC/Jabber client. It allows the CUPC/Jabber client to act as a phone in every manner in which one might expect a Cisco IP Phone to function. The tasks that need to be completed include:

- User/desk phone association
- Create CSF device

Step 4-1: User/Desk Phone Association

Check to be sure that all users are associated with their desk phones. Follow these steps to associate end users with their desk phones:

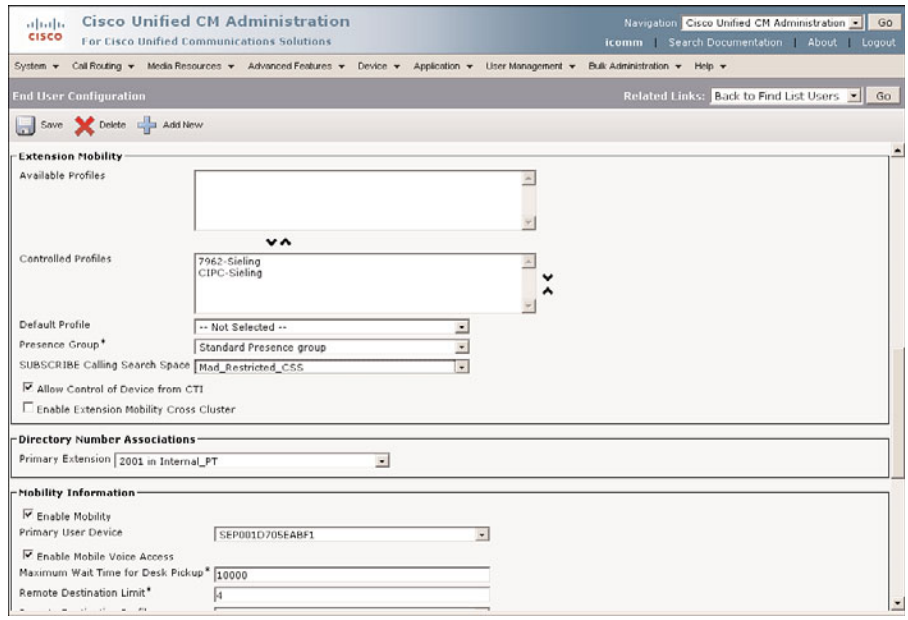
1. On the CCMAdmin page, navigate to **User Management > End User.**
2. Click **Find**. A list of all users will be presented.
3. Click the user in question to view his/her configuration.
4. Ensure that the desk phone device name shows in the Controlled Devices box.
5. Scroll down to the Extension Mobility section and select **Mad_Restricted_CSS** from the SUBSCRIBE Calling Search Space drop-down list. (It has no need to reach out to PSTN destinations.)
6. Ensure that the **Allow Control of Device from CTI** check box is selected.
7. In the Directory Number Associations section, select the user's primary extension from the Primary Extension drop-down list.
8. In the Mobility Information section, if not already checked, select the **Enable Mobility** check box.
9. Select the user's desk phone from the drop-down list next to it.

   Figure 14-28 shows this section of the End User Configuration screen.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

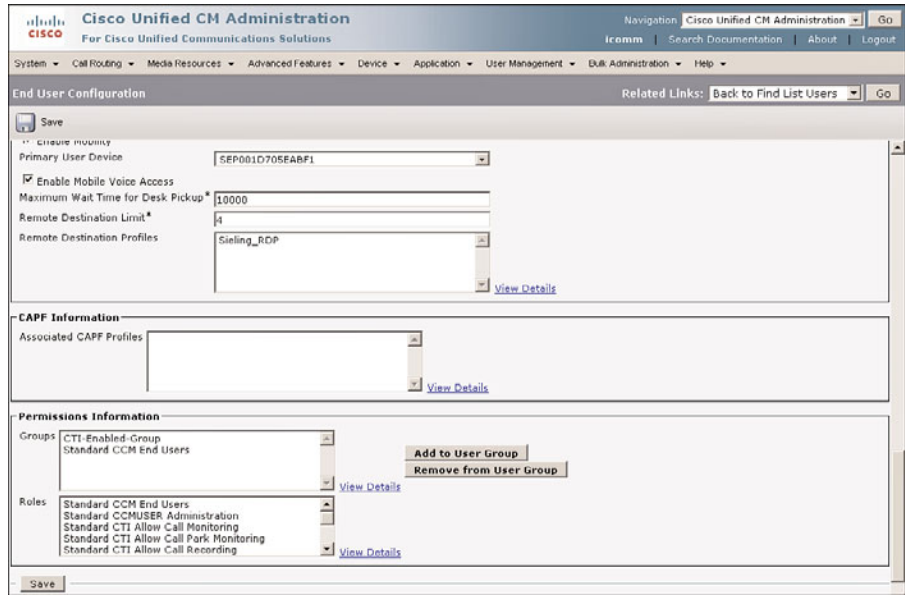
Figure 14-28 End User Configuration



10. Scroll all the way down to the Permission Information section at the bottom of the User page and check the group membership.

    All end users should be members of the Standard CCM End User group (add any missing users to the group, if not already listed as a member). In addition, add CUPC/Jabber enabled users to the CTI-Enabled Group you created earlier. This ensures that they have all the rights/permissions they'll need for desk phone control and similar features. Figure 14-29 shows the User Configuration Permissions information.

Figure 14-29 User Configuration—Permissions Information



11. Click **Save** to complete the configuration.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 4-2: Create CSF Device in CUCM

CUCM provides call control for the soft phone features in CUPC/Jabber. To do so, CUPC/Jabber must be defined in CUCM as a phone. Follow these steps to create the CSF device in CUCM:

1. To do this, open the CUCM CCMAdmin page and navigate to **Device > Phone > Add New**.
2. In the Phone Type drop-down list, scroll down and select **Cisco Unified Client Service Framework** (for CUPC 8.0 and higher).
3. Click **Next**.
4. At this point, the configuration is like any other phone. As of the release of CUPC 8, the naming convention requirements were removed. Typical convention, though not required, is to use "CSF" or "SEP" as a prefix to the user ID. Having a naming convention simplifies troubleshooting by easily identifying the device type and ensuring that it's unique nature throughout the system.

   With the release of Cisco Jabber for Windows and Cisco Jabber for Mac, CUPC is no longer in service. However, the naming rules remained unspecified to support backward compatibility. In the end, whatever naming convention makes sense for your purposes will work as long as each is unique and meaningful.
5. Enter the device name according to the user for whom it is being configured.
6. Configure the following parameters to match the user's desk phone configuration:
   - Description: **CUPC/Jabber**
   - Device Pool: **Madison DP**
   - Phone Button Template: **Standard Client Services Framework**
   - Calling Search Space: **Mad_Employee_CSS**
   - AAR Calling Search Space: **Mad_Unrestricted_CSS**
   - Device Mobility Mode: **On**
   - Owner User ID: <*username of the phone*>
   - Mobility User ID: <*username for the phone*>
   - Primary Phone: <*MAC address of the desk phone*>

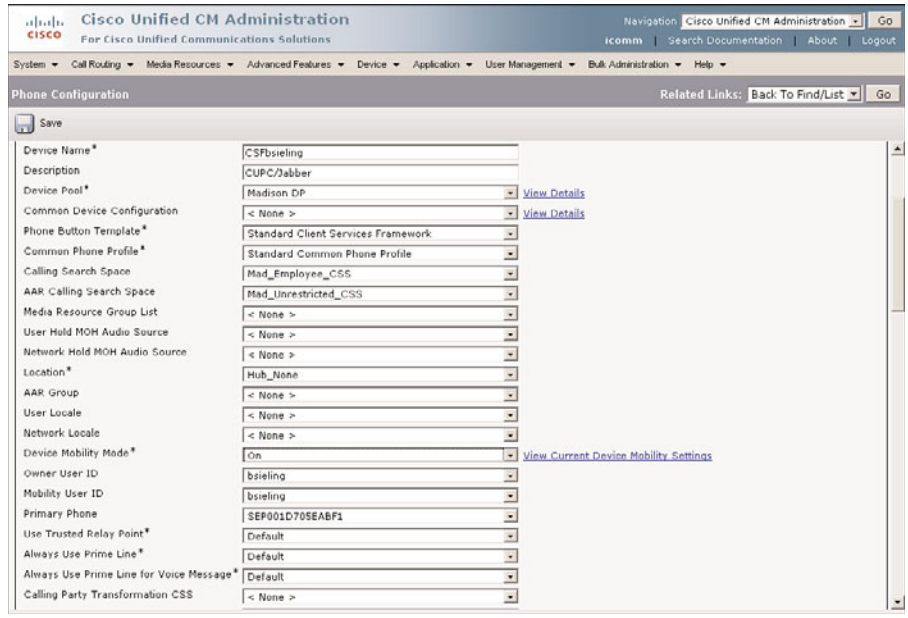
   Figure 14-30 shows how this device configuration page should look.

   Of particular note in the figure are the Owner User ID, Mobility User ID, and Primary Phone fields. Also of importance is the Allow Control of Device from CTI check box. Make sure that it is selected to allow the desktop client and the desk phone to communicate. These must be configured for CUPC/Jabber to function properly.
7. Scroll down to the Protocol Specific Information section.
8. Select **Cisco Unified Client Services Framework – Standard SIP Non-Secure** from the Device Security Profile drop-down list.
9. Select **Mad_Employee_CSS** from the SUBSCRIBE Calling Search Space drop-down list.
10. Select **Standard SIP Profile** from the SIP Profile drop-down list.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

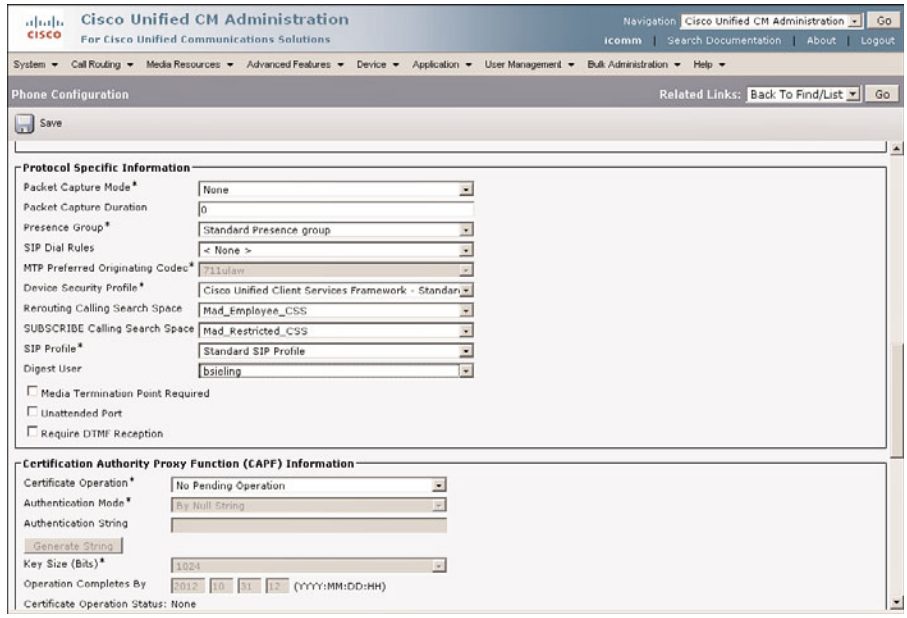
Figure 14-30 CSF Device Configuration Page



11. Select the *<username for the phone>* from the Digest User drop-down list.

Figure 14-31 shows how this should look as part of a CSF device configuration.

Figure 14-31 CSF Device Configuration Page, Continued



12. Click **Save** to complete the configuration.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Note: The Jabber client will need DNS entries to successfully contact the various servers, even if you have them connected using IP addresses. See https://supportforums.cisco.com/docs/DOC-24134 for more details.

Congratulations! The configuration and integration of Cisco Unified Presence Server are complete. Users should now be able to log in to CUPC/Jabber and take advantage of IM, Presence, desk phone control, click to call, soft phone capabilities, and more.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CHAPTER 15

Troubleshooting Cisco Unified Communications Manager Express (CUCME)

A network engineer's greatest asset is being able to avoid problems with advance planning and testing. The second greatest asset is to solve problems quickly and accurately after they happen. This chapter explores the Cisco-recommended troubleshooting process and gives you the chance to spot problems.

Lab 15-1: Troubleshooting Process

Equipment Required

No equipment is required for this lab.

Learning Objectives

Upon completion of this lab, you will be able to

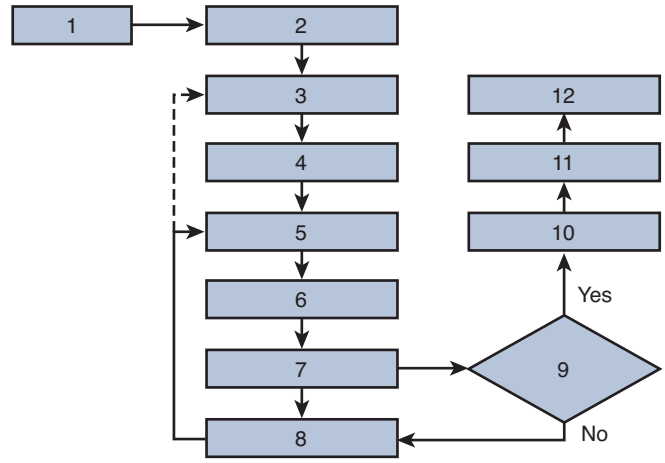
- Use Cisco troubleshooting methodology
- Verify the phone boot process

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Complete the Troubleshooting Methodology Diagram

Figure 15-1 Troubleshooting Methodology Diagram



Using the diagram in Figure 15-1, number each of the troubleshooting methodology steps:

_____ Create Action Plan

_____ Document Facts

_____ Observe Results

_____ Gather Facts

_____ Do Problem Symptoms Stop?

_____ Define Problem

_____ Problem Resolved

_____ Start

_____ Utilize Process

_____ Consider Possibilities

_____ Finished

_____ Implement Action Plan

Task 2: Phone Boot Process

Understanding the phone boot process is essential to troubleshooting phone problems. Number the following list in the order that they occur during the phone boot process:

_____ The phone gets IP address information from DHCP, including option 150.

_____ The phone learns the voice VLAN information by using CDP.

_____ The phone registers with one or more Call Agents.

_____ The phone downloads the configuration file from the TFTP server.

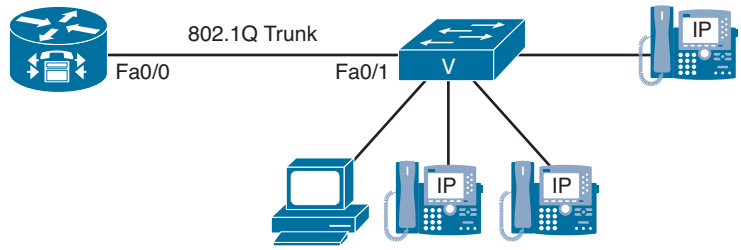
_____ The phone receives power, which might involve receiving PoE from the switch.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab 15-2: Troubleshooting CUCME Configuration

Figure 15-2 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router with voice IOS (see Scenario note)
- Switch that supports voice VLANs (see Scenario note)
- Two or more IP phones (three or more is ideal)

Learning Objectives

Upon completion of this lab, you will be able to troubleshoot common VoIP setup and configuration problems.

Scenario

In this challenge, StartCo, a business with 15 employees, had another technician install a small-business phone system, but it doesn't work. You have been brought in to fix the system and get the first four phones working.

Note: The configurations that are shown in Tasks 2 and 3 are from a 2811 router running IOS Release 12.4(24)T2 and a 2960 switch running IOS Release 12.2(53)SE. Other hardware and IOS versions should work but might require adjustments. If you don't have this equipment, try to find as many mistakes as you can from reading the configurations.

Task 1: Desired Configuration

The requirements for the system are

- 10.225.0.1 /24 for the voice VLAN.
- 10.220.0.1 /24 for the data VLAN.
- 10.221.0.1 /24 for the management VLAN.
- The VLAN numbers should match the second octet of the subnet IP address.
- The first ten addresses for both data and voice VLANs should be reserved for static devices.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- The first desk phone should have number 1000 assigned.
- The second desk phone should have number 1001 assigned.
- The third desk phone should have number 1002 assigned.
- The IP Communicator on a PC should have number 1003 assigned.
- All lines should be dual-line.
- StartCo should be on the display of all phones.
- When any phone calls another, the name as well as the number should show.
- The Phone Directory button should show the names for all phones and be able to dial.

Task 2: Router Configuration

Example 15-1 shows the documentation from the router. Write all the corrections, additions, and deletions necessary to fix the configuration to match the requirements in Task 1. If possible, test your configuration on a router to verify.

Example 15-1 StartCo Router Configuration

```
hostname StartCoRouter
!
ip dhcp excluded-address 10.220.0.1 10.221.1.10
!
ip dhcp pool Data
   network 10.220.0.0 255.255.255.0
   default-router 10.230.0.1
!
ip dhcp pool Voice
   network 10.225.0.0 255.255.255.0
   default-router 10.225.0.1
   option 150 ip 11.226.0.1
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.220
 encapsulation dot1Q 220
 ip address 10.220.0.1 255.255.255.0
!
interface FastEthernet0/0.221
 encapsulation dot1Q 121
 ip address 10.222.0.1 255.255.255.0
!
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
interface FastEthernet0/0.225
 encapsulation dot1Q 126
 ip address 10.225.0.1 255.255.255.0
!
telephony-service
 no auto-reg-ephone
 max-ephones 2
 max-dn 6
 exit
!
ephone-dn  1  dual-line
 number 1000
 name Person 1
!
ephone-dn  2
 number 1001
 name Person 2
!
ephone-dn  3
 number 1002
 name Person 3
!
ephone  1
 mac-address 00aa.bbbb.ccdd
 button  1:1
!
ephone  2
 mac-address 00bb.1234.abcd
 button  1:1
!
ephone  3
```

Task 3: Switch Configuration

Example 15-2 shows the documentation from the switch. Write all the corrections, additions, and deletions necessary to fix the configuration to match the requirements in Task 1. If possible, test your configuration on a switch to verify.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Example 15-2 StartCo Switch Configuration

```
vlan 220
 name Data
!
vlan 221
 name Management
!
vlan 255
 name Voice
!
hostname StartCoSwitch
!
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 220
 switchport mode access
 no cdp enable
 shutdown
!
interface FastEthernet0/3
 switchport access vlan 220
 switchport mode access
 no cdp enable
 power inline never
!
interface FastEthernet0/4
 switchport access vlan 220
 switchport mode access
 no cdp enable
 power inline never
!
interface FastEthernet0/5
 switchport access vlan 220
 switchport mode access
 no cdp enable
 power inline never
!
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
interface FastEthernet0/6
 switchport access vlan 220
 switchport mode access
 no cdp enable
 power inline never
!
<output omitted>
!
interface Vlan221
 ip address 10.221.0.2 255.255.255.0
!
ip default-gateway 10.223.0.1
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

This page intentionally left blank

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

CHAPTER 16

Troubleshooting CUCM

There is a great deal to be learned in troubleshooting CUCM, in general. There are so many pieces that must properly align to build a stable and robust Unified Communications solution. The best advice that can be given in a particular situation is to use the troubleshooting methodology provided in both the CCNP Voice Certification Guide and this lab manual. As you get more practice at implementing and troubleshooting the things that commonly go awry, you will begin to get a sense of where certain types of problems can and cannot arise. Just as valuable a tool is the simple drawing. Draw out the traffic flow and call flow and direction (inbound or outbound), and in the majority of cases, the problem will present itself to you clearly. Information is the key element in any troubleshooting endeavor.

Lab 16-1: Troubleshooting Process

Equipment Required

No equipment is required for this lab.

Learning Objectives

Upon completion of this lab, you will be able to

- Verify the phone boot process
- Use Cisco troubleshooting methodology

Task 1: Complete the Troubleshooting Methodology Diagram

Using the diagram in Figure 16-1, number each of the following troubleshooting methodology steps:

_____ Create Action Plan

_____ Document Facts

_____ Observe Results

_____ Gather Facts

_____ Do Problems Symptoms Stop?

_____ Define Problem

_____ Problem Resolved

_____ Start

_____ Utilize Process

_____ Consider Possibilities

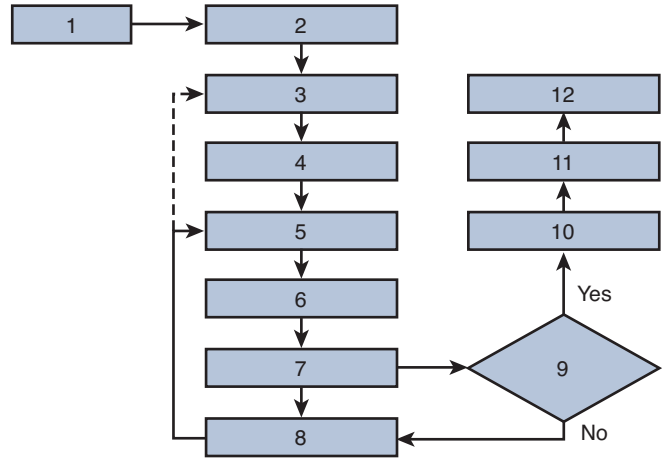
_____ Finished

_____ Implement Action Plan

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 16-1 Troubleshooting Methodology Diagram



Task 2-1: Understand the Phone Boot Process

Understanding the phone boot process is essential to troubleshooting phone problems. Number the following list in the order that the items occur during the phone boot process:

_____ The phone gets IP address information from DHCP, including option 150.

_____ The phone learns the VLAN information from CDP.

_____ The phone registers with one or more Call Agents.

_____ The phone downloads the configuration file from the TFTP server.

_____ The phone receives power, which might involve receiving PoE from the switch.

Task 2-2: Playing "What If?"

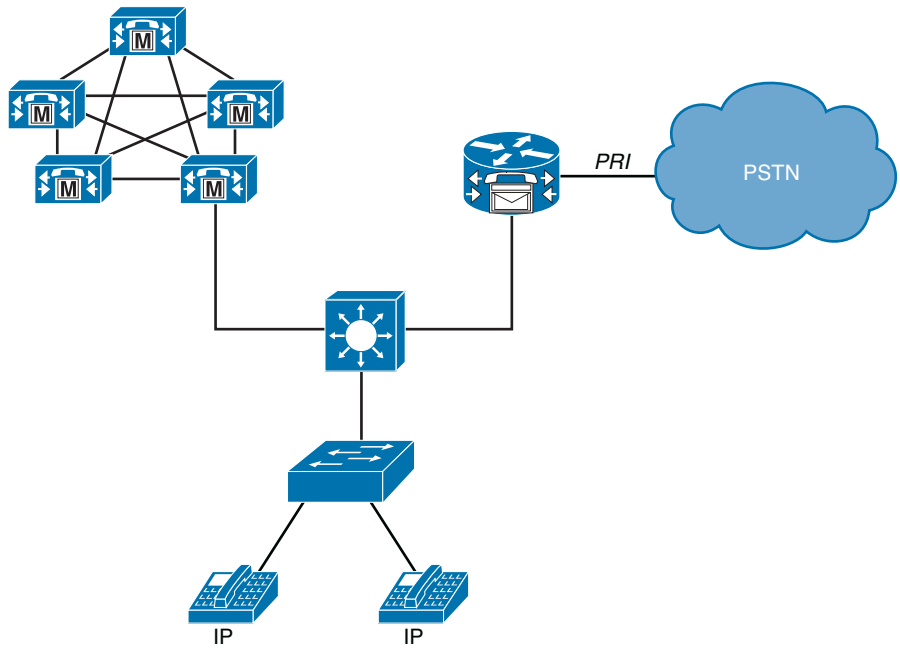
Now that you understand the phone's boot process, put some of that knowledge to use along with the troubleshooting flowchart. This task will be a game of "What if?". A number of scenarios will be presented. Using your understanding of general networking, the phone boot process, and other aspects covered thus far, figure out the most likely source of the problem. Possible answers will follow at the end of the task.

For purposes of this task, use Figure 16-2 as a topological example.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 16-2 "What If?" Topological Diagram



1. What if the phone is connected to the switch but does not power up?

2. What if the phone receives power but does not receive an IP address?

3. What if the phone receives an IP address but does not register to CUCM?

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. What if the phone registers to CUCM and functions normally when initially configured, but when set up at the end user's location, it will not accept configuration changes? That is, changes are made on the phone device page or DN page in CUCM but will not take effect on the phone itself. The phone will, however, respond to a Reset command issued by CUCM.

5. What if the phone registers to CUCM but cannot call anywhere, even to its neighbors?

6. What if a phone calls another phone, only to ring once and drop the call?

7. What if a phone suddenly returns a fast busy signal in the middle of dialing digits?

8. What if a phone returns a fast busy signal after all digits are dialed? Wait, isn't this the same as the last question?

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

9. What if a phone is configured in CUCM but will not make contact with the TFTP server, even though the option 150 has been verified and DHCP issues ruled out?

10. What if the phone boots onto the incorrect VLAN?

The purpose of the "What if?" scenarios is to get your mind moving along the lines necessary to address issues that occur regularly in a world of diverse network topologies and architectures. Remember the advice given in the beginning of this lab. Use Figure 16-2 to map the issue, or draw it out yourself and eliminate possible issues based on available information

Task 3: Dialed Number Analyzer

In troubleshooting call flow, the Dialed Number Analyzer is an excellent tool. It will show the call path from end to end.

Step 3-1: Activate Services

If the Cisco Dialed Number Analyzer and Cisco Dialed Number Analyzer Server services are not already active on CUCM, follow the steps in Lab 9-2, Task 3 to activate them.

Step 3-2: Dialed Number Analyzer

The Dialed Number Analyzer is one of the most useful tools available in CUCM. It is accessed via the Serviceability page.

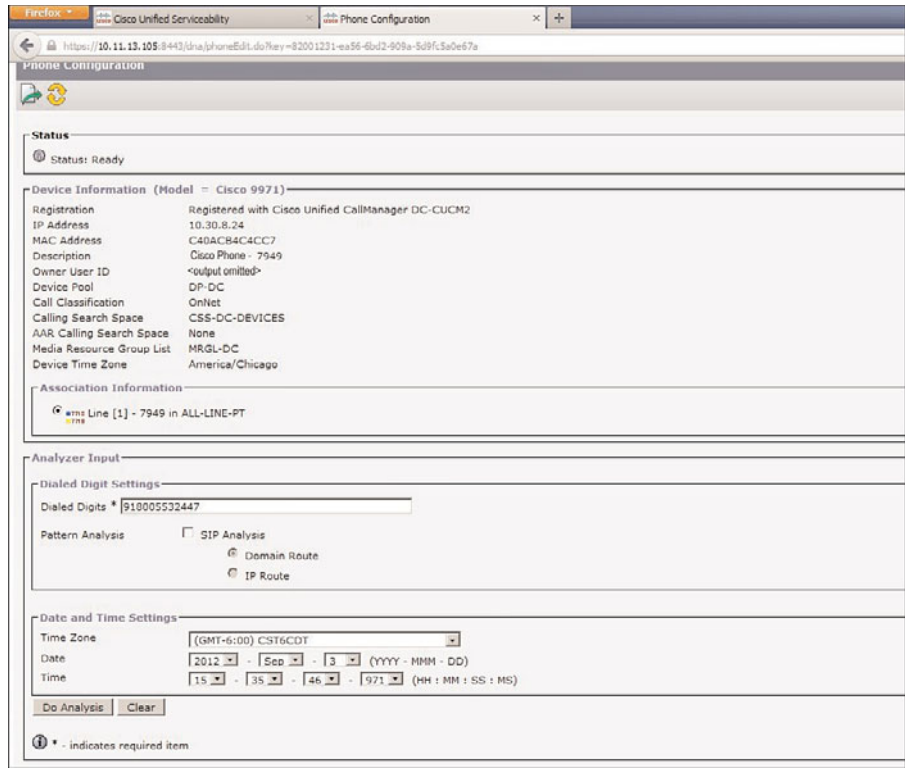
1. Access the CUCM Unified Serviceability page.
2. Navigate to **Tools > Dialed Number Analyzer**. A new window will open. The analysis can be run from the perspective of an individual phone or gateway to test its CSS and call flow validity.
3. Navigate to the **Analysis > Phones** menu.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

4. On the Find and List Phones page, click the hyperlinked device name of the phone assigned to your user account.
5. In the Association Information section, click the **Line [1]** radio button to analyze a call that would be placed from line button 1.
6. In the Analyzer Input section, enter the desired phone number to test in the Dialed Digits field. Figure 16-3 shows an example of this page.

Figure 16-3 Dialed Number Analyzer Phone Configuration



7. Click the **Do Analysis** button to see the results.

Example 16-1 shows the output from a production system. A screen shot wouldn't have been sufficient.

Example 16-1 Dialed Number Analyzer Analysis Output

```
Calling Party Information
    Calling Party = 7949
    Partition = ALL-LINE-PT
    Device CSS = CSS-DC-DEVICES
    Line CSS = CSS-LINE-LD
    AAR Group Name =
    AAR CSS =
Dialed Digits = 918005522447
Match Result = RouteThisPattern
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
    Matched Pattern Information
        Pattern = 9.18[0678][0678]XXXXXXX
        Partition = ALL-LINE-PT
        Time Schedule =
    Called Party Number = 918005532447
    Time Zone = America/Chicago
    End Device = RL-DC
    Call Classification = OffNet
    InterDigit Timeout = NO
    Device Override = Disabled
    Outside Dial Tone = NO

Call Flow

    TranslationPattern :Pattern=
        Partition =
        Positional Match List = 9:18005532447
        Calling Party Number = 7949
        PreTransform Calling Party Number =
        PreTransform Called Party Number =
        Calling Party Transformations
            External Phone Number Mask = NO
            Calling Party Mask =
            Prefix =
            CallingLineId Presentation =
            CallingName Presentation =
            Calling Party Number = 7949
        ConnectedParty Transformations
            ConnectedLineId Presentation =
            ConnectedName Presentation =
        Called Party Transformations
            Called Party Mask =
            Discard Digits Instruction =
            Prefix =
            Called Number =
    Route Pattern :Pattern= 9.18[0678][0678]XXXXXXX
        Positional Match List = 9:18005532447
        DialPlan =
        Route Filter
            Filter Name =
            Filter Clause =
        Require Forced Authorization Code = No
        Authorization Level = 0
        Require Client Matter Code = No
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
        Call Classification =
        PreTransform Calling Party Number = 7949
        PreTransform Called Party Number = 918005532447
        Calling Party Transformations
            External Phone Number Mask = YES
            Calling Party Mask =
            Prefix =
            CallingLineId Presentation = Allowed
            CallingName Presentation = Allowed
            Calling Party Number = 7949
        ConnectedParty Transformations
            ConnectedLineId Presentation = Default
            ConnectedName Presentation = Default
        Called Party Transformations
            Called Party Mask =
            Discard Digits Instruction = None
            Prefix =
            Called Number = 918005522447
    Route List :Route List Name= RL-DC
        RouteGroup :RouteGroup Name= RG-DC
            PreTransform Calling Party Number = 7949
            PreTransform Called Party Number = 918005532447
            Calling Party Transformations
                External Phone Number Mask = Default
                Calling Party Mask =
                Prefix =
                Calling Party Number =
            Called Party Transformations
                Called Party Mask =
                Discard Digits Instructions =
                Prefix =
                Called Number =
            Device :Type= MGCPT1PRIPort
                End Device Name = S0/SU0/DS1-0@DC-3945-vg02.customer.org
                PortNumber = 0
                Device Status = Registered
                AAR Group Name =
                AAR Calling Search Space =
                AAR Prefix Digits =
                Call Classification =
                Calling Party Selection =
                CallingLinePresentation =
                ConnectedLinePresentation =
                Number Of Strip Digits =
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
                CallerID DN =
            Device :Type= MGCPT1PRIPort
                End Device Name = S0/SU0/DS1-1@DC-3945-vg02.customer.org
                PortNumber = 0
                Device Status = Registered
                AAR Group Name =
                AAR Calling Search Space =
                AAR Prefix Digits =
                Call Classification =
                Calling Party Selection =
                CallingLinePresentation =
                ConnectedLinePresentation =
                Number Of Strip Digits =
                CallerID DN =

Alternate Matches

    Note: Information Not Available
```

In this example, note the shaded output. The first shaded line shows the result of the digit analysis as RouteThisPattern. That means it has a call path. The shaded lines that follow show the route list/route group selection all the way down the outbound port on the PRI. Note that there are two possible PRIs through which the call could route. This provides invaluable information in troubleshooting call problems.

Task 4: CUCM Reports

CUCM has a large array of available reporting capabilities. This task will take you through a number of those capabilities as they pertain to troubleshooting.

Step 4-1: Route Plan Report

The Route Plan Report is a big-picture view of all route patterns in the system at the time the report is run. As a system evolves, phones are added and removed over time. As phones and directory numbers (DN) are removed, they don't always clean up after themselves properly. The phone will be removed, but the DN will simply be orphaned. Orphaned DNs can cause all kinds of trouble because they're essentially a match to a route pattern that goes nowhere and causes calling conflicts.

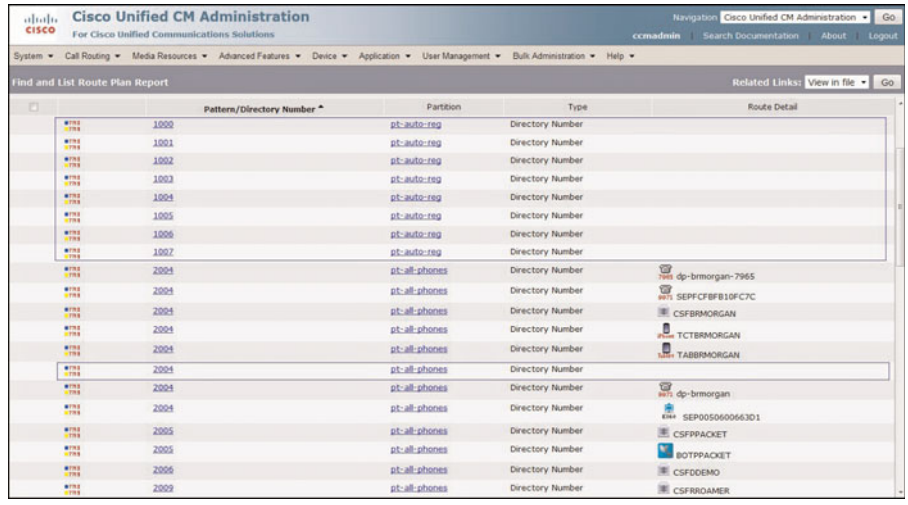
It is important to run a Route Plan Report on occasion simply to weed out these orphaned DNs. To do so, open the CCMAdmin page and then choose **Call Routing > Route Plan Report**. Figure 16-4 shows the output from a Route Plan Report.

Orphaned DNs are likely to pop up on clusters where autoregistration is enabled, as is the case in the figure. These autoregistered DNs can be deleted at will with no ramifications. This will return those DNs to the autoregistration pool. But, they can also pop up in places where they might not be so out of the way. The figure also shows that there's an orphaned instance of DN 2004, which can cause issues in reaching 2004 on occasion.

https://t.me/learningnets

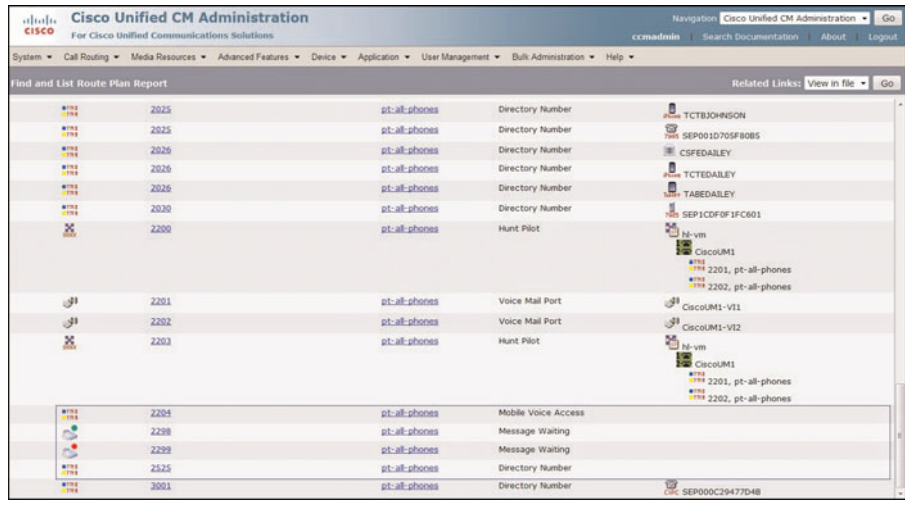
From the Library of Aliwarman Tarihoran

Figure 16-4 Route Plan Report Output



Anytime a pattern exists with no route detail, it is suspect. Note, that the word *suspect* was used. This means that it's not always an orphaned DN. Figure 16-5 shows an example of when it might be okay to have no route detail.

Figure 16-5 Route Plan Report Output Continued



The box in the figure highlights a few DNs with no route detail. Note that these have specific uses including Mobile Voice Access Pilot, Message Waiting Indicator (MWI) on/off, and so on. There is one sneaky-looking entry there for DN 2525. It shows as a directory number and it shows to have no route detail. That one is certainly an orphan and should be deleted. The point is to avoid deleting DNs solely based on their lack of a route detail.

If you're the less adventurous type, there is a filtering capability in the Route Plan Report that will show only unassigned DNs. When you choose **Call Routing > Route Plan Report**, there is a filter query at the top of the page. The far-left field is the Find field. Set it to Unassigned DN, and it should show you any orphans.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

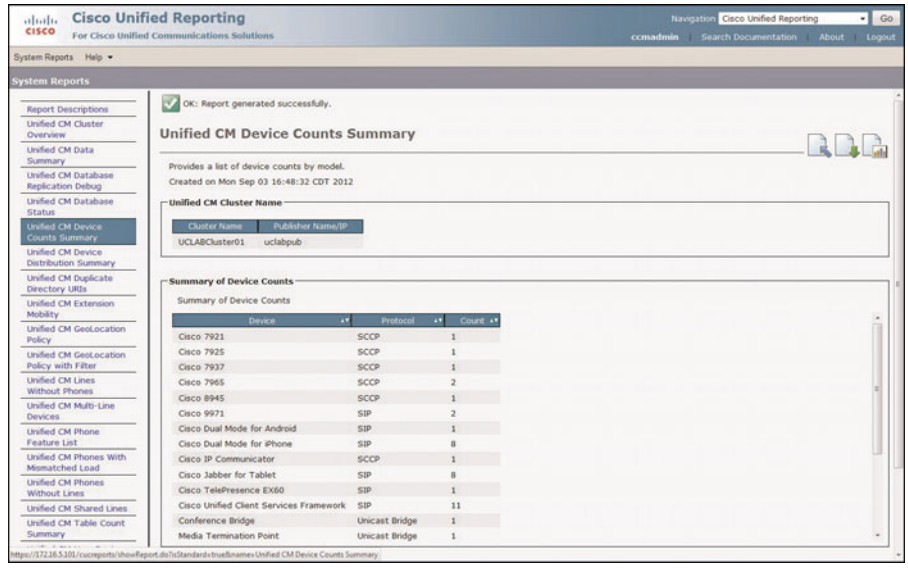
Step 4-2: Cisco Unified Reporting

One of the more powerful, yet most overlooked, tools in the CUCM arsenal is the Cisco Unified Reporting tool. It has status information of great value when evaluating, auditing, or troubleshooting a CUCM cluster configuration.

Access the tool and spend some time getting familiar with it and the information contained within the available reports.

1. To get to the tool, open the CCMAdmin page.
2. Click the drop-down Navigation menu at the upper-right corner. Select Cisco Unified Reporting and log in with the Application Administrator credentials.
3. Click System Reports and look at the list of reports that are there.
4. Click any report, and then click **Generate New Report** to get the most up-to-date info. Handily enough, the first report is Report Descriptions. Read through the descriptions and run any report that strikes you as being valuable. For purposes of this discussion, Figure 16-6 shows the partial output of the Unified CM Device Counts Summary report.

Figure 16-6 Unified CM Device Counts Summary Report



This report shows the device distribution across the cluster by type and protocol. It's a great report for keeping track of how many phones are in use and what types of phones are in use.

Get familiar with the reports and the information that can be gleaned from each. These are great sources of information in an easily read/comprehended format.

Step 4-3: Call Detail Record Analysis and Reporting

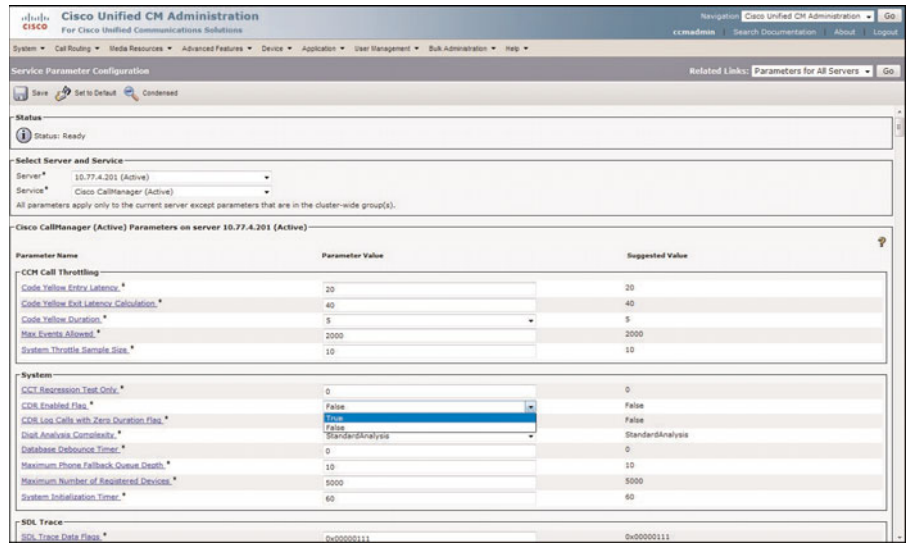
Call detail records (CDR) are kept by CUCM and maintained for a certain amount of time based on the file sizes of each individual CDR file in the system.

It is worthy to mention at this point that CDR is not enabled in CUCM by default. Thus, if you are looking at the CDR Analysis and Reporting (CAR) utility and wondering why it lacks information, keep in mind that you need to enable CDR reporting in the Service System Parameters. Figure 16-7 shows the Service System Parameters screen.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 16-7 Service Parameters Screen



1. On the CCMAdmin page, choose **System > Service Parameters**, select the node you want to configure, and select the CallManager Service.
2. Scroll down to the CDR Enabled Flag field, set it to **True**, and then click **Save**. This has to be done on each node in the cluster.

If the **Cisco SOAP – CDROnDemand Service** and **Cisco CAR Web Service** services are not already active on CUCM, follow the steps in Lab 9-2, Task 3 to activate them.

The CAR system provides an interface through which additional reporting can be run. These reports include usage reports (billing, top *N* users, and so on), system reports, device reports, and more. To access the CAR system, navigate to the Serviceability page and then choose **Tools > CDR Analysis and Reporting**. This will launch the tool in a new window. Be sure to allow pop-ups.

After CDR is enabled, you'll need to place a few calls to both on- and off-net destinations to generate some traffic. When you're happy with the number of calls, head back to the tool and run a Usage Report for the top *N* users by Number of Calls. You'll have the option to export the report to the .csv or .pdf format.

After you have your top user, run a CDR search based on the user's DN. To do so, choose **CDR > Search > By User/Phone Number/SIP URL**.

Familiarize yourself with other reports within the system. Again, the amount of data to which you will have access in the cluster will be very limited as a lab system, even more so as a lab system which only just now enabled CDR.

Step 4-4: Real Time Monitoring Tool (RTMT)

The RTMT utility can be the single most useful tool of all for troubleshooting issues with a CUCM cluster.

The tool needs to be installed on your desktop. Once installed, access it and familiarize yourself with its capabilities.

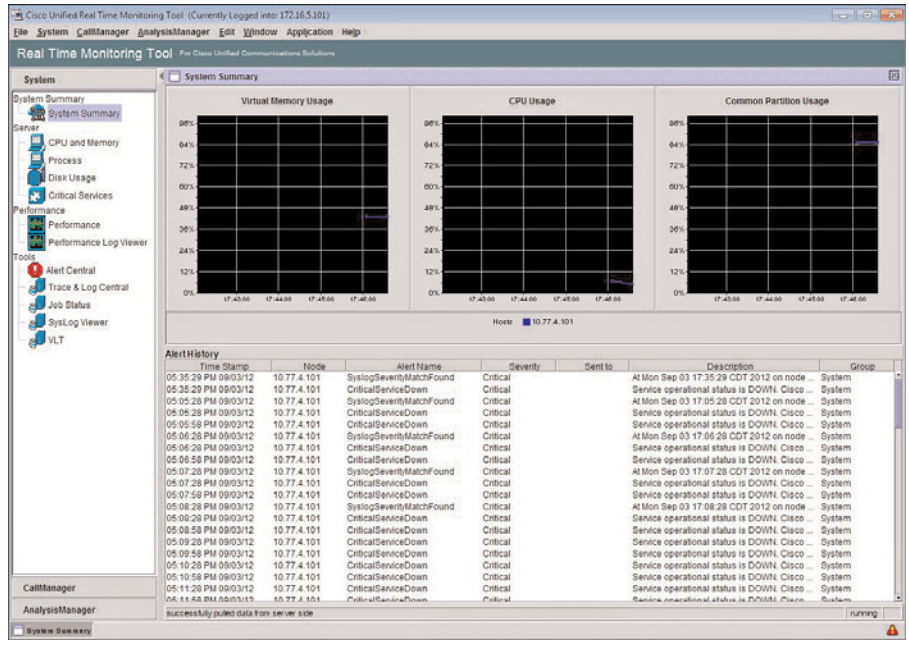
1. The tool can be downloaded from CUCM itself by opening the CCMAdmin page, choosing **Application > Plugins**, and clicking **Find**. The tool will be at the bottom of the list.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

2. Click the download link for your platform (Windows or Linux).
3. After it is downloaded, run the installer and launch the utility. Figure 16-8 shows the startup screen of the RTMT after it is launched.

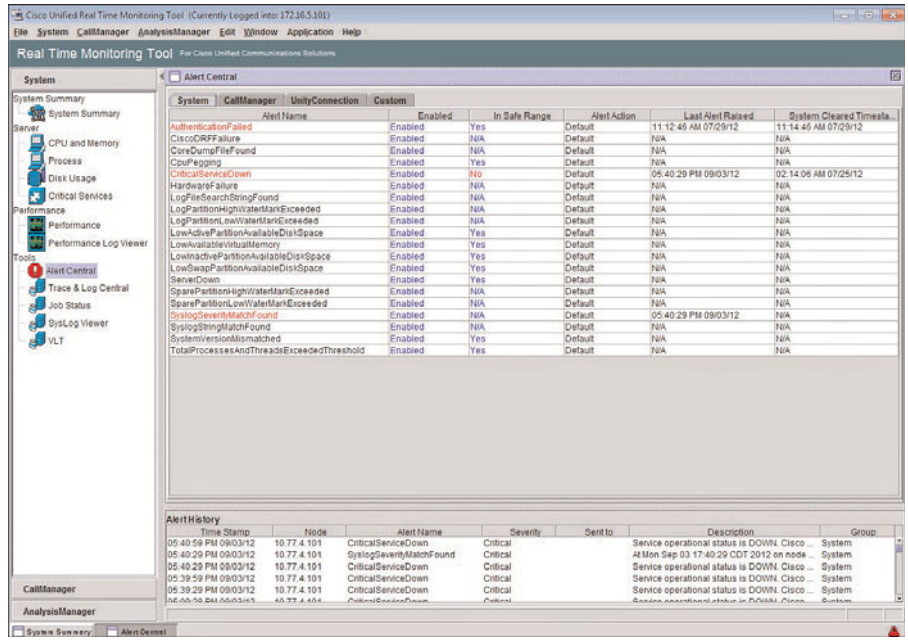
Figure 16-8 RTMT System Summary Screen



The dashboard view presented includes a navigation bar down the left side, a graphical view of memory/CPU/disk usage across the top, and an alert history at the bottom.

For system alerts, there is a specific view called Alert Central. It is visible on the left-side navigation bar, with a stop sign next to it. Figure 16-9 shows the Alert Central screen.

Figure 16-9 RTMT Alert Central Screen



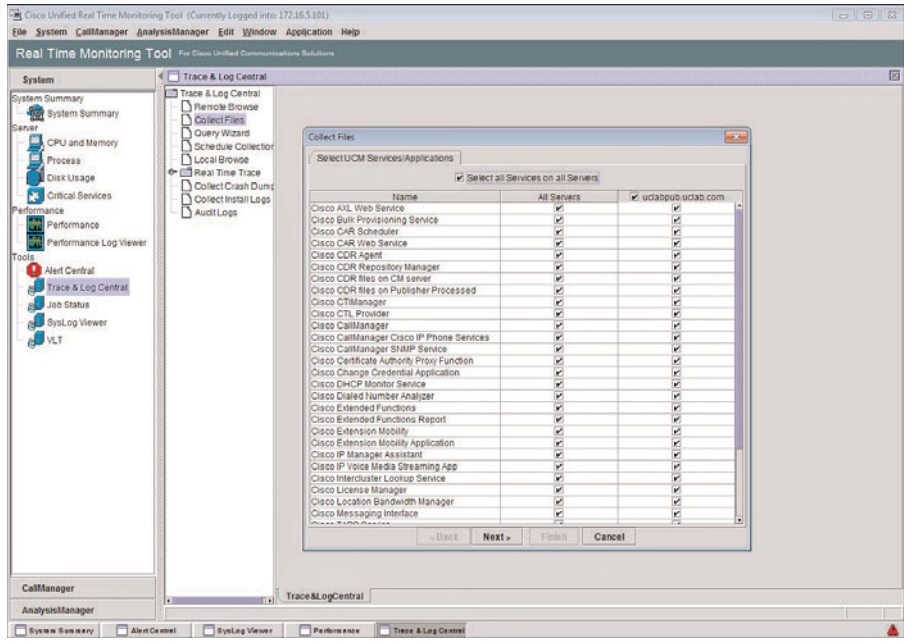
https://t.me/learningnets
From the Library of Aliwarman Tarihoran

Anything that really needs attention will be listed in red text in the top pane, while alerts continue to stream across the bottom as in the System Summary screen. This provides a good overview of the health of the system.

If you're really in trouble and need to open a service request with Cisco TAC, they're going to need a description of the problem, the full version of the CUCM cluster, and the trace files. The trace files are easily collected and bundled using the RTMT. Follow these steps:

1. Along the left side in the navigation bar is an entry called **Trace & Log Central**. Click it to open the Trace & Log Central utility window.
2. Within that window is an entry called **Collect Files**. Click it to open the Collect Files window. Figure 16-10 shows this progression.

Figure 16-10 RTMT Trace & Log Central



3. If you really want to be thorough, select the **Select all Services on all Servers** check box, as this will pull everything you might need from all nodes in the cluster.
4. Click **Next** and repeat the process for UCM Services (first screen), System Services/Applications.
5. Choose where to save the files. There are other options there regarding whether or not to zip the files and what date/time range should be included in the files. Specify a directory to which the file(s) should be downloaded.
6. Click **Finish**.
7. Attach the resulting file(s) to the TAC case where the assigned engineer can begin analysis. The file collection and download process will take a few minutes on a production system. Be patient with it.

RTMT is a powerful and feature-rich tool. The more time you spend with it, the better prepared you'll be when it comes to monitoring call capacity, trending call volume, or troubleshooting.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

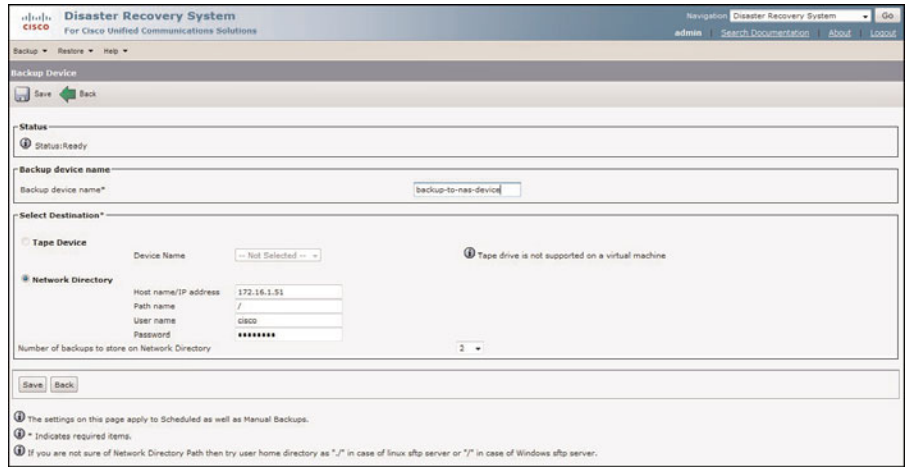
Step 4-5: Disaster Recovery System

Regular, reliable system backups are crucial to any mission-critical application. Call control is no different. Cisco has included the Disaster Recovery System (DRS) with CUCM. To access it, open the CCMAdmin page and the drop-down Navigation menu. Select Disaster Recovery System and log in using the System Administration credentials (the same credentials used for OS access).

To back up or restore a system, backup devices must be defined. These can be tape backups (physical servers only) or network locations (Secure File Transfer Protocol [SFTP]). To create a backup device, follow these steps:

1. Choose **Backup > Backup Device** and then click **Add New**.
2. Provide a meaningful, descriptive name for the backup device, and then select the backup destination. Figure 16-11 shows the Backup Device page.

Figure 16-11 DRS Backup Device Page



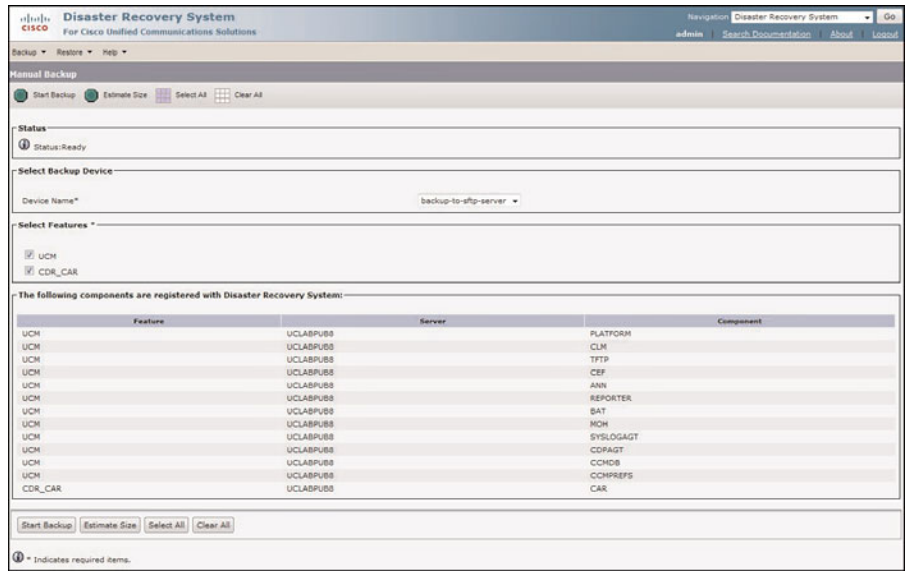
With the backup device specified, backup jobs can be scheduled or run manually. To do so, follow these steps:

1. To schedule a backup, choose **Backup > Scheduler** and then click **Add New**.
2. Specify the newly created backup destination, and then set the time/date and recurrence of the backup. Then, click **Save**.
3. To perform an immediate, manual backup, choose **Backup > Manual Backup**, and then provide the backup device name. Select the features that you want to back up.
4. Click **Start Backup**. Figure 16-12 shows the Manual Backup screen.
5. To restore a backup, choose **Restore > Restore Wizard**, select the backup destination, and click **Next**.
6. Select the items to be restored. At this point, the DRS system will make contact with the backup destination to see what backups are available.
7. You will be presented with a drop-down menu that allows the selection of the backup .tar file to be utilized in the restore. Select the file and click **Next**. The restore process takes quite a while, even for a small system. The backup process is much faster. So don't try to judge one from the other.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 16-12 DRS Manual Backup Screen



The DRS system is fairly simple, overall. Get familiar with the interface and its capabilities. Remember, you must use SFTP to perform the backup/restore processes. Don't assume that every company or customer will have one for use with the system. Always come prepared with one of your own for those worst-case scenarios.

This concludes Lab 16.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

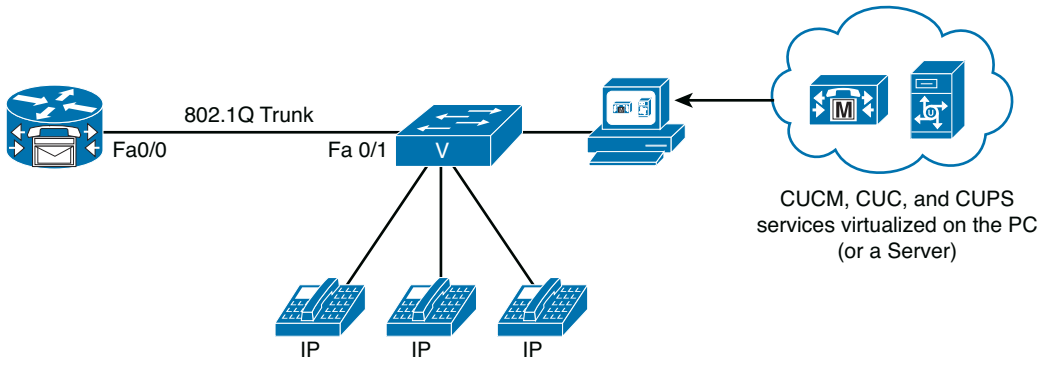
CHAPTER 17

Monitoring Cisco Unity Connection

This chapter explores reports and tools that help operate and troubleshoot Cisco Unity Connection (CUC).

Lab 17-1: Cisco Unity Connection Reports

Figure 17-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- Switch that supports voice VLANs
- Cisco Unified Communications Manager (CUCM) Server or PC with VMware Workstation installed and a VM of CUCM
- Cisco Unity Connection (CUC) Server or PC with VMware Workstation installed and a VM of CUC
- Three or more IP Phones registered (desk phone or soft phone on PC or Windows VM)
- Lab configuration from Lab 13-3 or later

Learning Objectives

Upon completion of this lab, you will be able to understand the basic capabilities of Cisco Unity Connection's reporting functions.

Scenario

Shiny Objects Inc. (SOI) is happy the with voicemail system. However, a voicemail solution is not a "plug, play, and forget" solution; it requires ongoing maintenance. SOI want to know more about reports that can keep the system functioning optimally.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 1: Prepare the System

The CUC reports won't show much activity if you did not use the CUC system extensively in Chapter 13, "Cisco Unity Connection." Before you start to look at the reports, it will help to put the system into a more real-world situation.

Step 1-1: Leave Unheard Messages

Leave a few voicemails (from more than one phone) on one of the accounts that you do not listen to. (The unheard messages will show up in a later report.)

Step 1-2: Examine Authentication Rule Settings

Back in Step 1-2 of Lab 13-2, you created the "Low Security" authentication rules to assign to users for the lab. It is useful to see the results that an administrator would see when an account is locked out. Examine the settings established for that authentication rule.

On the Cisco Unity Connection Administration page, navigate to **System Settings > Authentication Rules** and click the **Low Security** authentication rule. Note that the settings should be set so that three failed attempts within 30 minutes will trigger a one-minute lockout.

Step 1-3: Lock Out an Account

From a phone (use a different phone than the one with unheard messages), use the **Messages** button to connect to voicemail. Enter any PIN other than the correct one and press the pound (#) key. Hang up and repeat three more times. During the final attempt, the system will say "Your account is locked and cannot be opened. For help, contact your system administrator." At this point, your account will be locked for the next minute and will not even respond to the correct PIN. Leave the account locked to see it in a later report.

Step 1-4: Adjust Report Configuration

CUC has settings that control report and log file settings. By default, the report collection only runs every 30 minutes. Change the value to five minutes for the lab environment so that you don't have to wait for up to a half-hour for your recent activity to show in the reports.

On the Cisco Unity Connection Administration page, navigate to **System Settings > Advanced > Reports**. Enter **5** in the Minutes Between Data Collection Cycles field and click the **Save** button. Figure 17-2 shows this page.

Note: Some earlier versions of CUC might be using seconds or even milliseconds for the data collection cycles time units. If this is the case for you, adjust the values to be equal to five minutes.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 17-2 CUC Report Configuration

Task 2: Cisco Unity Connection Serviceability Page

Like CUCM, Unity Connection has a Cisco Unified Serviceability page that functions in a very similar manner to that of CUCM. Unlike CUCM, however, Unity Connection has a separate utility called Cisco Unity Connection Serviceability. The Cisco Unity Connection Serviceability page is an interface built specifically for accessing the core services and components of Cisco Unity Connection.

Step 2-1: Access the Cisco Unity Connection Serviceability Page

There are two ways to access the Cisco Unity Connection Serviceability page:

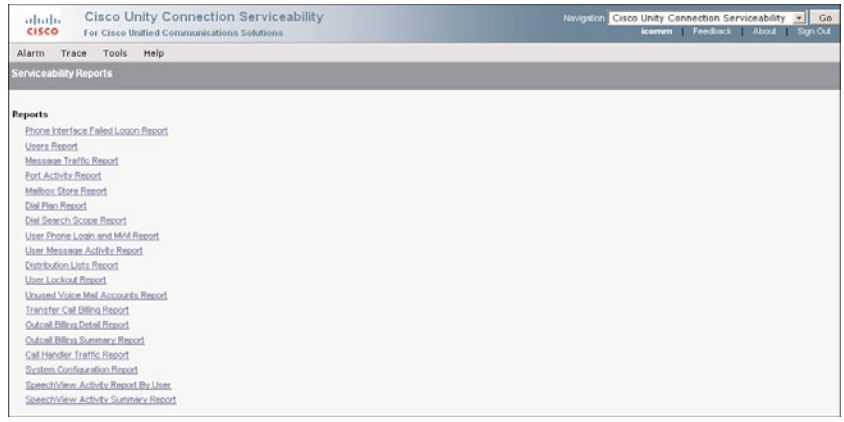
- From the Navigation drop-down menu inside CUC
- Directly, using the https://<*cuc-ip-address*>/cuservice URL

On the Cisco Unity Connection Serviceability page, navigate to **Tools > Reports**.

Note: If you do not see the **Reports** item on the Tools menu, and instead see **Service Activation**, you are on the Cisco Unified Serviceability page. Make sure to select the Cisco Unity Connection Serviceability page.

Figure 17-3 shows the Serviceability Reports page.

Figure 17-3 CUC Serviceability Reports



https://t.me/learningnets

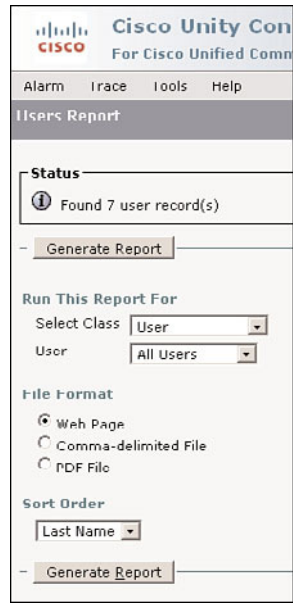
From the Library of Aliwarman Tarihoran

Step 2-2: Examine the Users Report

The first report to examine is the Users report. It shows a summary of the users, their extensions, and if the account is locked, among other things.

1. Click **Users Report**. (It is the second item down in the list of reports.)
2. The Users Report page allows you to pick various formats to get the results and sort orders. For now, leave the File Format setting at **Web Page** and the Sort Order field at **Last Name**. Figure 17-4 shows this page.

Figure 17-4 Users Report Selection Page



3. Click the **Generate Report** button. Figure 17-5 shows an example of this page. Notice that in Figure 17-5, user bsieling has a locked account.

Figure 17-5 Users Report Page

https://t.me/learningnets

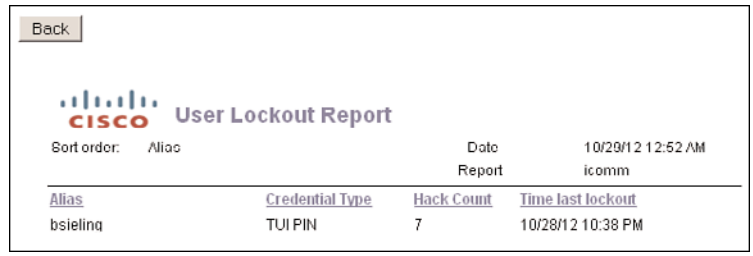
From the Library of Aliwarman Tarihoran

Step 2-3: Examine the User Lockout Report

The User Lockout report shows any accounts that are currently locked for violations of the Authentication Rules.

1. Use the **Back** button in your browser or navigate back to the Reports page.
2. Click **User Lockout Report**.
3. Click the **Generate Report** button. Figure 17-6 shows an example of this page. TUI PIN in this figure stands for Telephone User Interface PIN, to differentiate it from the user web page log in failures. Notice that even though the lockout only lasts one minute, the account is locked until the PIN is entered correctly (unless the **Administrator Must Unlock** check box is selected in the authentication rule).

Figure 17-6 User Lockout Page



4. Use the phone with the locked voicemail account to log in to the account with the correct PIN and unlock it.
5. Click the **Back** button and run the User Lockout report again. The status should show "Unable to find any report data based on the parameter(s)." The User Lockout report only shows accounts that are currently locked (and might require administrator intervention to unlock).

Step 2-4: Examine the Phone Interface Failed Logon Report

To see a history of locked accounts, use the Phone Interface Failed Logon report.

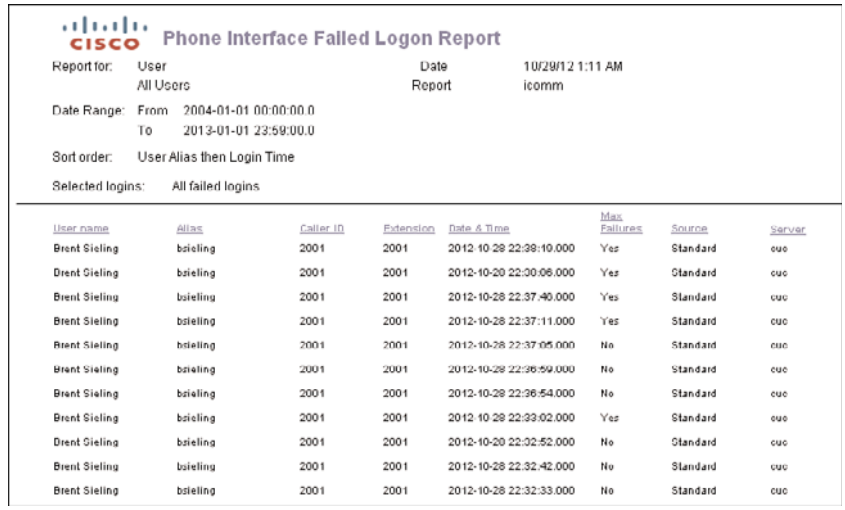
1. Use the **Back** button in your browser or navigate back to the Reports page.
2. Click **Phone Interface Failed Logon Report**.
3. The report covers previously failed logons, so it is necessary to change the Date Range To drop-down lists to the current (or a future) date. The easiest way to do this is to change the To year drop-down list to next year's selection.
4. Click the **Generate Report** button. Figure 17-7 shows an example of this page. Notice in Figure 17-7 in the Max Failures column, that some of the failures did not result in the account being locked, and some did.

While the User Lockout page only shows currently locked accounts, the Phone Interface Failed Logon report shows the history of locked accounts, even if the account is not locked at this time.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure 17-7 Phone Interface Failed Logon Report



Phone Interface Failed Logon Report

Report for: User — Date: 10/29/12 1:11 AM
All Users — Report: icomm

Date Range: From 2004-01-01 00:00:00.0
To 2013-01-01 23:59:00.0

Sort order: User Alias then Login Time

Selected logins: All failed logins

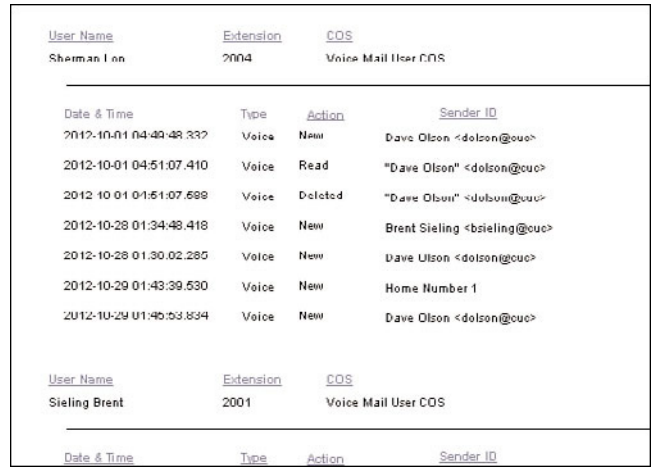
User name	Alias	Caller ID	Extension	Date & Time	Max Failures	Source	Server
Brent Sieling	bsieling	2001	2001	2012-10-28 22:38:10.000	Yes	Standard	cuc
Brent Sieling	bsieling	2001	2001	2012-10-28 22:38:06.000	Yes	Standard	cuc
Brent Sieling	bsieling	2001	2001	2012-10-28 22:37:40.000	Yes	Standard	cuc
Brent Sieling	bsieling	2001	2001	2012-10-28 22:37:11.000	Yes	Standard	cuc
Brent Sieling	bsieling	2001	2001	2012-10-28 22:37:05.000	No	Standard	cuc
Brent Sieling	bsieling	2001	2001	2012-10-28 22:36:59.000	No	Standard	cuc
Brent Sieling	bsieling	2001	2001	2012-10-28 22:36:54.000	No	Standard	cuc
Brent Sieling	bsieling	2001	2001	2012-10-28 22:33:02.000	Yes	Standard	cuc
Brent Sieling	bsieling	2001	2001	2012-10-28 22:32:52.000	No	Standard	cuc
Brent Sieling	bsieling	2001	2001	2012-10-28 22:32:42.000	No	Standard	cuc
Brent Sieling	bsieling	2001	2001	2012-10-28 22:32:33.000	No	Standard	cuc

Step 2-5: Examine the User Message Activity Report

The User Message Activity report shows information about the messages in the system, such as their source.

1. Use the **Back** button in your browser or navigate back to the Reports page.
2. Click **User Message Activity Report**.
3. Don't forget to change the date range before you click the **Generate Report** button. Figure 17-8 shows an example of this page. Notice in Figure 17-8 that the Action column shows that for the Lon Sherman account, the first message (from Dave Olson) was read and deleted, but there are currently four new messages that have not been heard.

Figure 17-8 User Message Activity Report



User Name	Extension	COS
Sherman Lon	2004	Voice Mail User COS

Date & Time	Type	Action	Sender ID
2012-10-01 04:49:48.332	Voice	New	Dave Olson <dolson@cuc>
2012-10-01 04:51:07.410	Voice	Read	"Dave Olson" <dolson@cuc>
2012-10-01 04:51:07.589	Voice	Deleted	"Dave Olson" <dolson@cuc>
2012-10-28 01:34:48.418	Voice	New	Brent Sieling <bsieling@cuc>
2012-10-28 01:30:02.285	Voice	New	Dave Olson <dolson@cuc>
2012-10-29 01:43:39.530	Voice	New	Home Number 1
2012-10-29 01:45:53.834	Voice	New	Dave Olson <dolson@cuc>

User Name	Extension	COS
Sieling Brent	2001	Voice Mail User COS

Date & Time	Type	Action	Sender ID

Step 2-6: Examine Other Reports

Spend some time examining the other reports. Given the limited use of the system so far, the following reports might be the most interesting to look at:

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- Message Traffic report
- Port Activity report
- Mailbox Store report
- User Phone Login and MWI report
- Call Handler Traffic report
- System Configuration report

Task 3: Real-Time Monitoring Tool and Serviceability Reports Archive

Lab 13-1 introduced the Real-Time Monitoring Tool (RTMT) by using the Port Monitor to examine calls into the system. As shown in Figure 13-30, RTMT can monitor the server performance, including such information at memory, CPU, and disk partition usage. This is fine if you are looking at RTMT often, but how can you examine this information when you are not looking at RTMT? CUC can store the server health and performance information for later examination.

Step 3-1: Activate the Cisco Serviceability Reporter Service

On the Cisco Unified Serviceability page, navigate to **Tools > Service Activation**. Select the **Cisco Serviceability Reporter** check box and click **Save**.

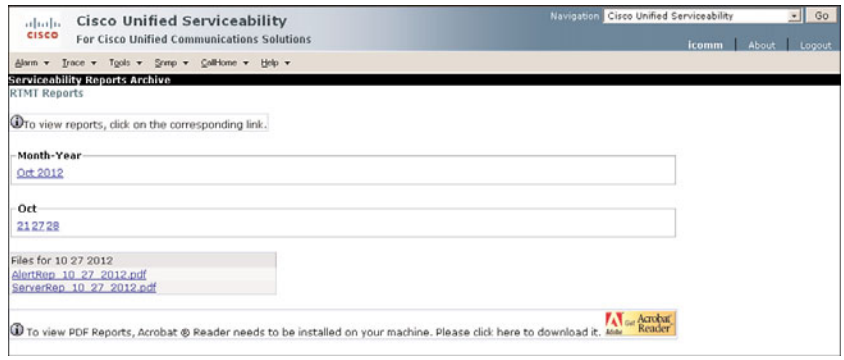
Note: Many of the settings on the **System Settings > Advanced > Reports** page apply to the Serviceability Reports Archive, as shown in Figure 17-2. For example, the **Days to Keep Data in Reports Database** affects how long the information will be accessible in the database.

Step 3-2: Examine RTMT Reports

After the Serviceability Reporter is active, it will start collecting information for the reports. On the Cisco Unified Serviceability page, navigate to the new **Tools > Serviceability Reports Archive** menu.

Click the hyperlink for the month and year, and then the report for the day you want to inspect. There are two reports: one for Alerts and another for the Server, and they are produced as Acrobat files. Depending on the browser you are using, you might need to right-click a hyperlink and save the file to the desktop. See Figure 17-9 for an example of this page.

Figure 17-9 Serviceability Reports Archive – RTMT Reports



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

This page intentionally left blank

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Pod	Host Name	VLAN Name	VLAN #	IP Address	DHCP Pool Exclusion	DHCP Pool	Default Router	DHCP Option 150	Extension # Range	First E.164 DID #	FXS #1
Pod 1	RtrPod1	Management	11	10.11.0.1/24							
		Data	10	10.10.0.1/24	10.10.0.1 - 10.10.0.10	10.10.0.0/24	10.10.0.1	10.10.0.1			
		Voice	15	10.15.0.1/24	10.15.0.1 - 10.15.0.10	10.15.0.0/24	10.15.0.1	10.15.0.1	5000 - 5029	5105555000	5555028
	SwPod1		11	10.11.0.2/24			10.11.0.1				
Pod 2	RtrPod 2	Management	21	10.21.0.1/24							
		Data	20	10.20.0.1/24	10.20.0.1 - 10.20.0.10	10.20.0.0/24	10.20.0.1	10.20.0.1			
		Voice	25	10.25.0.1/24	10.25.0.1 - 10.25.0.10	10.25.0.0/24	10.25.0.1	10.25.0.1	5030 - 5059	5105555030	5555058
	SwPod 2		21	10.21.0.2/24			10.21.0.1				
Pod 3	RtrPod 3	Management	31	10.31.0.1/24							
		Data	30	10.30.0.1/24	10.30.0.1 - 10.30.0.10	10.30.0.0/24	10.30.0.1	10.30.0.1			
		Voice	35	10.35.0.1/24	10.35.0.1 - 10.35.0.10	10.35.0.0/24	10.35.0.1	10.35.0.1	5060 - 5089	5105555060	5555088
	SwPod 3		31	10.31.0.2/24			10.31.0.1				

https://t.me/learningnets
From the Library of Aliwarman Tarihoran

Pod	Host Name	VLAN Name	VLAN #	IP Address	DHCP Pool Exclusion	DHCP Pool	Default Router	DHCP Option 150	Extension # Range	First E.164 DID #	FXS #1
Pod 4	RtrPod 4	Management	41	10.41.0.1/24							
		Data	40	10.40.0.1/24	10.40.0.1 - 10.40.0.10	10.40.0.0/24	10.40.0.1	10.40.0.1			
		Voice	45	10.45.0.1/24	10.45.0.1 - 10.45.0.10	10.45.0.0/24	10.45.0.1	10.45.0.1	5100 - 5129	5105555100	5555128
	SwPod 4		41	10.41.0.2/24			10.41.0.1				
Pod 5	RtrPod 5	Management	51	10.51.0.1/24							
		Data	50	10.50.0.1/24	10.50.0.1 - 10.50.0.10	10.50.0.0/24	10.50.0.1	10.50.0.1			
		Voice	55	10.55.0.1/24	10.55.0.1 - 10.55.0.10	10.55.0.0/24	10.55.0.1	10.55.0.1	5130 - 5159	5105555130	5555158
	SwPod 5		51	10.51.0.2/24			10.51.0.1				
Pod 6	RtrPod 6	Management	61	10.61.0.1/24							
		Data	60	10.60.0.1/24	10.60.0.1 - 10.60.0.10	10.60.0.0/24	10.60.0.1	10.60.0.1			
		Voice	65	10.65.0.1/24	10.65.0.1 - 10.65.0.10	10.65.0.0/24	10.65.0.1	10.65.0.1	5160 - 5189	5105555160	5555188
	SwPod 6		61	10.61.0.2/24			10.61.0.1				
Pod 7	RtrPod 7	Management	71	10.71.0.1/24							
		Data	70	10.70.0.1/24	10.70.0.1 - 10.70.0.10	10.70.0.0/24	10.70.0.1	10.70.0.1			
		Voice	75	10.75.0.1/24	10.75.0.1 - 10.75.0.10	10.75.0.0/24	10.75.0.1	10.75.0.1	5200 - 5229	5105555200	5555228
	SwPod 7		71	10.71.0.2/24			10.71.0.1				

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Pod	Host Name	VLAN Name	VLAN #	IP Address	DHCP Pool Exclusion	DHCP Pool	Default Router	DHCP Option 150	Extension # Range	First E.164 DID #	FXS #1
Pod 8	RtrPod 8	Management	81	10.81.0.1/24							
		Data	80	10.80.0.1/24	10.80.0.1 - 10.80.0.10	10.80.0.0/24	10.80.0.1	10.80.0.1			
		Voice	85	10.85.0.1/24	10.85.0.1 - 10.85.0.10	10.85.0.0/24	10.85.0.1	10.85.0.1	5230 - 5259	5105555230	5555258
	SwPod 8		81	10.81.0.2/24			10.81.0.1				
Pod 9	RtrPod 9	Management	91	10.91.0.1/24							
		Data	90	10.90.0.1/24	10.90.0.1 - 10.90.0.10	10.90.0.0/24	10.90.0.1	10.90.0.1			
		Voice	95	10.95.0.1/24	10.95.0.1 - 10.95.0.10	10.95.0.0/24	10.95.0.1	10.95.0.1	5260 - 5289	5105555260	5555288
	SwPod 9		91	10.91.0.2/24			10.91.0.1				
Pod 10	RtrPod 10	Management	101	10.101.0.1/24							
		Data	100	10.100.0.1/24	10.100.0.1 - 10.100.0.11	10.100.0.0/24	10.100.0.1	10.100.0.1			
		Voice	105	10.105.0.1/24	10.105.0.1 - 10.105.0.11	10.105.0.0/24	10.105.0.1	10.105.0.1	5300 - 5329	5105555300	5555328
	SwPod 10		101	10.101.0.2/24			10.101.0.1				
Pod 11	RtrPod11	Management	111	10.111.0.1/24							
		Data	110	10.110.0.1/24	10.110.0.1 - 10.110.0.10	10.110.0.0/24	10.110.0.1	10.110.0.1			
		Voice	115	10.115.0.1/24	10.115.0.1 - 10.115.0.10	10.115.0.0/24	10.115.0.1	10.115.0.1	5330 - 5359	5105555330	5555358
	SwPod11		111	10.111.0.2/24			10.111.0.1				

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Pod	Host Name	VLAN Name	VLAN #	IP Address	DHCP Pool Exclusion	DHCP Pool	Default Router	DHCP Option 150	Extension # Range	First E.164 DID #	FXS #1
Pod 12	RtrPod12	Management	121	10.121.0.1/24							
		Data	120	10.120.0.1/24	10.120.0.1 - 10.120.0.10	10.120.0.0/24	10.120.0.1	10.120.0.1			
		Voice	125	10.125.0.1/24	10.125.0.1 - 10.125.0.10	10.125.0.0/24	10.125.0.1	10.125.0.1	5360 - 5389	5105555360	5555388
	SwPod12		121	10.121.0.2/24			10.121.0.1				
Pod 13	RtrPod13	Management	131	10.131.0.1/24							
		Data	130	10.130.0.1/24	10.130.0.1 - 10.130.0.10	10.130.0.0/24	10.130.0.1	10.130.0.1			
		Voice	135	10.135.0.1/24	10.135.0.1 - 10.135.0.10	10.135.0.0/24	10.135.0.1	10.135.0.1	5400 - 5429	5105555400	5555428
	SwPod13		131	10.131.0.2/24			10.131.0.1				
Pod 14	RtrPod14	Management	141	10.141.0.1/24							
		Data	140	10.140.0.1/24	10.140.0.1 - 10.140.0.10	10.140.0.0/24	10.140.0.1	10.140.0.1			
		Voice	145	10.145.0.1/24	10.145.0.1 - 10.145.0.10	10.145.0.0/24	10.145.0.1	10.145.0.1	5430 - 5459	5105555430	5555458
	SwPod14		141	10.141.0.2/24			10.141.0.1				
Pod 15	RtrPod15	Management	151	10.151.0.1/24							
		Data	150	10.150.0.1/24	10.150.0.1 - 10.150.0.10	10.150.0.0/24	10.150.0.1	10.150.0.1			
		Voice	155	10.155.0.1/24	10.155.0.1 - 10.155.0.10	10.155.0.0/24	10.155.0.1	10.155.0.1	5460 - 5489	5105555460	5555488
	SwPod15		151	10.151.0.2/24			10.151.0.1				

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Pod	Host Name	VLAN Name	VLAN #	IP Address	DHCP Pool Exclusion	DHCP Pool	Default Router	DHCP Option 150	Extension # Range	First E.164 DID #	FXS #1
Pod 16	RtrPod16	Management	161	10.161.0.1/24							
		Data	160	10.160.0.1/24	10.160.0.1 - 10.160.0.10	10.160.0.0/24	10.160.0.1	10.160.0.1			
		Voice	165	10.165.0.1/24	10.165.0.1 - 10.165.0.10	10.165.0.0/24	10.165.0.1	10.165.0.1	5500 - 5529	5105555500	5555528
	SwPod16		161	10.161.0.2/24			10.161.0.1				
Pod 17	RtrPod17	Management	171	10.171.0.1/24							
		Data	170	10.170.0.1/24	10.170.0.1 - 10.170.0.10	10.170.0.0/24	10.170.0.1	10.170.0.1			
		Voice	175	10.175.0.1/24	10.175.0.1 – 10.175.0.10	10.175.0.0/24	10.175.0.1	10.175.0.1	5530 - 5559	5105555530	5555558
	SwPod17		171	10.171.0.2/24			10.171.0.1				
Pod 18	RtrPod18	Management	181	10.181.0.1/24							
		Data	180	10.180.0.1/24	10.180.0.1 - 10.180.0.10	10.180.0.0/24	10.180.0.1	10.180.0.1			
		Voice	185	10.185.0.1/24	10.185.0.1 - 10.185.0.10	10.185.0.0/24	10.185.0.1	10.185.0.1	5560 - 5589	5105555560	5555588
	SwPod18		181	10.181.0.2/24			10.181.0.1				
Pod 19	RtrPod19	Management	191	10.191.0.1/24							
		Data	190	10.190.0.1/24	10.190.0.1 - 10.190.0.10	10.190.0.0/24	10.190.0.1	10.190.0.1			
		Voice	195	10.195.0.1/24	10.195.0.1 - 10.195.0.10	10.195.0.0/24	10.195.0.1	10.195.0.1	5600 - 5629	5105555600	5555628
	SwPod19		191	10.191.0.2/24			10.191.0.1				

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Pod	Host Name	VLAN Name	VLAN #	IP Address	DHCP Pool Exclusion	DHCP Pool	Default Router	DHCP Option 150	Extension # Range	First E.164 DID #	FXS #1
Pod 20	RtrPod20	Management	201	10.201.0.1/24							
		Data	200	10.200.0.1/24	10.200.0.1 - 10.200.0.11	10.200.0.0/24	10.200.0.1	10.200.0.1			
		Voice	205	10.205.0.1/24	10.205.0.1 - 10.205.0.11	10.205.0.0/24	10.205.0.1	10.205.0.1	5630 - 5659	5105555630	5555658
	SwPod20		201	10.201.0.2/24			10.201.0.1				
Instructor	RtrPod21	Management	211	10.211.0.1/24							
		Data	210	10.210.0.1/24	10.210.0.1 - 10.210.0.12	10.210.0.0/24	10.210.0.1	10.210.0.1			
		Voice	215	10.215.0.1/24	10.215.0.1 - 10.215.0.12	10.215.0.0/24	10.215.0.1	10.215.0.1	5660 - 5689	5105555660	5555688
	SwPod21		211	10.211.0.2/24			10.211.0.11				

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

APPENDIX B

IP Addressing and Phone Extensions for Cisco Unified Communications Manager (CUCM) Labs (Chapters 8–14 and 16–17)

Although many of the IP address settings used for the CUCM labs are the same as those in Appendix A, there are some differences. The DHCP option 150 needs to point to the CUCM server for both the data and voice VLANs. The extensions and the direct inward dialing (DID) numbers used are different, and the usernames for populating the system are provided.

Note: The usernames provided for the pods fit one of two categories: students who alpha-tested this lab book in my class, or students at Madison College who achieved a Cisco certification. (In some cases, they fit both categories.)

Common numbers for all pods, and the labs where they are created:

6010 - 6019	Call park	Lab 11-2
6020 - 6029	Directed call park	Lab 11-2
6501	Call pickup group	Lab 11-2
6900	Shared line	Lab 11-2
7800	Mobile voice access	Lab 12-1
7901	Intercom to 7902	Lab 11-2
7902	Intercom to 7901	Lab 11-2
8000	Pilot for SCCP voice mail	Lab 13-1
8050	Message waiting indicator on	Lab 13-1
8051	Message waiting indicator off	Lab 13-1
8101	SCCP port for voice mail	Lab 13-1
8102	SCCP port for voice mail	Lab 13-1
8500	SIP trunk for voice mail	Lab 13-1

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Pod	VLAN Name	VLAN #	IP Address	DHCP Option 150	Extension # Range	First DID #	CUC Pilot #	Usernames
Pod 1	Management	11	10.11.0.1/24					Chris Dahl
	Data	10	10.10.0.1/24	10.10.0.5				Daniel Yanta
	Voice	15	10.15.0.1/24	10.10.0.5	2100-2199	5105552100	2190	William Reynolds
Pod 2	Management	21	10.21.0.1/24					Krzysztof Petrynko
	Data	20	10.20.0.1/24	10.20.0.5				Todd Forman
	Voice	25	10.25.0.1/24	10.20.0.5	2200-2299	5105552200	2290	Alan Souvannasone
Pod 3	Management	31	10.31.0.1/24					Robert Rockweiler
	Data	30	10.30.0.1/24	10.30.0.5				Louis Glauner
	Voice	35	10.35.0.1/24	10.30.0.5	2300-2399	5105552300	2390	Ady Xiong
Pod 4	Management	41	10.41.0.1/24					Christian Richeson
	Data	40	10.40.0.1/24	10.40.0.5				Caleb Peyton
	Voice	45	10.45.0.1/24	10.40.0.5	2400-2499	5105552400	2490	Cody Gzibovskis
Pod 5	Management	51	10.51.0.1/24					Michael Osborne
	Data	50	10.50.0.1/24	10.50.0.5				Steve Hallet
	Voice	55	10.55.0.1/24	10.50.0.5	2500-2599	5105552500	2590	James Frederick
Pod 6	Management	61	10.61.0.1/24					Ian Chen
	Data	60	10.60.0.1/24	10.60.0.5				Mark McClung
	Voice	65	10.65.0.1/24	10.60.0.5	2600-2699	5105552600	2690	John Gooch

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Pod	VLAN Name	VLAN #	IP Address	DHCP Option 150	Extension # Range	First DID #	CUC Pilot #	Usernames
Pod 7	Management	71	10.71.0.1/24					Spencer George
	Data	70	10.70.0.1/24	10.70.0.5				Rodney Austin
	Voice	75	10.75.0.1/24	10.70.0.5	2700-2799	5105552700	2790	Weston Annoye
Pod 8	Management	81	10.81.0.1/24					Robert Westervelt
	Data	80	10.80.0.1/24	10.80.0.5				Peter Fischer
	Voice	85	10.85.0.1/24	10.80.0.5	2800-2899	5105552800	2890	Mitch Louther
Pod 9	Management	91	10.91.0.1/24					James Albrecht
	Data	90	10.90.0.1/24	10.90.0.5				John Gehring
	Voice	95	10.95.0.1/24	10.90.0.5	2900-2999	5105552900	2990	Bryan Lewis
Pod 10	Management	101	10.101.0.1/24					Jeremy Jorgenson
	Data	100	10.100.0.1/24	10.100.0.5				Michael Nagel
	Voice	105	10.105.0.1/24	10.100.0.5	3000-3099	5105553000	3090	Jeremy Reynolds
Pod 11	Management	111	10.111.0.1/24					Peter Reinhold
	Data	110	10.110.0.1/24	10.110.0.5				Eric Buss
	Voice	115	10.115.0.1/24	10.110.0.5	3100-3199	5105553100	3190	Sutra Ginder
Pod 12	Management	121	10.121.0.1/24					Justin Patterson
	Data	120	10.120.0.1/24	10.120.0.5				Darrel Dean
	Voice	125	10.125.0.1/24	10.120.0.5	3200-3299	5105553200	3290	DeAnne Pasold
Pod 13	Management	131	10.131.0.1/24					Jacob Pharo
	Data	130	10.130.0.1/24	10.130.0.5				Hui-Chun Kuo
	Voice	135	10.135.0.1/24	10.130.0.5	3300-3399	5105553300	3390	Long Lee

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Pod	VLAN Name	VLAN #	IP Address	DHCP Option 150	Extension # Range	First DID #	CUC Pilot #	Usernames
Pod 14	Management	141	10.141.0.1/24					Kodzo Agbovi
	Data	140	10.140.0.1/24	10.140.0.5				Brian Mullinex
	Voice	145	10.145.0.1/24	10.140.0.5	3400-3499	5105553400	3490	David Gower
Pod 15	Management	151	10.151.0.1/24					Sheila Garcia
	Data	150	10.150.0.1/24	10.150.0.5				Joseph Studnicka
	Voice	155	10.155.0.1/24	10.150.0.5	3500-3599	5105553500	3590	John Endries
Pod 16	Management	161	10.161.0.1/24					Tenzin Palden
	Data	160	10.160.0.1/24	10.160.0.5				Curtis Severson
	Voice	165	10.165.0.1/24	10.160.0.5	3600-3699	5105553600	3690	Matt Minnis
Pod 17	Management	171	10.171.0.1/24					Ashley Kieler
	Data	170	10.170.0.1/24	10.170.0.5				Dan Zweig
	Voice	175	10.175.0.1/24	10.170.0.5	3700-3799	5105553700	3790	Dan Pearce
Pod 18	Management	181	10.181.0.1/24					Reid Wilson
	Data	180	10.180.0.1/24	10.180.0.5				Don Bartkowaik
	Voice	185	10.185.0.1/24	10.180.0.5	3800-3899	5105553800	3890	Timothy Jaberg
Pod 19	Management	191	10.191.0.1/24					Paul Sutter
	Data	190	10.190.0.1/24	10.190.0.5				Todd Coplien
	Voice	195	10.195.0.1/24	10.190.0.5	3900-3999	5105553900	3990	Bryan Manicke

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Pod	VLAN Name	VLAN #	IP Address	DHCP Option 150	Extension # Range	First DID #	CUC Pilot #	Usernames
Pod 20	Management	201	10.201.0.1/24					Daniel Gavin
	Data	200	10.200.0.1/24	10.200.0.5				Zach Dorman-Jones
	Voice	205	10.205.0.1/24	10.200.0.5	4000-4099	5105554000	4090	Jeramie Karns
Instructor	Management	211	10.211.0.1/24					David Olson
	Data	210	10.210.0.1/24	10.210.0.5				Ryan Knebel
	Voice	215	10.215.0.1/24	10.210.0.5	2000-2099	5105552000	2090	Lon Sherman

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

This page intentionally left blank

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

APPENDIX C

Building Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUC), and Cisco Unified Presence (CUPS) Servers in VMware Workstation

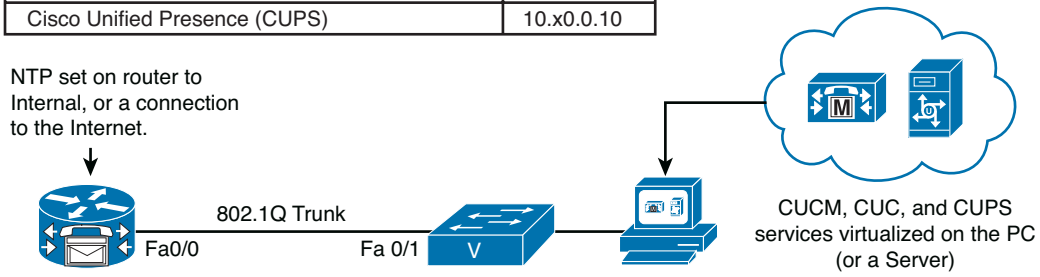
The ICOMM v8 (CCNA Voice) Certification exam focuses heavily on enterprise Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUC), and Cisco Unified Presence (CUPS) servers. Cisco currently sells an appliance with this software installed; however, you can run this software inside a virtual machine. Note that the configuration that follows is for a lab setup only. To run a production system in a virtual environment requires using Cisco-approved hardware; after all, this is a company's phone system! For a production system, Cisco has templates for VMware ESXi servers. However, for a lab environment, VMware Workstation works great, and this appendix will show you how to use it to set up the virtual machines. It might also be possible to run the images using different server emulation software. Search the Internet for instructions.

The media (CD/DVD or an .ISO file) will be either the original installer (which is bootable) or an upgrade (which is not bootable). Both versions will work in VMware Workstation, but VMware will not be able to detect the OS of the upgrade media, so the OS will need to be manually selected. Instructions for both installer and upgrades are included.

Lab C-1: Build Cisco Unified Communications Manager (CUCM) Image

Figure C-1 Topology Diagram

Server	IP Address
Cisco Unified Communication Manager (CUCM)	10.x0.0.5
Cisco Unity Connection (CUC)	10.x0.0.8
Cisco Unified Presence (CUPS)	10.x0.0.10



Equipment Required

This lab uses the following equipment:

- Cisco router.
- Switch that supports voice VLANs.
- Lab configuration from Lab 3-2. (Network Time Protocol [NTP] *must* be accessible or simulated on the router for the build to complete.)

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- PC with VMware Workstation installed and enough disk space and memory. This lab demonstrates VMware Workstation 8 on a machine with 8 GB RAM. (The results are identical with VMware 7.x.) Note: CUCM can be installed on a PC with only 4 GB RAM, but the Unity Connection VM requires 4 GB to build, so the host machine would be page-swapping memory, causing extremely slow performance.
- Access to the install DVD or ISO file for CUCM and Unity Connection (both installs are on the same media). (This lab shows both versions, 8.6.2 and 8.5.1. Versions later than 6.0 should work but might require work-arounds. Specifically, any CUCM before version 8.0 was not designed to run in VMware, so search the Internet for solutions on the installation.)

Task 1: Configure and Cable Devices

Cable the router, switch, and PC together as shown in the topology diagram. Apply the configuration from Labs 3-1 and 3-2 to the router and switch. Make sure that the router is receiving NTP from the Internet or another Cisco router as detailed in Lab 3-2, as an NTP server with a stratum less than or equal to 6 is required to install CUCM.

Note: If you only have access to one router, and are unable to connect to the internet, NTP can be forced to be active on the single router, as detailed in Lab 3-2, step 1-4, option B.

Task 2: Build the Virtual Machine

Step 2-1: New Virtual Machine

Open VMware Workstation and choose **File > New > Virtual Machine**. The New Virtual Machine Wizard appears, as shown in Figure C-2.

Figure C-2 New Virtual Machine Wizard

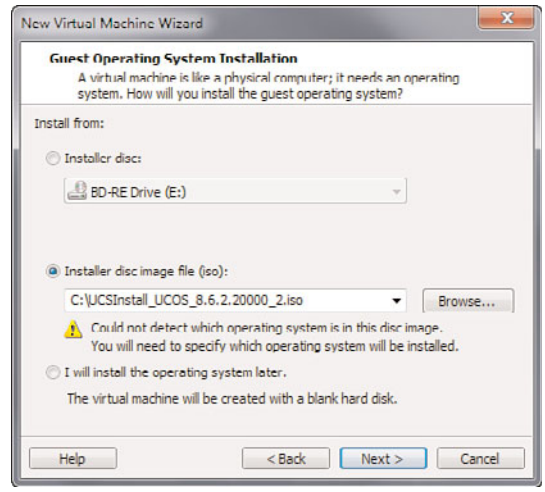
Step 2-2: Choose Install Media

If you have the CUCM DVD inserted, choose the drive the disc is in from the Installer disc drop-down list. If you are using an ISO file, click the **Installer Disc Image File (iso)** radio button, click the **Browse** button, and navigate to the location of the ISO file. See Figure C-3.Click **Next**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure C-3 Guest Operating System Installation



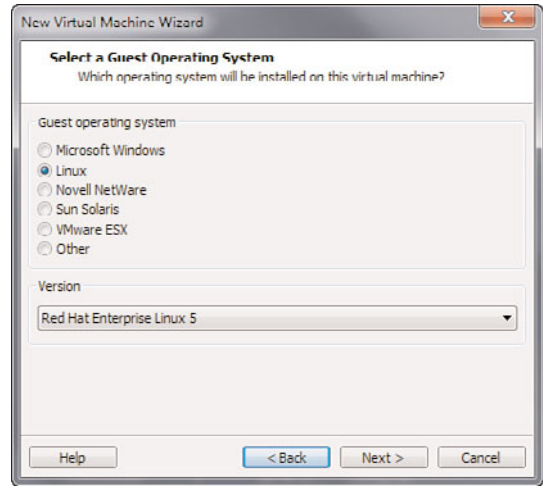
Note: For the original installer media (which is bootable) VMware Workstation discovers the version of Red Hat Linux used as the base OS, but for the upgrade media (which is not bootable) the Linux base OS is not discovered by VMware Workstation, so the next step varies depending on the version of CUCM media you have.

Step 2-3a: New Virtual Machine Wizard

(*For upgrade media (non-bootable) installs only*. If installing from original media, skip to Step 2-3b.)

Select the **Linux** radio button under the Guest Operating System, and from the Version drop-down list, for CUCM 8.6.*x*, select **Red Hat Enterprise Linux 5**. (Make sure that you do not select the 64-bit version.) (See Figure C-4a.) If installing CUCM 8.5.*x*, select **Red Hat Enterprise Linux 4**. Click **Next**. Proceed to Step 2-4.

Figure C-4a Guest OS Selection



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-3b: Personalize Linux Install Information

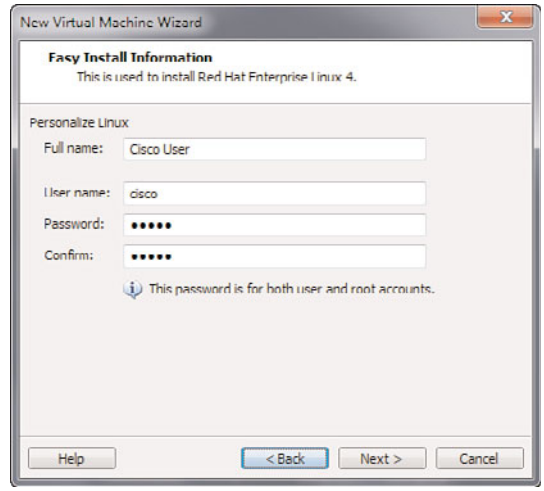
(*For original media (bootable) installs only*. If installing from upgrade media, skip to Step 2-4.)

Because VMware Workstation autodiscovers the Red Hat Linux 4 OS on the media, the Easy Install for Linux requires some information. Enter the following (see Figure C-4b):

- Full Name: **Cisco User**
- User Name: **cisco**
- Password: **cisco**
- Confirm: **cisco**

Click **Next**.

Figure C-4b Easy Install Information



Note: These names and passwords are for use only in a lab setting. A production server should use a far more complex username and password, because this will become the Linux root account on the server.

Step 2-4: Choose Machine Name and File Location

Enter the virtual machine name as **CUCM** and add the version of CUCM you are using, as shown in Figure C-5. Click the **Browse** button and navigate to the location where you want to save the virtual machine. Click **Next**.

Step 2-5: Specify Disk Capacity

Enter **100** for the Maximum disk size (GB), and leave the **Split virtual disk into multiple files** radio button selected. See Figure C-6.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure C-5 Naming the Virtual Machine

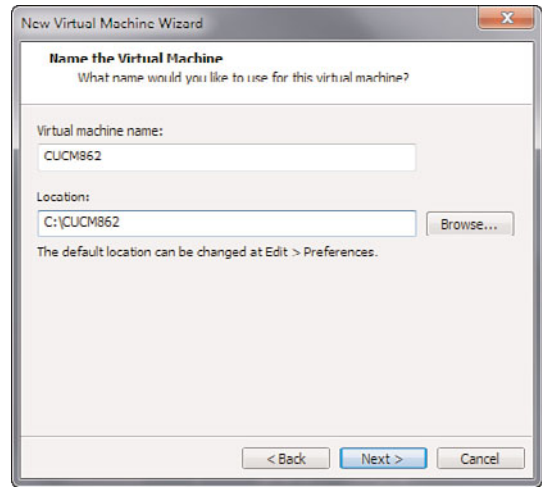
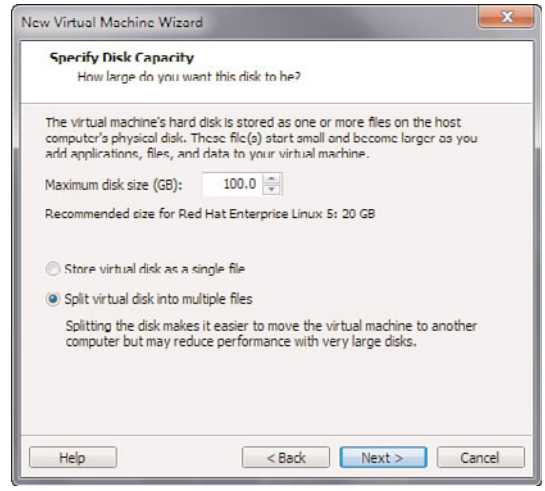


Figure C-6 Specify Disk Capacity



Note: CUCM 8.5 and 8.6 only require 80 GB to build, but VMware Workstation 7 and 8 do not allocate all the disk space up front. Instead the file grows as it is used; thus 80 GB becomes a maximum. The disk size is one of the few things that cannot be changed after the machine is built, so it is better to set it higher than needed now.

Step 2-6: Customize Hardware

The virtual machine settings are displayed. The memory and network adapter settings need to be changed before the machine can be built. Click the **Customize Hardware** button.

In the Hardware window,

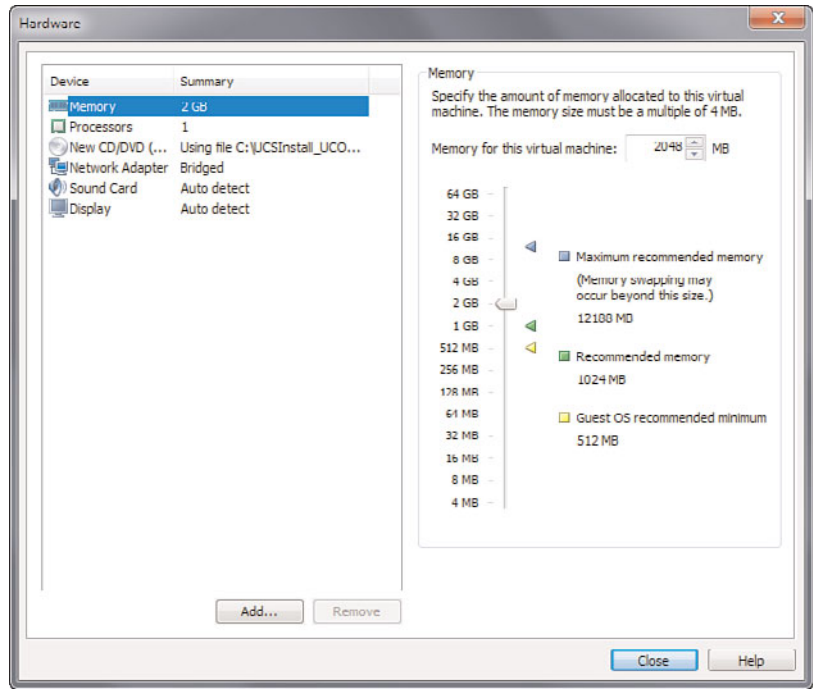
1. Click **Memory** and enter **2048** in the **Memory for this virtual machine** field, as shown in Figure C-7.
2. Click **Network Adapter** and click the **Bridged** radio button.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

3. Optimize the machine by removing unnecessary hardware, such as the floppy drive, USB controller, and printer.
4. Click **OK** to return to the hardware summary. All of these options can be easily changed after the VM is built.

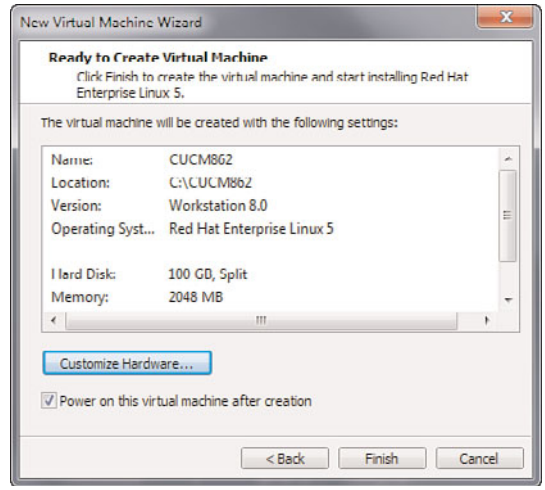
Figure C-7 Hardware Options



Step 2-7: Create Virtual Machine

Review the settings for the virtual machine and click **Finish**, as shown in Figure C-8.

Figure C-8 Hardware Settings Summary



https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 3: CUCM Installer

The CUCM installer automatically starts after the virtual machine is built.

Step 3-1: Optional Media Check

Note: No VMware tools are installed, so you need to click in the VM window to have the keyboard output sent to the VM. Press Ctrl+Alt to return your keyboard and mouse focus to the host machine.

The installer starts and several pages of text go by before the blue-background DVD Found window displays, as shown in Figure C-9. This is a classic command-line interface (CLI) text installer—the mouse will not work here! Notice that the key commands used to navigate the items are at the bottom of the screen. (The arrow keys move between elements and the Enter key selects.) The DVD Found window asks whether you want to check the media. This item is optional. If you suspect that your media might have problems, select **Yes**. Otherwise, press **Tab** to select the **No** option and press **Enter**.

Figure C-9 DVD Media Check

Note: Selecting **Yes** is recommended the first time that you use the media, as a corrupted IOS can cause the install to fail over two-thirds of the way in. (I speak from personal experience on this!)

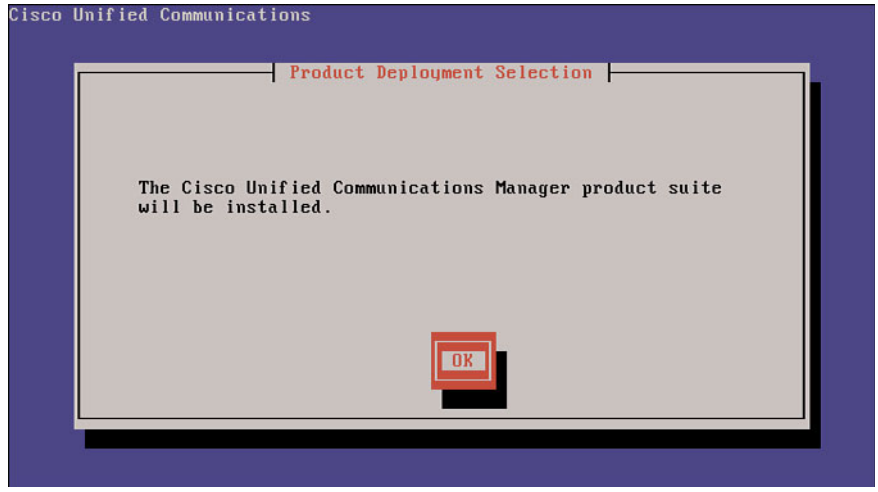
Step 3-2: Product Selection

Because the memory and hard disk space are too low for Cisco Unity Connection to be installed, only the CUCM product suite can be installed (see Figure C-10). Press **Enter**.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

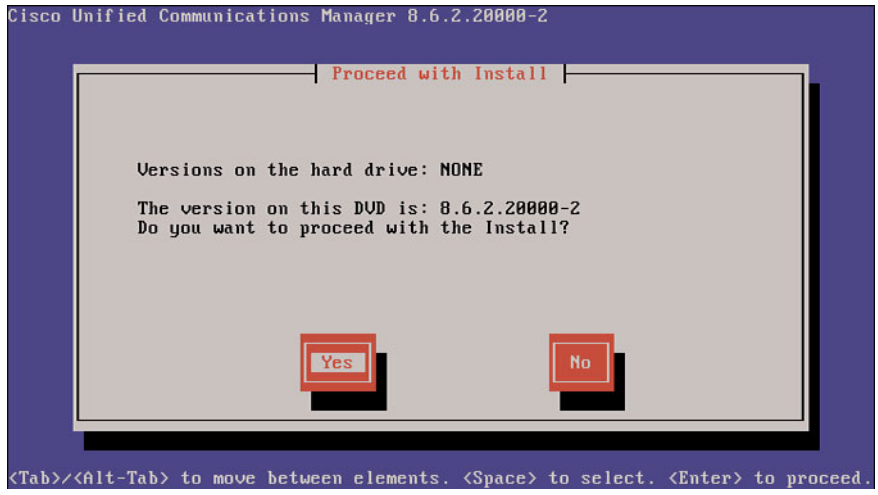
Figure C-10 Product Deployment Selection



Step 3-3: Install Verification

The installer verifies that the machine doesn't already have a previous version of CUCM installed and notifies you of the version you are installing. See Figure C-11. Press **Enter** using the **Yes** option.

Figure C-11 Install Version Verification



Step 3-4: Platform Install Wizard

See Figure C-12. Press **Enter** on the **Proceed** option.

Step 3-5: Apply Patch

Patches can be applied after the system is up and running. See Figure C-13. Press **Enter** on the **No** option.

Step 3-6: Basic Install

See Figure C-14. Press **Enter** to continue.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure C-12 Platform Installation Wizard

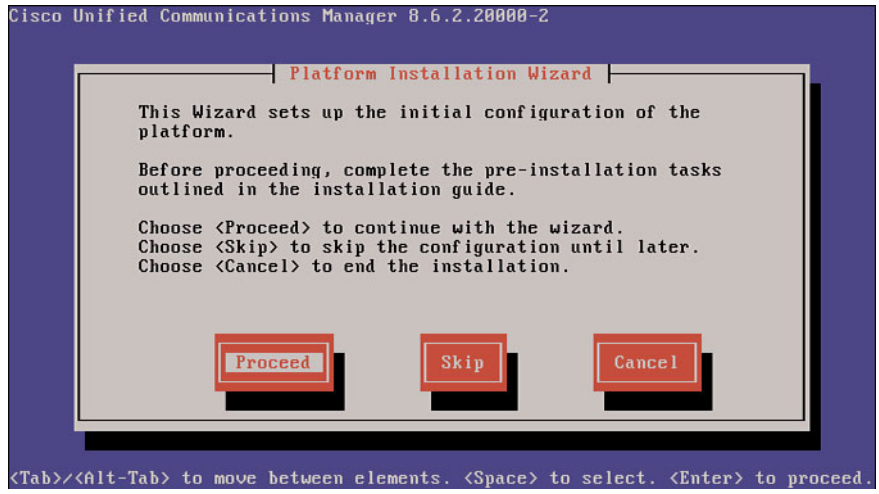


Figure C-13 Apply Patch

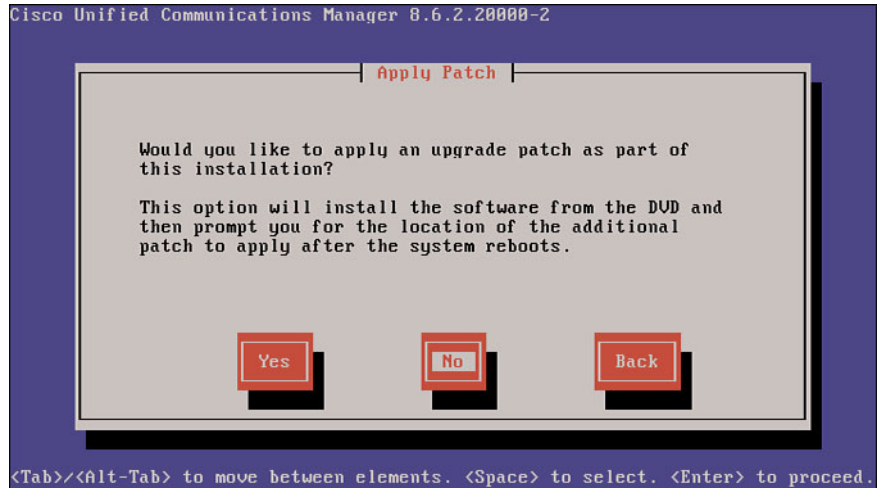
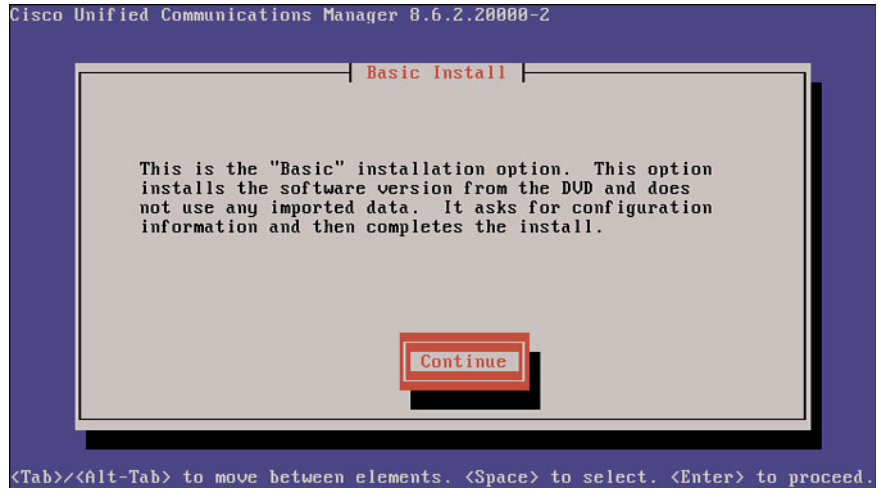


Figure C-14 Basic Install



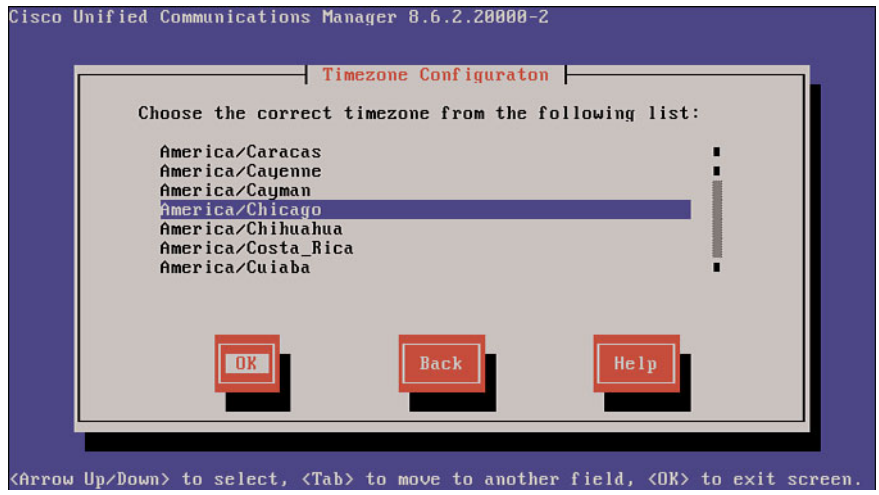
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-7: Time Zone Selection

Use the up- and down-arrow keys to choose your time zone from the list. See Figure C-15. Press **Tab** to select the **OK** option and press **Enter**.

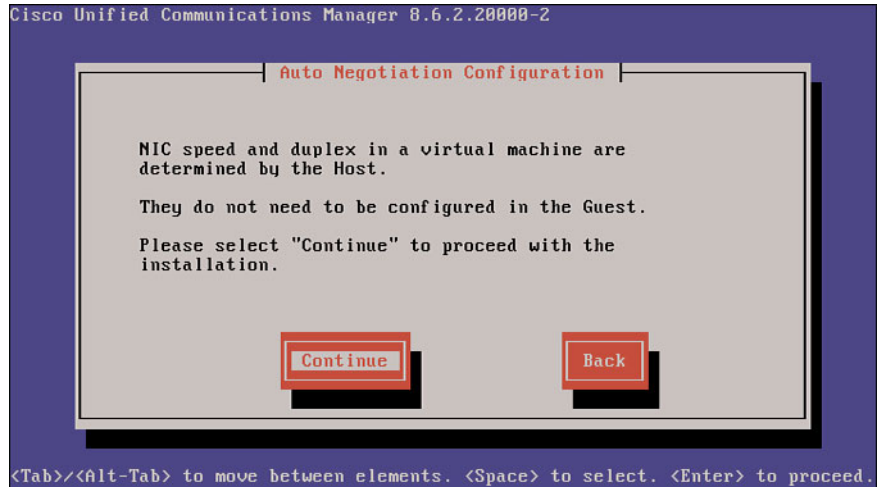
Figure C-15 Time Zone Configuration



Step 3-8: NIC Configuration

Allow autonegotiation of the network interface card (NIC). See Figure C-16. Press **Enter** to continue.

Figure C-16 NIC Autonegotiation Configuration



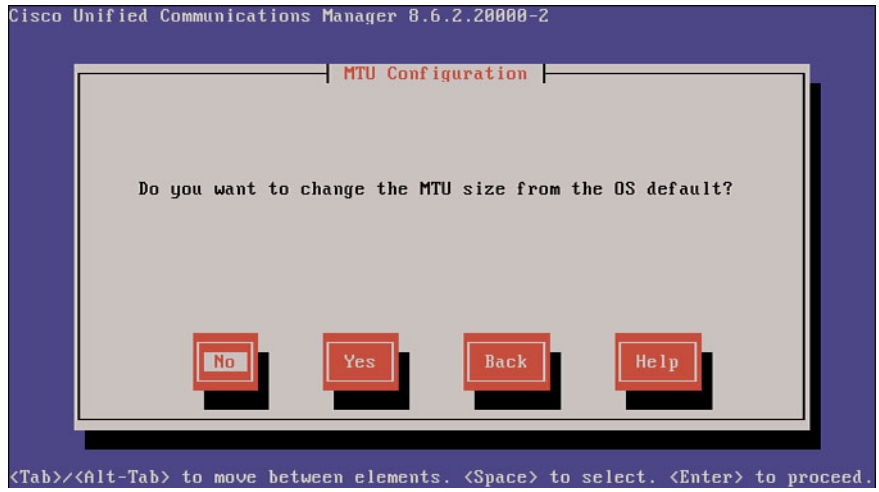
Step 3-9: MTU Configuration

The default MTU settings are fine; see Figure C-17. Press **Enter** on the **No** option.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

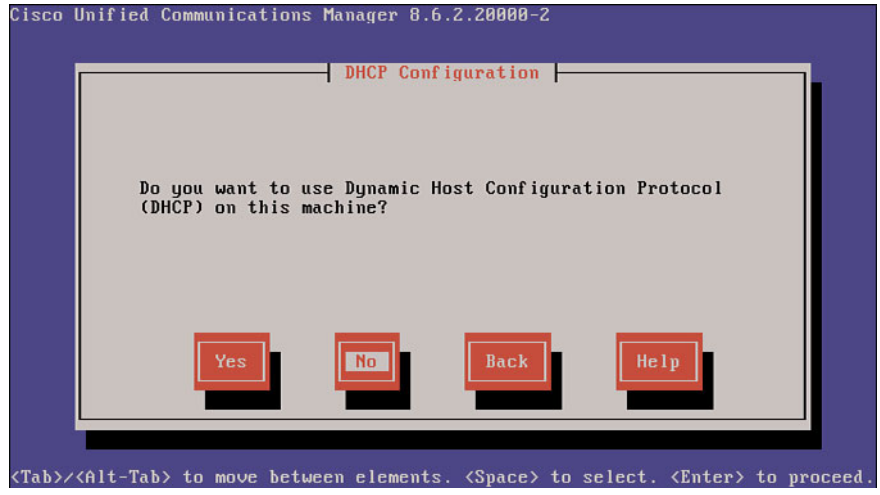
Figure C-17 MTU Configuration



Step 3-10: DHCP Configuration

We want to statically assign the IP address. See Figure C-18. Press **Enter** on the **No** option.

Figure C-18 DHCP Configuration



Step 3-11: Assign IP Address

Enter the following information, where *x* is your pod number:

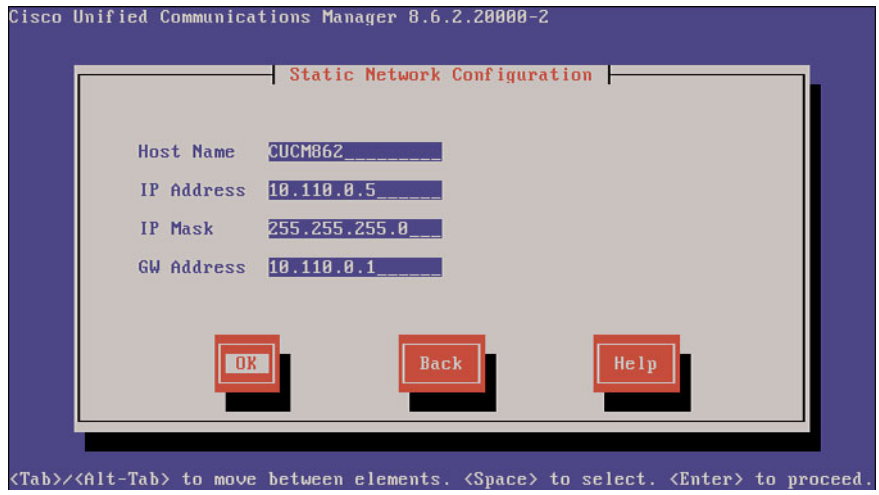
- Host Name: Enter **CUCM** and add the version of CUCM you are using.
- IP Address: **10.*x*0.0.5**
- IP Mask: **255.255.255.0**
- GW Address: **10.*x*0.0.1**

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

See Figure C-19. Press **Enter** on the **OK** option.

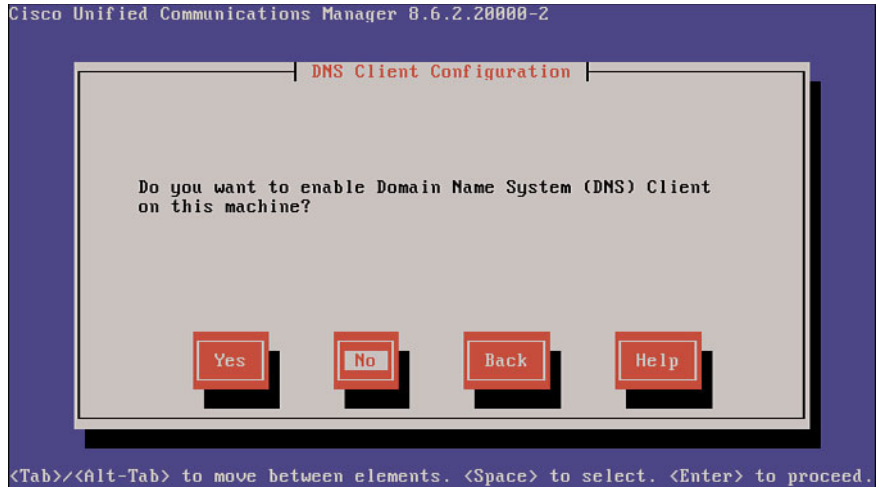
Figure C-19 Static Network Configuration



Step 3-12: DNS Client Configuration

For reasons explained in Chapter 10, "CUCM Call Flows," *Official Cert Guide CCNA-Voice 640-461,* it is better not to use Domain Name System (DNS) for the CUCM clients. Press **Tab** to select the **No** option and press **Enter**, as shown in Figure C-20.

Figure C-20 DNS Client Configuration



Step 3-13: Platform Administrator Login

CUCM creates two different administrator accounts during the install. The platform administrator has access to server settings, but not the telephony settings. This account is designed for staff operating the servers in the data center so that they can change IP addresses, back up the server, and so on, without being able to make changes to the phones or phone users. The application administrator will be created later.

https://t.me/learningnets

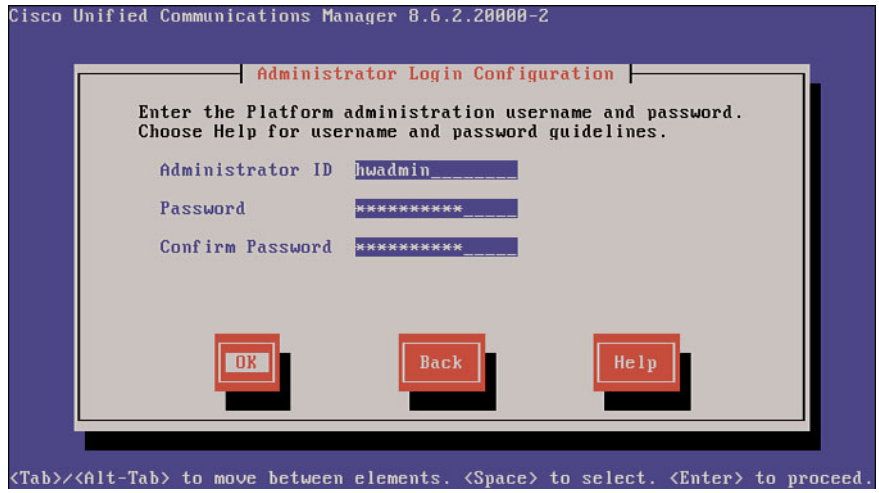
From the Library of Aliwarman Tarihoran

The password must be at least six characters long, and the system rejects passwords that seem too close to dictionary words. For this lab, use the following:

- Administrator ID: **hwadmin**
- Password: **thehwadmin**
- Confirm Password: **thehwadmin**

See Figure C-21. Press **Enter** on the **OK** option.

Figure C-21 Administrator Login Configuration



Step 3-14: Certificate Information

CUCM creates a security certificate for the server. Enter the following:

- Organization: **SOI**
- Unit: **IT**
- Location: ***<Your city>***
- State: ***<Your state>***
- Country: ***<Your country>***

See Figure C-22. Press **Enter** on the **OK** option.

Step 3-15: First Node Configuration

See Figure C-23. Press **Enter** on the **Yes** option.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure C-22 Certificate Information

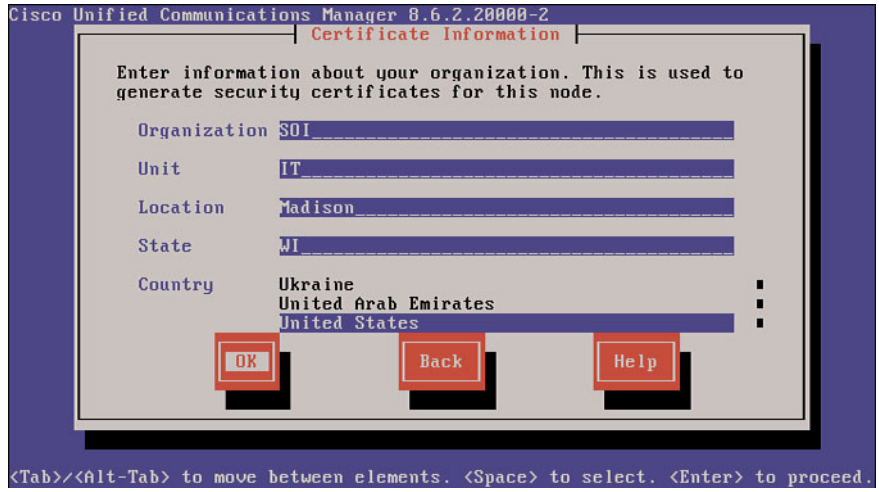
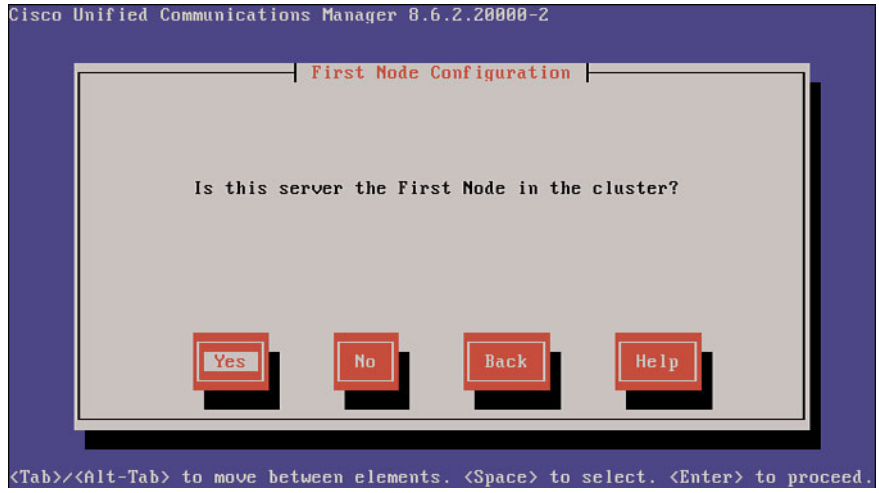


Figure C-23 First Node Configuration



Note: If you are interested in creating more than one CUCM server in the cluster, consult the CUCM install guides first, as there are a few steps to complete prior to building the second, and subsequent, servers.

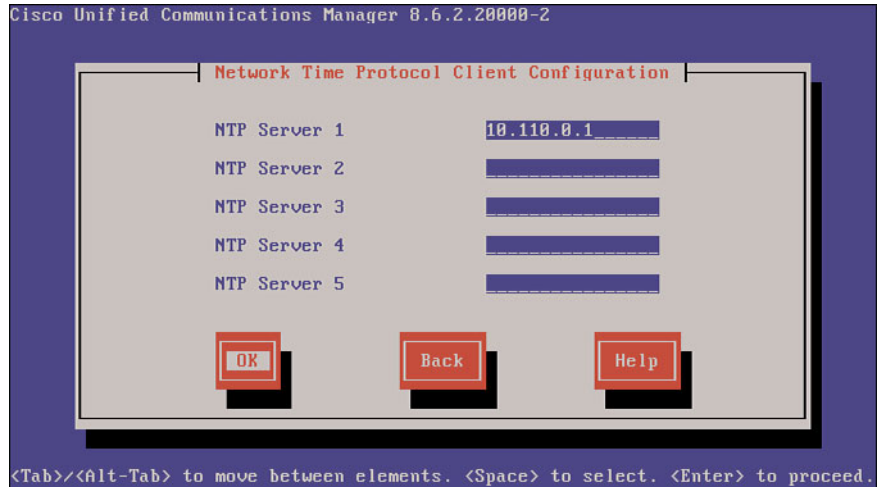
Step 3-16: NTP Client Configuration

Enter the IP address of the NTP server. (In this lab, it is your router at **10.*x*0.0.1**, where *x* is your pod number.) See Figure C-24. Press **Enter** on the **OK** option.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

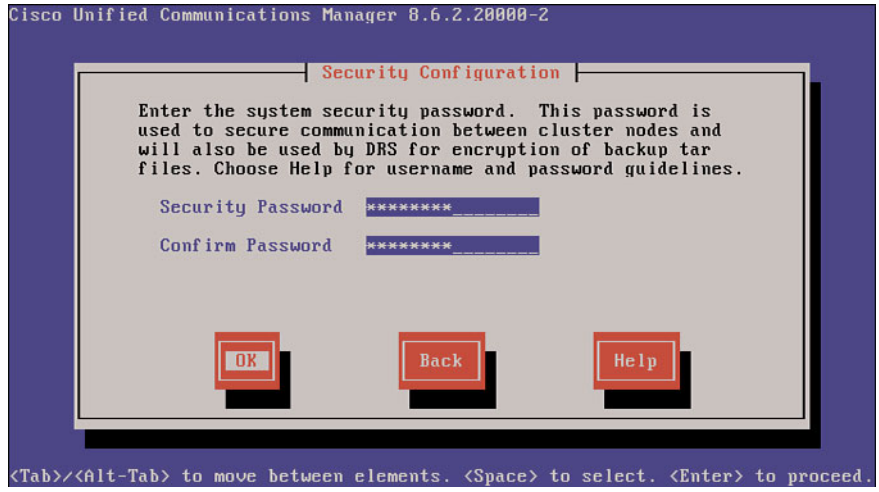
Figure C-24 NTP Client Configuration



Step 3-17: System Security Password

The security password is used for database exchanges between the servers in a CUCM cluster, and for securing backup encryption. For this lab, enter **ccnacert** for the security password and confirm password. See Figure C-25. Press **Enter** on the **OK** option.

Figure C-25 Security Configuration



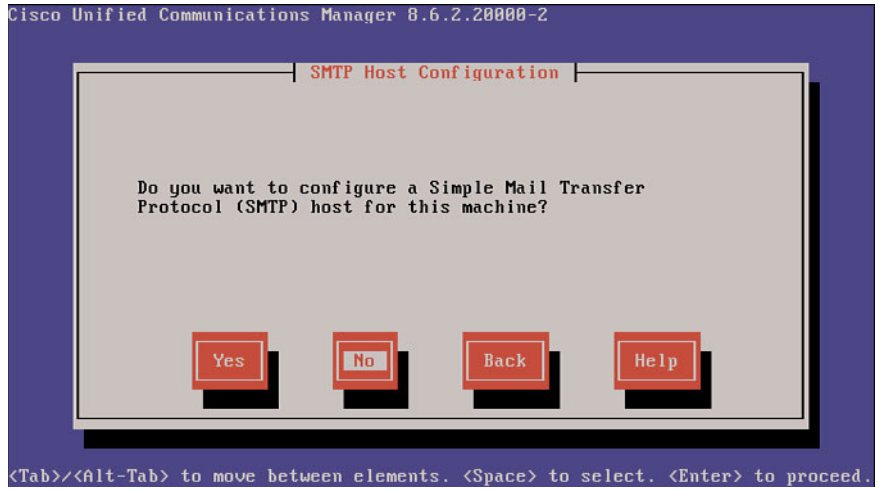
Step 3-18: SMTP Host Configuration

Because there is no email server in the lab, press **Tab** to select the **No** option and press **Enter**, as shown in Figure C-26.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure C-26 SMTP Host Configuration



Step 3-19: Application User Configuration

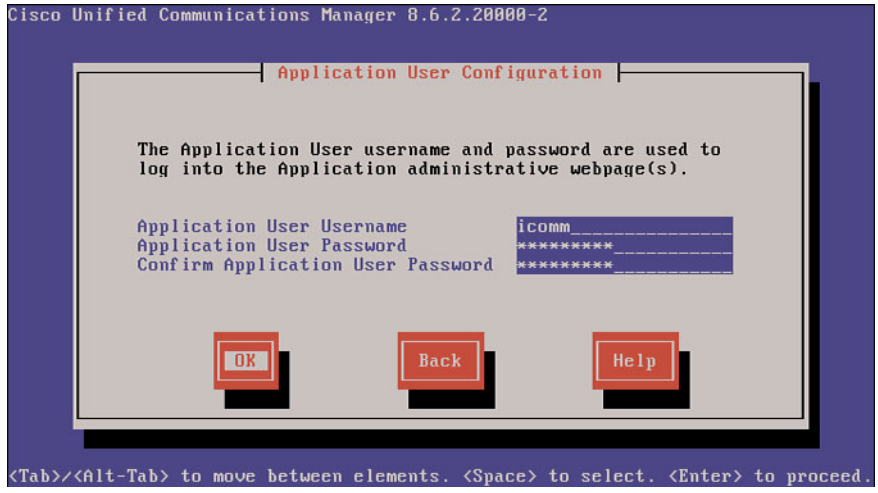
It is now time to create the second administrator account. The application administrator can make changes to telephony settings, but not the server settings. This account is designed for staff who add phones and users to the system but are not responsible for maintaining the servers in the data center.

The password must be at least six characters long, and the system rejects passwords that seem too close to dictionary words. For this lab, enter the following:

- Application User Username: **icomm**
- Application User Password: **ccnavoice**
- Confirm Application User Password: **ccnavoice**

See Figure C-27. Press **Enter** on the **OK** option.

Figure C-27 Application User Configuration



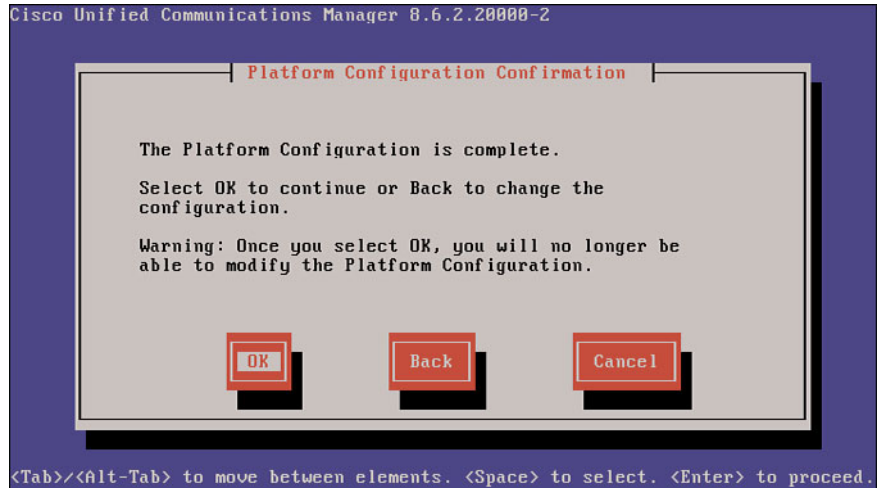
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-20: Platform Configuration Confirmation

This is your last chance to go back and change anything. When you proceed, the system begins installing the software. See Figure C-28. Press **Enter** on the **OK** option.

Figure C-28 Platform Configuration Confirmation



Step 3-21: Waiting for the Install to Complete

For 8.5.x installs, the Red Hat Enterprise GUI installer runs for a while, and then for both 8.5.x and 8.6.x, the text installer runs through many steps. This portion could take some time to complete—from 45 minutes to over two hours.

Note: The VM window might go completely black; this is just the screen saver. Press the spacebar (while the cursor focus is in the VM) and the status will show again.

When the installer is done, the standard CUCM CLI login prompt will show See Figure C-29. When logging into the CLI, use the hwadmin account you just created (password: thehwadmin).

Figure C-29 CUCM CLI Login

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 4: VMware Tools Upgrade for Original Install Media

(*For original media installs only*. If you installed from upgrade media, skip to Task 5.)

Note: Failure to update the VMware Tools will break network connectivity after a reboot.

The VMware Tools include specialized drivers for virtual drivers, and depend on the version of VMware. The tools installed from the CUCM media are designed for ESXi; they will not work properly for Workstation and need to be upgraded. Unfortunately, the tools cannot be upgraded until the VMware Red Hat Easy Install is finished, and this requires the VM to be shut down.

Step 4-1: Shutting Down the CUCM Server

To shut down the VM, log in to the CLI using the hwadmin account (password: thehwadmin). Then, enter the **utils system shutdown** command, and respond **yes** to the **Do you really want to shut down?** prompt. See Figure C-30.

Figure C-30 CLI Shutdown Process

```
Cisco Unified Communications Manager 8.6.2.20000-2
CUCM862 login: hwadmin
Password:
Last login: Wed Dec 12 02:30:39 on tty1
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        2 vCPU: Intel(R) Core(TM) i7 CPU         920  @ 2.67GHz
        Disk 1: 100GB
        2048 Mbytes RAM

admin:utils system shutdown

Do you really want to shutdown ?

Enter (yes/no)? yes_
```

Step 4-2: Removing Autoinstall ISO

After the VM is powered off, from the VM menu, select **Settings**. Click the CD/DVD (IDE) that has a summary of "Using file autoinst.iso" and click the **Remove** button, as shown in Figure C-31.

Note: Updating the tools requires a virtual CD/DVD drive, so leave the CD/DVD for the CUCM ISO attached to the machine.

You can leave the other settings as they are, or if your machine has extra resources, increase the memory or number of processors available to the VM. (If you increase the other settings, don't forget to account for the requirements of the Unity Connection, Unified Presence, and Windows server VMs needed in later labs.)

Click **OK** to close the Settings window and click the **Power On This Virtual Machine** icon to start the VM back up.

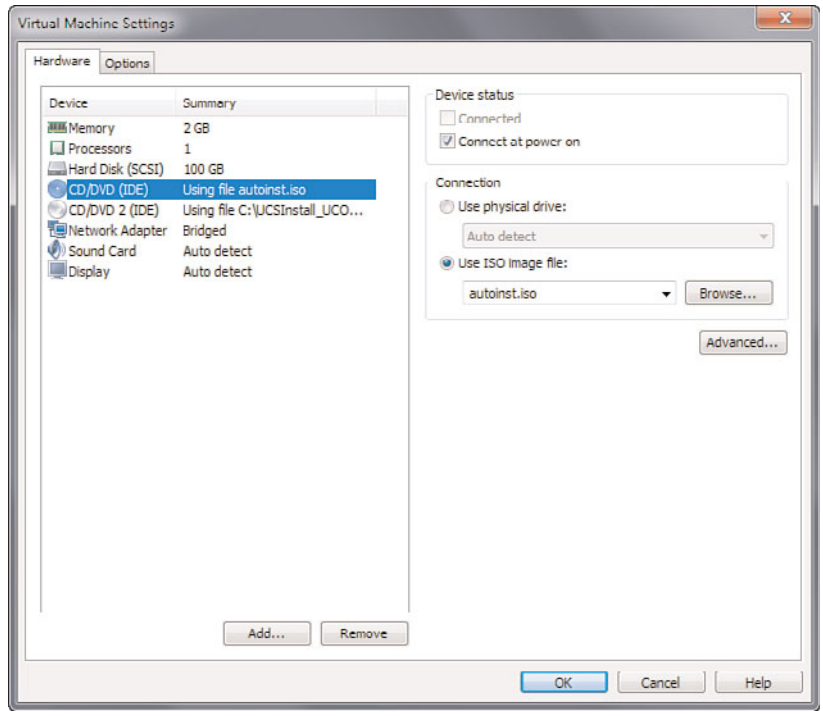
Step 4-3: Upgrading VM Tools

After the VM is powered up, log back in to the CLI to get to the command prompt. Press **Ctrl+Alt** to return the keyboard and mouse control to the host, and from the VM menu, select the **Update VMware Tools** item to mount the virtual CD. (If you run into problems, select the **Cancel VMware Tools Installation** item from the VM menu and try again.)

https://t.me/learningnets

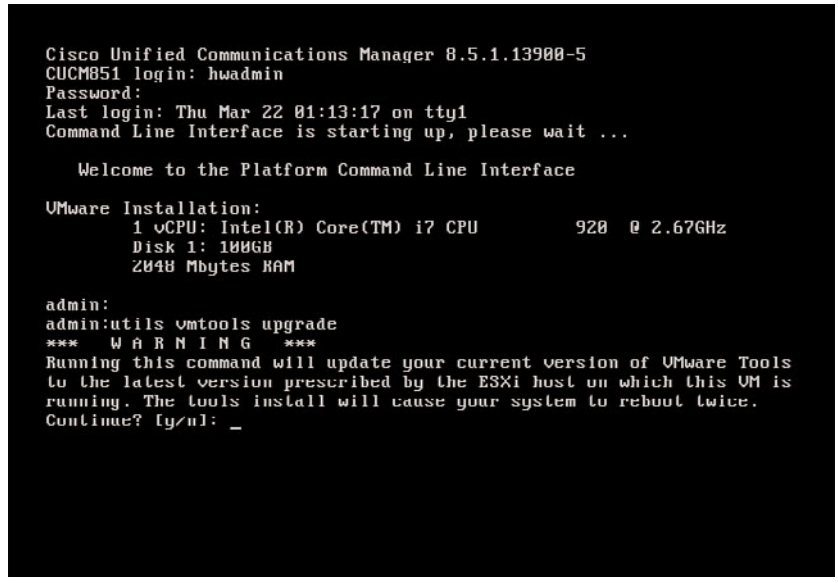
From the Library of Aliwarman Tarihoran

Figure C-31 Remove Autoinstall CD/DVD Virtual Drive



From the CUCM CLI, enter the **utils vmtools upgrade** command and enter **y** at the **Continue? (y/n)** prompt. (The **y** will not show on the screen.) See Figure C-32.

Figure C-32 VMware Tools Install in 8.5.x



The installer will notify you of the current tools version and the new tools version before starting the script that will remove the old tools and install the new version. The VM will reboot twice during the process, and the tools upgrade is complete when the command prompt allows you to log in again.

Skip to Task 6.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Task 5: VMware Tools Upgrade for Upgrade Media

(*For upgrade media installs only.* If you are using the original full install media, skip to Task 6.)

The VMware Tools include specialized drivers for virtual drivers and depend on the version of VMware. Luckily, the upgrade install media no longer seems to install older drivers, so the upgrade to the current version of tools is relatively painless.

Step 5-1: Upgrading VM Tools

Log in to the CLI using the hwadmin account (password: thehwadmin). Press **Ctrl+Alt** to return the keyboard and mouse control to the host, and from the VM menu, select the **Update VMware Tools** item to mount the virtual CD. (If you run into problems, select the **Cancel VMware Tools Installation** item from the VM menu and try again.)

From the CUCM CLI, enter the **utils vmtools upgrade** command and enter **y** at the **Continue? (y/n)** prompt, as shown in Figure C-33.

Figure C-33 VMware Tools Install in 8.6.x

```
CUCM862 login: hwadmin
Password:
Last login: Sat Apr 21 20:56:10 on tty1
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        1 vCPU: Intel(R) Core(TM) i7 CPU         920  @ 2.67GHz
        Disk 1: 100GB
        2048 Mbytes RAM

admin:utils vmtools upgrade

VMware Tools are out-of-date. Proceeding with tools upgrade.

***   W A R N I N G   ***
Running this command will update your current version of VMware Tools
to the latest version prescribed by the ESXi host on which this VM is
running. The tools install will cause your system to reboot twice.

Continue (y/n)?y

Starting VMware Tools upgrade ...
_
```

The server will start installing the new version. The VM will reboot twice during the process, and the tools upgrade is complete when the command prompt allows you to log in again.

Step 5-2: Shutting Down the CUCM Server

To shut down the VM, log in to the CLI using the hwadmin account (password: thehwadmin). Then enter the **utils system shutdown** command, and respond **yes** to the **Do you really want to shut-down?** prompt. Refer to Figure C-30.

Task 6: Entering Descriptions in the System (Optional)

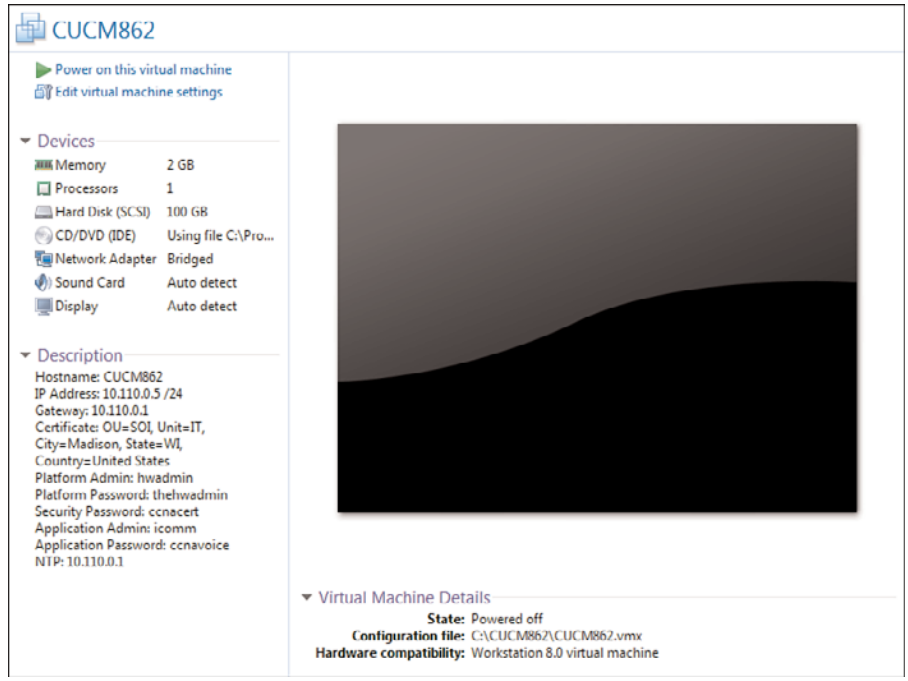
Given all the IP addresses, usernames, and passwords you just created, it is a good idea to note those that you used so that you don't forget them and later end up locked out of the VM. VMware has a

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Description section (Notes in VMware 7) for each VM. This is a good place to store information for a lab server. (This would be a security risk for a production server, however.) Before you forget, enter all the items you entered while building the server in the description. See Figure C-34 for an example.

Figure C-34 VMware Notes



Task 7: Tips for Cisco Unified Communications Servers and VMware Workstation

- When starting a Unified Communications server VM image that is shutdown, it takes time for all of the services to load. Even if the command prompt is responding, the services for the administrative web pages might not be loaded yet. On really slow machines, tested in the classroom, it took as long 20 minutes to completely boot a CUCM server from an external USB 2.0 hard drive. (See the next tip to help with this problem.)
- While I would not attempt this in a production environment, to avoid having the class wait for the servers to start up, I have used the VMware **Suspend** and **Resume** options on the VMs successfully for weeks at a time. (Make sure your NTP source is accurate, and never goes back in time.) If you follow this tip, to avoid any possibility of problems, make frequent backups of the VM.
- VMware Workstation has a handy feature called Snapshot. A snapshot takes an image of the VM and allows you to experiment with the VM, and later restore the VM back to the point in time when the snapshot was made. This can be a great feature when experimenting with new features without worrying about losing your previous work. (Using a snapshot is recommended when doing Lab 9-9.) However, snapshots do not replace the necessity of backups. VMware recommends that you create no more than two or three snapshots without reverting back, or the performance will degrade on the VM. See VMware knowledge base article 1025279 for more details. Also be aware that if you take a snapshot of a running VM, the entire contents of the RAM of the VM gets saved to disk as a file, which can quickly increase the disk space used by the VM.

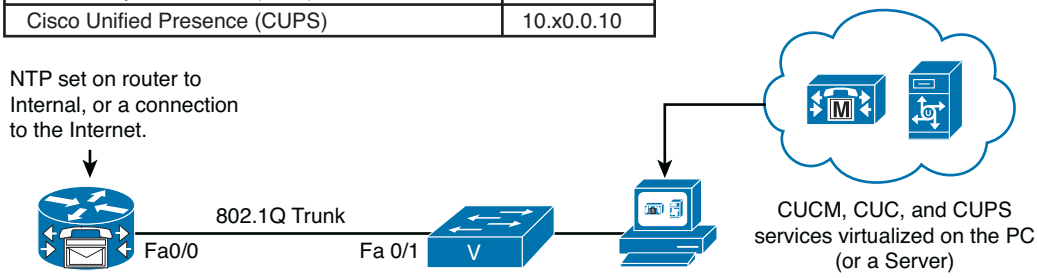
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab C-2: Build Cisco Unity Connection (CUC) Image

Figure C-34 Topology Diagram

Server	IP Address
Cisco Unified Communication Manager (CUCM)	10.x0.0.5
Cisco Unity Connection (CUC)	10.x0.0.8
Cisco Unified Presence (CUPS)	10.x0.0.10



Equipment Required

This lab uses the following equipment:

- Cisco router.
- Switch that supports voice VLANs.
- Lab configuration from Lab 3-2. (NTP *must* be accessible or simulated on the router for the build to complete.)
- PC with VMware Workstation installed and enough disk space and memory. This lab demonstrates VMware Workstation 8 on a machine with a minimum of 8 GB RAM. (The results are identical with VMware 7.x.) Note: The Unity Connection VM requires 4 GB to build, so a host machine with 4 GB RAM would be page-swapping memory, causing *extremely* slow performance.
- Access to the install DVD or ISO file for CUCM and Unity Connection. (This lab shows both versions, 8.6.2 and 8.5.1. Versions later than 6.0 should work, but might require work-arounds. Specifically, any CUC before version 8.0 was not designed to run in VMware, so search the Internet for solutions on the install.)

Task 1: Configure and Cable Devices

Cable the router, switch, and PC together as shown in the topology diagram. Apply the configuration from Labs 3-1 and 3-2 to the router and switch. Make sure that the router is receiving NTP from the Internet or another Cisco router as detailed in Lab 3-2, as an NTP server with a stratum less than or equal to 6 is required to install CUC.

Task 2: Build the Virtual Machine

Note: The process to install and build the Cisco Unity Connection (CUC) server is nearly identical to installing the CUCM server. In fact, the software is on the same ISO file or DVD that was used for building the CUCM server. Repeat *all* the tasks in Lab C-1, but make the following changes in the steps indicated.

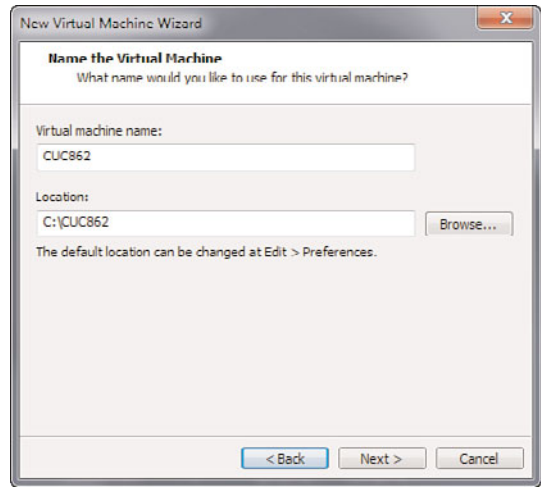
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-4: Choose Machine Name and File Location

Enter the virtual machine name as **CUC** and add the version of CUC you are using. Click the **Browse** button and navigate to the location where you want to save the virtual machine. Click **Next**. See Figure C-36.

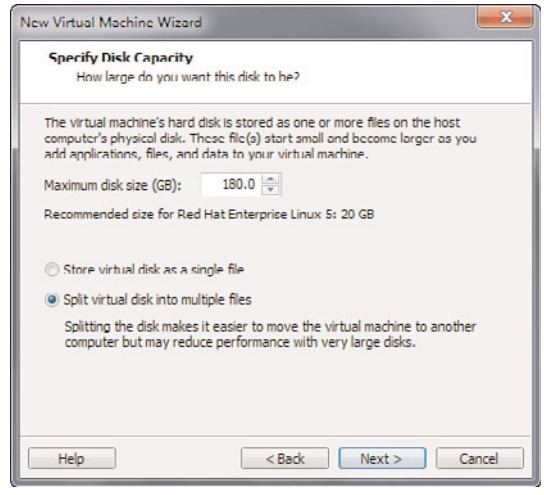
Figure C-36 CUC Naming the Virtual Machine



Step 2-5: Specify Disk Capacity

Enter **180** for the Maximum disk size (GB), and leave the **Split virtual disk into multiple files** radio button selected. See Figure C-37.

Figure C-37 CUC Specify Disk Capacity



Note: CUC 8.5 and 8.6 require only 160 GB to build, but VMware Workstation 7 and 8 do not allocate all the disk space up front. Instead, the file grows as it is used; thus the 160 GB becomes a maximum. The disk size is one of the few things that cannot be changed after the machine is built, so it is better to set it higher than needed now.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-6: Customize Hardware

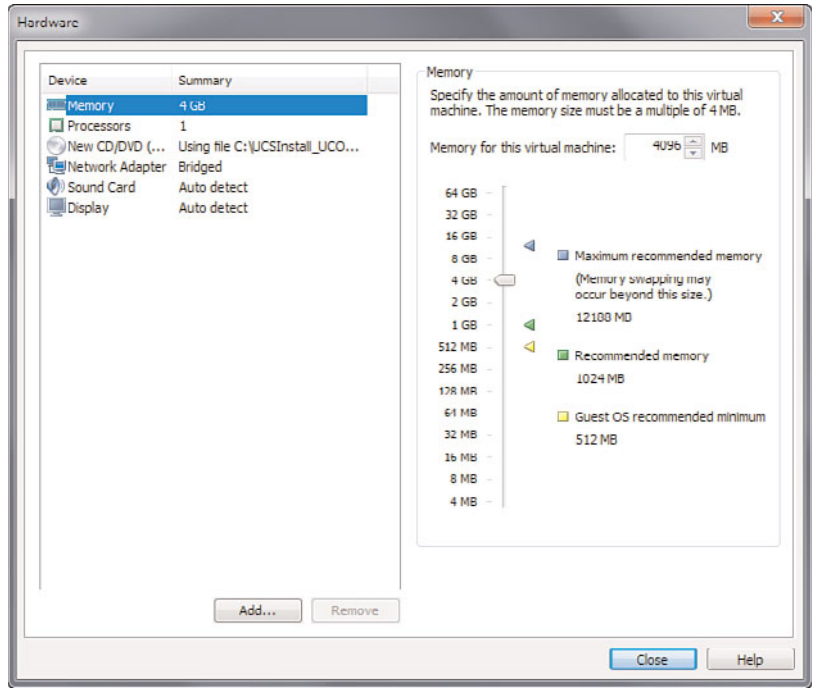
The virtual machine settings are displayed. The memory and network adapter settings need to be changed before the machine can be built. Click the **Customize Hardware** button.

Note: CUC 8.5 and 8.6 require a minimum of 4 GB RAM and 160 GB of disk space, or the option to install will not even show up. The install will also fail if you allocate more than one processor to the VM during the build.

In the Hardware window,

1. Click **Memory** and enter **4096** in the **Memory for this virtual machine** field, as shown in Figure C-38.
2. Click **Network Adapter** and click the **Bridged** radio button.
3. Optimize the machine by removing unnecessary hardware, such as the floppy drive, USB controller, and printer.
4. Click **OK** to return to the hardware summary. All of these options can be easily changed after the VM is built.

Figure C-38 CUC Hardware Options



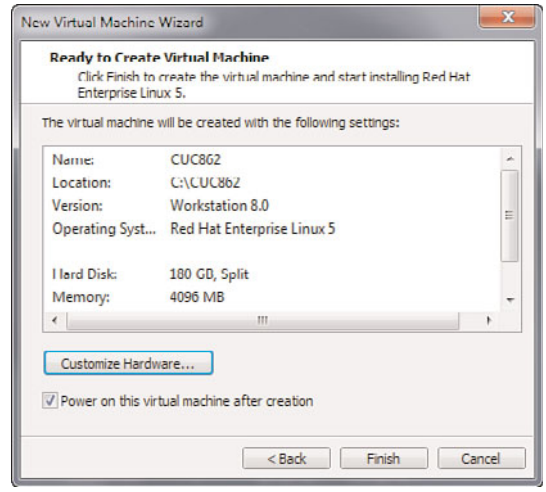
Step 2-7: Create Virtual Machine

Review the settings for the virtual machine and click **Finish**, as shown in Figure C-39.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure C-39 CUC Hardware Settings Summary

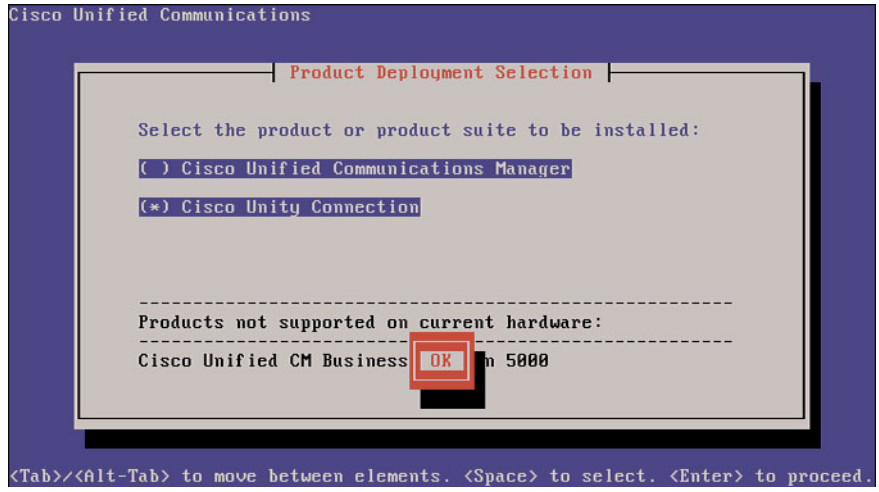


Task 3: CUC Installer

Step 3-2: Product Selection

Now that the server has more memory and hard disk space, the installer offers the option to select CUC. Press the **Tab** key to move to the **Cisco Unity Connection** item and press the spacebar to select. See Figure C-40. Press **Tab** again to select the **OK**, and press **Enter**.

Figure C-40 CUC Product Deployment Selection



Step 3-11: Assign IP Address

Enter the following information, where *x* is your pod number (see Figure C-41):

- Host Name: Enter **CUC** and add the version of CUC you are using.
- IP Address: **10.*x*0.0.8**

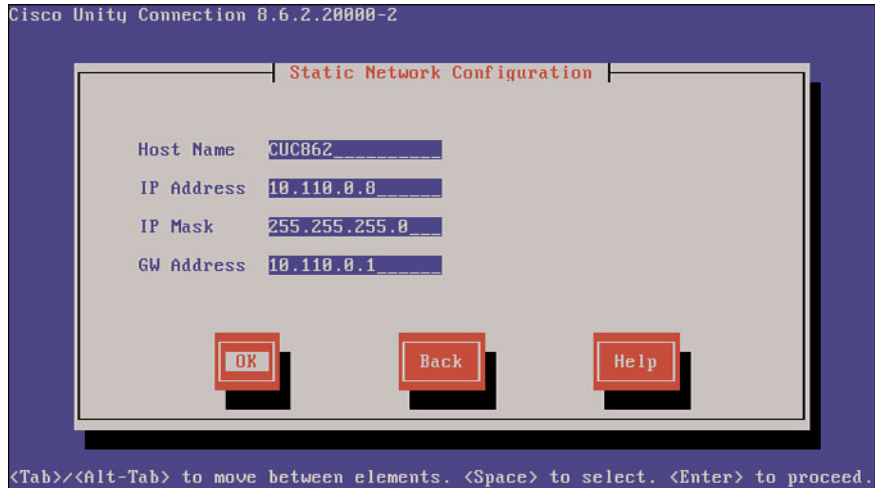
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

- IP Mask: **255.255.255.0**
- GW Address: **10.*x*0.0.1**

Press **Enter** on the **OK** option.

Figure C-41 CUC Static Network Configuration



Step 3-15: First Node Configuration

Press **Enter** on the **Yes** option.

Note: The CUC server is not part of the CUCM cluster, so it will still be the first node in a new cluster.

Step 3-17: System Security Password

The security password used must be the same one used when installing CUCM. For this lab, enter **ccnacert** for the security password and confirm password. Press **Enter** on the **OK** option.

Task 4: VMware Tools Upgrade for Original Install Media

Step 4-2: Removing Autoinstall ISO

Leave the number of processors at 1 to make sure that the system is stable.

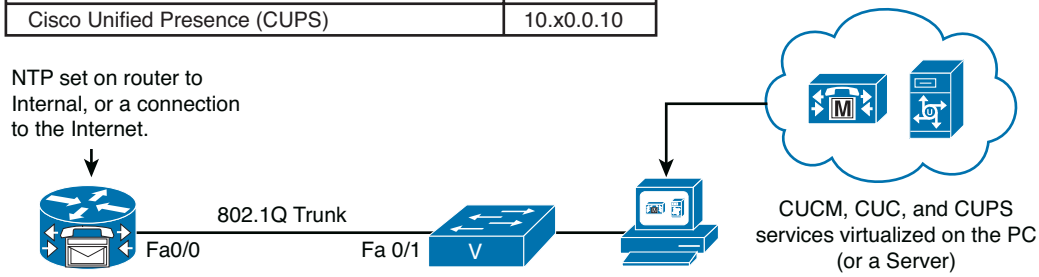
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Lab C-3: Build Cisco Unified Presence Server (CUPS) Image

Figure C-42 Topology Diagram

Server	IP Address
Cisco Unified Communication Manager (CUCM)	10.x0.0.5
Cisco Unity Connection (CUC)	10.x0.0.8
Cisco Unified Presence (CUPS)	10.x0.0.10



Equipment Required

This lab uses the following equipment:

- Cisco router.
- Switch that supports voice VLANs.
- Lab configuration from Lab 3-2. (NTP *must* be accessible or simulated on the router for the build to complete.)
- PC with VMware Workstation installed and enough disk space and memory. This lab demonstrates VMware Workstation 8 on a machine with a minimum of 8 GB RAM. (The results are identical with VMware 7.x.)
- Access to the install DVD or ISO file for Cisco Unified Presence (CUPS). (This lab shows version 8.6.3.)

Note: CUPS provides a 90-day trial license. Unless you have valid licenses, wait to build the CUPS virtual machine until needed to avoid having the trial license expire.

Task 1: Configure and Cable Devices

Cable the router, switch, and PC together as shown in the topology diagram. Apply the configuration from Labs 3-1 and 3-2 to the router and switch. Make sure that the router is receiving NTP from the Internet or another Cisco router as detailed in Lab 3-2, as an NTP server with a stratum less than or equal to 6 is required to install CUPS.

Task 2: Build the Virtual Machine

Note: The process to install and build the Cisco Unified Presence Server (CUPS) is nearly identical to installing the CUCM server. Repeat all the tasks in Lab C-1, but make the following changes in the steps indicated.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 2-2 Choose Install Media

The CUPS software is on a different DVD or ISO file than the CUCM or CUC. Locate the correct media for CUPS.

Step 2-4: Choose Machine Name and File Location

Enter the virtual machine name as **CUPS** and add the version of CUPS you are using. Click the **Browse** button and navigate to the location where you want to save the virtual machine. Click **Next**.

Step 2-5: Specify Disk Capacity

Enter **100** for the Maximum disk size (GB), and leave the **Split virtual disk into multiple files** radio button selected.

Note: CUPS 8.5 and 8.6 require only 80 GB to build, but VMware Workstation 7 and 8 do not allocate all the disk space up front. Instead, the file grows as it is used; thus the 80 GB becomes a maximum. The disk size is one of the few things that cannot be changed after the machine is built, so it is better to set it higher than needed now.

Step 2-6: Customize Hardware

The virtual machine settings are displayed. The memory and network adapter settings need to be changed before the machine can be built. Click the **Customize Hardware** button.

In the Hardware window:

1. Click **Memory** and enter **2048** in the **Memory for this virtual machine** field.
2. Click **Network Adapter** and click the **Bridged** radio button.
3. Optimize the machine by removing unnecessary hardware, such as the floppy drive, USB controller, and printer.
4. Click **OK** to return to the hardware summary. All of these options can be easily changed after the VM is built.

Note: Both 8.5.x and 8.6.x will allow you to run the VM with more then one processor.

Task 3: CUPS Installer

Step 3-11: Assign IP Address

Enter the following information, where *x* is your pod number:

- Host Name: Enter **CUPS** and add the version of CUPS you are using.
- IP Address: **10.*x*0.0.10.**
- IP Mask: **255.255.255.0.**
- GW Address: **10.*x*0.0.1.**

Press **Enter** on the **OK** option.

Step 3-15: First Node Configuration

Press **Enter** on the **Yes** option.

Note: The CUPS server is not part of the CUCM cluster, so it will still be the first node in a new cluster.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-17: System Security Password

The security password used must be the same one used when installing CUCM. For this lab, enter **ccnacert** for the security password and confirm password. Press **Enter** on the **OK** option.

Task 7: CUPS Postinstallation Deployment Wizard

After the CUPS virtual machine is built and the VMware Tools are updated, there are a few special steps involved. The first time you access the web interface of the CUPS server, a postinstallation deployment wizard will run. This wizard will only run the first time you connect, so don't connect to the CUPS server until directed to do so in Lab 14-1.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

This page intentionally left blank

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

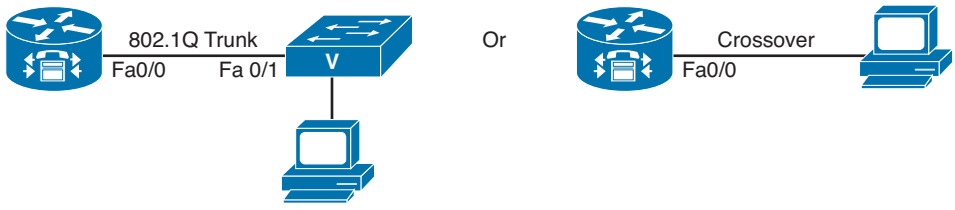
APPENDIX D

Configuring the Cisco Unified Communications Manager Express Router

This appendix explores configuring the router to have an IOS and describes the support files necessary for CUCME to function. The process to upgrade (or downgrade) the firmware on the phones is also covered.

Lab D-1: Configuring the CUCME Router

Figure D-1 Topology Diagram



Equipment Required

This lab uses the following equipment:

- Cisco router
- PC with TFTP software
- (Optional) Switch that supports voice VLANs

Learning Objectives

Upon completion of this lab, you will be able to

- Upgrade the IOS to support CUCME
- Install the optional support files
- Upgrade/downgrade firmware on the phone

Task 1: Obtain the Desired Version of the IOS and CUCME Support Files

To obtain the latest files, a valid Cisco Support Contract is required. Alternatively, you can reinstall the existing version of the IOS and support files if you have them. If not, read the examples provided in the lab.

Note: If you work at a Cisco Networking Academy that has signed up for Academy Maintenance, you should be able to download the IOS at no cost and order the hardware at a discount. Check the Academy website or talk with your Academy Support Center about how to do this.

---

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 1-1: Examine Your Router Hardware

Important: Before downloading the latest versions of the IOS and support files, make sure that the router in question has the appropriate amount of RAM and flash to support the new version. Newer versions of the IOS and support files can easily exceed the memory or flash file space on a standard router. Use the **show version** command to verify your existing IOS version and the amount of RAM and flash. In Example D-1, this 2811 router is running the Release 12.4(24)T1 IOS with the advanced enterprise feature set, has 256 MB of RAM (add the two numbers together), and a 64-MB compact flash card.

Example D-1 show version Command

```
Router# show version
Cisco IOS Software, 2800 Software (C2800NM-ADVENTERPRISEK9-M), Version 12.4(24)T1,
  RELEASE SOFTWARE (fc3)
<output omitted>
System returned to ROM by power-on
System image file is "flash:c2800nm-adventerprisek9-mz.124-24.T1.bin"
<output omitted>
Cisco 2811 (revision 53.50) with 247808K/14336K bytes of memory.
Processor board ID
2 FastEthernet interfaces
3 Serial interfaces
1 Channelized/Clear T1/PRI ports
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

After you know the RAM and flash size of your router, you can determine which IOS you will need.

Step 1-2: Understand CUCME and IOS Version

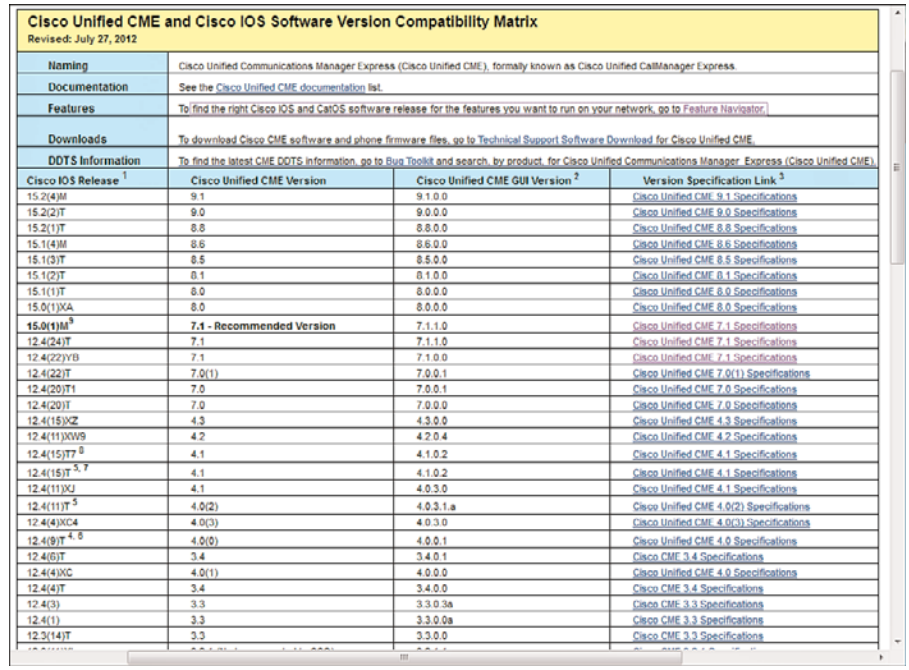
For each version of CUCME, there are recommended IOS versions to use. To see the recommended IOS versions, go to Cisco.com and search for "Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix." See Figure D-2 for an example of this page.

If you know which CUCME version you want to run, the IOS version listed in the left column is the recommended IOS version you should use. (The labs in this lab book were written using CUCME version 7.1). Likewise, if you do not have the ability to download IOS images from Cisco.com, the matrix will tell you what version of CUCME your current IOS will support. The next step is to verify whether the IOS feature set supports CUCME.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Figure D-2 Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix



Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix
Revised: July 27, 2012

Naming	Cisco Unified Communications Manager Express (Cisco Unified CME), formally known as Cisco Unified CallManager Express.
Documentation	See the Cisco Unified CME documentation list.
Features	To find the right Cisco IOS and CatOS software release for the features you want to run on your network, go to Feature Navigator.
Downloads	To download Cisco CME software and phone firmware files, go to Technical Support Software Download for Cisco Unified CME.
DDTS Information	To find the latest CME DDTS information, go to Bug Toolkit and search, by product, for Cisco Unified Communications Manager Express (Cisco Unified CME).

Cisco IOS Release [1]	Cisco Unified CME Version	Cisco Unified CME GUI Version [2]	Version Specification Link [3]
15.2(4)M	9.1	9.1.0.0	Cisco Unified CME 9.1 Specifications
15.2(2)T	9.0	9.0.0.0	Cisco Unified CME 9.0 Specifications
15.2(1)T	8.8	8.8.0.0	Cisco Unified CME 8.8 Specifications
15.1(4)M	8.6	8.6.0.0	Cisco Unified CME 8.6 Specifications
15.1(3)T	8.5	8.5.0.0	Cisco Unified CME 8.5 Specifications
15.1(2)T	8.1	8.1.0.0	Cisco Unified CME 8.1 Specifications
15.1(1)T	8.0	8.0.0.0	Cisco Unified CME 8.0 Specifications
15.0(1)XA	8.0	8.0.0.0	Cisco Unified CME 8.0 Specifications
15.0(1)M [9]	**7.1 - Recommended Version**	7.1.1.0	Cisco Unified CME 7.1 Specifications
12.4(24)T	7.1	7.1.1.0	Cisco Unified CME 7.1 Specifications
12.4(22)YB	7.1	7.1.0.0	Cisco Unified CME 7.1 Specifications
12.4(22)T	7.0(1)	7.0.0.1	Cisco Unified CME 7.0(1) Specifications
12.4(20)T1	7.0	7.0.0.1	Cisco Unified CME 7.0 Specifications
12.4(20)T	7.0	7.0.0.0	Cisco Unified CME 7.0 Specifications
12.4(15)XZ	4.3	4.3.0.0	Cisco Unified CME 4.3 Specifications
12.4(11)XW9	4.2	4.2.0.4	Cisco Unified CME 4.2 Specifications
12.4(15)T7 [8]	4.1	4.1.0.2	Cisco Unified CME 4.1 Specifications
12.4(15)T [5, 7]	4.1	4.1.0.2	Cisco Unified CME 4.1 Specifications
12.4(11)XJ	4.1	4.0.3.0	Cisco Unified CME 4.1 Specifications
12.4(11)T [5]	4.0(2)	4.0.3.1.a	Cisco Unified CME 4.0(2) Specifications
12.4(4)XD4	4.0(3)	4.0.3.0	Cisco Unified CME 4.0(3) Specifications
12.4(9)T [4, 6]	4.0(0)	4.0.0.1	Cisco Unified CME 4.0 Specifications
12.4(6)T	3.4	3.4.0.1	Cisco CME 3.4 Specifications
12.4(4)XC	4.0(1)	4.0.0.0	Cisco Unified CME 4.0 Specifications
12.4(4)T	3.4	3.4.0.0	Cisco CME 3.4 Specifications
12.4(3)	3.3	3.3.0.3a	Cisco CME 3.3 Specifications
12.4(1)	3.3	3.3.0.0a	Cisco CME 3.3 Specifications
12.3(14)T	3.3	3.3.0.0	Cisco CME 3.3 Specifications

Step 1-3: Understand IOS Feature Sets

Note: It is nearly impossible to cover all the possible router hardware and IOS versions. You should verify this information by searching for data sheets for your specific hardware on Cisco.com.

As an example of the difficulty in explaining all possibilities, consider IOS 15.x. IOS 15.x for the newer 2900 and 3900 ISR2 routers is a single image with licenses required to enable various features, such as voice. However, IOS 15.x for older 2800 and 3800 ISR routers still has different feature sets for the same IOS version.

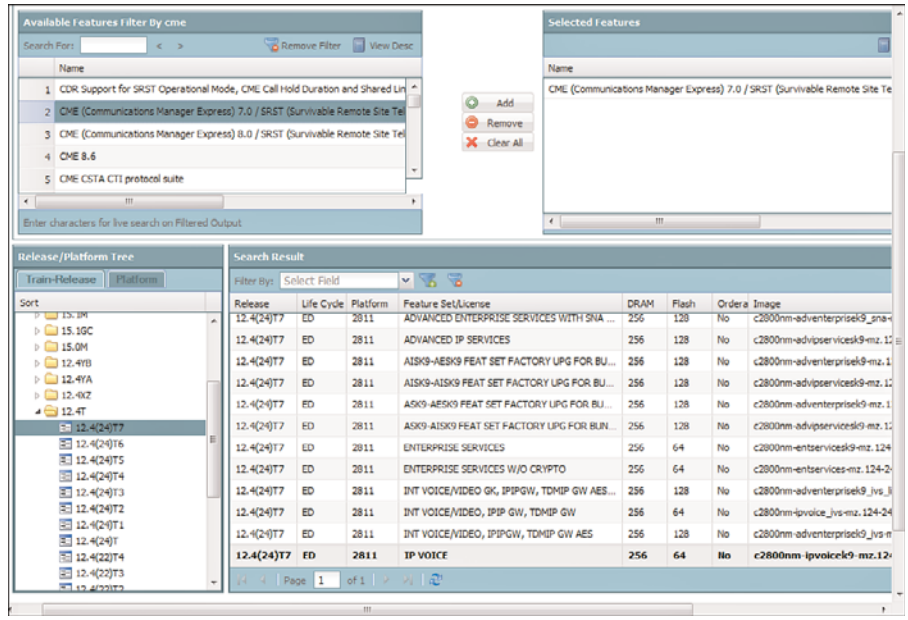
The CUCME functionality is built into selected IOS versions (except for ISR2 routers, which just require a license). To determine which IOS has voice features, you should access the Cisco Feature Navigator (search for "Cisco Feature Navigator" on Cisco.com).

1. In the Feature Navigator, select **Search by Feature**.
2. Search for **CME**, and select the version of CME you want to use.
3. Click the **Add** button to move the version to the **Selected Features** box.
4. Click **Continue** (on the far right of the page).
5. The IOS Release/Platform navigation pane opens below.
6. Select and open the version of the IOS that you are interested in. The Search Result pane shows the various router hardware, feature set, and RAM/flash requirements. Figure D-3 shows some of the feature sets for a 2811 router and CUCME version 7. Notice in Figure D-3 that some versions only require 64 MB of flash, while others require 128 MB. (Do not forget that support files also take up space.) Based on the information in Figure D-3, the router in Example D-1 would not be able to run the Advanced IP Services feature set (not enough flash space), and should use the Enterprise Services or IP Voice feature set instead.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

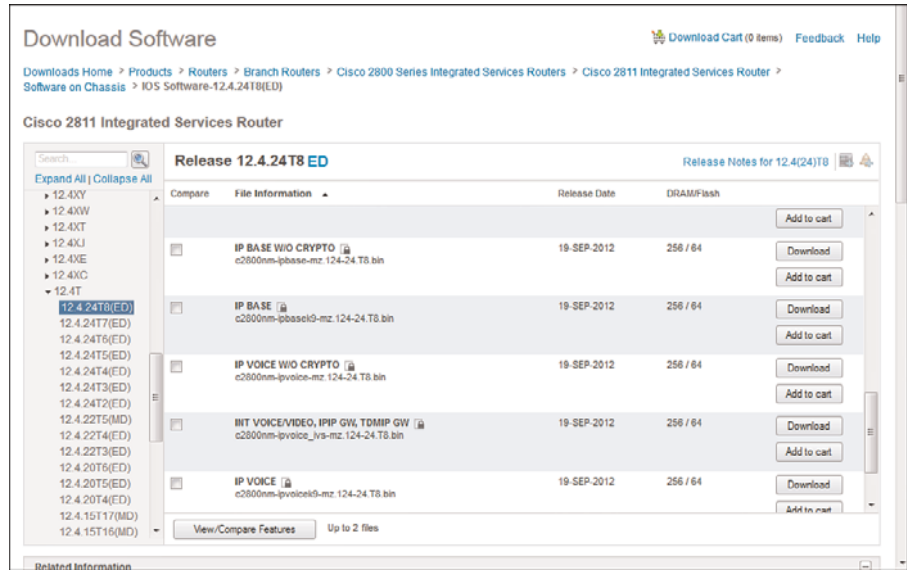
Figure D-3 Cisco Feature Navigator



Step 1-4: Obtain IOS Files

If you have a Cisco.com account with download rights to the IOS software, you can go to the Support Download site and navigate to the router hardware model and IOS version to download the file. Figure D-4 shows some of the IOS Release 12.4(24)T download feature sets for a 2811 router.

Figure D-4 IOS Download Selection



Note: It might seem that a 12.4-25b IOS version is a higher level IOS than 12.4-24T8, but the *T* in the name indicates that this is a different release train (that is, development path). The *T* release train of the IOS is where new features are developed before they become part of the mainline version for the next IOS. Newer, more experimental features are found first in the *T* release version, so it might be more advanced than a higher numbered, non-T version.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 1-5: Determine Phone Firmware Files

Look at the "Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix" webpage discussed in Step 1-2. In the far-right column is a link to the recommended phone firmware files for the version of CUCME selected. It will link you to a page for that version's supported firmware, platforms, memory, and voice products. If you scroll down the page, you will see the firmware files required for every model of phone that particular version of CUCME supports listed. In Figure D-5, you see that CUCME version 7.1 firmware for the 7940G and 7960G requires three files, while firmware for the 7941G and 7941G-GE requires eight files.

Figure D-5 CUCME Phone Firmware

Cisco Unified IP Phone **7940G** and **7960G**	P00308000500.loads* P00308000500.sb2 P00308000500.sbn	P0S3-08-6-02.loads* P0S3-08-6-02.sb2 P0S3-08-6-02.sbn	
Cisco Unified IP Phone **7941G** and **7941G GE**	apps41.8-4-1-23.sbn cnu41.8-4-1-23.sbn cvm41sccp.8-4-1-23.sbn dsp41.8-4-1-23.sbn jar41sccp.8-4-1-23.sbn SCCP41.8-4-2S.loads* term41.default.loads term61.default.loads	apps41.8-4-1-23.sbn cnu41.8-4-1-23.sbn cvm41sip.8-4-1-23.sbn dsp41.8-4-1-23.sbn jar41sip.8-4-1-23.sbn SIP41.8-4-2S.loads* term41.default.loads term61.default.loads	
Cisco Unified IP Phone **7942G** and **7962G**	jar42sccp.8-4-1-23.sbn apps42.8-4-1-23.sbn SCCP42.8-4-2S.loads* cnu42.8-4-1-23.sbn cvm42sccp.8-4-1-23.sbn dsp42.8-4-1-23.sbn term42.default.loads	apps42.8-4-1-23.sbn cnu42.8-4-1-23.sbn cvm42sip.8-4-1-23.sbn dsp42.8-4-1-23.sbn jar42sip.8-4-1-23.sbn SIP42.8-4-2S.loads* term42.default.loads	

Note: The Cisco IP Communicator soft phone does not have firmware. To update it, run a newer version of the installer software.

In most cases, the correct phone firmware is included with the support files for CUCME. (If you try to download the firmware by going to the phone model on Cisco.com, you are downloading the CUCM versions, which do not necessarily work with CUCME.)

Note: If you have 7940 or 7960 model phone, search on Cisco.com for "Cisco 7940 and 7960 IP Phones Firmware Upgrade Matrix." There are three different firmware upgrade procedures for these phone models, depending on the firmware they start with and the desired firmware version.

Note: If you have 7971G-GE, 7970G, 7961G-GE, 7961G, 7941G-GE, 7941G, 7911G, or 7906G model phones, search on Cisco.com for "Installing Firmware Release 8.5(3) for SCCP." Upgrading these models of phones that have older firmware to the 8.5(3) firmware first can avoid "Auth Fail" errors when they upgrade to the latest firmware version.[1]

[1] Franske, Ben; Inver Hills Community College

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

After you know the firmware necessary for your phones, you need to download the CUCME support files.

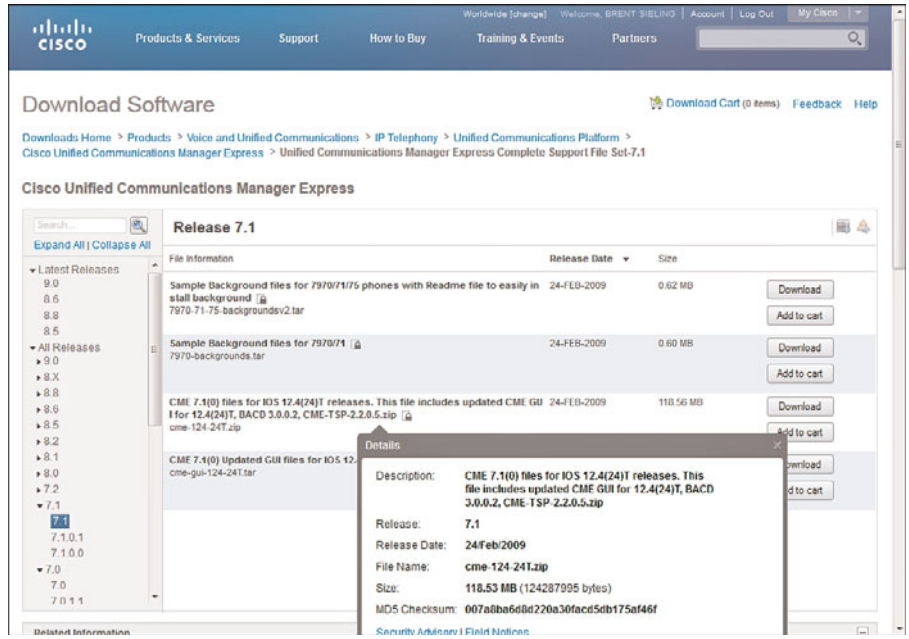
Step 1-6: Download CUCME Support Files

After the desired IOS is downloaded, and the phone firmware is determined, the next step is to download any desired support files. Support files can include

- Phone firmware
- CUCME GUI files
- Ringtones
- Background images for phones that support pictures on the display
- Auto-attendant files

If you have a Cisco.com account with download rights to the CUCME software, navigate to **Downloads Home > Products > Voice and Unified Communications > IP Telephony > Unified Communications Platform > Cisco Unified Communications Manager Express**. From the left side of the page, select the CUCME version you want to get support files for and download them. (Naturally, the support files need to match the version of CME in the IOS file you will run on the router.) Figure D-6 shows the support file download for CUCME version 7.1.

Figure D-6 CUCME Support File Download



Currently, Cisco provides a single .zip file that contains all the support files for the CUCME version. For some previous versions, the support files came as a single compressed .tar file (with names like cme-full.tar or cme-basic.tar) that could be uploaded to the router. However, with the introduction of more phone models, the size of the .tar file when uncompressed grew to the point that it would no longer fit on the flash file system of most routers.

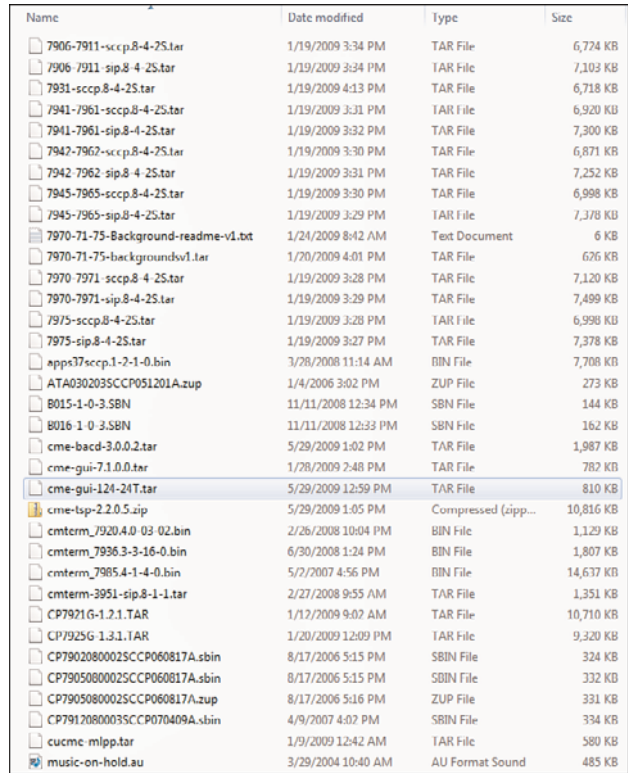
https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 1-6: Uncompress the Support Files to the TFTP Directory

The support file most likely contains many different files for the system. This lab will only focus on phone firmware and the GUI files. If the file you downloaded is a .tar file, it will be uncompressed on the router when you upload it, but if it is a .zip file, you need to uncompress the files into the directory that your TFTP software uses for uploading. See Figure D-7 for an example of the contents of the cme-124-24T.zip file uncompressed. (The files you see might be different, depending on the CUCME version you selected.)

Figure D-7 CUCME Support File Unzipped



Task 2: Upload the Files to the Router

With the IOS and support file ready, you can start the process of uploading to the router.

Step 2-1: Set Up the Router and PC

Configure the router interface and the PC with IP addresses in the same subnet; for this lab, it does not matter what they are. Verify that you can ping between the two devices. Start up the TFTP Server software on the PC.

Step 2-2: Back Up All Existing Files to the TFTP Server

As a good practice, you should back up *all* files from the flash and the router configuration to the TFTP server with the **copy flash:**<*filename*> **tftp** and the **copy running-config tftp** commands.

Step 2-3: Format the Flash

If you are going to continue with the same IOS you have currently, and just need to add the support files, skip to Step 2-5.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Caution: The following steps will reformat the file system on the router, deleting *all* files, including the IOS. Verify that a backup of the current IOS is on the TFTP server from the previous step.

The type of flash storage on the router (Class B or Class C) will determine the method of clearing the flash. Example D-2 shows the **format flash:** command on a 2811 router, which is using a Class C format. Class B systems will use the **erase flash:** command. Search Cisco.com for "Using the Cisco IOS File System" for information on how your router should have the flash memory cleared. Using the wrong method to clear the flash can cause the IOS upload to go slowly and ultimately fail.

Example D-2 Example of Formatting Class C Flash File System

```
RtrPodx# format flash:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "flash:".  Continue? [confirm]
Writing Monlib sectors....
Monlib write complete

Format: All system sectors written. OK...
<output omitted>
Format of flash: complete
```

Step 2-4: Upload the New IOS

Use the **copy tftp flash:** command to upload the IOS .bin file from the TFTP server to flash. Verify that the IOS is installed and correct before proceeding. If you encounter any problems or errors you are unable to fix, upload the previous IOS to ensure that the router will boot.

Step 2-5: Create Directory Structure

Note that some IP Phone models are identical, except for the number of buttons on the phone, so they use the same firmware. Thus, when looking at the phone firmware files, if you see 7942-7962-sccp.8-4-2S.tar, you know that this if for both a 7942 and a 7962 phone. Likewise, a 7970-7971-sccp.8-4-2S.tar file would be for both a 7970 and a 7971 phone.

The other distinction between files is the protocol used by the phone to communicate with the CME. Cisco supports both its proprietary Skinny Call Control Protocol (SCCP) and the newer Internet standard, Session Initiation Protocol (SIP). As a result, for the 7941 (or 7961) phones, you will see two firmware files: 7941-7961-*sccp*.8-4-2S.tar and 7941-7961-*sip*.8-4-2S.tar; the middle of the filename indicates which protocol is used. All these labs will focus on just SCCP, so don't bother with the SIP files.

In this lab example, it is assumed that the CUCME version is 7.1 and that you have three phone models: a 7975, a 7962, and a 7941. (Adjust firmware to fit your phone models and CUCME version.) With these phone models, you will need the 7941-7961-sccp.8-4-2S.tar, the 7942-7962-sccp.8-4-2S.tar, and the 7975-sccp.8-4-2S.tar files.

As mentioned previously, for some versions of the support files, the entire package was a .tar file, and when uploaded, it is uncompressed into flash. The .tar files would organize the files into various directories to keep the flash file system orderly. With the .zip files, however, the files can be just uploaded into the root directory of the flash file system. This does make configuring things easier, but it can result in one long directory list, with dozens of files. This lab will also show you how to create the

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

organized file structure that the .tar support files created. If you just want to copy the files to the root directory, skip the rest of this step.

However, if you were to just copy or archive the files to flash, you would end up with a disorganized mess in flash. To help organize them, you can manually create directories in the flash file system so that they look more like the structure from the .tar support files.

Use the **mkdir** command to create a directory called "phone," and then in the phone directory, create a subdirectory for each model of phone. Use the phone model names as a guide for the directory names. If you make a mistake, you can use the **rmdir** command to remove a directory. Example D-3 shows how this might look.

Example D-3 Example Creating Subdirectories in Flash

```
RtrPodx# mkdir flash:phone
Create directory filename [phone]?
Created dir flash:phone

RtrPodx# mkdir flash:phone/7941-7961
Create directory filename [phone/7941-7961]?
Created dir flash:phone/7941-7961

RtrPodx# mkdir flash:phone/7942-7962
Create directory filename [phone/7942-7962]?
Created dir flash:phone/7942-7962

RtrPodx# mkdir flash:phone/7975
Create directory filename [phone/7975]?
Created dir flash:phone/7975
Format of flash: complete
```

Step 2-6: Upload Phone Firmware Files

Because the phone firmware files on the TFTP server are compressed .tar files, to upload these to the router, they must be uncompressed to the router using the **archive tar** command. The following command format is used:

```
RtrPodx# archive tar /xtract tftp://<the IP address of your TFTP server>/<the tar
  filename on the TFTP server> flash:<path to place the file>
```

If you skipped creating the directories in Step 2-5, the commands to upload the firmware for a 7941 (or 7961) would look like Example D-4.

Example D-4 Example Uploading Phone Firmware to the Root of Flash

```
RtrPodx# archive tar /xtract tftp://10.0.0.10/7941-7961-sccp.8-4-2S.tar flash:
Loading 7941-7961-sccp.8-4-2S.tar from 10.0.0.10 (via FastEthernet0/0): !
extracting apps41.8-4-1-23.sbn (2915997 bytes)!!!!!!!!!!
extracting cnu41.8-4-1-23.sbn (459836 bytes)!!
extracting cvm41sccp.8-4-1-23.sbn (2660448 bytes)O!!!!!!!!!
extracting dsp41.8-4-1-23.sbn (539441 bytes)O!!
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
extracting jar41sccp.8-4-1-23.sbn (500440 bytes)O!!
extracting SCCP41.8-4-2S.loads (638 bytes)
extracting term41.default.loads (642 bytes)
extracting term61.default.loads (642 bytes)
[OK - 7086080 bytes]
```

If you created the directories in Step 2-5, the commands to upload the firmware for a 7941 (or 7961) would look like Example D-5.

Example D-5 Example Uploading Phone Firmware to Subdirectories

```
RtrPodx# archive tar /xtract tftp://10.0.0.10/7941-7961-sccp.8-4-2S.tar
  flash:phone/7941-7961
Loading 7941-7961-sccp.8-4-2S.tar from 10.0.0.10 (via FastEthernet0/0): !
extracting apps41.8-4-1-23.sbn (2915997 bytes)!!!!!!!!!!!
extracting cnu41.8-4-1-23.sbn (459836 bytes)!!
extracting cvm41sccp.8-4-1-23.sbn (2660448 bytes)O!!!!!!!!!!
extracting dsp41.8-4-1-23.sbn (539441 bytes)O!!
extracting jar41sccp.8-4-1-23.sbn (500440 bytes)O!!
extracting SCCP41.8-4-2S.loads (638 bytes)
extracting term41.default.loads (642 bytes)
extracting term61.default.loads (642 bytes)
[OK - 7086080 bytes]
```

Repeat this step for each phone firmware file you need to upload.

Step 2-8: Upload GUI Files

As noted previously, there are many different support files that could be uploaded. This lab will only focus on the GUI files. Some nonphone firmware support files include the following:

- cme-gui-124-24T.tar provides limited management of CME with a web browser.
- ringtones.tar provides alternate ringtones on the phones.
- cme-bacd-3.0.0.2.tar provides scripts and audio files for a basic auto-attendant.
- music-on-hold.au gives a sample music-on-hold audio file. (Note that this is not a .tar file.)

If you skipped creating the directories in Step 2-5, the commands to upload the GUI files look like Example D-6.

Example D-6 Example Uploading GUI Files to the Root of Flash

```
RtrPodx# archive tar /xtract tftp://10.0.0.10/cme-gui-124-24T.tar flash:
Loading CME-124-24T/cme-gui-124-24T.tar from 10.0.0.10 (via FastEthernet0/0): !
extracting admin_user.html (3987 bytes)
extracting admin_user.js (677822 bytes)!!
extracting CiscoLogo.gif (1029 bytes)O
extracting CME_GUI_README.TXT (617 bytes)
extracting Delete.gif (953 bytes)
extracting dom.js (16344 bytes)
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
extracting downarrow.gif (864 bytes)
extracting ephone_admin.html (6146 bytes)
extracting logohome.gif (4558 bytes)
extracting normal_user.html (3866 bytes)
extracting normal_user.js (78428 bytes)!
extracting Plus.gif (1347 bytes)
extracting sxiconad.gif (843 bytes)
extracting Tab.gif (174 bytes)
extracting telephony_service.html (2431 bytes)
extracting uparrow.gif (870 bytes)
extracting xml-test.html (9968 bytes)
extracting xml.template (3412 bytes)
[OK - 829440 bytes]
```

If you created the directories, the commands to upload the GUI files look like Example D-7.

Example D-7 Example Uploading GUI Files to a Subdirectory

```
RtrPodx# mkdir flash:gui
Create directory filename [gui]?
Created dir flash:gui

RtrPodx# archive tar /xtract tftp://10.0.0.10/cme-gui-124-24T.tar flash:/gui
Loading CME-124-24T/cme-gui-124-24T.tar from 10.0.0.10 (via FastEthernet0/0): !
extracting admin_user.html (3987 bytes)
extracting admin_user.js (677822 bytes)!!
<output omitted>
 sOK - 829440 bytes]
```

Step 2-9: Verify Files and Placement

If you skipped creating the directories in Step 2-5, just use the **dir flash:** command to verify that all the files are placed correctly.

If you created the directories in Step 2-5, you can use the **/recursive** option with the **dir** command to check your flash file structure. If you used the examples in the lab, it should look like Example D-8.

Example D-8 Example of Files with Subdirectory Structure

```
RtrPodx# dir /recursive flash:
Directory of flash:/*

Directory of flash:/

    1  -rw-    59932976   Feb 9 2010 23:13:40 +00:00  c2800nm-adventerprisek9_iv
s-mz.124-24.T2.bin
Directory of flash:/phone/
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
Directory of flash:/phone/7941-7961/

    6  -rw-     2915997   Feb 9 2010 23:19:36 +00:00  apps41.8-4-1-23.sbn
    7  -rw-      459836   Feb 9 2010 23:19:42 +00:00  cnu41.8-4-1-23.sbn
    8  -rw-     2660448   Feb 9 2010 23:20:00 +00:00  cvm41sccp.8-4-1-23.sbn
    9  -rw-      539441   Feb 9 2010 23:20:04 +00:00  dsp41.8-4-1-23.sbn
   10  -rw-      500440   Feb 9 2010 23:20:08 +00:00  jar41sccp.8-4-1-23.sbn
   11  -rw-         638   Feb 9 2010 23:20:10 +00:00  SCCP41.8-4-2S.loads
   12  -rw-         642   Feb 9 2010 23:20:10 +00:00  term41.default.loads
   13  -rw-         642   Feb 9 2010 23:20:10 +00:00  term61.default.loads
Directory of flash:/phone/

Directory of flash:/phone/7942-7962/

   14  -rw-     2918613   Feb 9 2010 23:20:38 +00:00  apps42.8-4-1-23.sbn
   15  -rw-      485066   Feb 9 2010 23:20:44 +00:00  cnu42.8-4-1-23.sbn
   16  -rw-     2659498   Feb 9 2010 23:21:00 +00:00  cvm42sccp.8-4-1-23.sbn
   17  -rw-      335003   Feb 9 2010 23:21:04 +00:00  dsp42.8-4-1-23.sbn
   18  -rw-      628112   Feb 9 2010 23:21:08 +00:00  jar42sccp.8-4-1-23.sbn
   19  -rw-         658   Feb 9 2010 23:21:10 +00:00  SCCP42.8-4-2S.loads
   20  -rw-         662   Feb 9 2010 23:21:10 +00:00  term42.default.loads
   21  -rw-         662   Feb 9 2010 23:21:12 +00:00  term62.default.loads
Directory of flash:/phone/

Directory of flash:/phone/7975/

   22  -rw-     2918613   Feb 9 2010 23:21:56 +00:00  apps75.8-4-1-23.sbn
   23  -rw-      485244   Feb 9 2010 23:22:02 +00:00  cnu75.8-4-1-23.sbn
   24  -rw-     2661855   Feb 9 2010 23:22:18 +00:00  cvm75sccp.8-4-1-23.sbn
   25  -rw-      335003   Feb 9 2010 23:22:22 +00:00  dsp75.8-4-1-23.sbn
   26  -rw-      757132   Feb 9 2010 23:22:26 +00:00  jar75sccp.8-4-1-23.sbn
   27  -rw-         638   Feb 9 2010 23:22:28 +00:00  SCCP75.8-4-2S.loads
   28  -rw-         642   Feb 9 2010 23:22:28 +00:00  term75.default.loads
Directory of flash:/gui/

   51  -rw-        3987   Feb 9 2010 23:30:10 +00:00  admin_user.html
   52  -rw-      677822   Feb 9 2010 23:30:14 +00:00  admin_user.js
   53  -rw-        1029   Feb 9 2010 23:30:16 +00:00  CiscoLogo.gif
   54  -rw-         617   Feb 9 2010 23:30:16 +00:00  CME_GUI_README.TXT
   55  -rw-         953   Feb 9 2010 23:30:16 +00:00  Delete.gif
   56  -rw-       16344   Feb 9 2010 23:30:18 +00:00  dom.js
   57  -rw-         864   Feb 9 2010 23:30:18 +00:00  downarrow.gif
   58  -rw-        6146   Feb 9 2010 23:30:18 +00:00  ephone_admin.html
   59  -rw-        4558   Feb 9 2010 23:30:18 +00:00  logohome.gif
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
60  -rw-        3866   Feb 9 2010 23:30:20 +00:00  normal_user.html
61  -rw-       78428   Feb 9 2010 23:30:20 +00:00  normal_user.js
62  -rw-        1347   Feb 9 2010 23:30:20 +00:00  Plus.gif
63  -rw-         843   Feb 9 2010 23:30:22 +00:00  sxiconad.gif
64  -rw-         174   Feb 9 2010 23:30:22 +00:00  Tab.gif
65  -rw-        2431   Feb 9 2010 23:30:22 +00:00  telephony_service.html
66  -rw-         870   Feb 9 2010 23:30:22 +00:00  uparrow.gif
67  -rw-        9968   Feb 9 2010 23:30:24 +00:00  xml-test.html
68  -rw-        3412   Feb 9 2010 23:30:24 +00:00  xml.template
```

Task 3: Commands to Upgrade or Downgrade Firmware on the Phones

To make the phone firmware files active, two steps are necessary: allow the router to send the files using TFTP and tell the phones what firmware to use. These commands are meant to be used as part of Lab 5-1 (used right after Step 2-3) or Lab 5-2 (as part of Step 2-1). Complete the labs up to that point, and then return to enter these commands.

Step 3-1: Allow the Router to Send TFTP Files from Flash

As part of the basic security for each router, it does not respond to TFTP requests for files. Because you are telling the phones in Lab 3-1 to use the router as the TFTP server, you need to allow the router to respond to the firmware requests. The **tftp-server** command enables the router to send the specified file using TFTP (which normally would be blocked). Do not forget that some phone models are identical, except for the number of buttons on the phone, so they use the same firmware. Thus, when looking at the phone firmware files, both a 7942 and a 7962 phone use *almost* the same files (there is one file that is unique for each model that influences the buttons allowed on each).

If you skipped creating the directories in Step 2-5, the commands to allow the router to send files for the 7942 (and 7962) phones are shown in Example D-9.

Note: Lines in the configuration that start with an exclamation point (!) are comments to explain the commands that follow, and do not need to be entered.

Example D-9 Example Allowing TFTP of Phone Firmware Files from the Root of Flash

```
RtrPodx(config)# tftp-server flash:apps42.8-4-1-23.sbn
RtrPodx(config)# tftp-server flash:cnu42.8-4-1-23.sbn
RtrPodx(config)# tftp-server flash:cvm42sccp.8-4-1-23.sbn
RtrPodx(config)# tftp-server flash:dsp42.8-4-1-23.sbn
RtrPodx(config)# tftp-server flash:jar42sccp.8-4-1-23.sbn
RtrPodx(config)# tftp-server flash:SCCP42.8-4-2S.loads
! The following command would only be needed for 7942 phones
RtrPodx(config)# tftp-server flash:term42.default.load
! The following command would only be needed for 7962 phones
RtrPodx(config)# tftp-server flash:term62.default.load
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

If you created the directories in Step 2-5, the commands to allow the router to send files for the 7942 (and 7962) phones are shown in Example D-10. Because the phone does not know about your folder structure on the router, it just requests the files it needs, but those files are not in the root directory. The **alias** command (like a shortcut) allows the file to be redirected to the actual location on the flash where the file is stored. For example, the first line in Example D-10 tells the router that the file located at flash:phone/7942-7962/apps42.8-4-1-23.sbn should be sent whenever a TFTP request comes in for file apps42.8-4-1-23.sbn.

Note: Lines in the configuration that start with an exclamation point (!) are comments to explain the commands that follow, and do not need to be entered.

Example D-10 Example Allowing TFTP of Phone Firmware Files from Subdirectories

```
RtrPodx(config)# tftp-server flash:phone/7942-7962/apps42.8-4-1-23.sbn alias
  apps42.8-4-1-23.sbn
RtrPodx(config)# tftp-server flash:phone/7942-7962/cnu42.8-4-1-23.sbn alias cnu42.8-
  4-1-23.sbn
RtrPodx(config)# tftp-server flash:phone/7942-7962/cvm42sccp.8-4-1-23.sbn alias
  cvm42sccp.8-4-1-23.sbn
RtrPodx(config)# tftp-server flash:phone/7942-7962/dsp42.8-4-1-23.sbn alias dsp42.8-
  4-1-23.sbn
RtrPodx(config)# tftp-server flash:phone/7942-7962/jar42sccp.8-4-1-23.sbn alias
  jar42sccp.8-4-1-23.sbn
RtrPodx(config)# tftp-server flash:phone/7942-7962/SCCP42.8-4-2S.loads alias
  SCCP42.8-4-2S.loads
! The following command would only be needed for 7942 phones
RtrPodx(config)# tftp-server flash:phone/7942-7962/term42.default.loads alias
  term42.default.load
! The following command would only be needed for 7962 phones
RtrPodx(config)# tftp-server flash:phone/7942-7962/term62.default.loads alias
  term62.default.load
```

Repeat this step for each phone firmware file you uploaded.

Step 3-2: Inform the Phone of the Updated Firmware to Load

After the files are loaded on the router and the router is configured to send the files using TFTP, the phone needs to be told what version of firmware to load. In telephony service, the **load** command does this. After the **load** command is issued with the correct protocol firmware file, the cnf files need to be re-created and the phone reset to discover the new firmware files. See Lab 5-1, Step 2-5 for more information about the cnf files. Example D-11 shows the commands necessary to load the new firmware for the three models of phones demonstrated for this lab. Notice in Example D-11 that the 7962 phone is related to the 7942 model, and thus uses the SCCP42 protocol file to indicate the correct firmware. (However, the term.default.load files are unique, but not indicated by this command. The phone will get the right file.)

Example D-11 Example Allowing TFTP of Phone Firmware Files from Subdirectories

```
RtrPodx(config)# telephony-service
RtrPodx(config-telephony)# load 7941 SCCP41.8-4-2S
RtrPodx(config-telephony)# load 7962 SCCP42.8-4-2S
RtrPodx(config-telephony)# load 7975 SCCP75.8-4-2S
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Step 3-3: Troubleshooting Firmware Loading on the Phones

There can be many reasons the phones do not get the correct firmware. Follow these steps to troubleshoot:

1. Verify that all the firmware files are in the specified location.
2. Verify that all the necessary **tftp-server** commands are entered correctly.
3. If the phone starts the firmware download but does not finish, or is stuck in a loop upgrading (or downgrading), use the **debug tftp events** command to see which file the phone is requesting, but failing to get. (The "locale" file is expected to fail, as you are not setting locales up as part of these labs.)
4. If the phone ignores the firmware change, verify that the **load** command in telephony service is correct, and make sure that the **create cnf-files** command is updating the phone configuration so that the phone knows that the new firmware is available.
5. If the phone has newer firmware (for example, if it has been connected to a CUCM system version 8.0 or greater), the phone might have a certificate that prevents it from acknowledging the CUCME system, as mentioned in the Hardware section. Follow the directions to remove the certificate so that the phone will listen to the CUCME system for requests to install the correct firmware.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

This page intentionally left blank

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

APPENDIX E

PSTN Simulator

The PSTN Simulator is a Cisco router with one or more T1/E1/PRI interfaces (and enough digital signal processor [DSP] resources to run the interfaces), configured to respond to incoming calls and to forward calls for other pods to the correct interface. The PSTN Simulator plays a unique audio file when any of the categories of phone numbers shown in Table E-1 are sent to the Simulator.

Table E-1 Audio Response Phone Number Categories

Call Category	Response
Emergency services (911)	Play hq_911.au file
Local numbers (7 digits)	Play mrrogers.au file
Long-distance (1+10 digits)	Play ld.au file
Service codes (N11)	Play info.au file
Toll-free numbers (1-800)	Play us_800.au file
Premium-rate numbers (1-900)	Play us_900.au file
International (011+unknown number of digits)	Play international file
Pod-to-pod (local or long-distance)	Send call to the interface assigned to the pod

The audio response is achieved by using the Tool Command Language (Tcl) scripts[1] paired with an audio file encoded as .au or .wav for each call category. To create the audio file, the same process for creating music-on-hold (MoH) files can be followed. The "Configuring Music on Hold" section of the *Cisco Unified Communications Manager Express System Administrator Guide states,* "This file should be in G.711 format. The file can be in .au or .wav file format, but the file format must contain 8-bit 8-kHz data; for example, ITU-T A-law or mu-law data format." Search the Internet for "cisco moh file format" to find information on programs to record and format audio files to the standard.

For each call category, there are two files: an audio file and the matching Tcl script. For example, to play an audio file for long-distance calls, an audio file, called ld.au, is uploaded to the router flash using TFTP. The ld.tcl file, shown in Example E-1, is also uploaded. Whenever the Tcl script is called in the router configuration, the audio file is played. See Example E-1, where the ld.tcl script references the ld.au file.

Example E-1 ld.tcl script

```
proc init { } {
    global param
    set param(interruptPrompt) true
    set param(abortKey) *
    set param(terminationKey) #
}

proc act_Setup { } {
```

[1] While I wish I could claim credit for creating the TCL scripts and initial configuration, I am forever indebted to David Mallory of Cisco for the files.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
    global dest
    leg setupack leg_incoming
    leg proceeding leg_incoming

    media play leg_incoming flash:ld.au
    fsm setstate CALLDISCONNECTED

}

proc act_Cleanup { } {
    call close
}

init
set callfsm(CALL_INIT,ev_setup_indication) "act_Setup,CALLDISCONNECTED"
set callfsm(CALLDISCONECCTED,ev_disconnected) "act_Cleanup,same_state"

set callfsm(CALLDISCONNECTED,ev_disconnected) "act_Cleanup,same_state"
set callfsm(CALLDISCONNECTED,ev_media_done)  "act_Cleanup,same_state"
set callfsm(CALLDISCONNECTED,ev_disconnect_done) "act_Cleanup,same_state"
set callfsm(CALLDISCONNECTED,ev_leg_timer) "act_Cleanup,same_state"

fsm define callfsm CALL_INIT
```

Note: The name of the audio file and the reference in the Tcl script are case sensitive and must match.

A separate Tcl file is needed for each audio file to be played. The only difference between the Tcl files is the audio file that is referenced.

Having a large number of interfaces is not required to build a PSTN Simulator. Example E-2 shows how to set up a PSTN Simulator with just two VWIC-1MFT-T1 interfaces for pods 1 and 2.

Note: Lines in the configuration that start with an exclamation point (!) are comments to explain the commands that follow, and do not need to be entered. The configuration is set up for the labs in Chapter 6, "Cisco Unified Communications Manager Express (CUCME) Dial Plans and QoS," but the comments show what to change for the labs to work with Chapter 10, "CUCM Dial Plan."

Example E-2 Two-Pod PSTN Router Configuration

```
hostname PSTN_Simulator

! The network-clock-participate command is needed for the PRI configuration for each
  network module and VWIC (see lab 6-2, step 3-2 for details).
network-clock-participate wic 0
network-clock-participate wic 1
!
no ip domain lookup
ip domain name soi.com
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
! The isdn switch-type command is needed for the PRI configuration (see lab 6-2, step
  3-1 for details).
isdn switch-type primary-ni

! The voice translation-rule converts all seven-digit and ten-digit dialed and
  dialing numbers (in the range of the pod phone numbers) to long-distance calls, to
  reduce the number of dial-peers needed later.
voice translation-rule 1
 rule 1 /^55550[0-5].$/ /1510&/
 rule 2 /^51055550[0-5].$/ /1&/
! The voice translation-rules for the CUCM labs would be:
! voice translation-rule 1
!  rule 1 /^5552[^12]..$/ /1510&/
!  rule 2 /^5105552[^12]..$/ /1&/

! The voice translation-profile applies the voice translation-rule to both the dialed
  number and the calling number.
voice translation-profile TenDIGITS
 translate called 1
 translate calling 1

! This application is used to call the 900 number tcl script
application
 service us_900 flash:us_900.tcl
 exit

! This application is used to call the long-distance number tcl script
application
 service ld flash:ld.tcl
 exit

! This application is used to call the emergency number (911) tcl script
application
 service 911 flash:hq_911.tcl
 exit

! This application is used to call the local numbers tcl script
application
 service local flash:mrrogers.tcl
 exit

! This application is used to call the info number tcl script
application
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 service info flash:info.tcl
 exit

! This application is used to call the international number tcl script
application
 service intl flash:international.tcl
 exit

! This application is used to call the toll-free number tcl script
application
 service us_800 flash:us_800.tcl
 exit

! The controller interface names will depend on the VWICs and network modules
  installed (adjust as necessary). Since this configuration has two single-port T1/PRI
  cards, there is one pod on each VWIC. The timeslots are configured to support 6 PRI
  channels for each interface (which might be limited by your PVDM resources) (see lab
  6-2, step 3-4 for details).
controller T1 0/0/0
 description Pod 1
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
controller T1 0/1/0
 description Pod 2
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
! Each of the controllers has a matching serial interface (see lab 6-2 for details)
  Note that the isdn protocol-emulate network command is what makes this the provider
  end of the circuit.
interface Serial0/0/0:23
 description Pod 1
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial0/1/0:23
 description Pod 2
 no ip address
 isdn switch-type primary-ni
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
! There is a voice-port for each controller and this is where the translation-profile
  is applied to convert seven-digit and ten-digit numbers to a long-distance number
  (for phone numbers in the ranges of the pods).
voice-port 0/0/0:23
 translation-profile incoming TenDIGITS
!
voice-port 0/1/0:23
 translation-profile incoming TenDIGITS
!
! Dial-peers 101 and 102 direct dialed numbers in the range of the pods to the
  correct interface. Since the translation-profiles are converting phone numbers in the
  range of the pods from seven-digit and ten-digits to long-distance, local calls to
  pods are using the long-distance dial-peers. Read the descriptions in each dial-peer
  to see which pod is configured.
dial-peer voice 101 pots
 description 1+10 digits to Pod 1
 destination-pattern 151055550[0-2].
 port 0/0/0:23
 prefix 51055550
! For the CUCM labs, dial-peer 101 would have a destination-pattern of 151055521..
  and a prefix of 51055521
!
dial-peer voice 102 pots
 description 1+10 digits to Pod 2
 destination-pattern 151055550[3-5].
 port 0/0/1:23
 prefix 51055550
! For the CUCM labs, dial-peer 102 would have a destination-pattern of 151055522..
  and a prefix of 51055522
!
! Dial-peers 800, 855, 866, 877, and 888 sends toll-free calls using the service
  command to the us_800 application, which calls the us_800.tcl script, which plays the
   us_800.au audio file.
dial-peer voice 800 pots
 service us_800
 incoming called-number 1800.......
!
dial-peer voice 855 pots
 service us_800
 incoming called-number 1855.......
!
dial-peer voice 866 pots
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 service us_800
 incoming called-number 1866.......
!
dial-peer voice 877 pots
 service us_800
 incoming called-number 1877.......
!
dial-peer voice 888 pots
 service us_800
 incoming called-number 1888.......

! Dial-peer 900 sends toll-free calls using the service command to the us_900
  application, which calls the us_900.tcl script, which plays the us_900.au audio file.
dial-peer voice 900 pots
 service us_900
 incoming called-number 1900.......
!
! Dial-peer 411 sends service code calls using the service command to the info
  application, which calls the info.tcl script, which plays the info.au audio file.
dial-peer voice 411 pots
 service info
 incoming called-number [2-8]11

! Dial-peer 123 directs the router to use direct-inward-dial for incoming calls (see
  lab 6-5, step 5-1 for details).
dial-peer voice 123 pots
 incoming called-number .
 direct-inward-dial
!
! Dial-peer 911 sends emergency calls using the service command to the 911
  application, which calls the hq_911.tcl script, which plays the hq_911.au audio file.
dial-peer voice 911 pots
 service 911
 incoming called-number 911
!
! Dial-peers 9100 to 9107 are created to carefully exclude the range of numbers for
  the 11 pods 1-510-555-2100 to 2299. This was done because the service command takes
  priority when routing calls. If a long-distance dial-peer was used that matched a
  pattern such as 1.......... long-distance calls to other pods would play the ld.tcl
  script. Instead calls to the pods do not match the patterns, and get directed to the
  correct interface in dial-peers 101 and 102.

! Dial-peer 9100 covers any 1+10 digit number that does not start with a 15
dial-peer voice 9100 pots
 service ld
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 incoming called-number 1[2-4,6-9].........

! Dial-peer 9101 covers any 1+10 digit number that does not start with 151
dial-peer voice 9101 pots
 service ld
 incoming called-number 15[^1].........
!
! Dial-peer 9102 covers any 1+10 digit number that does not start with 1510
dial-peer voice 9102 pots
 service ld
 incoming called-number 151[^0].......
!
! Dial-peer 9103 covers any 1+10 digit number that does not start with 15105
dial-peer voice 9103 pots
 service ld
 incoming called-number 15105[2-4,5-9]......
!
! Dial-peer 9104 covers any 1+10 digit number that does not start with 151055
dial-peer voice 9104 pots
 service ld
 incoming called-number 15105[^5].....
!
! Dial-peer 9105 covers any 1+10 digit number that does not start with 1510555
dial-peer voice 9105 pots
 service ld
 incoming called-number 151055[^5]....
!
! Dial-peer 9106 covers any 1+10 digit number that does not start with 15105555
dial-peer voice 9106 pots
 service ld
 incoming called-number 1510555[^5]...
! For the CUCM labs, dial-peer 9106 would have an incoming called-number of
  15105552[^12]..
!
! Dial-peer 9107 covers any 1+10 digit number that does not start with 151055550
dial-peer voice 9107 pots
 service ld
 incoming called-number 15105555[^0]..
! For the CUCM labs, dial-peer 9107 does not need to exist
!
! Dial-peer 9108 covers any 1+10 digit number that does not start with 151055550
  followed by a 0, 1, 2, 3, 4, or 5
dial-peer voice 9108 pots
 service ld
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 incoming called-number 151055550[^0-5].
! For the CUCM labs, dial-peer 9108 does not need to exist
!
! Dial-peer 9011 sends international calls using the service command to the intl
  application, which calls the international.tcl script, which plays the
  international.au audio file. Note that the seven dots after the 011 is just a
  arbitrary number to make sure the user dialed enough digits, since I am not aware of
  any county that uses less than seven-digits for phone numbers.
dial-peer voice 9011 pots
 service intl
 incoming called-number 011.......
!
! Dial-peer 7 sends seven-digit local calls using the service command to the local
  application, which calls the mrrogers.tcl script, which plays the mrrogers.au audio
  file. Since all local numbers for the pods were converted to long-distance numbers by
  the translation-profile, it is not necessary to avoid covering the numbers for the
  pods (which had to be done in dial-peers 9100 to 9108).
dial-peer voice 7 pots
 service local
 incoming called-number [2-9]......
!
line con 0
 exec-timeout 300 0
 logging synchronous
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
line vty 5 15
 privilege level 15
 login local
 transport input telnet ssh
```

Example E-3 shows a configuration from the router I used in my classroom for 11 pods and shows how the simulator can scale to a large number of pods. It is built with a Cisco 2811 router, running IOS Release 12.4(24)T6, with four VWIC-2MFT-T1 cards in the WIC slots, and an NM-HDV2-2T1/E1 module with a VWIC2-1MFT-T1/E1 installed, for a total of 11 interfaces. To run six channels on each interface, a PVDM2-64 and a PVDM2-32 modules are installed to provide the DSP resources. The current PSTN simulator I use takes two 2821 routers to run a total of 21 T1/PRI interfaces.

Note: Lines in the configuration that start with an exclamation point (!) are comments to explain the commands that follow, and do not need to be entered. The configuration is set up for the labs in Chapter 6, but the comments show what to change for the labs to work with Chapter 10.

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

Example E-3 11-Pod PSTN Router Configuration

```
hostname PSTN_Simulator

! The card type command is needed if Multiflex T1/E1 cards are installed (see the
  note in lab 6-2, step 2-1 for details). In this case the network module, and the
  VWIC2-1MFT-T1/E1 card installed in it, need to choose T1 or E1.
card type t1 1 0
card type t1 1 1

! The network-clock-participate command is needed for the PRI configuration for each
  network module and VWIC (see lab 6-2, step 3-2 for details).
network-clock-participate slot 1
network-clock-participate wic 0
network-clock-participate wic 1
network-clock-participate wic 2
network-clock-participate wic 3
!
no ip domain lookup
ip domain name soi.com

! The isdn switch-type command is needed for the PRI configuration (see lab 6-2, step
  3-1 for details).
isdn switch-type primary-ni

! The voice-card and dspfarm commands allow the PVDM resources to be shared between
  all of the interfaces. The voice-card 0 is for PVDM on the router motherboard, while
  the voice-card 1 is present only because of the PVDM on the network module.
voice-card 0
codec complexity flex
dspfarm
!
voice-card 1
codec complexity flex
dspfarm

! The voice translation-rule converts all seven-digit and ten-digit dialed and
  dialing numbers (in the range of the pod phone numbers) to long-distance calls, to
  reduce the number of dial-peers needed later.
voice translation-rule 1
 rule 1 /^5555[0-2]..$/ /1510&/
 rule 2 /^55553[0-5].$/ /1510&/
 rule 3 /^5105555[0-2]..$/ /1&/
 rule 4 /^51055553[0-5].$/ /1&/
! The voice translation-rules for the CUCM labs would be:
! voice translation-rule 1
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
!  rule 1 /^5552[^0]..$/ /1510&/
!  rule 2 /^5553[01]..$/ /1510&/
!  rule 3 /^5105552[^0]..$/ /1&/
!  rule 4 /^5105553[01]..$/ /1&/

! The voice translation-profile applies the voice translation-rule to both the dialed
  number and the calling number.
voice translation-profile TenDIGITS
 translate called 1
 translate calling 1

! This application is used to call the 900 number tcl script
application
 service us_900 flash:us_900.tcl
 exit

! This application is used to call the long-distance number tcl script
application
 service ld flash:ld.tcl
 exit

! This application is used to call the emergency number (911) tcl script
application
 service 911 flash:hq_911.tcl
 exit

! This application is used to call the local numbers tcl script
application
 service local flash:mrrogers.tcl
 exit

! This application is used to call the info number tcl script
application
 service info flash:info.tcl
 exit

! This application is used to call the international number tcl script
application
 service intl flash:international.tcl
 exit

! This application is used to call the toll-free number tcl script
application
 service us_800 flash:us_800.tcl
 exit
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
! The controller interface names will depend on the VWICs and network modules
  installed (adjust as necessary). Since this configuration has dual T1/PRI cards,
  there are two pods on each VWIC. The timeslots are configured to support 6 PRI
  channels for each interface (which might be limited by your PVDM resources) (see lab
  6-2, step 3-4 for details).
controller T1 0/0/0
 description Pod 1
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
controller T1 0/0/1
 description Pod 2
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
controller T1 0/1/0
 description Pod 3
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
controller T1 0/1/1
 description Pod 4
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
controller T1 0/2/0
 description Pod 5
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
controller T1 0/2/1
 description Pod 6
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
controller T1 0/3/0
 description Pod 7
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
controller T1 0/3/1
 description Pod 8
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24

! These two controller interfaces are located onboard the network module.
controller T1 1/0
 description Pod 9
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
controller T1 1/1
 description Pod 10
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24

! This controller interface is located on a single interface VWIC installed in the
  network module slot.
controller T1 1/0/0
 description Pod 11/Instructor
 framing esf
 linecode b8zs
 pri-group timeslots 1-6,24
!
! Each of the controllers has a matching serial interface (see lab 6-2 for details).
  Note that the isdn protocol-emulate network command is what makes this the provider
  end of the circuit.
interface Serial0/0/0:23
 description Pod 1
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial0/0/1:23
 description Pod 2
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial0/1/0:23
 description Pod 3
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial0/1/1:23
 description Pod 4
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial0/2/0:23
 description Pod 5
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial0/2/1:23
 description Pod 6
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial0/3/0:23
 description Pod 7
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 no cdp enable
!
interface Serial0/3/1:23
 description Pod 8
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial1/0:23
 description Pod 9
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial1/1:23
 description Pod 10
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial1/0/0:23
 description Pod 11/Instructor
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable

! There is a voice-port for each controller and this is where the translation-profile
  is applied to convert seven-digit and ten-digit numbers to a long-distance number
  (for phone numbers in the ranges of the pods).
voice-port 0/0/0:23
 translation-profile incoming TenDIGITS
!
voice-port 0/1/0:23
 translation-profile incoming TenDIGITS
!
voice-port 0/2/0:23
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 translation-profile incoming TenDIGITS
!
voice-port 0/3/0:23
 translation-profile incoming TenDIGITS
!
voice-port 0/0/1:23
 translation-profile incoming TenDIGITS
!
voice-port 0/1/1:23
 translation-profile incoming TenDIGITS
!
voice-port 0/2/1:23
 translation-profile incoming TenDIGITS
!
voice-port 0/3/1:23
 translation-profile incoming TenDIGITS
!
voice-port 1/0:23
 translation-profile incoming TenDIGITS
!
voice-port 1/1:23
 translation-profile incoming TenDIGITS
!
voice-port 1/0/0:23
 translation-profile incoming TenDIGITS
!
! Dial-peers 101 to 111 direct dialed numbers in the range of the pods to the correct
  interface. Since the translation-profiles are converting phone numbers in the range
  of the pods from seven-digit and ten-digits to long-distance, local calls to pods are
  using the long-distance dial-peers. Read the descriptions in each dial-peer to see
  which pod is configured.
dial-peer voice 101 pots
 description 1+10 digits to Pod 1
 destination-pattern 151055550[0-2].
 port 0/0/0:23
 prefix 51055550
! Dial-peer 101 would have a destination-pattern of 151055521.. and a prefix of
  51055521 for the CUCM labs.
!
dial-peer voice 102 pots
 description 1+10 digits to Pod 2
 destination-pattern 151055550[3-5].
 port 0/0/1:23
 prefix 51055550
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
! Dial-peer 102 would have a destination-pattern of 151055522.. and a prefix of
  51055522 for the CUCM labs.
!
dial-peer voice 103 pots
 description 1+10 digits to Pod 3
 destination-pattern 151055550[6-8].
 port 0/1/0:23
 prefix 51055550
! Dial-peer 103 would have a destination-pattern of 151055523.. and a prefix of
  51055523 for the CUCM labs.
!
dial-peer voice 104 pots
 description 1+10 digits to Pod 4
 destination-pattern 151055551[0-2].
 port 0/1/1:23
 prefix 51055551
! Dial-peer 104 would have a destination-pattern of 151055524.. and a prefix of
  51055524 for the CUCM labs.
!
dial-peer voice 105 pots
 description 1+10 digits to Pod 5
 destination-pattern 151055551[3-5].
 port 0/2/0:23
 prefix 51055551
! Dial-peer 105 would have a destination-pattern of 151055525.. and a prefix of
  51055525 for the CUCM labs.
!
dial-peer voice 106 pots
 description 1+10 digits to Pod 6
 destination-pattern 151055551[6-8].
 port 0/2/1:23
 prefix 51055551
! Dial-peer 106 would have a destination-pattern of 151055526.. and a prefix of
  51055526 for the CUCM labs.
!
dial-peer voice 107 pots
 description 1+10 digits to Pod 7
 destination-pattern 151055552[0-2].
 port 0/3/0:23
 prefix 51055552
! Dial-peer 107 would have a destination-pattern of 151055527.. and a prefix of
  51055527 for the CUCM labs.
!
dial-peer voice 108 pots
 description 1+10 digits to Pod 8
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
 destination-pattern 151055552[3-5].
 port 0/3/1:23
 prefix 51055552
! Dial-peer 108 would have a destination-pattern of 151055528.. and a prefix of
  51055528 for the CUCM labs.
!
dial-peer voice 109 pots
 description 1+10 digits to Pod 9
 destination-pattern 151055552[6-8].
 port 1/0:23
 prefix 51055552
! Dial-peer 109 would have a destination-pattern of 151055529.. and a prefix of
  51055529 for the CUCM labs.
!
dial-peer voice 110 pots
 description 1+10 digits to Pod 10
 destination-pattern 151055553[0-2].
 port 1/1:23
 prefix 51055553
! Dial-peer 110 would have a destination-pattern of 151055530.. and a prefix of
  51055530 for the CUCM labs.
!
dial-peer voice 111 pots
 description 1+10 digits to Pod11/Instructor
 destination-pattern 151055553[3-5].
 port 1/0/0:23
 prefix 51055553
! Dial-peer 111 would have a destination-pattern of 151055531.. and a prefix of
  51055531 for the CUCM labs.
!
! Dial-peers 800, 855, 866, 877, and 888 sends toll-free calls using the service
  command to the us_800 application, which calls the us_800.tcl script, which plays the
  us_800.au audio file.
dial-peer voice 800 pots
 service us_800
 incoming called-number 1800.......
!
dial-peer voice 855 pots
 service us_800
 incoming called-number 1855.......
!
dial-peer voice 866 pots
 service us_800
 incoming called-number 1866.......
!
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
dial-peer voice 877 pots
 service us_800
 incoming called-number 1877.......
!
dial-peer voice 888 pots
 service us_800
 incoming called-number 1888.......

! Dial-peer 900 sends toll-free calls using the service command to the us_900
  application, which calls the us_900.tcl script, which plays the us_900.au audio file.
dial-peer voice 900 pots
 service us_900
 incoming called-number 1900.......
!
! Dial-peer 411 sends service code calls using the service command to the info
  application, which calls the info.tcl script, which plays the info.au audio file.
dial-peer voice 411 pots
 service info
 incoming called-number [2-8]11

! Dial-peer 123 directs the router to use direct-inward-dial for incoming calls (see
  lab 6-5, step 5-1 for details).
dial-peer voice 123 pots
 incoming called-number .
 direct-inward-dial
!
! Dial-peer 911 sends emergency calls using the service command to the 911
  \application, which calls the hq_911.tcl script, which plays the hq_911.au audio
  file.
dial-peer voice 911 pots
 service 911
 incoming called-number 911
!
! Dial-peers 9100 to 9107 are created to carefully exclude the range of numbers for
  the 11 pods 1-510-555-2100 to 3199. This was done because the service command takes
  priority when routing calls. If a long-distance dial-peer was used that matched a
  pattern such as 1.......... long-distance calls to other pods would play the ld.tcl
  script. Instead calls to the pods do not match the patterns, and get directed to the
  correct interface in dial-peers 101-111.

! Dial-peer 9100 covers any 1+10 digit number that does not start with a 15.
dial-peer voice 9100 pots
 service ld
 incoming called-number 1[2-4,6-9].........
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
! Dial-peer 9101 covers any 1+10 digit number that does not start with a 151.
dial-peer voice 9101 pots
 service ld
 incoming called-number 15[^1].......
!
! Dial-peer 9102 covers any 1+10 digit number that does not start with a 1510.
dial-peer voice 9102 pots
 service ld
 incoming called-number 151[^0].......
!
! Dial-peer 9103 covers any 1+10 digit number that does not start with a 15105.
dial-peer voice 9103 pots
 service ld
 incoming called-number 15105[2-4,5-9]......
!
! Dial-peer 9104 covers any 1+10 digit number that does not start with a 151055.
dial-peer voice 9104 pots
 service ld
 incoming called-number 15105[^5].....
!
! Dial-peer 9105 covers any 1+10 digit number that does not start with a 1510555.
dial-peer voice 9105 pots
 service ld
 incoming called-number 151055[^5]....
!
! Dial-peer 9106 covers any 1+10 digit number that does not start with a 15105555.
dial-peer voice 9106 pots
 service ld
 incoming called-number 1510555[^5]...
! Dial-peer 9106 would have an incoming called-number of 151055520.. for the CUCM
  labs.
!
! Dial-peer 9107 covers any 1+10 digit number that does not start with a 15105555
  followed by a 0, 1, or 2.
dial-peer voice 9107 pots
 service ld
 incoming called-number 15105555[^0-2]..
! Dial-peer 9107 would have an incoming called-number of 15105553[^01].. for the CUCM
  labs.
!
! Dial-peer 9108 covers any 1+10 digit number that does not start with a 151055553
  followed by a 0, 1, 2, 3, 4, or 5.
dial-peer voice 9108 pots
 service ld
 incoming called-number 151055553[^0-5].
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran

```
! Dial-peer 9108 does not need to exist for the CUCM labs.
!
! Dial-peer 9011 sends international calls using the service command to the intl
  application, which calls the international.tcl script, which plays the
  international.au audio file. Note that the seven dots after the 011 is just a
  arbitrary number to make sure the user dialed enough digits, since I am not aware of
  any county that uses less than seven-digits for phone numbers.
dial-peer voice 9011 pots
 service intl
 incoming called-number 011.......
!
! Dial-peer 7 sends seven-digit local calls using the service command to the local
  application, which calls the mrrogers.tcl script, which plays the mrrogers.au audio
  file. Since all local numbers for the pods were converted to long-distance numbers by
  the translation-profile, it is not necessary to avoid covering the numbers for the
  pods (which had to be done in dial-peers 9100 to 9108).
dial-peer voice 7 pots
 service local
 incoming called-number [2-9]......
!
line con 0
 exec-timeout 300 0
 logging synchronous
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
line vty 5 15
 privilege level 15
 login local
 transport input telnet ssh
```

https://t.me/learningnets

From the Library of Aliwarman Tarihoran